UNIVERSITÉ LAVAL

Faculté des sciences et de génie

Département de génie électrique et de génie informatique

2005-2006

Rapport Annuel d'Activités

Laboratoire de Radiocommunications et de Traitement du Signal
Université Laval
Québec, QC, Canada
G1K 7P4

Téléphone : **(418) 656-2806** (*Directeur du LRTS*)
(418) 656-2984 (*Secrétariat*)
Télécopie : **(418) 656-3159**

Courriel : **lrts@gel.ulaval.ca**
Site WWW : **http ://lrts.gel.ulaval.ca/**

13 juillet 2006

(Rapport LRTS-06-01)

Ce rapport du Laboratoire de radiocommunications et de traitement du signal (LRTS) est le fruit d'une grande collaboration qui implique plusieurs personnes qui je tiens à remercier ici.

- Il y a d'abord les étudiants gradués actuels, à la maîtrise ou au doctorat, qui ont rédigé un résumé de leurs travaux de recherche ; j'ai inséré ces résumés dans diverses sections représentant les grands thèmes de recherche du LRTS.
- Les professeurs du LRTS qui ont révisé les textes dans la mesure du possible, ont élaboré la liste des destinataires potentiels, et m'ont fourni leur liste de publications faites entre 2001 et 2006.
- Finalement, deux anciens du LRTS, Anne-Laure Jousselme et Christophe Charrier, qui jadis, ont créé une classe LaTeX pour faire de beaux rapports annuels de laboratoire ; j'ai repris, modifié et amélioré cette classe pour produire le présent document.

Dominic Grenier
Directeur du LRTS

Québec, juillet 2006

©LRTS 2005-2006

Sommaire

Préambule ix

Laboratoire de Radiocommunication et Traitement du Signal (L.R.T.S.) xi

Site du LRTS xvii

I Communications 1

Performance Evaluation of Multirate OCDMA Systems in Optical Packet Network 3

Une méthode semi-analytique pour l'analyse des performances de récepteurs UWB de type RAKE 9

Architecture de routage hiérarchique multiniveaux pour les réseaux de capteurs sans fil 17

High-performance LDPC codes based on circulant permutation matrices 21

High-speed encoders of LDPC codes in 802.11n wireless local area networks and 802.16e broadband wireless systems 25

Parallel decoders for turbo codes in both 3G mobile systems and 802.16 broadband wireless access systems 29

Single carrier RRC matching in frequency domain with frequency domain equalization 35

Application des réseaux de capteurs dans les milieux confinés - Partie localisation 39

Egalisation aveugle et turbo égalisation dans les canaux sélectifs en fréquence stationnaires et non stationnaires. 47

Cadre généralisé pour l'échantillonnage non-uniforme : étude de performance et traitement numérique 55

Les codes à faible densité de parité 61

II Systèmes MIMO **69**

Sur la faisabilité d'une architecture distribuées pour les communications sans-fil mobile **71**

Schéma de codage spatio-temporel avec diversité de fréquence pour un système MIMO-OFDM **75**

Récepteur MIMO multiusager à traitement multi-couches spatio-temporel **81**

III VLSI **85**

Réalisation d'un algorithme de réception MIMO avec étude architecturale et virgule fixe **87**

Implantation FPGA de l'algorithme de chiffrement à courbes elliptiques **93**

Aspects matériels d'un réseau d'antennes intelligent dédié au *Wi-Fi* **99**

Un architecture régulière de circuit d'inversion de matrice pour le traitement MIMO **103**

FPGA implementation of a digital communication chain **107**

IV Fusion de données **117**

Utilisation des réseaux de Kohonen dans le processus de classification **119**

Representing fuzzy membership functions into random set formalism **125**

Vérification des protocoles de communication et d'agrégation en fusion d'informations **133**

Identification de l'impact de la fusion de l'information de la STANAG 1241 sous différents cadres de raisonnement **139**

Adaptive combination rule for the evidence theory **143**

General Measure of Uncertainty in Fuzzy Evidence Theory **151**

Calcul d'incidence généralisé modifié **157**

Scope of Contribution to Maritime Surveillance **165**

V Antennes et Radar **171**

Réseaux d'antennes en ondes millimétriques. **173**

Calibrage des réseaux d'antennes par réseaux de neurones artificiels **181**

Emploi du signal XM comme source d'opportunité d'un système non coopératif pour la détection passive cohérente **191**

Simulation de la section efficace radar sur une trajectoire **195**

Personnel du laboratoire **201**

Publications 2001-2006 **207**

Préambule

Laboratoire de Radiocommunication et Traitement du Signal (L.R.T.S.)

Le Laboratoire de Radiocommunications et de Traitement du Signal (LRTS) a comme objectif de coordonner et d'intégrer les programmes de recherche réalisés dans le vaste domaine des communications radio et du traitement du signal adapté à ces mêmes communications. Il est une composante de recherche au Département de génie électrique et de génie informatique de l'Université Laval.

Équipe de recherche du LRTS

Le LRTS compte actuellement une imposante équipe constituée d'une quarantaine d'étudiants gradués, de chercheurs post-doctoraux et d'assistants de recherche travaillant sous la direction d'un noyau de professeurs de carrière (Jean-Yves Chouinard, Paul Fortier, Dominic Grenier, et Sébastien Roy). En plus, le laboratoire bénéficie aussi de la collaboration de plusieurs professeurs associés dont le Dr Gilles Y. Delisle, professeur émérite, ancien professeur du LRTS et maintenant vice-président à la recherche à l'Institut International des Télécommunications (IIT-R), le Dr Éloi Bossé et la Dre Anne-Laure Jousselme du centre Recherche et développement pour la défense Canada à Valcartier (RDDC-V), le Dr Charles Despins, directeur de PROMPT-Québec, le Dr René Le de l'Université du Québec en Abitibi-Témiscamingue (UQAT), le Dr Elie Inaty de l'université de Malamand au Liban, le Dr Xianbin Wang du Centre de recherche sur les Communications (CRC) à Ottawa et le Dr Pierre-Martin Tardif.

Collaborations de recherche

Les membres de l'équipe de recherche du LRTS entretiennent entre eux des collaborations étroites. Les professeurs Chouinard, Fortier, Grenier et Roy dirigent conjointement plusieurs mémoires de maîtrise et thèses de doctorat. Les professeurs Fortier et Chouinard ont été coprésidents du *1995 Canadian Workshop on Information Theory* et sont les coéditeurs, avec A. Gulliver de l'Université de Victoria, du livre *Information Theory and Applications II : Fourth Canadian Workshop on Information Theory* publié dans la collection *Lecture Notes in Computer Science* chez Springer-Verlag. Les professeurs Roy et Chouinard sont les auteurs du chapitre *Réseaux d'antennes et systèmes MIMO reconfigurables* du traité scientifique *Les systèmes radiomobiles reconfigurables* publié en 2005 chez Lavoisier. Dernièrement, les professeurs Grenier et Chouinard ont initié un projet de recherche sur la détection passive radar bistatique.

Une caractéristique du laboratoire est son orientation vers des applications, orientation qui est accentuée grâce à des collaborations industrielles et gouvernementales, en particulier par le biais de contrats de recherche. Le laboratoire maintient toujours une recherche fondamentale d'avant-garde, et ces recherches fondamentales ont souvent leur source dans des problèmes identifiés lors de projets d'applications.

Le laboratoire recherche toujours activement l'établissement de nouvelles collaborations à l'externe comme à l'interne. Il est en bonne position pour interagir avec les chercheurs en optique-photonique du COPL, en intelligence artificielle et traitement d'image du LVSN, ou en VLSI à l'Université Laval.

Principaux thèmes de recherches

Les thèmes de recherches actuels au laboratoire sont les communications numériques mobiles et personnelles, les systèmes à entrées multiples et sorties multiples (MIMO), la conception VLSI pour les communications mobiles, le traitement d'antenne-réseau pour estimation d'angles d'arrivées et pour imagerie radar par ouverture synthétique inversée (ISAR), et la fusion de données (Projet collaboratif du CRSNG avec Lockheed-Martin Canada) les systèmes de télédiffusion numériques interactifs (en collaboration avec le CRC), la théorie de l'information et des codes correcteurs et ses applications. Le laboratoire et ses membres sont financés par des subventions individuelles, d'équipe, d'appareillage et d'infrastucture octroyées par les agences subventionnaires des gouvernements du Québec et du Canada pour la recherche académique : le Fonds québécois de la recherche sur la nature et les technologies (FQRNT) et le Conseil de recherches en sciences naturelles et en génie (CRSNG).

• Fusion de données

Le programme de recherches en fusion de données vise spécifiquement la fusion multi-capteurs et multi-plateformes de données provenant de différents capteurs et types de capteurs. Le projet collaboratif avec Lockheed-Martin Canada (LMC) est relié aux problèmes de combinaison d'informations pour la déclaration d'identité avec raisonnement sous incertitude. Il implique aussi des chercheurs du RDDC-Valcartier, soient les Drs Éloi Bossé, Anne-Laure Jousselme et Pierre Valin ; et un chercheur de LMC, le Dr Éric Lefebvre . Au cours des dernières années, des progrès importants ont été réalisés sous plusieurs aspects dans le cadre de l'évidence : combinaison adaptative en présence de conflits, définition de mesures de performance, dont une distance entre deux corps d'évidence) et de mesures du niveau d'incertitude (laquelle inclue l'ambiguïté, la non-spécificité et le flou), la classification supervisée avec classificateurs multiples, et, dernièrement, l'utilisation de cadres de raisonnement hybrides dont celui du calcul d'incidence et de Fagin-Halpern. Le professeur Grenier est co-auteur d'un chapitre du livre *Advances and Applications of DSmT for Information Fusion* qui sera publié cet été 2006 chez American Research Press.

• **Stations de base distribuées**

La conservation des avantages systémiques des réseaux d'antennes tout en introduisant l'avantage MIMO pour augmenter le débit nécessite non seulement que les terminaux soient dotés de réseaux d'antennes mais également que celui de la station de base / point d'accès ait un très grand nombre d'éléments (e.g. 20 ou plus).

À cause de contraintes physiques (coût, espace limité), il peut s'avérer impossible d'espacer les éléments suffisamment pour éviter d'introduire des corrélations dans le canal matriciel. De plus, on s'expose au phénomène hostile des "trous de serrure" qui se produit lorsque la station de base et le terminal sont éloignés ou dans certaines conditions de propagation particulières. Pour pallier à ces problèmes et pour permettre aux réseaux sans fil ad hoc un plus grand degré de flexibilité, nous étudions un certain nombre d'éléments menant au concept de réseau cognitif. L'originalité de l'infrastructure que nous développons réside dans son caractère adaptatif dynamique (nécessaire entre autres à l'exploitation efficace des réseaux d'antennes), qui n'est pas de nature uniquement locale (c-à-d limité à une station ou terminal) mais bien de nature globale, les divers éléments de l'infrastructure étant capables de coopération spontanée.

L'une des caractéristiques importante de notre vision est l'usage de stations de base distribuées (ci-après désignées "microstations"). Selon ce concept, un terminal donné s'interface avec l'infrastructure câblée non pas via une station de base unique au centre d'une cellule, mais en communiquant simultanément avec plusieurs microstations disséminées géographiquement.

Une telle solution présente plusieurs avantages car elle offre : (1) une diversité non seulement contre le multi-parcours, mais également contre l'obscurcissement (i.e. évanouissement lent) ; (2) une protection contre le phénomène des trous de serrure ; (3) une plus grande décorrélation du réseau amalgamé ; (4) une robustesse contre l'obstruction et les problèmes de couverture ; et, par rapport à la simple utilisation de réseaux d'antennes (i.e. non distribués) : (1) une capacité (en termes de nombre de liens actifs simultanément) accrue ; (2) une économie de puissance accrue ; (3) une minimisation plus poussée de l'interférence produite ; (4) une minimisation de la pollution électromagnétique et de l'effet éventuel sur la santé.

En combinaison avec des innovations au niveau de la couche réseau, ce schème rend la notion classique de cellule caduque. En effet, un terminal sera à tout instant pris en charge par un ensemble de microstations travaillant à l'unisson. Cet ensemble s'ajustera dynamiquement avec le déplacement du terminal de manière à ce que ce dernier soit toujours desservi par des microstations suffisamment proches, étant donné la portée radio et les conditions de propagation.

• **Systèmes de télédiffusion numériques**

L'étude des systèmes de télédiffusion numériques ont conduit à des travaux de recherche importants en collaboration avec des chercheurs du CRC : le Dr Yiyan Wu, Fellow de l'IEEE, et le Dr Xianbin Wang. Un projet de recherche stratégique du CRSNG sur les systèmes de télédiffusion numériques interactifs par liaisons terrestres vient d'être complété. Une nouvelle technique d'insertion de données a été développée pour la transmission d'information à hauts débits dans les signaux de télédiffusion, utilisant le multiplexage OFDM (Orthogonal Frequency Division Multiplexing) avec une dégradation imperceptible de la qualité de l'image : un brevet américain a été accordé en 2004. Un nouveau projet de recherche en équipe du FQRNT vient de

débuter avec les professeurs du LRTS et des chercheurs du CRC : ce projet consiste en l'étude des effets d'interférences statiques par la proximité des éoliennes des stations de télédiffusion ainsi que des interférences dynamiques causés par le mouvement de leurs pales.

• Modulation multiporteuse

Les travaux en systèmes de modulation multiporteuse touchent particulièrement l'OFDM, les systèmes combinant l'OFDM et le CDMA ainsi que la turbo égalisation, la turbo détection et les modulations adaptatives, le tout dans le contexte de liaisons sans fils, mobiles ou fixes. Plusieurs des étudiants ont également travaillé sur des projets reliés à la réalisation de puces VLSI, notamment pour faire des décodeurs, des filtres adaptatifs, des égaliseurs et des systèmes de modulation adaptative. Dans ce domaine, il y a eu collaboration avec des compagnies comme Wavesat (développement d'un modem OFDM), Lyrtech (système SignalMaster pour le traitement du signal) et Bestar Radio (récepteur numérique reconfigurable).

• Radars et antennes-réseaux

Les travaux sur le radar touchent principalement l'imagerie radar, donc le traitement des signaux captés par une antenne ou même un réseau d'antennes. Les algorithmes d'imagerie ISAR de type CLEAN (qu'on a rendu autofocus) et de type DSA (qu'on a généralisé à plusieurs diffuseurs dominants) ont été appliqués à des réseaux d'antennes suivant diverses architectures pour améliorer la résolution en portée transversale et la qualité du pistage. En imagerie SAR, l'utilisation du système propre des signaux combinés provenant de canaux radar multiples a été publiée dans le numéro spécial *New Trends and Findings in Antenna Array Processing for Radar* de l'European Journal on Signal Processing. L'article *Eigendecomposition of the multi-channel covariance matrix with applications to SAR-GMTI* rédigé par le Dr Ishuwa Sikaneta du centre de Recherche et développement pour la défense Canada à Ottawa (RDDC-O) s'est mérité le *Signal Processing Best Paper Award 2004* par l'European Association for Signal, Speech and Image Processing (EURASIP) en 2005.

L'estimation des directions d'arrivée (DOA) haute-résolution pour des sources cohérentes est aussi un sujet de recherche ; on cherche actuellement à se servir des angles d'arrivée dans la liaison montante pour estimer le canal de propagation de la liaison descendante.

• Systèmes VLSI

Les activités de recherche en VLSI concernent plus particulièrement le développement d'algorithmes de traitement de signal appliqués aux communications numériques conjointement avec leur réalisation efficace sous forme de circuit numérique. Le prototypage de ces composantes se fait surtout pour l'instant sur plate-forme FPGA, mais les activités évoluent actuellement pour englober la conception de puces numériques CMOS à haute vitesse. Parmi les applications abordées par le groupe à ce jour, on dénote entre autres la cryptographie à courbes elliptiques, les codres corercteurs d'erreur puissants (codes turbo et LDPC), les transcepteurs MIMO (e.g. récepteur espace-temps multi-couches), les opérateurs arithmétiques (inversion de matrices, logarithme, racine carrée), de même que les générateurs de nombres aléatoires.

• **Communications mobiles**

Nos travaux de recherche sur la théorie des communications et le traitement du signal pour les canaux de propagation sans fil ont permis de mettre au point une méthode innovatrice permettant de déduire des propriétés statistiques des gains complexes caractérisant la réponse impulsionnelle des canaux de propagation à large bande. En décomposant des réponses impulsionnelles expérimentales en valeurs et vecteurs propres, on démontre que le processus de propagation est dominé par seulement quelques modes orthogonaux, permettant ainsi la réalisation de détecteurs à complexité réduite. Un article écrit conjointement avec les Drs François Patenaude et John Lodge du CRC, a remporté le *1999 Neal Shepherd Best Propagation Paper Award* pour le meilleur article paru sur la propagation dans les *IEEE Transactions on Vehicular Technology*.

Site du LRTS

Le LRTS occupe une aile du deuxième étage du pavillon Adrien-Pouliot de l'Université Laval dont la murale de l'entrée principale apparaît sur la page titre. Un corridor traverse le laboratoire et se termine avec les derniers locaux du LRTS. Les bureaux des quatre professeurs et les locaux regroupant les bureaux des étudiants gradués, se retrouvent d'un côté du corridor alors que, les locaux hébergeant les équipements, salles informatique, salles de mesures, bibliothèque et salle de réunion se retrouvent de l'autre côté.

Les photos ci-dessous montrent l'environnement physique du LRTS. La photo de la Fig. 3 est une gracieuseté de Philippe Leroux ; toutes les autres – y compris celle en filigrane de la page titre – ont été prises et fournies par Dominic Grenier.

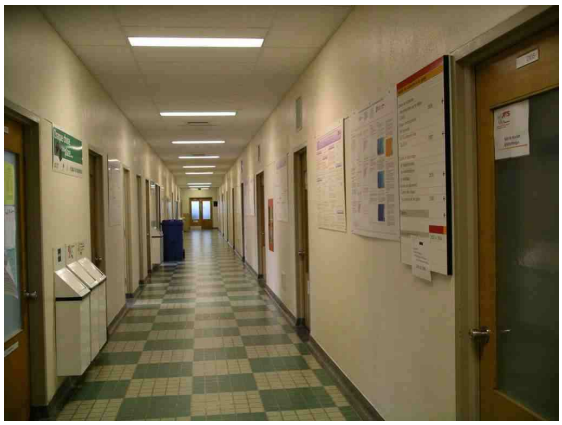


Fig. 1: Corridor traversant le LRTS ; les bureaux à gauche et les salles du laboratoire à droite.

Fig. 2: Salle multifonctionnelle – salle de réunion, de présentation et bibliothèque – le PLT-2105.

Fig. 3: Paul Fortier, Simon Mathieu et Dominic Grenier (et le bras droit de Sébastien Roy) lors de la pause-café quotidienne au PLT-2105.

Fig. 4: Chambre anéchoïdale dans la salle de caractérisations RF PLT-2107.

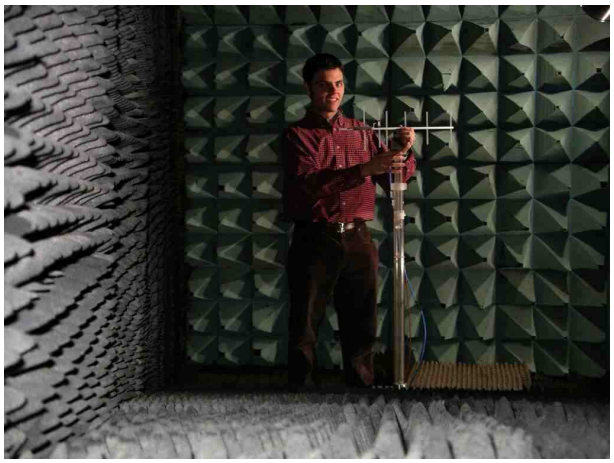


Fig. 5: Jean-Sébastien Néron faisant quelques ajustements d'une antenne dans la chambre anéchoïdale du PLT-2107.

Fig. 6: Salle de calcul numérique, le PLT-2109.

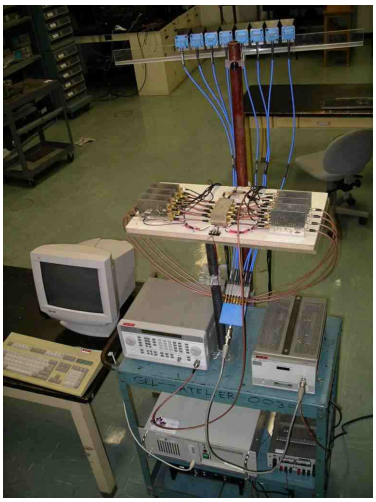


Fig. 7: L'antenne réseau en bande X pour des mesures expérimentales en DOA dans le PLT-2111.

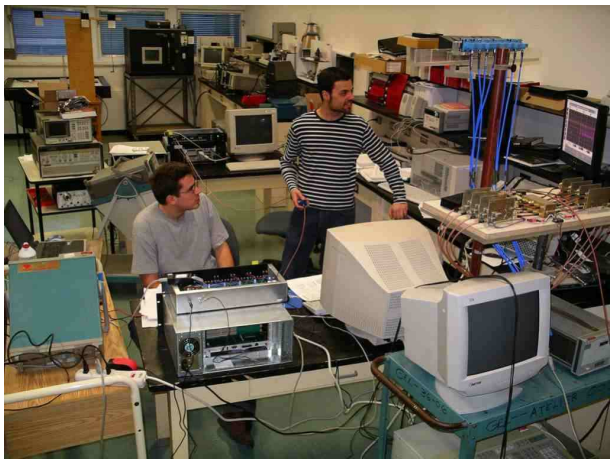


Fig. 8: Jean-Sébastien Néron et Hugo Bertrand travaillant sur un montage dans le PLT-2111.

Fig. 9: Vue approchée d'une station de prototypage MIMO (DSP SignalMaster de Lyretech et front-end RF de Comlab) dans le PLT-2111.

Fig. 10: Salle de calcul numérique, le PLT-2113.

Fig. 11: Un vrai ingénieur dans un vrai laboratoire de recherche : Jean-Yves Chouinard en 1980.

I

Communications

Table des Matières

Performance Evaluation of Multirate OCDMA Systems in Optical Packet Network 3

Une méthode semi-analytique pour l'analyse des performances de récepteurs UWB de type RAKE . . 9

Architecture de routage hiérarchique multiniveaux pour les réseaux de capteurs sans fil 17

High-performance LDPC codes based on circulant permutation matrices 21

High-speed encoders of LDPC codes in 802.11n wireless local area networks and 802.16e broadband wireless systems 25

Parallel decoders for turbo codes in both 3G mobile systems and 802.16 broadband wireless access systems 29

Single carrier RRC matching in frequency domain with frequency domain equalization 35

Application des réseaux de capteurs dans les milieux confinés - Partie localisation 39

Egalisation aveugle et turbo égalisation dans les canaux sélectifs en fréquence stationnaires et non stationnaires. 47

Cadre généralisé pour l'échantillonnage non-uniforme : étude de performance et traitement numérique . . 55

Les codes à faible densité de parité 61

Performance Evaluation of Multirate OCDMA Systems in Optical Packet Network

Robert Raad, *Étudiant au doctorat.*

Dr Paul Fortier, *Directeur de recherche.*

Dr Elie Inaty, *Co-directeur de recherche.*

Résumé – Deux protocoles MAC - le protocole S-ALOHA et le protocole "round robin" émetteur récepteur (R^3T) - sont proposés pour exploiter le potentiel des systèmes optique d'accès multiple par division de code (OCDMA) à taux binaire variable et ce, dans les réseaux optiques déployés pour les applications multimédia. On considère deux systèmes à taux variable. Le premier, récemment proposé, est l'OCDMA à saut rapide de fréquence avec chevauchement (O-FFH-OCDMA). Le deuxième est le système classique de l'OCDMA à saut rapide de fréquence et à gain variable (VPG-FFH-OCDMA). Les performances des deux systèmes, au niveau de la couche de lien de données, sont étudiées et comparées en utilisant les deux protocoles MAC proposés. Le "throughput" et le délai moyen des paquets ont été retenus comme critères. La métrique du First-Exit-Time (FET) est choisie pour étudier la stabilité du S-ALOHA/O-FFH-OCDMA étant donné la bi-stabilité du protocole choisi. Nos simulations montrent que les performances des systèmes OCDMA utilisant l'un ou l'autre des protocoles, sont comparables en termes de "throughput" mais S-ALOHA est meilleur en terme de délai. D'un autre coté, indépendamment du protocole utilisé, le système avec chevauchement (O-FFH-CDMA) possède toujours des meilleures performances que le système classique VPG-FFH-OCDMA. Finalement, le système S-ALOHA/O-FFH-OCDMA est plus stable que le S-ALOHA/VPG-FFH-OCDMA.

Abstract – In this paper, two media access control (MAC) protocols - S-ALOHA and round robin receiver transmitter (R^3T), have been proposed to exploit the potential of multirate optical code division multiple-access (OCDMA) systems in real optical networks for multimedia applications. Two multirate systems, the newly proposed overlapped optical fast frequency hopping CDMA (O-OFFH-CDMA) and the classical variable processing gain optical fast frequency hopping CDMA (VPG-OFFH-CDMA) systems, have been considered. The performances of both systems on the top of the data link layer have been studied and compared under the two proposed MAC protocols in terms of system throughput and average packet delay. In addition, the stability of S-ALOHA/O-OFFH-CDMA is also investigated in terms of first-exit-time (FET) metric owing to the bistable characteristic of the considered protocol. Simulations showed that the performances of OCDMA systems under both protocols are competitive in terms of throughput, but in terms of delay S-ALOHA is better. Also, regardless of the protocol used, the overlapped system always outperforms the VPG system. Finally, S-ALOHA/O-OFFH-CDMA is more stable than S-ALOHA/VPG-OFFH-CDMA.

1.1 Introduction

The increasing demand for multimedia services and the evolution of optical technology make OCDMA the subject of interest for many researchers in this field. This is because it offers an extremely sufficient bandwidth to support the existing and the future provisioned services in the ever-increasing packet-network. For this purpose, diverse transmitter-receiver architectures have been built for OCDMA systems, with the aim of assuring correct transmission and reception of the data over the optical channel, i.e. to minimize the bit error rate (BER) and maximize the signal-to-interference ratio (SIR) as much as possible. Such parameters resume the system behavior at the physical layer of the network. In addition, different coding techniques are investigated to adapt the lightwave to the OCDMA system and to further improve its performance at the physical layer. However, without bridging the physical layer and the data link layer, OCDMA systems will never be implemented in a real network.

1.2 System model

We consider the overlapped optical fast frequency hopping CDMA (OFFH-CDMA) as a high-speed optical communication system detailed in [1], [2] for multimedia applications. Let K terminal users be interconnected together in a star topology, offering the lower station to station link attenuation. Each terminal user is equipped with a fixed transmitter and a tunable receiver (FTTR) as an adopted nodal architecture.

S-ALOHA/OFFH-CDMA systems have been analyzed in detail in [3], [4]. Initially, the systems are empty and users generate new packets with probability P_0. Transmitted over the optical channel, some packets will be received correctly with a probability P_C and some will be received in error due collision and multiple-access interference (MAI). The terminal whose packets are incorrectly received is backlogged and it retransmits the defected packets after a random delay with a probability P_r. The backlogged terminal cannot generate new packets until all their blocked packets are retransmitted correctly. At the next time slot, the arrivals are composed of new packets and retransmitted packets. In general, the composite arrivals are modeled as a Markov chain.

Beside S-ALOHA protocol, we attempt to control the packet flow of users using the R^3T protocol described in [5]. We assume that a packet corresponds to one bit and L bits form a message so that the message length is equal to the packet length in S-ALOHA. Each user transmits his message with a probability A, called user's activity. After sending a request of timeout duration, if the transmitting station receives an acknowledgement, it transmits the first t packets following the go-back n protocol, where $n = t$ is the two-way propagation time in slots between the transmitting and receiving stations. Otherwise, it retransmits its last t packets in a round robin fashion.

Packet correct probability

In this paper we consider that all users employ ON-OFF keying (OOK) modulation scheme to transmit their data. In addition, the bit error rate (BER) is obtained from simulation using the Extended Hyperbolic Congruential Codes (EHC) and assuming Gaussian hypothesis to model the interference, and it is given by

$$P_b(i) = Q\big(\frac{1}{2} \times \sqrt{\mathrm{SIR}^{(i)}}\big) \tag{1.1}$$

In VPG system [3], multirate is achieved by varying the length of the user's signature and hence the processing gain (PG) G_V, so that increasing the transmission rate yields a reduction of G_V by the same amount such that the new transmission rate will be

$$R_s = \frac{X_b^{(V)}}{L} R_n(\text{bits / sec}) \tag{1.2}$$

where $X_b^{(V)} = \lfloor \alpha L \rfloor$ is the total number of bits per packet. Because the interference is counted at every bit position i, $P_b(i)$ may differ at each bit position. However, in VPG system $P_b(i)$ is the same for all i. Therefore, the packet correct probability at the desired user's receiver can be written as

$$P_c(K) = [1 - P_b(i)]^{X_b^{(i)}} \tag{1.3}$$

In the overlapped OCDMA system, [3], multirate is achieving in the fiber Bragg grating (FBG) by increasing the link transmission rate beyond the nominal rate without decreasing the processing gain. This introduces chip-overlapping among bits into the fiber in a given time slot. The number of overlapping chips between two consecutive bits is designated as the bit overlapping coefficient, ϵ_s , of the system. Therefore, increasing ϵ_s increases the bit rate to

$$R_s = \frac{X_b^{(0)}}{L} R_n(\text{bits / sec}) \tag{1.4}$$

where $X_b^{(0)} = \frac{LG-\epsilon_s}{G-\epsilon_s}$ is the total number of bits per packet. Since $P_b(i)$ differs at every bit position, then the packet correct probability at the desired user's receiver is given by

$$P_c(K) = \prod_{i=0}^{X_b^{(0)}-1} [1 - P_b(i)] \tag{1.5}$$

Performance evaluation

The OCDMA throughput under S-ALOHA as obtained in [3], [4], is the average number of successfully received packet S given that M packets are transmitted and K users are available in the system and it is expressed by

$$\beta(K) = E\{S\} = E\{E\{S|M\}\} = E\left[\sum_{S=0}^{K} S \binom{M}{S} P_C^S (1 - P_C)^{(M-S)}\right] \tag{1.6}$$

©LRTS 2005-2006

The average packet delay is defined by Little's theorem [6] as the average number of backlogged users over the system throughput as

$$D = \frac{\overline{n}}{\beta} \tag{1.7}$$

The system throughput under R^3T is computed in [5] as

$$\beta(K, A, t, \tau_0, L) = \frac{P_C(K) L_0 r_0}{L + (1 - P_C(K))(\min(t, L) - 1)(L - \min(t, L/2))} \tag{1.8}$$

where r_0 is the number of transmitting users in a given slot. The delay is given by

$$D = \frac{KA}{\beta(K, A, t, \tau_0, L)} \tag{1.9}$$

where KA is the average offered traffic.

1.3 Results and conclusions

In the simulation we have assumed that the number of users is $K = 12$, the processing gain is $G = 31$, the packet length under slotted ALOHA protocol is $L = 300$ bits/time slot and the message is one packet. Equivalently, under the R^3T protocol the packet length is one bit/time slot and $L = 300$ designates the message length in packets. Fig. 1.1 and Fig. 1.2 depict the throughput and the delay of the overlapped and the VPG systems under S-ALOHA in comparison with those under the R^3T protocol. In addition, Fig. 1.3 and Fig. 1.4 show the performance of both OCDMA systems under the R^3T protocol when the rate has increased from 714 bps to 843 bps. Finally, Fig. 1.5 investigates the stability of the OCDMA systems under S-ALOHA.

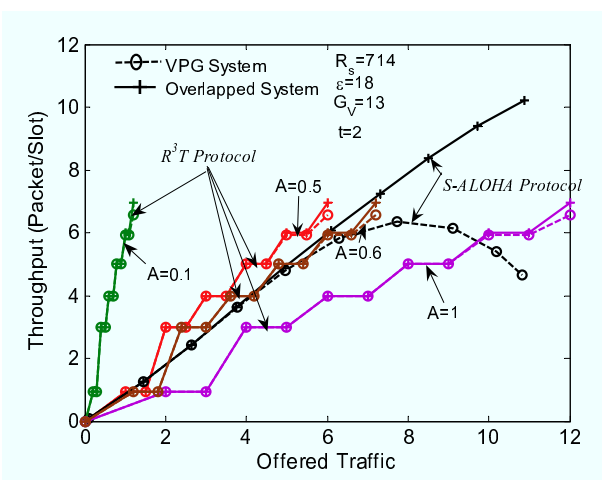


FIG. 1.1: The throughput versus the offered traffic of the multirate systems under the two MAC protocols : S-ALOHA and R^3T for a two-way propagation time of two time slots.

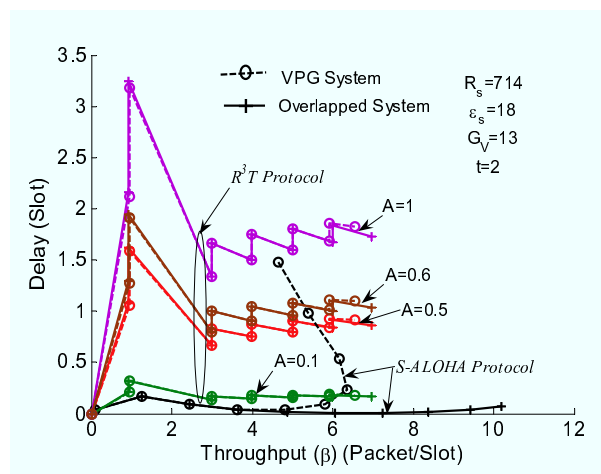


FIG. 1.2: The delay versus the throughput of the multirate systems under the two MAC protocols : S-ALOHA and R^3T for a two-way propagation time of two time slots.

As a result, the proposed protocols offer good throughput and acceptable delay, and they are appropriate to operate such systems at the link layer. Nevertheless, O-OFFH-CDMA has superior performances over VPG-OFFH-CDMA and is more stable as illustrated in the figures.

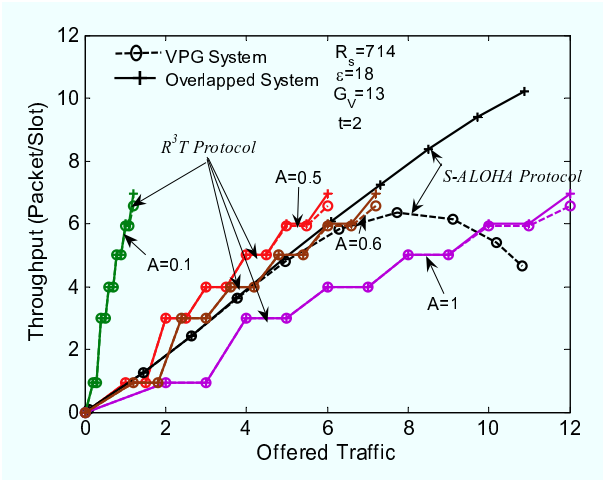


FIG. 1.3: The throughput versus the offered traffic of the multirate systems under the two MAC protocols : S-ALOHA and R^3T for a two-way propagation time of two time slots.

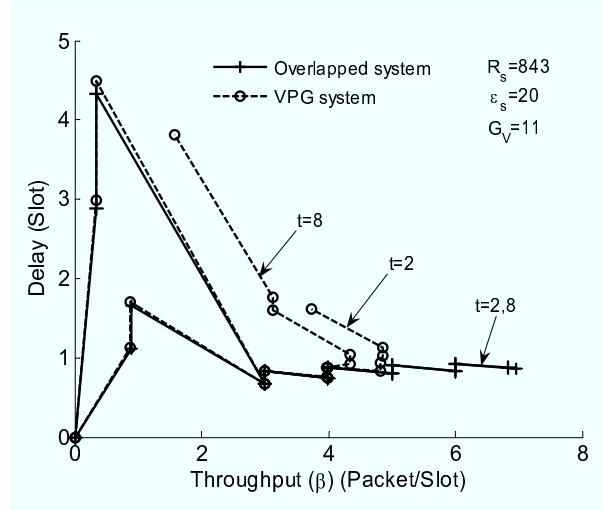


FIG. 1.4: Average delay versus throughput of OCDMA systems under R^3T protocol.

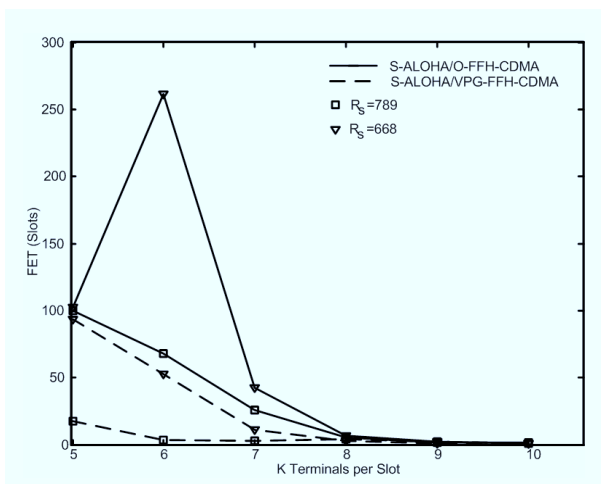


FIG. 1.5: FET at retransmission probability $P_r = 0.9$ implying that the more stable system is the one which operates at longer time in the stable region before it exits in the unstable region.

Bibliographie

[1] E. Inaty, H. M. H. Shalaby, and P. Fortier, "On the cutoff rate of a multiclass OFFH-CDMA system," *IEEE Trans. Commun.*, vol. 53, pp. 323–334, 2005.

[2] E. Inaty, H. M. H. Shalaby, and P. Fortier, "A new transmitter-receiver architecture for noncoherent multirate OFFH-CDMA system with optimal detection threshold," *IEEE J. Lightwave Technol.*, vol. 20, pp. 1885–1894, 2002.

[3] R. Raad, E. Inaty, P. Fortier, and H. M. H. Shalaby, "Optical S-ALOHA/CMDA system for multirate application : architecture, performance evaluation and system stability," *IEEE J. Lightwave Technol.*, vol. 24, pp. 1968–1977, 2006.

[4] D. Raychauhuri, "Performance analysis of random access packet-switched code division multiple access systems," *IEEE. Trans. Comm.*, vol. COM-29, no. 6, pp. 895–901, 1981.

[5] H. M. H. Shalaby, "Performance analysis of an optical CDMA random access protocol," *IEEE J. Lightwave Technol.*, vol. 22, pp. 1233–1241, 2004.

[6] G. N. Higginbottom, *Performance evaluation of communication networks.* Artech House Publishers, 1998.

Une méthode semi-analytique pour l'analyse des performances de récepteurs UWB de type RAKE

Michel Thériault, *Étudiant à la maîtrise.*
Leslie Ann Rusch, *Directrice de Recherche.*
Paul Fortier, *co-directeur de recherche.*

Résumé – Nous présentons une nouvelle méthode semi-analytique pour l'étude des performances d'un récepteur RAKE dans un système à ultra large bande basé sur l'accès multiple par répartition en code à séquence directe (DS-CDMA). Cette méthode à pour objectifs de fournir un outil pour faciliter l'étude d'un tel système et de mener à un modèle complètement analytique du système.

Abstract – We present a new semi-analytic method for the study of the performance of a RAKE receiver in a direct-sequence code-division multiple-access (DS-CDMA) based ultra wide-band (UWB) system. This method is intended as a tool to facilitate further performance studies of this type of system and, ultimately, to lead to a fully analytical model.

2.1 Introduction

La technologie à bande ultra large (UWB) a attiré beaucoup d'intérêt dans les dernières années. Les principaux attraits de la technologie sont d'importants taux de transmission, un faible coût et une faible consommation de puissance. De par sa nature, la technologie UWB opèrera nécessairement en présence d'interférents relativement puissants. L'accès multiple par répartition en code à séquence directe (DS-CDMA), qui est très efficace pour combattre l'interférence à bande étroite, est une technique qui peut potentiellement exploiter les principaux avantages de la technologie UWB [1, 2].

La méthode semi-analytique que nous proposons a pour but d'analyser les performances de récepteurs de type RAKE dans les systèmes UWB basés sur le DS-CDMA. Cette méthode est basée sur la décomposition analytique des différents éléments du signal présent au récepteur et permet d'obtenir une analyse du taux d'erreur binaire efficace en terme de temps de calcul. Cette méthode est aussi une première étape dans le but d'une étude complètement analytique d'un tel système.

2.2 Description du système

Signal transmis

Le signal généré au transmetteur est un paquet de $2M+1$ bits équiprobables modulé par déplacement de phase bivalente (BPSK), $\{b_m\} \in \{1,-1\}_{m=-M}^{M}$, et ce signal est étalé en fréquence par une séquence d'étalement $s(t)$. Si on considère le paquet en entier, le signal transmis est donné par

$$x(t) = \sum_{m=-M}^{M} b_m \sqrt{E_b} s(t - mT_s)\,, \tag{2.1}$$

où E_b est l'énergie d'un bit et T_s est la période d'un symbole.

La séquence d'étalement est un code PN de longueur N défini par

$$s(t) = A \sum_{i=0}^{N-1} a_i p(t - iT_c)\,, \tag{2.2}$$

où A est l'amplitude des impulsions et est ajusté de manière à ce que $s(t)$ ait une énergie unitaire, les termes $\{a_i\} \in \{1,-1\}_{i=1}^{N}$ forment un code PN, T_c est la période d'un chip et $p(t)$ est la forme du chip. Dans ce système, les chips sont des impulsions UWB qui incluent les effets des antennes de transmission et de réception. L'impulsion $p(t)$ utilisée est une impulsion fréquemment utilisée dans la littérature [3], soit :

$$p(t) = \left[1 - 4\pi\left(\frac{t}{\tau_m}\right)^2\right] \exp\left[-2\pi\left(\frac{t}{\tau_m}\right)^2\right]\,. \tag{2.3}$$

Signal reçu

Le signal reçu est défini par

$$r(t) = x(t) \otimes h(t) + n_{NB}(t) + n(t)\,, \tag{2.4}$$

où $x(t)$ est le signal transmis défini à l'équation (2.1).

$h(t)$ est la réponse impulsionnelle représentée sous forme de ligne de retard à prises :

$$h(t) = \sum_{l=0}^{L_p-1} \alpha_l \delta(t - \tau_l)\,. \tag{2.5}$$

Les canaux utilisés dans les simulations sont générés à l'aide du modèle de canal standard CM3 adopté par le comité 802.15.3a de l'IEEE [4].

$n_{NB}(t)$ est l'interférence à bande étroite et approxime un signal de type IEEE 802.11a par un processus gaussien aléatoire limité en fréquence affectant la même bande de fréquence que le signal 802.11a (soit une largeur de bande de 16.6 MHz centrée à 5.2 GHz.

$n(t)$ est un bruit blanc gaussien additif, définit par la densité spectrale de puissance $S_n(\omega) = N_0/2$.

2.3 Récepteurs

Forme générale du récepteur RAKE

Le récepteur RAKE est composé de L_r corrélateurs, ajustés à des délais différents, dont les sorties sont combinées de manière linéaire pour former le signal désiré.

La sortie du récepteur, après combinaison linéaire, est donc

$$z = \sum_{i=1}^{L_r} w_i \int_{\tau_i}^{\tau_i+T_s} r(t)s(t-\tau_i)\,\mathrm{d}t\,, \tag{2.6}$$

où w_i est le poids associé à la branche i et τ_i est le délai de cette même branche.

RAKE-MRC

La combinaison linéaire des branches du récepteur RAKE peut se faire de plusieurs manières. Le récepteur RAKE classique, tel que défini par Turin en 1980 [5], utilise la combinaison à ratio maximal (MRC) pour combiner la sortie des branches.

Soit $\boldsymbol{w}$, le vecteur des poids de la forme générale du récepteur RAKE, nous obtenons les poids suivants pour le récepteur RAKE-MRC :

$$\boldsymbol{w} = \boldsymbol{w}_{MRC}\,, \tag{2.7}$$

où $\boldsymbol{w}_{MRC}$ est le vecteur de poids qui maximise le rapport siganl à bruit si les entrées à combiner ne sont pas corrélées.

RAKE-MMSE

La combinaison minimisant l'erreur quadratique moyenne (combinaison MMSE) permet de combattre l'effet de la corrélation entre les branches du récepteur RAKE et d'obtenir une combinaison optimale en tout temps, au sens d'une solution de nature stochastique dans un environnement stationnaire (filtre de Wiener). Pour ce faire, on utilise l'inverse de la matrice de covariance de l'interférence plus bruit (matrice qui inclut l'effet de toutes les sources d'interférence et de bruit contenues dans le signal reçu), $\mathbf{R}_{I+N}$, pour déterminer les poids des branches pour la combinaison MMSE. Le poids des branches peut donc être donné par

$$\boldsymbol{w}_{MMSE} = \mathbf{R}_{I+N}^{-1}\boldsymbol{w}_{MRC}\,. \tag{2.8}$$

Puisque la combinaison MMSE est toujours optimale au sens de l'erreur quadratique moyenne, la combinaison MMSE est équivalente à la combinaison MRC lorsque les branches du récepteur RAKE ne sont pas corrélées. Dans ce cas, les poids sont identiques à un facteur d'échelle près.

©LRTS 2005-2006

2.4 Méthode semi-analytique

Cette section présente une méthode semi-analytique pour évaluer les performances du système défini dans les sections précédentes. La méthode est dite semi-analytique car elle permet d'obtenir une forme exacte du taux d'erreur binaire pour une réalisation de canal donnée.

Signal à la sortie d'une branche

Le signal à la sortie d'une branche du récepteur RAKE peut être divisé en trois composantes indépendantes :

$$z_i = S_i + n_{NB_i} + n_i \,. \tag{2.9}$$

Composante provenant des parcours multiples

La composante S_i provient des répétitions du signal transmis par les différents parcours multiples. Elle est définie par l'équation suivante :

$$\begin{aligned} S_i &= \sqrt{E_b} \sum_{l=0}^{L_p-1} \sum_{m=-M}^{M} b_m \alpha_l \times \int_{\tau_i}^{\tau_i+T_s} s(t - mT_s - \tau_l) s(t - \tau_i)\, \mathrm{d}t \\ &= S_{i,0} + S_{i,ISI} \,. \end{aligned} \tag{2.10}$$

Cette composante est elle-même formée de deux sous-composantes, soit $S_{i,0}$, la partie de S_i qui contribue au signal désiré, et $S_{i,ISI}$, la partie de S_i qui contribue à l'interférence intersymbole (ISI).

En supposant le bit désiré, b_0, connu, $S_{i,0}$ est défini par l'équation entièrement déterministe suivante :

$$\begin{aligned} S_{i,0} = b_0 \sqrt{E_b} \sum_{l \epsilon [0, L_p-1], x_l = 0} \alpha_l \times \int_{\tau_i}^{\tau_l + (x_l+1)T_s} s(t - x_l T_s - \tau_l) s(t - \tau_i)\, \mathrm{d}t \\ + b_0 \sqrt{E_b} \sum_{l \epsilon [0, L_p-1], x_l + 1 = 0} \alpha_l \times \int_{\tau_l + (x_l+1)T_s}^{\tau_i + T_s} s(t - (x_l+1)T_s - \tau_l) s(t - \tau_i)\, \mathrm{d}t \,. \end{aligned} \tag{2.11}$$

La composante $S_{i,ISI}$, cependant, contient deux séquences de variables aléatoires i.i.d. En utilisant le théorème de la limite centrale, on peut approximer $S_{i,ISI}$ à l'aide d'une variable aléatoire gaussienne de moyenne nulle et de variance $\mathrm{Var}(S_{i,ISI})$ définie par

$$\begin{aligned} \mathrm{Var}(S_{i,ISI}) = \sum_{l \epsilon [0, L_p-1], x_l \neq 0} \left(\sqrt{E_b} \alpha_l \times \int_{\tau_i}^{\tau_l + (x_l+1)T_s} s(t - x_l T_s - \tau_l) s(t - \tau_i)\, \mathrm{d}t \right)^2 \\ + \sum_{l \epsilon [0, L_p-1], x_l + 1 \neq 0} \left(\sqrt{E_b} \alpha_l \times \int_{\tau_l + (x_l+1)T_s}^{\tau_i + T_s} s(t - (x_l+1)T_s - \tau_l) s(t - \tau_i)\, \mathrm{d}t \right)^2 . \end{aligned}$$

Si l'on pose l'hypothèse que la corrélation entre les branches due à l'ISI est négligeable, on obtient la matrice $\boldsymbol{C}_{ISI}$ (matrice de covariance de l'interférence due aux parcours multiples) :

$$\mathbf{C}_{ISI} = \begin{bmatrix} \mathrm{Var}(S_{1,ISI}) & 0 & \cdots & 0 \\ 0 & \mathrm{Var}(S_{2,ISI}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{Var}(S_{L_r,ISI}) \end{bmatrix} . \tag{2.12}$$

Composante provenant de l'interférence à bande étroite

La composante n_{NB_i} provient de l'interférence à bande étroite. Elle est définie par l'équation suivante :

$$n_{NB_i} = \int_{\tau_i}^{\tau_i+T} n_{NB}(t) s(t-\tau_i)\,\mathrm{d}t\,. \tag{2.13}$$

En appliquant quelques simplifications proposées dans [6], l'élément (m,n) de la matrice de corrélation du NBI à la sortie des branches peut être représentée par l'approximation suivante :

$$[\mathbf{R}_{NB}]_{mn} \simeq |S(f_c)|^2 \frac{R_b}{SIR} \cos(2\pi f_c(\tau_m - \tau_n)) \times \mathrm{sinc}((\tau_m - \tau_n)W_{NB})\,. \tag{2.14}$$

Composante provenant du bruit thermique

La composante n_i provient du bruit thermique au récepteur. Elle est définie par l'équation suivante :

$$n_i = \int_{\tau_i}^{\tau_i+T} n(t) s(t-\tau_i)\,\mathrm{d}t\,. \tag{2.15}$$

Puisque $n(t)$ est un processus gaussien dont la moyenne est nulle et dont la fonction d'auto-corrélation est $\frac{N_0}{2}\delta(t)$, n_i est une variable aléatoire gaussienne de moyenne nulle et de variance $\sigma_n^2 = \frac{N_0}{2}$.

Matrice de corrélation interférence plus bruit

La matrice de corrélation interférence plus bruit, $\mathbf{R}_{I+N}$, peut être construite à partir des éléments définis dans les trois sous-sections précédentes :

$$\mathbf{R}_{I+N} = \mathbf{C}_{ISI} + \mathbf{R}_{NB} + \sigma_n^2 \mathbf{I}_{L_r}\,, \tag{2.16}$$

où $\mathbf{C}_{ISI}$ représente l'interférence due aux parcours multiples, $\mathbf{R}_{NB}$ représente l'interférence à bande étroite et $\sigma_n^2\mathbf{I}_{L_r}$ représente le bruit blanc gaussien ($\mathbf{I}_{L_r}$ représente la matrice identité de dimensions $(L_r \times L_r)$).

©LRTS 2005-2006

SNR et BER à la sortie du récepteur

Soit $\boldsymbol{s}_0$ le vecteur contenant les composantes parcours multiples de chaque branche du récepteur qui contribuent au signal désiré :

$$\boldsymbol{s}_0 = \left[\begin{array}{cccc} S_{1,0} & S_{2,0} & \cdots & S_{L_r,0} \end{array} \right]^T . \tag{2.17}$$

La forme générale du rapport signal à bruit à la sortie du récepteur, γ, est donné par l'expression suivante :

$$\gamma = \frac{(\boldsymbol{w}^H \boldsymbol{s}_0)^2}{\boldsymbol{w}^H \mathbf{R}_{I+N} \boldsymbol{w}} . \tag{2.18}$$

Pour un système BPSK, le taux d'erreur binaire en fonction du rapport signal à bruit à la sortie du récepteur est donné par [7] :

$$P_b = Q\left(\sqrt{2\gamma}\right) . \tag{2.19}$$

Pour déterminer le taux d'erreur binaire pour le récepteur RAKE-MRC, on remplace les poids $\boldsymbol{w}$ par les poids $\boldsymbol{w}_{MRC}$ dans l'équation (2.18), puis on applique l'équation (2.19) pour déterminer le taux d'erreur binaire.

On procède de la même manière pour le récepteur RAKE-MMSE en remplaçant les poids dans l'équation (2.18) par $\boldsymbol{w}_{MMSE}$.

2.5 Conclusion

La validité de la méthode semi-analytique proposée a été vérifiée par une comparaison avec des simulations par la méthode de Monte-Carlo effectuées avec le même système. Nous avons observé que la méthode semi-analytique reproduit adéquatement les effets de l'interférence à bande étroite. Dans le cas de l'ISI, on note que le comportement de la méthode semi-analytique est très proche de celui de la méthode de Monte-Carlo, bien que la méthode semi-analytique ignore la faible corrélation induite entre les branches du RAKE par l'ISI. Il est important de noter que pour un taux binaire supérieur à 100 Mb/s, la corrélation due à l'ISI ne pourrait pas être négligée.

La méthode semi-analytique est une première étape vers une étude complètement analytique de ce système. Il est aussi intéressant d'observer qu'à un taux binaire de 100 Mb/s, la méthode semi-analytique génère des résultats environ 100 fois plus rapidement que la simulation par la méthode de Monte-Carlo.

Bibliographie

[1] Q. Li and L. A. Rusch, "Multiuser Detection for DS-CDMA UWB in the Home Environment," *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 1701–1711, Decembre 2002.

[2] M. Thériault, L. A. Rusch, and P. Fortier, "Effect of RAKE Correlations on the Performance of Hybrid RAKE," in *Proc. of the 22nd Biennial Symposium on Communications*, pp. 322–324, mai 2004.

[3] M.-G. D. Benedetto and G. Giancola, *Understanding Ultra Wide Band Radio Fundamentals*. New Jersey : Prentice Hall Professional Technical Reference, first ed., 2004.

[4] A. F. Molisch, J. R. Foerster, and M. Pendergrass, "Channel Models for Ultrawideband Personal Area Networks," *IEEE Wireless Communications*, pp. 14–21, December 2003.

[5] G. L. Turin, "Introduction to Spread-Spectrum Antimultipath Techniques and Their Application to Urban Digital Radio," *Proc. of the IEEE*, vol. 68, pp. 328–353, March 1980.

[6] I. Bergel, E. Fishler, and H. Messer, "Narrowband interference suppression in time-hopping impulse-radio systems," in *IEEE conference on UWBST*, pp. 303–307, May 2002.

[7] J. G. Proakis, *Digital Communications*. New York : McGraw-Hill, fourth ed., 2001.

©LRTS 2005-2006

Architecture de routage hiérarchique multiniveaux pour les réseaux de capteurs sans fil

Simon Savary, *Étudiant au doctorat*
Jean-Yves Chouinard, *Directeur de recherche.*

Résumé – Nous développons une architecture de routage hiérarchique à plusieurs niveaux qui permettra un gain important en durée de vie par rapport aux protocoles existants dans des scénarios où des milliers de nœuds sont déployés pour la cueillette de données dans des environnements difficiles d'accès ou peu enclins à l'utilisation d'infrastructures filaires.

Abstract – We are developping a multilevel hierarchical routing architecture for wireless sensor networks. The new architecture promises an important network life time gain in comparison to existing protocols for thousand-nodes networks with data collecting scenarios in hostile environments.

3.1 Introduction

Forts des récents progrès dans les champs des télécommunications sans fil et de l'électronique numérique, les réseaux de capteurs sans fil jouissent d'un grand intérêt en recherche scientifique. Ces réseaux ouvrent la voie à de nouvelles applications des capteurs dans les environnements contrôlés grâce à leurs fonctionnalités augmentées : coopération, traitement des données, configuration automatique, etc.

Les applications des réseaux de capteurs sans fil sont multiples : surveillance et contrôle à distance de paramètres tels que la température, le pH du sol, la qualité de l'air d'usines à risque, mesure de paramètres de déformation et de pression d'une structure, informatisation de voitures, etc. Le plus souvent, les réseaux de capteurs trouvent leur intérêt dans des applications où le nombre de capteurs est très élevé (des centaines, des milliers) et leur déploiement aléatoire, où la zone de déploiement est difficile d'accès ou inadéquate pour des capteurs filaires et lorsqu'un entretien minimal du réseau est requis.

La contrainte directrice pour le design des algorithmes d'un réseau de capteurs sans fil est l'énergie disponible limitée. En effet, chaque capteur bénéficie d'une source d'énergie finie. Chacun disposant d'une unité radio, d'une unité de calcul et d'une mémoire, les dépenses dé'énergies doivent être minimisées. La plupart des protocoles doivent donc être repensés pour convenir aux besoins et contraintes des réseaux de capteurs sans fil.

Nous introduirons l'architecture hiérarchique LEACH avant de présenter notre architecture hiérarchique à plusieurs niveaux, puisque cette dernière est une version augmentée du protocole LEACH. Les avantages projetés seront aussi expliqués.

3.2 Architecture LEACH

LEACH, *Low Energy Adaptive Clustering Hierarchy* [1, 3], est une architecture de routage conçue expressément pour les réseaux de capteurs sans fil, où des groupes adaptatifs et rotatifs sont formés de façon à répartir les dépenses d'énergies dans le reéseau. La division du temps pour l'architecture LEACH est la période, d'une durée fixe. Chaque période p comporte une phase préparatoire et une portion en régime permanent.

Phase préparatoire

Au début d'une période, les capteurs entre dans la phase d'élection de k chefs de groupe, lesquels communiqueront directement avec la station de base distante. L'élection est probabiliste avec un critère imposant à tous les nœuds de devenir chef de groupe avant qu'un même nœud ne redevienne chef de groupe à son tour. Les $(n - k)$ nœuds non élus pour cette période jouent le rôle de simples capteurs.

Une fois élus, les k chefs de groupe transmettent une trame d'identification via un protocole d'accès multiple CSMA non-persistant. Les simples capteurs reçoivent ces trames et s'associent au chef de groupe dont le signal est le plus fort. Ils lui transmettent une trame d'association. Les groupes ainsi formés, les chefs de groupe établissent un schéma d'accès TDMA avec pour leur groupe respectif. La figure 3.1 présente la division en groupes à la fin de la phase préparatoire d'une période.

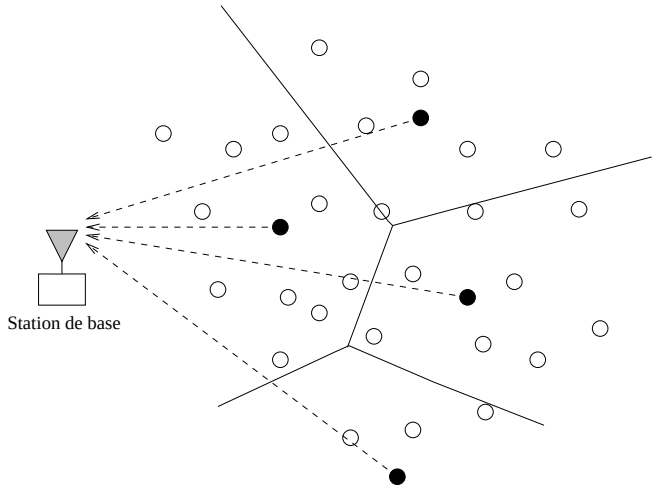


FIG. 3.1: Illustration du principe de regroupement du protocole LEACH. Les chefs de groupe sont en noir et les simples capteurs en blanc. Les lignes pleines identifient les limites de groupes. Les chefs de groupe communiquent directement à la station de base.

Régime permanent

Les groupes formés, la phase de transmission de données peut commencer. Pour le reste de la période courante, les simples capteurs transmettent leurs données directement à leur chef de

groupe, en ajustant leur puissance de transmission en conséquence. Les chefs de groupe reçoivent les données de leurs capteurs et utilisent la dernière tranche de temps de la trame TDMA, qui leur est réservée, pour compresser et envoyer ces données directement à la station de base. Cette opération est coûteuse et doit être faite parcimonieusement. À la fin d'une période, une nouvelle phase préparatoire débute une nouvelle période. De nouveaux nœuds deviendront chefs de groupe.

Protocoles dérivés de LEACH

Une version centralisée de LEACH, appelée LEACH-C [3], améliore la version originale en déléguant la tâche de formation des groupes à la station de base. Les nœuds doivent par contre connaître ou estimer leur position. La station de base répartit les rôles selon l'énergie restante dans chaque capteur. L'amélioration se mesure à 40% plus de données transmises à la station de base par quantité d'énergie dépensée.

Finalement, le protocole BCDCP, *Base-Station Controlled Dynamic Clustering Protocol* [5], est une autre version centralisée et améliorée de LEACH, qui propose le balancement des groupes et le routage entre les chefs de groupe, que LEACH et LEACH-C ne supportent pas. BCDCP surpasse LEACH-C d'environ 40% pour les données reçues à la station de base.

3.3 Nouvelle architecture proposée

Une architecture hiérarchique a l'avantage de réduire les distances de transmission au chef de groupe le plus près. Les architectures LEACH, LEACH-C et BCDCP comportent toutes trois un niveau hiérarchique. Les économies d'énergie apportées par ces protocoles sont notables pour des réseaux de taille modeste, soit environ 100 à 1000 capteurs. Pour des réseaux plus grands, les groupes peuvent devenir trop nombreux ou trop denses, réduisant ainsi les gains apportés par LEACH. Une solution est d'ajouter des niveaux de hiérarchie pour réduire la taille des sous-groupes. À l'instar de LEACH, les capteurs communiquent avec un chef de groupe, lui-même soumis à un chef de groupe de niveau supérieur. Le nombre de niveaux hiérarchique demeure un paramètre propre au nombre de nœuds du réseau.

Nous considérons en premier lieu une hiérarchie à trois niveaux, c'est-à-dire les simples capteurs, les chefs de groupe de niveau 1 et les chefs de groupe de niveau 2. La figure 3.2 illustre le principe. Les capteurs (niveau 0) communiquent leurs données au chef de groupe de niveau 1. Ceux-ci, séparés à leur tour en groupes, parlent à leur chef de groupe de niveau 2. La station de base, quant à elle, reçoit les données des capteurs de niveau 2.

Typiquement, les données accumulées par les capteurs sont spatialement et temporellement corrélées, par exemple lorsque la température est le paramètre d'intérêt. Les données peuvent donc être débarrassées de cette corrélation en passant d'un niveau à un autre dans la hiérarchie. Comme cette agrégation des données a un coût énergétique, celui-ci peut être distribué parmi les chefs de groupe en partageant la tâche entre les niveaux.

Un autre avantage d'une telle hiérarchie est que les capteurs peuvent alors être groupés en plus petit nombre que pour LEACH, réduisant du même coup le trafic de groupe et les retards dans le cas d'utilisation du TDMA. De plus, les groupes étant plus nombreux, les chefs de groupe se situent d'emblée plus près des capteurs, qui peuvent *ipso facto* réduire leur puissance de transmission.

©LRTS 2005-2006

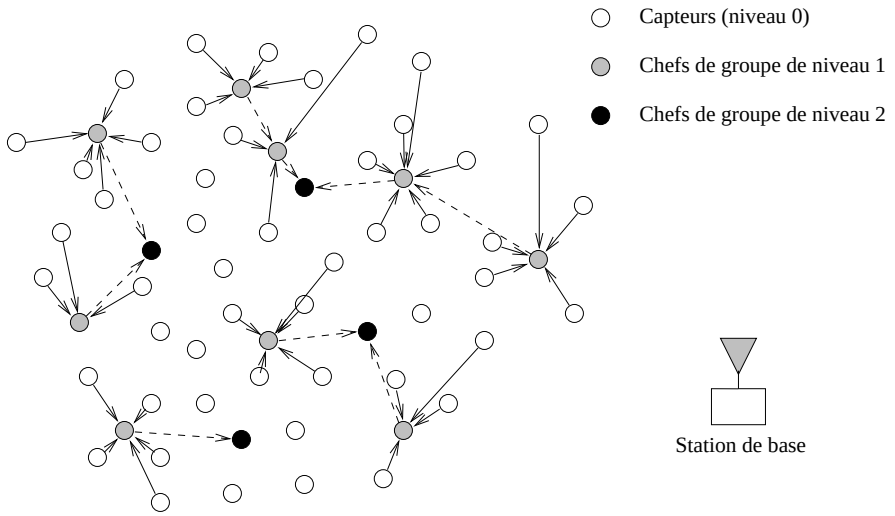


FIG. 3.2: Illustration de la hiérarchie à plusieurs niveaux de groupement. Cet exemple comporte 3 niveaux.

3.4 Conclusion

Une architecture de routage hiérarchique à trois niveaux a été décrite pour les réseaux de capteurs sans fil. Cette architecture se prête naturellement aux réseaux comportant des milliers de nœuds et promet de bonnes économies d'énergies, au moins équivalentes à celles obtenues par le protocole LEACH, mais pour des réseaux de taille plus modeste. L'extension à plus de trois niveaux sera développée et analysée dans un avenir rapproché.

Bibliographie

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Proceeedings of the 33rd Hawaii International Conference on System Sciences*, janvier 2000.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, vol. 40, pp. 102–114, août 2002.

[3] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, octobre 2002.

[4] J. N. Al-Karaki, and A. E. Kamal, *Routing Techniques in Wireless Sensor Networks. Wireless Communications*, pp. 6–28, décembre 2004.

[5] S. D. Muruganathan, D. C. F. Ma, R. I. Bhasin, and A. O. Fapojuwo, "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. S8 ?S13, mars 2005.

High-performance LDPC codes based on circulant permutation matrices

Zhiyong He, *Étudiant au doctorat.*
Paul Fortier, *Directeur de recherche.*
Sébastien Roy, *Co-directeur de recherche.*

Résumé – Nous proposons une classe de codes LDPC (Low Density Parity Check) construite à partir de matrices de permutation circulantes. Étant caractérisés par une complexité de codage linéaire, les codeurs proposés atteignent des capacités au-dessus de 1 Gbits/sec. Pour un taux d'erreur inférieur à 10^{-10}, les codes proposés conviennent aux applications à rendement élevé et à grande vitesse, telles que les réseaux sans fil à grande vitesse, les systémes mobiles futurs, réseaux de grandes distances, Gigabit Ethernet, stockage magnétiques et optiques des données.

Abstract – We propose a class of LDPC codes which are constructed from circulant permutation matrices. Being characterized by linear encoding complexity, the encoders of the proposed codes attain throughputs in the Gbits/sec. Having no bit-error-rate floor down to 10^{-10}, the proposed codes are suitable for high-performance and high-speed applications, such as high-speed wireless networks, future mobile system, long-haul optical channels, Gigabit Ethernet, magnetic and optical data storages.

4.1 Introduction

Because of their excellent performance and the existence of effective decoding schemes, low density parity check (LDPC) codes introduced by Gallager [1] have recently received a lot of interest for reliable high speed communication applications such as long-haul optical channels and magnetic storage. Several standards have been recently proposed which suggested the incorporation of LDPC codes : 802.3 Gigabit Ethernet, 802.11n high-throughput wireless local area networks (LAN), 802.16 broadband wireless access systems, and Digital Video Broadcast (DVB) satellite communications. Because of their many applications, a great deal of research effort has been directed towards LDPC code construction, their performance analysis, structural study, as well as encoding and decoding of LDPC codes. In this work, we discuss techniques for the construction of high-performance codes.

Several approaches to code construction have been introduced in the recent literature, such as random code construction, construction based on repeat-accumulate codes, finite geometries, and Reed-Solomon (RS) codes, and construction based on circulant permutation matrices. We have constructed LDPC codes based on circulant permutation matrices because of their simple structure which dramatically reduces the storage requirements associated with the parity check matrix in encoders and decoders [2] [3] [4] [5]. Since their parity-check matrices consist of circu-

lant permutation sub-matrices, the hardware complexity and the routing congestion of parallel decoders can be dramatically reduced compared to randomly-constructed LDPC codes.

4.2 Proposed LDPC codes

We propose a class of irregular LDPC codes characterized by the following parity-check matrix $\mathbf{H} = [\mathbf{H_S}|\mathbf{H_P}]$ in which each column and each row have non-constant degrees, i.e. the parity-check matrix is made up of a $J \times L$ array of circulant submatrices as follows :

$$\mathbf{H} = \left[\begin{array}{ccc|cccc} \mathbf{H}_{1,\ 1} & \cdots & \mathbf{H}_{1,\ L-J} & \mathbf{I} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \mathbf{H}_{J-1,\ 1} & \cdots & \mathbf{H}_{J-1,\ L-J} & \mathbf{H}_{J-1,\ L-J+1} & \cdots & \mathbf{H}_{J-1,\ L-2} & \mathbf{I} & \mathbf{I}(q-1) \\ \mathbf{H}_{J,\ 1} & \cdots & \mathbf{H}_{J,\ L-J} & \mathbf{H}_{J,\ L-J+1} & \cdots & \mathbf{H}_{J,\ L-2} & \mathbf{I} & \mathbf{I} \end{array}\right]. \tag{4.1}$$

For $1 \leq j \leq J$ and $1 \leq l \leq L$, the sub-matrix $\mathbf{H}_{j,l}$ in position (j, l) within $\mathbf{H}$ is either a $q \times q$ null matrix or a $q \times q$ circulant matrix obtained by circulating the rows of the identity matrix $\mathbf{I}$ to the right by $C_{j,l}$ places, i.e. $\mathbf{H}_{j,l} \equiv \mathbf{I}(C_{j,l})$. The shifting coefficient $C_{j,l}$ is randomly chosen in such a way as to avoid short cycles in the code's Tanner graph. To distinguish from conventional columns and rows, we refer to a column (row) of sub-matrices within $\mathbf{H}$ as a block-column (block-row). Hence, matrix $\mathbf{H}$ has J block-rows and L block-columns (BC).

An important contribution in equation (4.1) is that four sub-matrices $\begin{bmatrix} \mathbf{I} & \mathbf{I}(q-1) \\ \mathbf{I} & \mathbf{I} \end{bmatrix}$ which compose a dual-diagonal matrix by row and column permutations are used at the lower-right corner of $\mathbf{H_P}$ to lower the error floor and reduce encoding complexity [3]. Thus, by putting the rows of $\mathbf{H}_{J-1} = [\mathbf{H}_{J-1,1} \ \cdots \ \mathbf{H}_{J-1,L-2} \quad \mathbf{I} \quad \mathbf{I}(q-1)]$ and $\mathbf{H}_J = [\mathbf{H}_{J,1} \ \cdots \ \mathbf{H}_{J,L-2} \quad \mathbf{I} \quad \mathbf{I}]$ into the odd and even rows of $\mathbf{H}$, respectively, the proposed matrix is characterized by a triangular plus dual-diagonal form. Being characterized by a triangular matrix, the encoding complexity of the proposed codes is linearly proportional to the block length. The implementation results into FPGA devices indicate that the encoders for this class of LDPC codes support throughputs over 10 Gbits/sec using only several hundreds of exclusive-OR gates [5].

4.3 Code construction for low error floors

Two main causes of error floors in LDPC codes are known to be 1- a small minimum distance, and 2- low-weight pseudo-codewords. A classical measure of the "goodness" of a code is the code's minimum Hamming distance which is defined as the minimum number of coordinates in which any two distinct codewords differ. Analogous to the role of minimum Hamming distance in maximum likelihood (ML) decoding, the minimum pseudo-codeword weight has been shown to be a leading predictor of performance in iterative belief propagation (BP) decoding [6]. Some pseudo-codewords which do not constitute valid codewords but cause failures in the BP decoder are typically referred to as stopping sets in a binary erasure channel or trapping sets in an AWGN channel or in a binary symmetric channel.

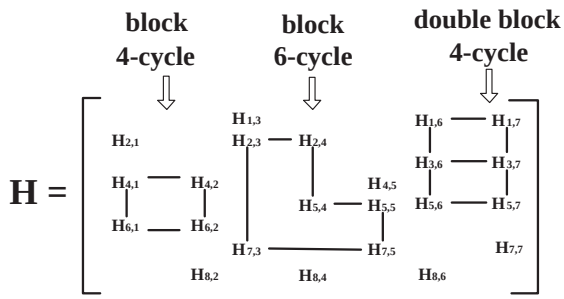


Fig. 4.1: Block cycles in matrix **H**. Unmarked spaces are null sub-matrices.

To design high-performance LDPC codes with low error floors, we propose a progressive approach in which matrix **H** is constructed BC-by-BC starting from the rightmost BC (recall that BC refers to block-column) to the leftmost BC within **H**, where the column degree of each BC increases from the smallest degree for the rightmost BC to the largest degree for the leftmost BC. To increase both the minimum distance of the codewords and the minimum pseudo-codeword weight, the position and the shifting coefficient of each circulant matrix are carefully chosen during code construction.

The position of each circulant matrix : Each circulant matrix in each BC should be carefully positioned to reduce short block cycles in **H**. Between two arbitrary BCs with a degree of 3, block 4-cycles and block 6-cycles should be avoided, while double block 4-cycles and block 6-cyclse should be reduced between two arbitrary BCs with a degree of 4. A block 4-cycle indicates that two BCs are linked via two block-rows, while a block 6-cycle indicates that three BCs are linked via three block-rows, where a circulant matrix in position (j, l) within **H** stands for a link of BC l with block-row j. Fig. 4.1 shows an intuitive example for short block cycles within H. A double block 4-cycle in Fig. 4.1 indicates that two BCs are linked via three block-rows.

The shifting coefficient of each circulant matrix : To optimize the cycle structure, the shifting coefficients of the circulant matrices for BCs with degree 2 and 3 are chosen to avoid cycles of length 4, 6, or 8. Then, the coefficients for BCs with degree 4 are chosen to avoid cycles of lengths 4 and 6. Finally, the short cycle of length 6 must be composed of high-degree BCs.

4.4 Performance analysis

We have observed the error floors of various LDPC codes by performing simulations with binary phase-shift keying (BPSK) modulation in an AWGN channel. The iterative BP decoder stops when either a valid codeword is found or 50 decoding iterations are reached. The experimental results indicate that both the minimum distances and the error floors can be improved by decreasing the fraction of columns with minimum degree in **H**. As an example, Fig. 4.2 compares the frame error rate (FER) and the bit error rate (BER) of two codes characterized by the parity-check matrix in (4.1). The minimum distances are upper-bounded at 26 and 73 for Code 1 with λ_2= 0.263 and Code 2 with λ_2= 0.124, respectively, where λ_2 denotes the fraction of columns with a minimum degree of 2 in **H**. It is shown in Fig. 4.2 that the slope of the error curves in the waterfall region increases with increasing minimum distance. No BER floor down to 10^{-10} was observed for Code 2.

©LRTS 2005-2006

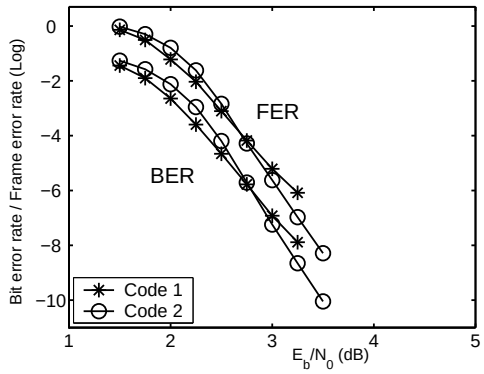


FIG. 4.2: BER and FER comparisons between code 1 and code 2. The two codes have a code length of 1944 and a code rate of 2/3.

4.5 Future applications

Because of their excellent performance and their simple structures, LDPC codes based on circulant permutation matrices are very suitable for high-speed and high-performance applications in advanced digital communication. By optimizing both the degree distributions and the cycle structures during code construction, we designed LDPC codes having no BER floor down to 10^{-10} which can be used in broadband wireless access networks or optical communications. To design irregular LDPC codes for magnetic and optical data storage where a BER floor of 10^{-15} is often required, we can further optimize the cycle structures during code construction by reducing the fraction of columns with small degree in $\mathbf{H}$ and decreasing the size of each submatrix (i.e. increasing the number of block-rows).

Bibliographie

[1] R. G. Gallager, "Low-Density Parity-Check Codes," *Ph. D Thesis*, Cambridge, MA : MIT. Press, 1963.

[2] Z. He, P. Fortier, and S. Roy, "Design of high-performance low-density parity-check codes using interleaver approach," *IEE Electronics Letters*, vol. 41, pp. 1390-1391, Dec. 2005.

[3] Z. He, P. Fortier, and S. Roy, "A class of irregular LDPC codes with low error floor and low encoding complexity," *IEEE Communications Letters*, vol. 10, no. 5, pp. 372-374, May 2006.

[4] Z. He, S. Roy, and P. Fortier, "Capacity-approaching LDPC codes with low error floors for high-speed digital communications," *Proc. of the 23rd Biennial Symposium on Communications*, Kingston, Canada, pp. 10-14, May 30 - June 1, 2006.

[5] Z. He, S. Roy, and P. Fortier, "Encoder architecture with throughput over 10 Gbit/sec for quasi-cyclic low density parity check codes," *Proc. of IEEE International Symposium on Circuits and Systems*, Kos, Greece, May 21-24, 2006.

[6] C. Kelley and D. Sridhara, "Pseudocodewords of Tanner graphs," *Submitted to IEEE Transactions on Information Theory*, submitted in June 2005.

High-speed encoders of LDPC codes in 802.11n wireless local area networks and 802.16e broadband wireless systems

Zhiyong He, *Étudiant au doctorat.*
Paul Fortier, *Directeur de recherche.*
Sébastien Roy, *Co-directeur de recherche.*

Résumé – Nous avons conçu des encodeurs à haute-vitesse pour deux classes de codes LDPC (Low Density Parity Check). La première classe est caractérisée par une matrice ayant une forme double-diagonale approximative et a été employée dans les normes 802.11n et 802.16e. Comparativement à la première classe, la deuxième classe de codes LDPC, qui est caractérisée par une matrice combinant les formes triangulaire et double-diagonale, donne des faibles taux d'erreurs et abaisse la complexité de codage. Les résultats d'implémentation dans les dispositifs FPGA indiquent que les deux classes de codes LDPC supportent des débits de plus de 600 Mbps en utilisant quelques dizaines de portes OU-exclusif.

Abstract – We have designed high-speed encoders for two classes of low-density parity-check (LDPC) codes. The first class of LDPC codes, characterized by a parity-check matrix having an approximate dual-diagonal form, has been used in the IEEE 802.11n and 802.16e standards. Compared to the first class, the second class of LDPC codes, characterized by a matrix in a triangular plus dual-diagonal form, exhibits a lower error floor and lower encoding complexity. The implementation results into FPGA devices indicate that the encoders for the two classes of LDPC codes support throughputs over 600 Mbps using only several tens of exclusive-OR gates.

5.1 Introduction

Advanced error correction codes, the so-called low-density parity-check (LDPC) codes, have been included into both the IEEE 802.11n standard for wireless local area networks (LAN) and the IEEE 802.16e standard for broadband wireless access systems to enhance robustness and to reduce transmission power in these systems. In this paper, we discuss high-speed implementations of the encoders for the LDPC codes specified in the 802.11n and 802.16e standards. Further, to minimize the hardware costs and the memory requirements of such encoders, we propose a class of high-performance codes which can be encoded in linear time, by designing the parity check matrix in a triangular plus dual-diagonal form [1] [2] [3]. The hardware costs of the encoders are compared in detail between the proposed LDPC codes and the LDPC codes specified in the 802.11n and 802.16e standards.

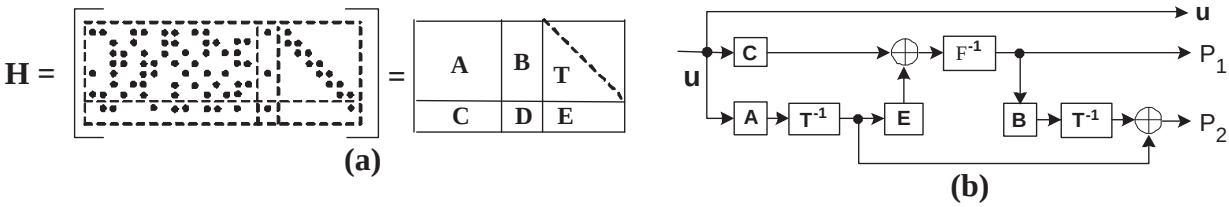


FIG. 5.1: Encoders for 802.11n and 802.16e standards. (a) Parity-check matrix $\mathbf{H}$ in an approximate dual-diagonal form. Solid points are circulant permutation matrices of $\mathbf{I}$ and unmarked spaces are null sub-matrices. (b) Block diagram of the encoder architecture.

5.2 Encoders for the codes in 802.11n and 802.16e standards

The LDPC codes specified in 802.11n and 802.16e standards are characterized by a parity-check matrix $\mathbf{H} = [\mathbf{H_S}|\mathbf{H_P}]$ in which each column and each row have non-constant degrees, i.e. the parity-check matrix is made up of a $J \times L$ array of circulant submatrices as follows :

$$\mathbf{H} = \left[\begin{array}{ccc|ccc} \mathbf{H}_{1,\ 1} & \cdots & \mathbf{H}_{1,\ L-J} & \mathbf{H}_{1,\ L-J+1} & \cdots & \mathbf{H}_{1,\ L} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{J,\ 1} & \cdots & \mathbf{H}_{J,\ L-J} & \mathbf{H}_{J,\ L-J+1} & \cdots & \mathbf{H}_{J,\ L} \end{array}\right]. \tag{5.1}$$

For $1 \leq j \leq J$ and $1 \leq l \leq L$, the sub-matrix $\mathbf{H}_{j,l}$ in position (j, l) within $\mathbf{H}$ is either a $q \times q$ null matrix or a $q \times q$ circulant matrix obtained by circulating the rows of the identity matrix $\mathbf{I}$ to the right by $C_{j,l}$ places, i.e. $\mathbf{H}_{j,l} \equiv \mathbf{I}(C_{j,l})$. To reduce encoding complexity, the parity part $\mathbf{H_P}$ has an approximate dual-diagonal form. Fig. 5.1(a) shows matrix $\mathbf{H}$ of the LDPC code specified in the 802.16e standard with a code rate of 2/3. To encode such a code, matrix $\mathbf{H}$ is divided into six submatrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{T}$. Let $\mathbf{x} = (\mathbf{u}, \mathbf{p_1}, \mathbf{p_2})$, where $\mathbf{u}$ denotes the systematic part, $\mathbf{p_1}$ and $\mathbf{p_2}$ combined denote the parity part. From the encoding equation $\mathbf{Hx^T} = \mathbf{0^T}$, we get the following encoding algorithm [4] :

$$\mathbf{p_1^T} = \mathbf{F^{-1}}(-\mathbf{ET^{-1}A} + \mathbf{C})\mathbf{u^T}, \tag{5.2}$$

$$\mathbf{p_2^T} = \mathbf{T^{-1}}(\mathbf{Au^T} + \mathbf{Bp_1^T}), \tag{5.3}$$

where $\mathbf{F} = -\mathbf{ET^{-1}B} + \mathbf{D}$. A block diagram of the encoding procedure is shown in Fig. 5.1(b). The systematic bits vector $\mathbf{u}$ is multiplied step-by-step by sub-matrices $\mathbf{A}$, $\mathbf{C}$, $\mathbf{T}^{-1}$, $\mathbf{E}$, $\mathbf{F}^{-1}$, $\mathbf{B}$, and $\mathbf{T}^{-1}$ to obtain the parity bits $\mathbf{p}_1$ and $\mathbf{p}_2$. Since $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$, $\mathbf{T}$ are sparse matrices, the multiplications are simply implemented with several exclusive-OR (XOR) gates. Thus, the encoding complexity mainly depends on the sub-matrix $\mathbf{F}^{-1}$. For the LDPC codes in the 802.11n and 802.16e standards, the sub-matrices $\mathbf{B}$, $\mathbf{D}$ and $\mathbf{E}$ are randomly chosen in such a way that the sub-matrix $\mathbf{F}^{-1}$ becomes the identity matrix.

$$\begin{bmatrix} H_{S1} & I & 0 & 0 & 0 \\ H_{S2} & H_{2,(L-3)} & I & 0 & 0 \\ H_{S3} & H_{3,(L-3)} & H_{3,(L-2)} & I & I(q-1) \\ H_{S4} & H_{4,(L-3)} & H_{4,(L-2)} & I & I \end{bmatrix} \times \begin{bmatrix} u^T \\ P_1^T \\ P_2^T \\ P_3^T \\ P_4^T \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Downarrow$$

Layer 1: $H_{S1}\, u^T = P_1^T$

Layer 2: $H_{S2}\, u^T + H_{2,(L-3)}\, P_1^T = P_2^T$

Last layer: $\begin{bmatrix} H_{S3} \\ H_{S4} \end{bmatrix} u^T + \begin{bmatrix} H_{3,(L-3)} \\ H_{4,(L-3)} \end{bmatrix} P_1^T + \begin{bmatrix} H_{3,(L-2)} \\ H_{4,(L-2)} \end{bmatrix} P_2^T = \begin{bmatrix} I & I(q-1) \\ I & I \end{bmatrix} \begin{bmatrix} P_3^T \\ P_4^T \end{bmatrix}$

Fig. 5.2: Layered encoding algorithm deduced from encoding equation $\mathbf{H}\ \mathbf{x} = \mathbf{0}$.

5.3 Layered encoders for the proposed LDPC codes

A main drawback of the LDPC codes in 802.11n and 802.16e standards is that $\mathbf{H}$ has at least $(J-1) \times q$ columns of degree 2 which may result in a high error floor. Thus, we propose a class of irregular LDPC codes in which $\mathbf{H_P}$ has a triangular plus dual-diagonal form in [1] . As an example, consider $J = 4$ in (5.1). The proposed LDPC code is characterized by the following matrix.

$$\mathbf{H} = \left[\begin{array}{ccc|cccc} \mathbf{H}_{1,\ 1} & \cdots & \mathbf{H}_{1,\ L-4} & \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{H}_{2,\ 1} & \cdots & \mathbf{H}_{2,\ L-4} & \mathbf{H}_{2,\ L-3} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{H}_{3,\ 1} & \cdots & \mathbf{H}_{3,\ L-4} & \mathbf{H}_{3,\ L-3} & \mathbf{H}_{3,\ L-2} & \mathbf{I} & \mathbf{I}(q-1) \\ \mathbf{H}_{4,\ 1} & \cdots & \mathbf{H}_{4,\ L-4} & \mathbf{H}_{4,\ L-3} & \mathbf{H}_{4,\ L-2} & \mathbf{I} & \mathbf{I} \end{array}\right]. \tag{5.4}$$

Four sub-matrices $\begin{bmatrix} \mathbf{I} & \mathbf{I}(q-1) \\ \mathbf{I} & \mathbf{I} \end{bmatrix}$ which together form a dual-diagonal matrix after a number of row and column permutations are used at the lower-right corner of $\mathbf{H}$ to lower the error floor and to reduce encoding complexity [1]. Consider a partitioning of $\mathbf{x}$ into 5 parts, i.e. $\mathbf{x} = (\mathbf{u}, \mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3, \mathbf{p}_4)$, where $\mathbf{u}$ denotes the systematic part and $(\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3, \mathbf{p}_4)$ denotes the parity part. Since $\mathbf{H}$ has a triangular plus dual-diagonal form, the encoding equation $\mathbf{H}\ \mathbf{x^T} = \mathbf{0^T}$ is naturally broken down into a *layered encoding algorithm* which is shown in Fig. 5.2.

The hardware implementation of the proposed layered encoder is decribed in [2]. At first, the systematic bits vector $\mathbf{u}$ is multiplied by $\mathbf{H_{S1}}$ to get the parity bits $\mathbf{p}_1$. Then, the vector $(\mathbf{u}, \mathbf{p}_1)$ is multiplied by $\mathbf{H_{S2}}$ and $\mathbf{H_{2,(L-3)}}$ to get the vector $\mathbf{p}_2$, and so on. Since all the sub-matrices are sparse matrices, the multiplication is simply implemented with several XOR gates.

5.4 Results

We implemented encoders for three LDPC codes into Xilinx Virtex-II FPGA devices. Both the code specified in 802.16e standard and the code proposed by the TGn Sync group within the 802.11n workgroup are characterized by the parity-check matrix in an approximate dual-diagonal

TAB. 5.1: XOR gates utilization and speeds of the encoders for two LDPC codes.

	M=3				M=9			
	RAM (bits)	XOR gates	Speed (Mbps)	Latency (μs)	RAM (bits)	XOR gates	Speed (Mbps)	Latency (μs)
Code in 802.16e	3528	38	600	7.68	3816	112	1800	2.56
Code in 802.11n	3528	41	600	7.68	3816	121	1800	2.56
The proposed code	1872	34	600	3.84	1872	103	1800	1.28

form, while the proposed code is characterized by a matrix in a triangular plus dual-diagonal form. To increase encoding speed, XOR processing for matrix-vector multiplications were implemented in parallel by using repeatedly M processors $t = m/M$ times, where m is the number of rows in each matrix and M is the degree of parallelism. The systematic bits $\mathbf{u}$ and the intermediate vector were stored into the dual-port Random Access Memory (RAM) with one port for writing and one port for reading. The memory requirements, the XOR gate statistics, the encoding speeds, and the encoding latencies of several encoders are listed in Table 5.1, where the encoding speed was determined by using an encoding clock frequency of 100 MHz. Compared to the codes in the 802.16e and 802.11n standards, the proposed code brings a saving in memory resources of 50% and a reduction in latency of the same order. Because of their very low error floor [1] [3], the proposed LDPC codes are suitable for high-performance and high-speed applications in digital communications, including wireless communications.

Bibliographie

[1] Z. He, P. Fortier, and S. Roy, "A class of irregular LDPC codes with low error floor and low encoding complexity," *IEEE Communications Letters*, vol. 10, no. 5, pp. 372-374, May 2006.

[2] Z. He, S. Roy, and P. Fortier, "Encoder architecture with throughput over 10 Gbit/sec for quasi-cyclic low density parity check codes," *Proc. of IEEE International Symposium on Circuits and Systems*, Kos, Greece, May 21-24, 2006.

[3] Z. He, S. Roy, and P. Fortier, "Capacity-approaching LDPC codes with low error floors for high-speed digital communications," *Proc. of the 23rd Biennial Symposium on Communications*, Kingston, Canada, pp. 10-14, May 30 - June 1, 2006.

[4] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2894- 2900, Aug. 2005.

Parallel decoders for turbo codes in both 3G mobile systems and 802.16 broadband wireless access systems

Zhiyong He, *Étudiant au doctorat.*
Paul Fortier, *Directeur de recherche.*
Sébastien Roy, *Co-directeur de recherche.*

Résumé – Cet article présente trois architectures parallèles désignées respectivement, décodage à fenêtre glissante avec réchauffement (*sliding window* ou *SW*), décodage à fenêtre glissante sans réchauffement (*warm-up free SW*) et décodage à fenêtre parallèle sans réchauffement (*parallel window* ou *PW*), pour le décodage de codes turbo courts et longs destinés tant aux systèmes mobiles de troisième génération (3G) qu'aux systèmes sans fil à large bande tombant sous l'égide de la norme IEEE 802.16. Pour supporter des capacités de 10 Mbps ou plus dans les système 3G, le décodeur 4-parallèle avec une architecture SW avec réchauffement qui peut atteindre des vitesses de décodage de 30 Mbps est recommandé. Pour décoder les codes turbo prévus par la norme 802.16, le décodeur 8-parallèle avec une architecture SW sans réchauffement est recommandé pour les blocs de longueur 512 à 4096 bits afin d'atteindre des débits de plus de 70 Mbps, alors que le décodeur 8-paralléle avec une architecture PW est suggéré pour les blocs courts de 48 à 512 bits afin de réduire au minimum les besoins en stockage tout en maximisant la vitesse de décodage.

Abstract – This paper presents three parallel architectures, the so-called warm-up sliding window (SW), warm-up-free SW, and warm-up-free parallel window (PW) architectures, for decoding short and long turbo codes specified for both third generation (3G) mobile systems and broadband wireless systems as defined by the IEEE 802.16 standard. To support an overall throughput of more than 10 Mbps in 3G systems, the 4-parallel decoder with a warm-up SW architecture which attains decoding speeds of up to 30 Mbps is recommended. For turbo codes in the 802.16 standard, the 8-parallel decoder with warm-up-free SW architecture is recommended for long blocks ranging from 512 to 4096 bits in size to attain the specified throughput of up to 70 Mbps, while the 8-parallel decoder with a warm-up-free PW architecture is suggested for the short blocks (between 48 to 512 bits) to minimize the storage requirement and to maximize the decoding speed.

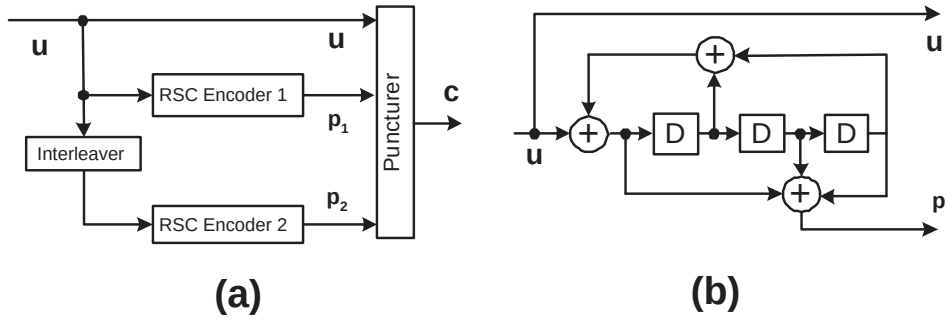


FIG. 6.1: Turbo codes in 3G systems and 802.16 broadband wireless access systems. (a) General encoder for turbo codes. (b) Recursive systematic convolutional (RSC) encoder.

6.1 Introduction

TURBO codes, first introduced by Berrou et al. [1] in 1993, have received a lot of interest, as they offer a very powerful error correction technique which allows transmission of data at rates near the channel capacity with arbitrarily low probability of error. They have been chosen for third generation (3G) mobile systems and are part of the IEEE 802.16 standard for broadband wireless access systems. For application in these wireless systems, high throughput of turbo codes is a critical issue. For example, an overall throughput of more than 10 Mbps for a wireless terminal is required in order to support high-speed data packet access in 3G systems, while the IEEE 802.16 specifications specify data rates reaching 70 Mbps. However, a turbo decoder, inherently has a low throughput and a large latency because of the iterative decoding process. A standard turbo decoder comprises two soft-input soft-output (SISO) decoders as well as a de-interleaver. Its throughput is typically up to 10-20 times lower than the throughput of its component SISO decoders, assuming that 5-10 decoding iterations are performed. A parallel decoding architecture is usually favored to increase the throughput and reduce the latency (e.g. [2]). In this paper, we provide some solutions for the high-speed hardware implementation of parallel decoders [3] [4] [5].

6.2 Turbo codes in 3G systems and 802.16 systems

Prior to discussing the decoder implementation, we introduce the turbo codes used in 3G mobile systems and 802.16 broadband wireless access systems. As shown in Fig. 6.1 (a), a typical encoder for turbo codes consists of four parts, i.e., two recursive systematic convolutional (RSC) encoders, an interleaver, and a puncturing unit. The first RSC encoder encodes the information bits in the original order, while the second RSC encoder encodes the interleaved information sequence. The two RSC encoders are most likely chosen to be the same so that VLSI implementation is easier. The RSC encoder with 3 shift registers for turbo codes used in the 3G system and 802.16 wireless network is shown in Fig. 6.1 (b).

The turbo principle in turbo codes improves dramatically the bit-error-rate (BER) performance in data transmissions by cleverly integrating bit concatenation in a random approach where the randomness is provided by an interleaver. However, the interleaver between two component encoders increases the hardware complexity of a parallel decoder. In a M-parallel decoder, an

information block is divided into M sub-blocks, these being assigned to M parallel component decoder processors. At each iteration, the M component decoders read (write) the extrinsic information from (into) M memory modules in sequential order for the decoding of the first constituent code and in an interleaved order for the decoding of the second constituent code. The M component decoders will likely collide when reading (writing) their inputs (outputs) for the second decoding, i.e. several component decoders will simultaneously attempt get access to the same memory cell.

To avoid collisions in accesses to memory modules, collision-free management can be performed for the low-degree parallel decoder, e.g., $M \leq 4$, by adding small buffers to assist memory accesses. Since the number of collisions increases with an increasing degree of parallelism, collision-free interleavers have to be used for highly parallel decoders. In [3] [5],we proposed a two-level mapping approach for designing collision-free interleavers for highly parallel decoders.

6.3 Parallel decoders for long turbo codes

The commonly-used algorithm for decoding turbo codes is the maximum *a posteriori* probability (MAP) algorithm. In order to reduce the computational complexity of the MAP algorithm, it is generally implemented in the logarithmic domain, resulting in the so called log-MAP algorithm. To implement an M-parallel decoder for long turbo codes, the sliding window (SW) approach, in which M sub-blocks are divided into many SWs and the M component decoders process these SW sequentially, has been used to reduce the memory requirements of the path metrics.

A. Warm-up SW architecture

In order to initialize the boundary distributions of the path metrics for each sub-block, these component decoders have to warm up for several clock cycles at each iteration. To perform the warm-up process, an overlapping of L information bits between adjacent sub-blocks is arranged for each sub-block (e.g. [2])). However, with an increasing number of sub-blocks, the warm-up process reduces the decoding throughput substantially. To minimize the decoding delay, we proposed a warm-up-free architecture for highly-parallel decoders.

B. Warm-up-free SW architecture

Instead of the warm-up process using two overlapped sliding windows, the warm-up-free architectures use the path metrics that were computed in the previous iteration of the adjacent sub-block to initialize the path metrics for each sub-block in the next iteration. To compare the performances between the proposed warm-up-free architecture and the warm-up architecture, we performed simulations by assuming binary phase-shift keying (BPSK) modulation and an AWGN channel. No difference between warm-up and warm-up-free architectures is observed after 5 iterations [5].

To compare decoding speed and hardware cost between warm-up and warm-up-free parallel architectures, we implemented a series of parallel decoders into a Xilinx FPGA Spartan-3 device. The decoding speeds of the parallel decoders with two architectures are compared in Fig. 6.2 as a function of the block size, where the decoding speed was calculated by using a decoding clock frequency of 100 MHz and 6 decoding iterations. Few differences between the decoding speeds of the warm-up and warm-up-free architectures are observed for the 4-parallel decoders for the

©LRTS 2005-2006

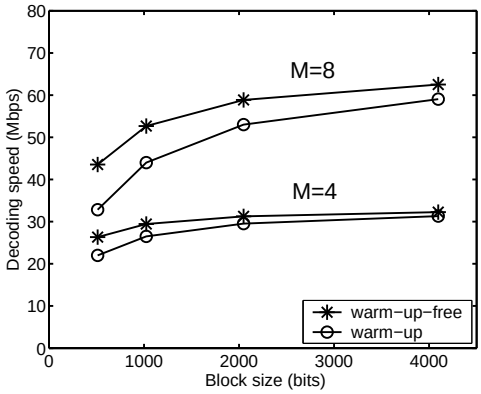


FIG. 6.2: Decoding speeds of 4-parallel and 8-parallel decoders with warm-up and warm-up-free architectures.

TAB. 6.1: Total memory costs in kbits for 8-parallel decoders with sliding window (SW) and parallel window (PW) architectures.

Block length (bits)	256	512	1024	2048	4096
Warm-up SW	27.5	33.9	46.7	72.3	123.5
Warm-up-free SW	28.1	34.5	47.3	72.9	124.1
Warm-up-free PW	16.8	33.4	66.7	133.3	266.3

long turbo codes of more than 1000 bits. However, for the highly parallel decoders with $M = 8$, the proposed warm-up-free architecture increases the speed by 6-34% compared to the warm-up architecture.

6.4 Parallel decoders for short turbo codes

It is clearly shown in Fig. 6.2 that the decoding speed of the SW architectures decreases with decreasing block size. We propose a warm-up-free parallel window (PW) architecture for decoding turbo codes with short block length. To implement an M-parallel decoder with PW architecture, an information block is divided into M windows, and M parallel component decoder processors in parallel. The detailed decoding principle of the proposed parallel decoder can be found in [4] [5]. For a short turbo code of $N \leq$1000 bits, the warm-up-free PW architecture increases the speed by 10-100% compared to the warm-up-free SW architecture.

The total memory costs for storing the input signals, the extrinsic information and the path metrics in the 8-parallel decoders with SW and PW architectures are listed in Table 6.1. The warm-up-free SW architecture increases the memory requirement by only 1% compared to the

TAB. 6.2: Application for two architectures.

Parallel architectures	sliding window	parallel window
Sub-block length (bits)	≥ 64	≤ 64

warm-up SW architecture. On the other hand, the total storage requirements in the warm-up-free PW architecture listed in Table 6.1 increase with block length. Considering the tradeoff between hardware cost and decoding speed, the warm-up-free PW architecture is a good candidate suitable for decoding short turbo codes, while the warm-up-free parallel SW architecture is better suited for long turbo codes. Table 6.2 summarizes the application of two warm-up-free architectures for various sub-block lengths.

6.5 Conclusion and discussion

This work presents three parallel architectures for decoding turbo codes, i.e. the so-called warm-up sliding window (SW), warm-up-free SW, and warm-up-free parallel window (PW) architectures. To support an overall throughput of more than 10 Mbps in 3G system, the 4-parallel decoder with a warm-up SW architecture which attains decoding speeds of up to 30 Mbps is recommended for turbo codes with specified block lengths between 40 and 5114 bits. For turbo codes with block lengths between 48 and 4096 bits, as specified for 802.16 wireless networks, the 8-parallel decoder with a warm-up-free SW architecture is recommended for long blocks (512–4096 bits) to attain the specified throughput of up to 70 Mbps, while the 8-parallel decoder with warm-up-free PW architecture is suggested for the short blocks (48–512 bits) to minimize storage requirements.

Because of high decoding complexity, it is difficult to implement a parallel decoder with decoding speeds of more than several hundreds Mbps into an FPGA device. Turbo codes are ill-suited to high-speed applications in the Gbit/s region, such as long-haul optical channels and Gigabit Ethernet. For these high-speed applications, we will discuss in a separate paper the serious competitor of turbo codes, the so-called low-density parity check (LDPC) codes, which has the same performance as turbo code and whose decoder can attain a throughput of several Gbits/s.

Bibliographie

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding : Turbo- codes," *Proc. Int. Conferences on Communications (ICC'93)*, vol. 2, pp. 1064-1070, May 1993.

[2] Z. Wang, Z. Chi, and K. K. Parhi, "Area-efficient high-speed decoding schemes for turbo decoders," *IEEE Transaction on very large scale integration (VLSI) systems*, vol. 10, no. 6, pp. 902-912, Dec. 2002.

[3] Z. He, S. Roy, and P. Fortier, "High-speed and low-power design of parallel turbo decoder," *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 6018-6021, Kobe, Japan, May 23-26, 2005.

[4] Z. He, S. Roy, and P. Fortier, "High-speed decoder for short and long turbo codes in wireless communications," *Proc. of The Ninth Canadian Workshop on Information Theory*, pp. 46-49, Montreal, Canada, June 5-8, 2005.

[5] Z. He, P. Fortier, and S. Roy, "Highly-parallel decoding architectures for convolutional turbo codes," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, submitted on June 1, 2005, accepted on May 12, 2006 for publication.

©LRTS 2005-2006

Single carrier RRC matching in frequency domain with frequency domain equalization

Rujiang Wang, *Ph.D student*
Gilles Y. Delisle, *Directeur de recherche.*

Résumé – Le travail consiste à étudier l'effet de filtrage du RRC dans le SC-FDE avec l'utilisation d'une modulation d'ordre supérieure. Une erreur de filtrage survient généralement dans le processus de suppression du préfixe cyclique et nous présentons ici une méthode qui permet de résoudre ce problème. Par la suite, les performances du filtrage dans le domaine du temps et des fréquences sont comparés. Cette comparaison révèle que le filtrage dans le domaine des fréquences n'est pas seulement efficace dans sa mise en oeuvre mais il est également plus robuste à l'erreur de filtrage. Nous mettons aussi l'emphase sur la caractéristique SC-FDE du préfixe cyclique dans l'étude.

Abstract – The effect of rooted raised cosine (RRC) matching in single carrier with frequency domain equalization (SC-FDE) with high order modulation is investigated. There is a matching error after cyclic prefix (CP) is removed and a method to solve this problem is presented. Then, the performances of time and frequency domain matching are compared. Frequency domain matching is not only more computationally efficient than time domain matching, but it is also more robust to the matching error. The cyclic characteristic of SC-FDE is emphasized in the context.

7.1 Introduction

High efficient equalization is crucial in broadband communication. Because of its simple equalization structure, orthogonal frequency division multiplexing (OFDM) is widely accepted as an effective means to combat inter-symbol interference (ISI) in time dispersive channels. In recent years, SC-FDE has attracted a lot of attention due to some of its advantages, such as low linear power amplifier, phase noise and synchronization requirement, as compared to the OFDM scheme.

For SC-FDE, just like any single carrier transmission scheme, it has to be implemented on bandlimited channel in order to comply with the spectral regulation [1]. Both pulse shaping and distorted channel response need matched filtering to improve signal to noise (S/N) ratio at the receive side. Implementing matched filtering in time domain demands a lot of computing power, which is almost proportional to the square of the channel memory length. On the other hand,

matched filtering in frequency domain is very efficient thanks to FFT. Both time and frequency domain RRC matching result in block edge symbol distortion due to the anticausal nature of RRC pulse [2]. The edge error can be eliminated by accounting for the length of the RRC pulse in the FFT block.

7.2 RRC matching error in SC-FDE

SC-FDE, just as OFDM, has a blockwise transmission structure with low complexity frequency domain equalization solution [3]. If continuous time representation of the original symbol sequence of the ith transmitted block is $s_i(t)$ for $t \in [0, T_{FFT}]$, then the cyclically extended block denoted by $\hat{s}_i(t)$ is given by

$$\hat{s}_i(t) = \begin{cases} s_i(t) & \text{if } t \in [0, T_{FFT}] \\ s_i(t + T_{FFT}) & \text{if } t \in [-T_G, 0] \\ 0 & \text{else} \end{cases} \tag{7.1}$$

The overall transmit signal can then be written as

$$s(t) = \sum_i \hat{s}_i(t - i(T_{FFT} + T_G)) \tag{7.2}$$

With the added CP, the linear convolution of the ith block with the channel impulse response becomes a circular convolution, denoted as '$\otimes$', for $s_i(t)$ when the channel impulse response length is equal or less than the CP length. The received block $\hat{r}_i(t)$ can be written as

$$\hat{r}_i(t) = \hat{s}_i(t) * h(t) = s_i(t) \otimes h(t) \tag{7.3}$$

within the interval $t \in [-T_G + T_h, T_{FFT}]$ in which T_G denotes the CP length and T_h is the channel impulse response length. The restriction of $\hat{r}_i(t)$ to the interval $[0, T_{FFT}]$ contains exactly one period of the cyclically extended signal $\hat{r}_i(t)$ and is denoted by $\widetilde{r}_i(t)$. Then, the Fourier transform of (7.3) is :

$$\widetilde{R}_i(nf_0) = S_i(nf_0)H(nf_0) \tag{7.4}$$

in which nf_0 is the FFT bins. Thus, frequency domain equalization scheme can be applied to each block $\hat{r}_i(t)$, individually.

Generally, RRC pulse shaping filter is implemented at the transmitter and receiver at the same time in order to improve SNR besides no ISI [1]. Because RRC is an anticausal pulse, its precursor transverses some previous symbols, as shown in Fig. 7.1. Thus, the pre- and post-cursor of RRC make the FFT block edges blurred. Considering RRC shaping, the FFT block content is not strictly cyclic as the previous assumption, because the RRC precursor depends on its data symbols. One solution is FFT block shifting advance to include the precursor in the FFT block. This also solves the problem with the end of FFT block contamination by next block. It should be noted that this operation can only be performed when the channel impulse response length plus the RRC precursor is less or equal to the CP guard interval.

At the receiver, RRC matched filtering is performed to improve SNR. Although RRC matching can be implemented in time or frequency domain, there are some differences in the process. First,

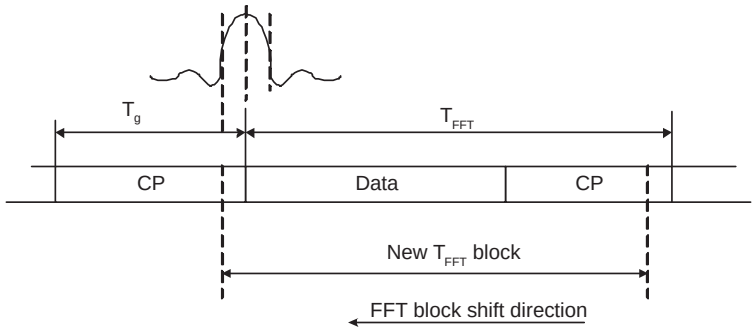


FIG. 7.1: Edge error of the first data symbol.

time domain matching is very computing demanding because it is a linear convolution process. In contrast, convolution implemented in frequency domain requires simpler multiplication. Of course, it needs CP to transform linear convolution to circular convolution. Second, the result of time domain matching is the autocorrelation of the RRC response. Suppose a RRC pulse has L (L is integer and bigger than 1) length precursor, the matched pulse has a precursor 2*L length. Time domain matching will make the precursor of matched RC pulse transverses more CP symbols. To include the entire resultant RC precursor in FFT block requires two times the length of that in frequency domain matching. Otherwise, decreasing FFT block advance shifting will cause distortion.

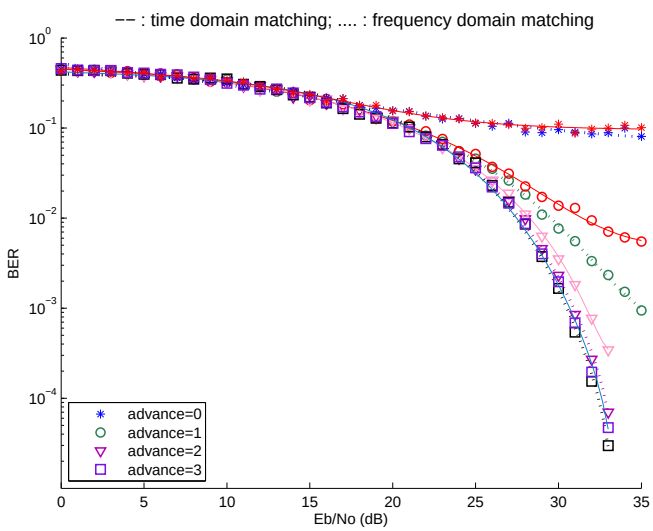


FIG. 7.2: Time and frequency domain matching comparison.

7.3 Simulation results

To compare frequency domain matching with time domain matching, the performance of a zero forcing (ZF) equalizer in a channel modeled as $1/\sqrt{2}$, 0, 0, $1/\sqrt{2}$ is evaluated. This channel has a deep null around 0.5 normalized frequency. The roll-off of RRC is 0.25 with 6 symbol delay and two times oversampling. One data block has 64 QAM64 symbols plus 12 symbol length CP. The performance, shown in Fig. 7.2, converges as FFT shifting advance increases. For frequency domain matching, advancing 2 symbols almost converges to the advancing 3 symbol case. The ideal case is that FFT shift advancing all the 6 RRC delay symbols to obtain true cyclic convolution. In reality it is not necessary advancing so much because the energy in the tails of RRC pulse is limited, and the delayed path will compensate for the distorted edge RRC symbols in the process of equalization. On this figure, the frequency domain matching converges to the ideal result more rapidly than time domain matching. The reason is that RRC basically is a kind of low pass filter, it can smooth the distorted RRC precursor of the edge symbols after CP discarding.

7.4 Conclusion

The function of equalization is to restore the multipath to the ideal impulse response. It requires the signal to be free of non-linear distortion in the matching process. Any nonlinear distortion will spread over all symbols through frequency domain equalization normally on the basis of block transmission. For SC-FDE, signal cyclic characteristic is crucial to get good result. Frequency domain matching ensures signal better cyclic fidelity than that in time domain matching when FFT shift advancing is limited. Thus, frequency domain matching is not only efficient than time domain matching, it is also elegant in signal quality.

Bibliographie

[1] J. G. Proakis. *Digital Communications*. McGraw Hill, New York, 2000.

[2] H. Witschnig, G. Obberger, A. Springer, and A. Koppler. The effect of blockwise transmission on higher-order modulation schemes for SC-FDE. In *The 5th International Symposium on Wireless Personal Multimedia Communications, Oct.*, volume 3, pages 1323–1327, Oct. 2002.

[3] H. Sari, G. Karam, and I. Jeanclaude. Frequency domain equalization of mobile radio and terrestrial broadcast channels. In *Proc. Globecom'94, San Francisco, Nov.-Dec.*, pages 1–5, 1994.

Application des réseaux de capteurs dans les milieux confinés - Partie localisation

Abdellah Chehri, *Étudiant doctorat.*
Paul Fortier, *Directeur de recherche.*
Pierre-Martin Tradif, *Co-directeur de recherche.*

Résumé – Les technologies sans fil offrent de nouvelles perspectives dans le domaine des télécommunications et des réseaux, comme par exemple, les réseaux de capteurs. Plus récemment, on assiste à l'émergence des réseaux de capteurs sans fil. En particulier, les réseaux de micro capteurs sans fil ont été identifiés comme étant parmi les technologies les plus importantes du 21e siècle. Dans ce projet, nous nous intéressons aux réseaux de capteurs pour l'application de la radiolocalisation dans l'environement minier.

Abstract – Wireless technologies offer new prospects for telecommunications and networks, such as sensor networks. More recently, we have seen the emergence of wireless sensor networks. In particular, wireless microsensor networks have been identified as one of the most important technologies for the 21st century. In this project, we are interesting in wireless sensor networks for radiolocation applications in the underground mine environment.

8.1 Introduction

Dans la première partie du projet, les capteurs étudiés sont assez simples. L'idée principale est que chaque capteur doit déterminer sa position à l'intérieur de la mine en se servant des signaux émis par les capteurs voisins. Évidemment, si un capteur est mobile, il faut mettre à jour sa position de façon continue. Pour les capteurs fixes, on envisage d'abord une position "câblée", i.e. la position est entrée dans le capteur lorsqu'il est installé. Cette approche a, en théorie, l'avantage d'une grande précision, mais elle a l'inconvénient d'exiger la position exacte lors de l'installation, ce qui peut s'avérer très fastidieux. Une seconde approche serait de fixer les capteurs sans connaître leur position, et de laisser le réseau (soit de façon centralisée ou distribuée) calculer les différentes positions.

Pour effectuer une localisation, le système doit être capable de fonctionner en point à point, de disposer d'un algorithme d'estimation de position centralisé (où toutes les opérations se font au niveau d'un noeud central), ou d'une façon décentralisée (où chaque noeud se localise de façon autonome) [1]. Pour se localiser, la majorité des approches se basent sur l'estimation de la

distance entre noeuds et *beacon* (les noeuds de référence [2]) qui se fait à l'aide des mesures de RSS (Received Signal Strength), technique dont l'avantage réside dans la simplicité du dispositif de mesure. Une autre technique se base sur des mesures de temps d'arrivée. Le TOA (Time of Arrival) peut être mesuré à l'aide de plusieurs types de signaux, soit le DSSS [3] (Direct Sequence Spread Spectrum), ou l'Ultra Wideband (UWB) [4]. Nous utilisons les deux approches. Ceci nécessite donc aussi l'analyse du canal minier pour ces types de technologies.

La technologie UWB est connue pour ses avantages uniques dans le cadre d'applications de localisation de précision [5]. Une partie de notre étude sera consacrée aux mesures expérimentales pour la caractérisation du canal en UWB (3-5 GHz) dans le milieu minier afin de pouvoir faire une analyse réelle du problème de localisation dans les réseaux de capteurs.

8.2 Localisation dans les réseaux de capteurs

Dans les réseaux de capteurs, les noeuds sont déployés dans un environnement où il n'y a aucune connaissance a priori de leur position. Le problème d'estimer les coordonnées spatiales du noeud est désigné sous le nom de localisation. La localisation est devenue une information à grande valeur ajoutée, que ce soit d'un point de vue économique ou civil. Une solution immédiate qui vient à l'esprit est le GPS [6] ou système de positionnement global. Cependant le GPS ne fonctionne que dans les milieux extérieurs. Deuxièmement, les récepteurs de GPS sont coûteux et rendent le noeud volumineux en taille et gourmand en énergie. Dans le cadre d'un environnement minier, il est donc nécessaire de chercher d'autres moyens pour estimer la position des noeuds.

Les procédés employés pour déterminer une position sont généralement basés sur des calculs géométriques comme la triangulation (en mesurant des angles par rapport à des points fixes ou des noeuds connaissant leur position) et la trilatération (en mesurant la distance entre les noeuds).

Technologies pour la localisation

Pour connaître la distance entre deux noeuds, quatre techniques sont couramment utilisées à savoir l'estimation de la distance, la reconnaissance par apprentissage, la détermination de l'angle d'arrivée et celle du temps d'arrivée.

Estimation de la distance C'est sans doute la méthode la plus intuitive et la plus directe. Il s'agit d'estimer la distance parcourue par le signal reçu en mesurant son intensité à la réception. La puissance à l'émission est connue à travers le paramètre de contrôle de puissance. En utilisant une formule simple de propagation, il est possible d'avoir une estimation de la distance. En répétant le même principe sur deux stations de base (dont la position est connue), trouver la position du noeud devient possible en calculant l'intersection des cercles.

Reconnaissance à base d'apprentissage Cette méthode ressemble au problème de la reconnaissance de caractère où, à partir de mesures diverses, on essaie de trouver la zone de localisation

la plus probable dans laquelle le noeud est susceptible de se trouver. Cette décision s'effectue moyennant une base d'apprentissage composée de mesures recueillies sur le terrain.

Angle d'arrivée C'est une technique connue qui a suscité de nombreuses publications ces dernières années. Il s'agit d'estimer l'angle d'arrivée d'un signal sur un réseau de plusieurs capteurs espacés d'une longueur d'onde [7].

Temps d'arrivée Quand des noeuds sont synchronisés, un seul paquet aller simple est nécessaire pour connaître le temps de propagation et estimer la distance entre les noeuds. Toutefois, si les noeuds ne sont pas synchronisés, deux paquets doivent être utilisés pour estimer le temps aller-retour du signal entre les noeuds. Les radars civils et militaires ou encore le GPS utilisent cette approche. Les méthodes de localisation basées sur l'UWB utilisent elles aussi le TOA.

Récemment de nombreuses approches pour le problème de localisation dans les réseaux de capteurs ont été proposées. Nous pouvons les classifier en deux catégories : approches basées sur la connectivité et approches basées sur les mesures [8].

Méthodes de localisation basées sur la connectivité

Dans cette méthode, nous employons les caractéristiques de connectivité radio pour localiser un capteur. Bien que cette méthode seule ne puisse pas fournir une localisation précise, elle fournit une bonne indication sur la proximité d'un noeud, ce qui est utile pour certaines tâches de réseau telles que le routage géographique.

Le système de localisation GPS-less [9] est un exemple d'un système de localisation basé sur la connectivité. Dans ce système, un ensemble de *beacon* ou balises transmettent des signaux de référence. D'autres noeuds (avec des positions inconnues) peuvent se localiser au centre de surface des noeuds de référence desquels ils peuvent recevoir ces signaux de références. Les meilleurs résultats sont obtenus quand les noeuds sont arrangés sous forme d'un modèle de maille (grille).

L'approche d'estimation convexe des positions [10] permet de localiser également des noeuds en utilisant la connectivité. Dans cette méthode de localisation, tous les noeuds doivent communiquer leur information de connectivité à un point central qui résout le problème d'optimisation (algorithme linéaire ou semi-défini) et estime alors la position de chaque noeud. Avec un placement judicieux des noeuds de références sur le périmètre du réseau, les auteurs ont montré que la position du noeud peut être estimée avec un ordre de 0,64 à 0,72 R (où R est le rayon de transmission radio) pour une densité de 5,6 (nombre de voisins par noeud).

Une proposition plus récente basée sur la graduation multidimensionnelle (Multidimensional scaling, MDS) peut résoudre des positions relatives entre les différents noeuds sans exiger aucun noeud de référence [11]. Pour cela, il faut employer une formulation classique de MDS qui prend l'information de connectivité des noeuds comme variable d'entrées et crée une carte relative bidimensionnelle des noeuds qui préserve les rapports de voisinage.

©LRTS 2005-2006

Les approches basées sur des mesures

Une grande source de diversité dans les algorithmes basés sur les mesures provient des différentes propositions au sujet de la distribution des erreurs de mesure. Quelques systèmes supposent que le bruit est gaussien, alors que d'autres supposent que l'erreur de mesure est proportionnelle à la distance.

Un système comportant un algorithme de localisation qui n'exige pas des noeuds de référence est basé sur des mesures de distance à l'aide du ToF (Time of Flight ou temps de vol), et l'utilisation des équations géométriques pour l'estimation des positions. En premier lieu, tous les noeuds calculent leurs positions par rapport à leurs voisins ; ces coordonnées relatives seront ensuite fusionnées pour produire des coordonnées globales à l'aide d'un ensemble d'équations géométriques. L'estimation de la position par cette méthode ne donne pas des résultas précis. Ceci est dû aux mesures de ToF et au problème de propagation d'erreur. Cependant nous pouvons utiliser cette méthode pour évaluer la position du noeud et pour d'autres applications (tel que le routage géographique).

Une autre méthode de localisation [12] concerne la position et l'orientation d'un noeud qui peuvent être estimées en utilisant des signaux acoustiques. Chaque source produit un signal acoustique connu qui est détecté par les noeuds voisins. Les noeuds à leur tour mesurent le ToA et le DoA du signal capté, et propagent cette information à un centre de traitement d'information (central information-processing center CIP). Ce dernier fusionne ces données en utilisant un critère de maximum de vraisemblance pour obtenir la position et l'orientation des noeuds.

Une autre approche de localisation dans les réseaux ad-hoc a été développée à l'Université UCLA (dans le cadre du projet GLORE [13]). Le système de localisation se compose des iPAQs standards (émetteurs/récepteurs ultrasons) et des noeuds. Le système fonctionne en deux phases : les iPAQs se localisent entre eux pour produire des cordonnées relatives en 3D (self configuration), puis on détermine la position des noeuds (simples émetteurs).

L'algorithme de positionnement est un algorithme centralisé basé sur un modèle de relaxation d'un ressort avec des constantes de raideur non linéaires : les ressorts sont modélisés de telle sorte qu'ils sont plus faciles à se comprimer qu'à s'étirer. Ceci à l'effet de favoriser les petites distances plutôt que les grandes distances, ce qui est plus conforme aux erreurs produites lors de mesures des distances avec les signaux acoustiques.

Le système de localisation Ad-hoc [14] explore trois méthodes alternatives de propagation : DV-hop, DV-distance, et Euclidienne. Dans la méthode DV-hop, les noeuds de références propagent leurs positions à l'intérieur du réseau, chaque noeud fait suivre l'information de positions des *beacon* à ses voisins et construit une table qui comporte : ID identificateur du *beacon*, position, et distance du saut (hop distance).Quand un *beacon* reçoit un des paquets propagés avec la position des différents *beacons*, il utilise cette information pour calculer la distance de saut moyenne entre deux *beacons*. La distance du saut moyenne calculée est diffusée de nouveau dans le réseau. Les noeuds qui reçoivent ce message d'information sur la distance du saut moyenne

peuvent estimer les distances par rapport aux *beacons*. Une fois ces distances calculées et en utilisant la technique de triangulation, le noeud peut alors calculer sa position. L'approche de DV-distance est similaire au DV-hop, mais en utilisant la puissance du signal reçu (RSS) pour mesurer la distance noeud-*beacon*. Bien que cette approche donne de bons résultats d'estimation, elle est également plus sensible à l'erreur de mesure, puisque la puissance du signal reçu est considérablement influencée par l'environnement de propagation (interférence, multi-trajets).

La méthode euclidienne emploie la mesure directe entre le noeud et les *beacons*. Chaque noeud pour lequel nous pouvons avoir deux mesures de distance peut calculer sa position par des lois géométriques. Une autre approche [15] emploie un algorithme appelé Hop-TERRAIN similaire au DV-hop en combinaison avec une phase de raffinement basée sur le critère des moindres carrés. Le Hop-TERRAIN cherche le nombre de saut à chaque *beacon*, ensuite il emploie les positions des *beacons* pour estimer la longueur des sauts moyens. Cette dernière sera diffusée dans le réseau. Chaque noeud qui reçoit un message avec la longueur du saut moyen estime sa distance par rapport à chaque *beacon* en multipliant la distance moyenne du saut par le nombre des sauts. En phase d'amélioration (raffinement), chaque noeud emploie une mesure plus précise de distance par rapport à ses voisins pour obtenir une estimation plus raffinée à l'aide du critère des moindres carrés. L'approche de multilatération collaborative [16] utilise un processus à trois phases pour estimer les positions des noeuds.

Pendant la première phase, les noeuds calculent un ensemble des positions initiales en formant un ensemble de boîtes autour des noeuds. Ensuite les noeuds s'organisent en groupes pour raffiner les positions estimées initiales par la méthode des moindres carrés. La phase d'amélioration est présentée dans deux modèles de calcul, centralisé ou distribué. Le modèle centralisé exige une information globale du réseau entier. Le modèle distribué est une approximation du modèle centralisé dans lequel chaque noeud est responsable pour calculer sa propre position en communiquant avec ses proches voisins (les voisins à un seul saut).

En plus des approches basées sur les distances, certains travaux s'intéressent à l'utilisation des mesures d'orientation (angulaire). Le travail décrit dans [7] est un exemple qui emploie des mesures d'angle (Angle of Arrival) pour déterminer la position d'un noeud.

8.3 Étude du canal UWB dans les environements miniers

La technologie UWB est utilisée dans les systèmes de communications sans fil pour deux types d'applications. Les communications haut débit représentent le premier type d'application, avec un débit au-dessus de 100 Mb/s (802.15.3a). La deuxième application se concentre sur des bas débits en dessous de 1 Mbit/s, habituellement dans le contexte des réseaux de capteurs et pour des systèmes de positionnement.

Plusieurs travaux se sont intéressés à l'étude du canal ultra large bande. On peut citer deux travaux notamment. Dans [17], les auteurs ont évalué les fluctuations du canal UWB avec deux scénarios, le premier consiste à placer des antennes à des endroits différents pour étudier le

©LRTS 2005-2006

comportement spatial du canal, et le deuxième scénario se base sur la présence des personnes mobiles entre les deux antennes fixe. Par conséquent, le canal varie temporellement. Le but est d'étudier ce comportement temporel. Les deux cas sont importants pour notre système, car dans une mine le placement des noeuds est primordial et souvent la présence des travailleurs engendre des variations temporelles. Un autre travail intéressant est celui de Johan Karedal et al. [18]. Son originalité réside dans l'étude du canal dans un environnement industriel. Ces environnements ont des propriétés uniques de propagation (grand nombre d'objets métalliques, dimension des halls et des objets). Il est donc essentiel de connaître le comportement des canaux UWB dans des environnements chaotique tel que peut l'être l'environnement minier.

8.4 Conclusion

Nous avons présenté les différentes méthodes d'estimation de position employées dans les réseaux de capteurs. En dépit des efforts récents de recherches, et de la diversité des solutions proposées, plusieurs défis demeurent encore à atteindre. Dans les approches les plus couramment proposées, le manque de données expérimentales a empêché jusqu'ici l'évaluation de plusieurs d'algorithmes de localisation dans des conditions réalistes. En outre, la nature multidimensionnelle du problème suggère de prendre en considération les différents techniques de mesures afin d'améliorer la robustesse et la précision des systèmes de localisation.

D'un point de vue théorique, la caractérisation fondamentale du comportement des erreurs de localisation sous différentes distributions des erreurs de mesure est toujours un axe de recherche active. Il faut noter que la localisation des noeuds est un problème spécifique d'application elle-même, puisque chaque application est susceptible d'avoir ses propres conditions en termes de précision et de puissance de consommation. La localisation de noeud doit être explorée dans le contexte de chaque application.

Pour notre application de localisation dans une mine, l'approche qui nous séduit, est l'estimation de la position en ne considérant que la connectivité des noeuds. Cette méthode nous semble être celle qui énonce le moins de suppositions quant aux caractéristiques techniques des noeuds et du réseau. Nous avons choisi d'utiliser cette approche simple pour estimer la position des noeuds dans notre étude.

Bibliographie

[1] A. Savvides, "Dynamic fine-grained localization in ad hoc networks of sensors", ACM/IEEE MOBICOM, pp. 166-179, Rome, 2001.

[2] N. Patwari, A. O Hero, M. Perkins et N. S. Correal, "Relative location estimation in wireless sensor networks", Signal Processing, IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 51, pp. 2137 - 2148, août 2003.

[3] B. B. Peterson, C. Miecik, R. Hartnett, P. M. Thompson, J. Mendoza et H. Nguyen, "Spread spectrum indoor geolocation", Journal of the Institute of Navigation, vol. 45, no. 2, pp. 97 - 102, 1998.

[4] N. S. Correal, S. Kyperountas, Q. Shi et M. Welborn, "An ultra wideband relative location system", IEEE Conf. on Ultra Wideband Systems and Technologies, nov. 2000.

[5] R. J. Fontana, E. Richley et J. Barney, "Commercialization of an ultra wideband precision asset location system", IEEE Conference on Ultra Wideband Systems and Technologies, pp. 369 - 373, 16-19 nov. 2003.

[6] F. van Diggelen, "Indoor GPS theory and implementation", IEEE Position Location and Navigation Symposium, pp. 240 - 247, 15-18 avr. 2002.

[7] D. Nicolescu et B. Nath, "Ad-hoc Positioning System using AoA", Proceedings of the IEEE/INFOCOM 2003, San Francisco, C.A, avr. 2003.

[8] A. Savvides, M. Srivastava, L. Girod et D. Estrin, "Localization in sensor networks", Ch. 15, *Wireless Sensor Networks*, Kluwer Academic Publishers, mai 2004.

[9] N. Bulusu, J. Heidemann et D. Estrin, "GPS-less low-cost outdoor localization for very small devices", IEEE Personal Communications, vol. 7, pp. 28-34, oct. 2000.

[10] L. Doherty, L. El Ghaoui et K. S. J. Pister, "Convex position estimation in wireless sensor networks", Proceeding of Infocom 2001, avr. 2001.

[11] Y. Shang, W. Rumel, Y. Zhang et M. F Romhez , "Localization from mere connectivity", Proceedings of the 4 ACM of mobile ad-Hoc networking, Annapolis, MD, juin 2003.

[12] R. L. Moses et R. M. Peterson, "Self-calibration of sensor networks in unattended ground sensors technologies and applications", Proc. SPIE, vol. 4743, pp. 108-119, avr. 2002.

[13] L. Girod, V. Bychkovsky, J. Elson et D.Estrin. "Locating tiny sensors in time and space : a case study", Proceedings of the International Conference on Computer Design (ICCD 2002), Freiburg, Allemagne, sept. 2002.

[14] D. Nicolescu et B. Nath, "Ad-Hoc positioning system", Proceeding of IEEE Globecom, nov. 2001.

[15] C. Savarese, J. Rabay et K. Langendoen, "Robust positioning algorithms for distributed Ad-Hoc Wireless sensor networks", USENIX Technical annual conference, juin 2002.

[16] A. Savvides, H. Park et M. B. Srivastava, "The n-hop multilateration primitive for node localization problems", Proceeding of Mobile Ad-Hoc Networking and Applications, pp. 443 - 451, 2003.

[17] P. Pagani et P. Pajusco, "Experimental assessment of the UWB channel variability in a dynamic indoor environment", 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 4, pp. 2973 - 2977, 5-8 sept. 2004.

[18] J. Karedal, S. Wyne, P. Almers, F. Tufvesson et A. F. Molisch, "UWB channel measurements in an industrial environment", IEEE Global Telecommunications Conference, vol. 6, pp. 3511 - 3516, 9 nov. - 3 déc. 2004.

©LRTS 2005-2006

Egalisation aveugle et turbo égalisation dans les canaux sélectifs en fréquence stationnaires et non stationnaires.

Abdellah Berdai, *Étudiant à la maîtrise.*
Huu Tuê Huynh, *Directeur de recherche.*
Jean-Yves Chouinard, *Codirecteur de Recherche.*

Résumé – Nous étudions à travers ce travail de recherche les méthodes d'égalisation entraînée et aveugle dans les canaux de communications sélectifs en fréquence stationnaires et non stationnaires. Ces méthodes d'égalisation trouvent leur place dans un grand nombre d'applications telles que les télécommunications sans fil, le traitement de la parole, etc.
L'objectif de l'égalisation entraînée est d'identifier les données émises à partir des observations issues de l'antenne et des séquences d'apprentissage préalablement connues par le récepteur. Alors que l'égalisation aveugle consiste à identifier les données émises uniquement à partir des observations issues de l'antenne. Les méthodes aveugles n'ont donc connaissance a priori ni des signaux émis ni de canal.
Dans le cadre de notre recherche, nous proposons trois modèles d'égalisation : deux modèles autodidactes (sans séquence d'apprentissage) pour l'égalisation dans les canaux sélectifs en fréquence et stationnaires, et un modèle entraîné (avec séquence d'apprentissage) pour l'égalisation dans les canaux sélectifs en fréquence et non stationnaires.

Abstract – In this research work, we study the blind and trained equalization methods over stationary and non stationary frequency selective channels. These equalization methods find their place in a large number of applications such as wireless systems, speech processing, ...
The objective of trained equalization is to identify the transmitted data from the received signals and from training sequences known beforehand by the receiver. Whereas blind equalization identify the transmitted data only from the received signals. Blind methods do not have a prior information about transmitted signals, nor the channel.
Within the framework of our research, we propose three equalization models : two blind models (without training sequence) for the equalization over the stationary frequency selective channels, and a trained model (with a training sequence) for the equalization over non stationary frequency selective channels.

9.1 Egalisation aveugle dans les canaux stationnaires et sélectifs en fréquence

En nous appuyant sur les architectures des égaliseurs aveugles proposés dans [1, 2, 3] et l'architecture proposée dans [4], nous proposons un égaliseur bidirectionnel aveugle constitué de deux égaliseurs à retour de décision montés en parallèle. Le premier égaliseur égalise d'une manière habituelle : on commence l'égalisation à partir du premier symbole reçu. Le deuxième égaliseur traite la version contradictoire de la séquence reçue. Nous signalons ici que notre égaliseur n'utilise aucune séquence d'apprentissage et aucun algorithme d'arbitrage. L'égaliseur que nous proposons conduit à des performances similaires à celles de l'égaliseur à retour de décision (DFE.LMS) piloté par séquences d'apprentissage et des performances largement supérieurs à celles des égaliseurs aveugles conventionnel dans les canaux A et B de Proakis [3]. Le schéma de principe de l'égaliseur que nous proposons est donné à la figure 9.1. Il consiste en : deux égaliseurs aveugles montés en parallèle, un bloc de permutation et un bloc de sélection et arrangement des symboles.

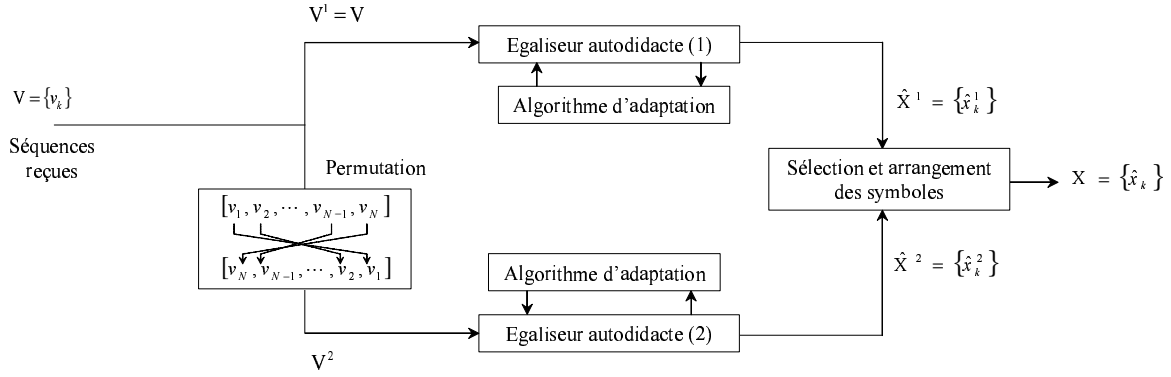


FIG. 9.1: Architecture de l'égaliseur bidirectionnel autodidacte proposé.

Pour former notre égaliseur bidirectionnel autodidacte, nous utilisons l'architecture proposée dans [5]. Dans cet article, Kim propose l'utilisation d'un filtre transverse pour adapter les erreurs issues du circuit de décision dans un but de les utiliser pour alléger la corrélation du bruit en sortie de l'égaliseur à retour de décision. Il démontre analytiquement que l'erreur quadratique moyenne minimale (EQMM) de l'égaliseur à retour de décision (DFE) classique est supérieure à l'EQMM du DFE utilisant les erreurs de décision. Il démontre également, à partir des simulations, que les performances de l'égaliseur DFE.LMS utilisant le retour d'erreur sont largement supérieures à celles de l'égaliseur DFE.LMS classique pour une modulation par déplacement de phase linéaire (BPSK) et pour une égalisation entraînée dans le contexte du canal stationnaire.
Dans notre cas, nous utilisons la même architecture proposé dans [5], mais pour un égaliseur à retour de décision en mode de décision directe DD.DFE.LMS et une modulation 4QAM.
Afin de situer les performances de l'égaliseur bidirectionnel DD.DFE.LMS - DD.DFE.LMS, nous comparons ses courbes de taux d'erreur symbole (TES) à celles de l'égaliseur DFE.LMS entraîné et à celles de l'égaliseur DD.DFE.LMS pour les deux canaux A et B de Proakis.

Les courbes de taux d'erreur symbole données aux figures 9.2 et 9.3, montrent que les performances de l'égaliseur bidirectionnel DD.DFE.LMS - DD.DFE.LMS autodidacte sont similaires à celles de l'égaliseur DFE.LMS entraîné et largement supérieures à celles de l'égaliseur DD.DFE.LMS sur toute la plage du rapport signal à bruit pour les deux canaux A et B de Proakis. Ces résultats, démontrent que l'utilisation des égaliseurs D.DFE.LMS dans l'architecture bidirectionnel permet de réduire considérablement les interférences entre symboles.

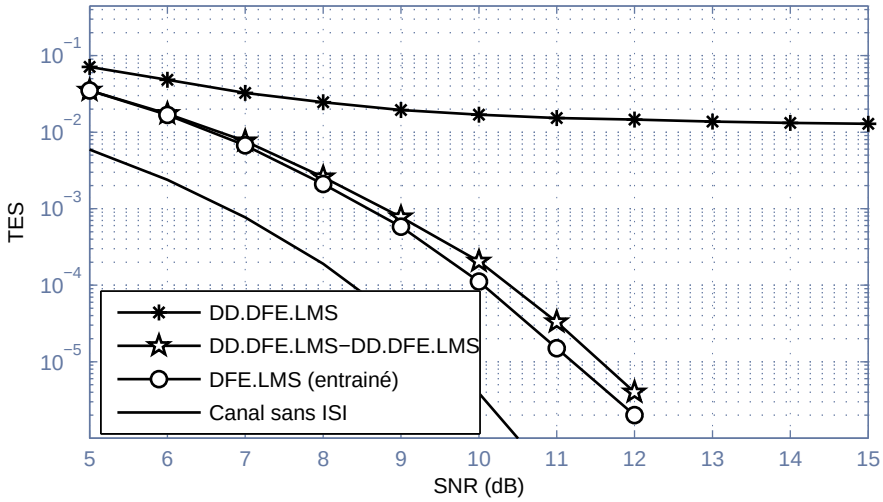


Fig. 9.2: TES de l'égaliseur bidirectionnel DD.DFE.LMS - DD.DFE.LMS (Canal A de Proakis).

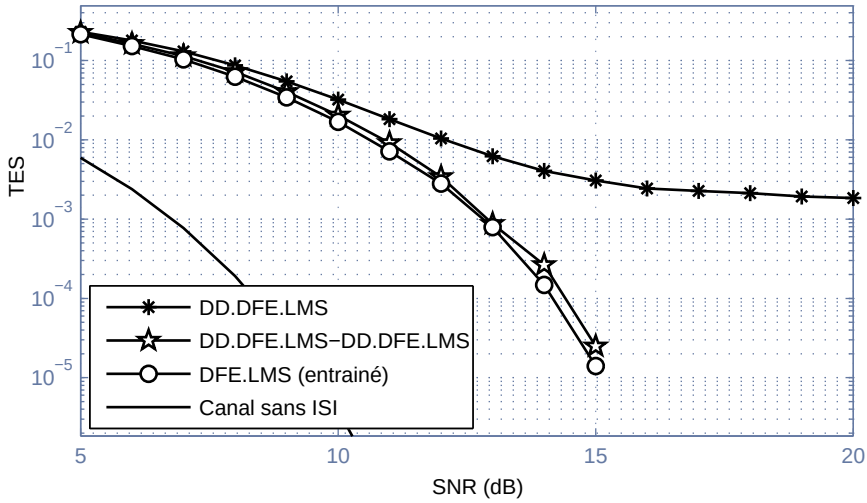


Fig. 9.3: TES de l'égaliseur bidirectionnel DD.DFE.LMS - DD.DFE.LMS (Canal B de Proakis).

9.2 Turbo égalisation aveugle dans les canaux sélectifs en fréquence et stationnaires

Notre approche d'égalisation des canaux stationnaires et sélectifs en fréquence est similaire à celle proposée par Laot [6] et par Ammari [7] : la différence réside dans le fait que notre égaliseur annuleur d'interférences exploite les erreurs de décision pour alléger la corrélation du bruit en sortie de l'annuleur d'interférences. Ceci permet d'obtenir de meilleures performances en terme d'erreur quadratique moyenne. Cette approche est inspirée de celle préconisée par Kim [5].
L'architecture globale du turbo égaliseur proposé est donnée à la figure 9.4. Le principe consiste en un traitement itératif où, à chaque itération i, le turbo égaliseur utilise les données issues du canal et l'information qu'il a produit pour procéder à l'itération $i+1$.
Pour chaque itération $i > 1$, le turbo égaliseur commence par égaliser les données issues du canal en utilisant les données estimées par le décodeur de canal à l'itération $i-1$. Ces décisions souples sont données par :

$$\bar{x}_k^{i-1} = \tanh\left(\frac{\Pi\left(\Lambda\left(\hat{c}_k\right)\right)}{2}\right) \tag{9.1}$$

où $\Lambda\left(\hat{c}_k\right)$ est l'estimation du bit $\hat{c}_k$ fournie par le décodeur.
Une fois, la séquence reçue égalisée par l'annuleur d'interférence, le décodeur de canal passe à l'estimation de la séquence égalisée $\{\hat{x}_k\}$,après déscentrelacement. Pour ce faire, il utilise ses informations extrinsèques calculées à l'itération $i-1$.
Ce traitement itératif se poursuit de la même manière et, après certain nombre d'itérations, le décodeur prend une décision sur les symboles émis.

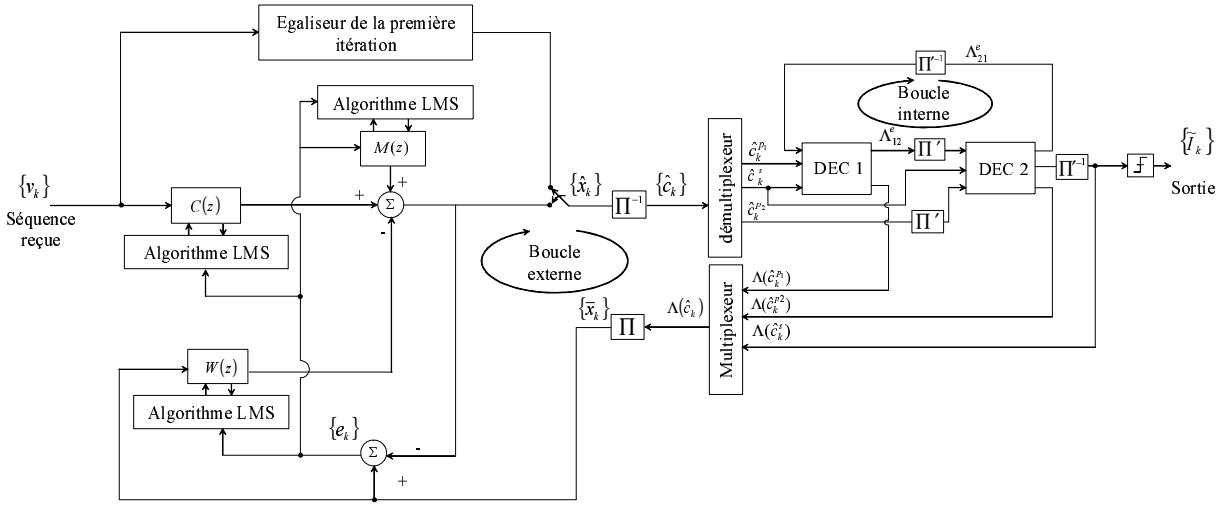


FIG. 9.4: Schéma du turbo égaliseur aveugle proposé.

Afin de situer les performances de notre turbo égaliseur, nous comparons ses courbes de TEB pour un canal stationnaire et sélectif en fréquence à celles d'un canal AWGN sans interférence entre symboles (ISI) et aussi à celles d'un égaliseur à retour de décision piloté par les vraies données transmises. Le codeur turbo simulé est constitué de deux codeurs convolutifs récursifs et systématiques (RSC) de longueur de contrainte $K = 5$ et de polynôme générateur $(1, 21/37)_o$.

Sur les figures 9.6 et 9.5 nous avons tracé le TEB en fonction du rapport E_b/N_0 à la sortie du décodeur de canal pour les canaux A et B de Proakis. Deux itérations du turbo égaliseur sont suffisantes pour déclancher le phénomène turbo à un rapport $E_b/N_0 = 3$ dB pour le canal A de Proakis et $E_b/N_0 = 4.5$ dB pour la canal B de Proakis. Dès lors, le rapport Eb/N_0 est supérieur à 2.2 (canal A) et 3.5 dB (canal B), le turbo égaliseur conduit à de meilleures performances que l'égaliseur à retour de décision piloté par les vraies données.
Nous signalons ici, que l'utilisation de la boucle interne du turbo égaliseur permet d'améliorer les performances globales du turbo égaliseur en terme d'itérations. Le TEB est amélioré à partir de la deuxième itération du turbo égaliseur. Contrairement aux turbo égaliseurs utilisant les codeurs convolutifs [8, 6]. Ces derniers, nécessitent au moins quatre itérations pour améliorer les performances en termes de taux d'erreur binaire.

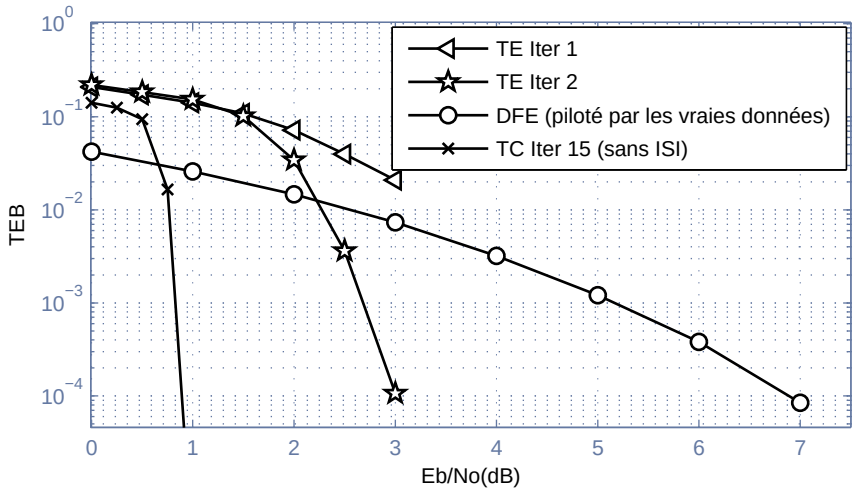


Fig. 9.5: TEB en sortie du décodeur LOG-MAP (canal A de Proakis).

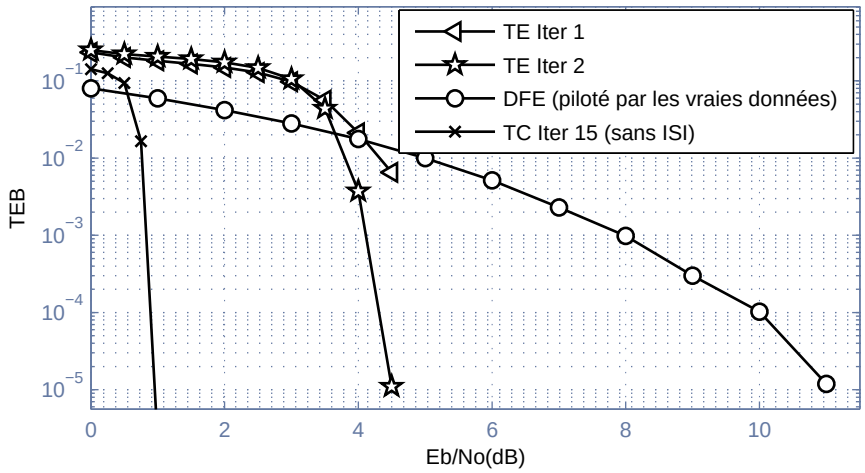


Fig. 9.6: TEB en sortie du décodeur LOG-MAP (canal B de Proakis).

9.3 Turbo égalisation dans les canaux sélectifs en fréquence et non stationnaires

L'architecture du turbo égaliseur que nous proposons pour les canaux de Rayleigh corrélés non stationnaires et sélectifs en fréquence, est presque similaire à l'architecture que nous avons proposé pour les canaux stationnaires et sélectifs en fréquence. La différence réside dans le choix de la structure et l'algorithme de l'égaliseur de la première itération et de l'égaliseur AI. Il y a aussi le facteur de fiabilité du canal de transmission qui nécessite une redéfinition en raison des variations du canal de transmission multi trajets. L'architecture globale du turbo égaliseur est donnée par la figure 9.7. Il consiste en un annuleur d'interférence modifié en mode d'adaptation directe, un estimateur de canal, un turbo décodeur, et un égaliseur de la première itération.

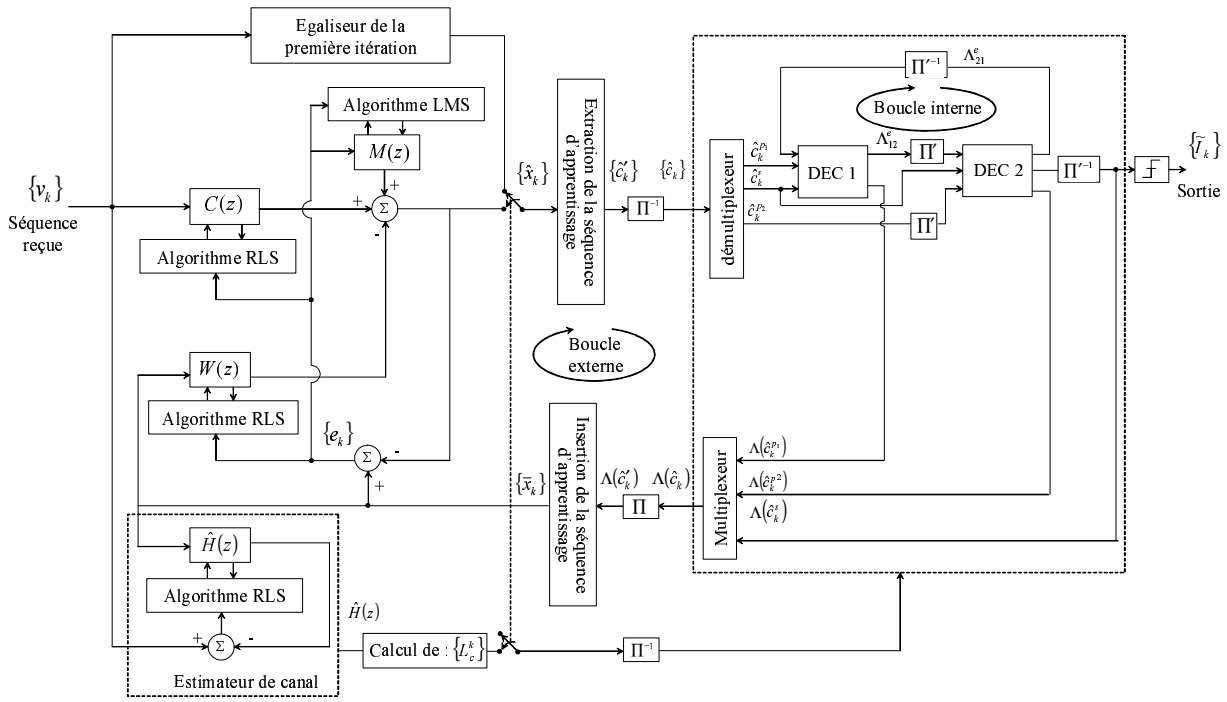


FIG. 9.7: structure du turbo égaliseur pour les canaux non stationnaires, sélectifs en fréquence.

Afin d'analyser les performances du turbo égaliseur dans le canal de Rayleigh corrélé et sélectif en fréquence, nous fixons la vitesse de transmission à 148 Kbits/s et la fréquence porteuse est 2 Ghz. La vitesse du mobile est fixée à 80 Km/s. Le canal de Rayleigh corrélé et sélectif en fréquence que nous utilisons est un canal à trois trajets et est généré selon la modèle de Beaulieu [9]. Le codeur turbo simulé est constitué de deux codeurs convolutifs de longueur de contrainte $K = 5$ et de polynôme générateur $(1, 21/37)_o$ (i.e en octal). Pour favoriser la convergence de l'égaliseurs de la première itération DFE.RLS appartenant au turbo égaliseur, on utilise une séquence d'apprentissage périodique qui représente 20% du flux de données : soit 25 symboles d'apprentissage pour 125 symboles émis. Les symboles d'apprentissage émis sont supposés connus du turbo égaliseur à la réception.

La figure 9.8, représente le taux d'erreur binaire (TEB) en sortie de l'égaliseur de la première itération DFE.RLS et en sortie de l'égaliseur annuleur d'interférences au deuxième et troisième itération. La courbe en trait hachuré correspond au TEB d'une modulation BPSK sans interférences entre symboles. On voit (figure 9.8) que le principe de la turbo égalisation fonctionne bien pour cette fréquence Doppler normalisées ($f_m = 0.001$), le TEB en sortie de l'égaliseur annuleur d'interférences est inférieur à celui d'un canal sans interférences entre symbole (ISI). Ceci démontre que l'annuleur de l'interférences supprime les ISI est fournit des données blanches au décodeur de canal.

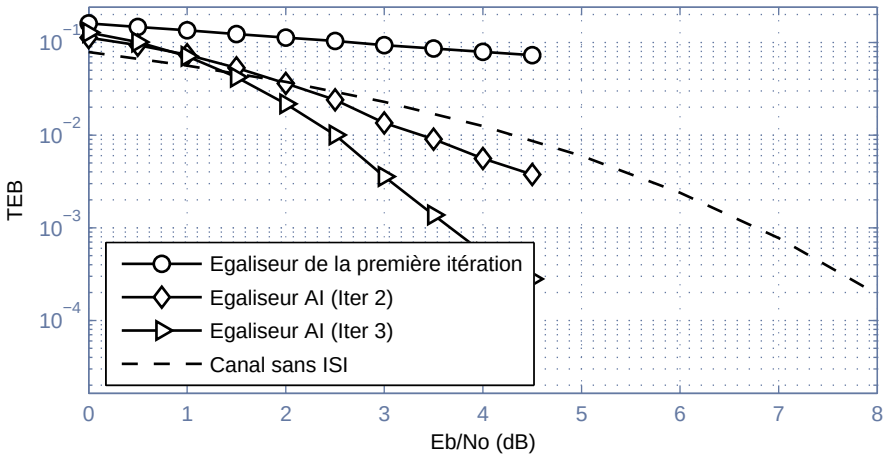


Fig. 9.8: TEB en sortie de l'égaliseur à la première itération et en sortie de l'AI, $f_m = 0.001$, trois trajets.

La figure 9.9, représente le TEB en fonction du rapport $Eb/N0$ en sortie du décodeur de canal de l'itération 1 à l'itération 3 pour la fréquence Doppler normalisée $f_m = 0.001$. Nous constatons que les performances en terme de taux d'erreur binaire sont relativement proches à celles d'un canal sans interférences entre symbole et avec codage. La différence en terme du rapport $Eb/N0$ à un TEB égale à 10^{-3} est de l'ordre de 2.5 dB.

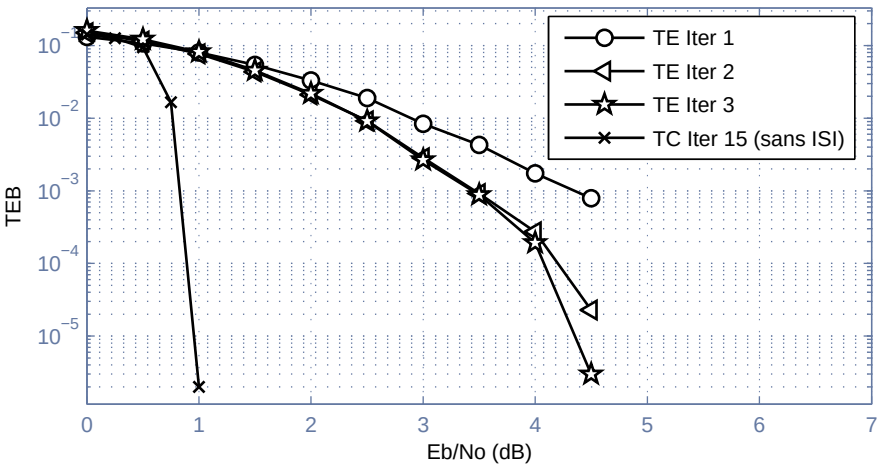


Fig. 9.9: TEB en sortie du décodeur de canal, $f_m = 0.001$, trois trajets.

Bibliographie

[1] Y. Sato. A method of self-recovering equalization for multilevel amplitude-modulation systems. *IEEE Trans on Commun*, pages 679–682, 1975.

[2] D. N. Godard. Self-recovering equalization and carrier tracking in two-dimensional data communication systems. *IEEE Trans on Commun*, pages 1867–1875, 1980.

[3] J. G. Proakis. *Digital Communications*. Thomas Gasson, New York, 4th edition, 2001.

[4] Xiang-guo and Tang Zhi Ding. Contradictory block arbitration for bi-directional decision feedback equalizers. *IEEE*, pages 283–286, 2002.

[5] M.S. Eun J. S. Choi D. W. Kim, S. H. Han and Y. S. Cho. An adaptive decision feedback equalizer using error feedback. *IEEE Trans on Consumer Elec*, pages 468–477, 1996.

[6] C. Laot A. Glavieux and J. Labat. Turbo équalization over fréquency selective channel. *International Symposiun on Turbo Codes*, pages 96–102, 1997.

[7] H. T. Huynh M. L. Ammari and P. Fortier. Turbo detection of turbo coded symbols over time varying frequency selective rayleight fading channel. *IEEE Canadian Workshop on Information Theory*, pages 12–15, 2001.

[8] I. Fijalkow A. Roumy and D. Pirez. Joint equalization and decoding : why choose the iterative solution ? *IEEE VTC 1999*, pages 2989–2993, 1999.

[9] D. J. Young and N. C. Beaulieu. The generation of correlated rayleigh random variates by inverse discrete fourier transform. *IEEE Trans on Commun*, pages 1114–1127, 2000.

Cadre généralisé pour l'échantillonnage non-uniforme : étude de performance et traitement numérique

Simon Mathieu, *Étudiant au 3e cycle.*
Sébastien Roy, *Directeur de recherche.*
Jean-Yves Chouinard, *Co-directer de Recherche.*

Résumé – En exploitant la théorie de l'échantillonnage parallèle, on propose une nouvelle architecture de récepteur qui s'appuie sur les récentes avancées du traitement spatio-temporel. On s'appuie sur une étude de capacité qui nous indique qu'il est possible, en augmentant le nombre de récepteurs, de compenser la diminution de la cadence d'échantillonnage.

Abstract – By using the parallel sampling theory, we propose a new receiver structure, which relies on recent outcomes of spatio-temporal processing techniques. We use a capacity study that indicates that it is possible to compensate for the reduction of sampling rate by increasing the number of receptors.

10.1 Introduction

La récupération d'un signal analogique est une étape essentielle et délicate qui influence directement la performance de tout système numérique. Afin de simplifier la conception, cette étape est souvent idéalisée à un échantillonneur parfait, sans égard au nombre limite de bits possible pour représenter un échantillon. Cette idéalisation est autrement plus critique lorsque la cadence d'échantillonnage requise par le système est élevée. En effet, plus la cadence est grande, plus l'échantillonneur est sensible aux erreurs de synchronisation, *i.e.* des déviations par rapport à l'instant idéal d'échantillonnage. À titre d'exemple, la plage dynamique requise et la vitesse pour une radio reconfigurable est très grande (dans certains cas, elle peut atteindre plus d'un gigahertz). Ces conditions d'opération sont motivées par la versatilité exigée d'un radio–récepteur que l'on souhaite à la fois multibandes et multistandards.

Nous présenterons brièvement quelques préceptes de base de la théorie de l'échantillonnage. Avant de faire le lien vers le récepteur, nous détaillerons l'impact que le sous-échantillonnage induit sur la capacité d'un système.

10.2 Théorie de l'échantillonnage

Considérons un signal quelconque d'énergie finie $x(t)$ défini pour un domaine D ($\forall t \in D$). L'opération d'échantillonnage est une représentation différente de $x(t)$ avec un nombre dénombra-

ble de valeurs de $x(t)$. Ainsi, on obtient l'expression suivante

$$x(t) = \sum_n x(\lambda_n) S_n(t), \tag{10.1}$$

où les paramètres temporels λ_n forment une collection de points du domaine D et l'ensemble $\{S_n(t)\}$ est un ensemble de fonctions dépendant des points λ_n.

Une des contraintes qui va guider le choix des instants λ_n est la nécessité d'avoir une représentation (10.1) unique de $x(t)$. Nous voulons ainsi nous assurer que deux signaux $x_1(t)$ et $x_2(t)$ ne puissent pas avoir la même suite de valeurs $x_1(\lambda_n)$ et $x_2(\lambda_n)$. D'un point de vue mathématique, cette unicité est certifiée, dans l'espace des fonctions à largeur de bande limitée, [1] $PW^2_{\pi w}$ lorsque les fonctions $e^{j\lambda_n x}$ forment une base complète pour l'espace $L^2(-\pi w, \pi w)$.

Intrinsèquement, le fonctionnement de tous les échantillonneurs disponibles n'est jamais parfait. Qu'ils soient composé d'une série de comparateurs ou d'une mémoire flash, la cadence d'échantillonnage ne sera jamais constante, impliquant du coup une irrégularité entre les instantes d'échantillonnage. Dans sa version idéale, un échantillonneur récupère des échantillons à tous les $\frac{n}{w}$, $n \in \mathcal{Z}$, avec w en radians/sec. Sans perte de généralité, considérons l'espace normalisé $L^2(-\pi, \pi)$ de telle sorte que les échantillons sont récupérés à tous les n. Considérons les $\lambda_n \in \mathcal{R}$, $n \in \mathcal{Z}$, alors l'espacement maximal entre l'échantillonnage idéal et la valeur réelle est :

$$|n - \lambda_n| \leq \frac{1}{4}$$

Ce critère, du mathématicien russe Kadec [1], assure que la base formée des $e^{j\lambda_n x}$ formera une base de Riesz pour l'espace $L^2(-\pi, \pi)$. En terme de conception (et d'ingénierie), cela signifie que l'on peut tolérer une déviation par rapport à l'instant optimal d'échantillonnage sans compromettre la représentation d'un signal analogique avec une série de valeurs numériques (*cf. équation 2.1*).

10.3 Récepteur

L'architecture du récepteur que l'on propose est un récepteur qui exploite le paradigme MIMO afin de tirer profit des degrés de liberté qu'offre le domaine spatial. Ainsi, un processeur spatio-temporel est formé d'une banque d'égaliseurs adaptatifs qui combattent conjointement l'interférence entre les symboles et l'interférence entres les canaux. Ce processeur spatio-temporel suit une banque de filtres adaptatifs qui pallient un échantillonnage imparfait. Pour y parvenir :

- On éclate l'échantillonnage en plusieurs petits échantillonneurs cadencés moins vite. La théorie de l'échantillonnage parallèle nous permet de faire le lien entre un seul échantillonneur rapide et plusieurs échantillonneurs fonctionnant parallèlement à une cadence inférieure.

[1] Formellement, ce type d'espace se dénomme Paley-Wiener. Pour $\sigma > 0$ et $1 \leq p \leq \infty$, on dénote par PW^p_σ, la classe de fonctions pour laquelle la représentation suivante tient :

$$f(z) = \int_{-\sigma}^{\sigma} g(u) e^{jzu} du, \quad z \in C,$$

pour une fonction g quelconque appartenant à $L^p(-\sigma, \sigma)$.

– On traite chaque processus d'échantillonnage comme un problème de filtrage adaptatif. Ainsi, les degrés de liberté que nous offrent l'adaptivité permettent de relâcher les contraintes sur l'acuité de l'horloge, sur la nature et sur la qualité des différents canaux.
– On effectue un suivi rapide des variations dans l'échantillonnage de telle sorte que des phénomènes rapides telle que la gigue de phase puisse être pistés et compensés.

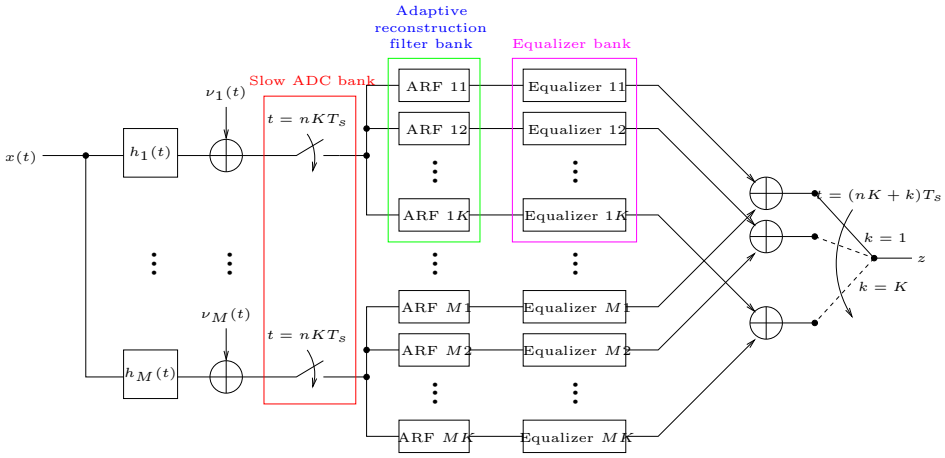


Fig. 10.1: L'architecture du récepteur.

10.4 Gigue de phase

Sans entrer dans les détails des fonctions de reconstruction, qui, au cas idéal, sont des sinus-cardinal $\mathrm{sinc}(t)$, l'opération d'échantillonnage reviens à discétiser un processus continu, $x(t)$, en construisant la séquence x_n :

$$x_n = x(nT),$$

où T est la période entre deux échantillons successif. Lorsque l'instant d'échantillonnage dévie de l'instant optimal, on récupère les échantillons à tous les

$$\lambda_n = nT + \delta_n,$$

où δ_n modélise la déviation temporelle. On appelle gigue de phase, le décalage temporel qu'induit le fonctionnement et la circuiterie de l'échantillonneur. La déviation δ_n est bornée de telle sorte que l'erreur entre le signal original et sa reconstruction à l'aide des échantillons décalés sera bornée. La borne usuelle généralement admise est

$$|\delta_n| \leq \delta \leq \min(w^{-1}, e^{-1/2}), \qquad n \in \mathcal{Z}$$

pour w la largeur de bande maximale du signal.

Par un développement en série de Taylor, il est possible d'obtenir une forme plus commode pour l'analyse mathématique. Le signal échantillonné

$$y_n = x(\lambda_n) = x(nT + \delta_n),$$

se réécrit avec le premier terme du développement en série comme

$$y_n \approx x(nT) + x'(nT) \cdot \delta_n. \tag{10.2}$$

Cette expression est valide sous des conditions très larges mais essentiellement on suppose l'approximation valide lorsque toutes les dérivées de x existent. On admet en général que cette approximation est valide si la déviation δ_n est beaucoup plus petite que l'inverse de la fréquence maximale du signal.

Le modélisation de la déviation δ_n n'est pas un sujet très étoffé dans la littérature scientifique. Peu de modèles existent. Cela s'explique partiellement par la grande diversité de circuits d'échantillonnage, chacun ayant leur architecture de synchronisation des horloges, leur interférences internes, etc. Le modèle retenu par Da Dalt, Hartenec et Wiesbauer [4] est un modèle à deux composantes. La première composante est une source de bruit gaussien filtré par un filtre passe bas (du type Butterworth). Cette source essaie de transposer le comportement de la boucle à verrouillage de phase de l'horloge d'échantillonnage. La seconde composante est une composante périodique (on somme 3 harmoniques) qui provient du couplage et des interférences entre les traces des circuits. La figure 2 présente un diagramme en bloc du modèle.

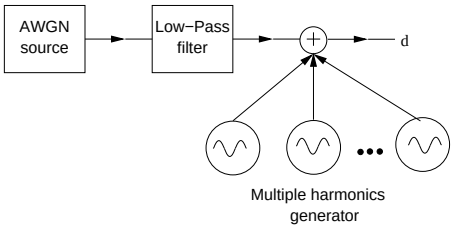


FIG. 10.2: Modèle du bruit de phase proposé à deux composantes : une déviation lente modélisé par un générateur d'harmoniques auquel se superpose une déviation rapide obtenu à l'aide d'un générateur de bruit blanc filtré.

10.5 Capacité

On suppose que le canal ne possède pas de directions d'arrivée privilégiées et qu'il est inconnu au transmetteur. Une telle situation nous conduit à modéliser, pour le cas MIMO, des signaux transmis statistiquement indépendants et équipuissants. On posera donc comme matrice de corrélation des signaux transmis $\mathbf{R_{xx}} = E(\mathbf{x}\mathbf{x}^H) = \mathbf{I}_{M_T}$. Cette expression se réduit à un scalaire pour le cas SIMO.

La capacité théorique d'un lien SIMO avec la contrainte de puissance transmise énoncée précédemment et une largeur de bande limitée s'exprime dans le domaine des fréquences par [2], [3] :

$$\mathcal{C} = W \int_{-\frac{W}{2}}^{\frac{W}{2}} \log_2 \left(1 + \frac{E_x}{\sigma_n^2} \mathbf{h}(f)^H \mathbf{h}(f)\right) df, \quad \text{[bps]}, \tag{10.3}$$

où $(\cdot)^H$ dénote la transposition et la conjugaison, $\mathbf{h}(f) = \mathcal{F}[\mathbf{h}(t)]$ est le spectre du canal vectoriel, E_x est la puissance moyenne du signal x, et σ_n^2 est la puissance du bruit.

S'il y a sous-échantillonnage d'un facteur entier K quelconque, il faut tenir compte du repliement spectral dans la mesure de la capacité. Si le spectre d'un signal échantillonné au taux de Nyquist est périodique de fréquence W, on peut aisément montrer que le spectre d'un signal sous-échantillonné est périodique avec une fréquence de $\frac{W}{K}$. La bande utile du point de vue de la capacité est donc réduite d'un facteur K. De plus, elle contient K composantes spectrales superposées dues au repliement spectral. On peut assimiler chacune de ces composantes spectrales à des sources d'information distinctes transmettant à un taux de $\frac{W}{K}$. Cette hypothèse s'effectue sans perte de généralité, bien qu'elle semblera plus naturelle avec un signal multiporteuses de type OFDM, où les diverses sous-bandes se superposant transmettent véritablement des symboles différents.

Afin de prendre en compte le repliement spectral induit par le sous-échantillonnage, on pose

$$h_{n,k}(f) = \begin{cases} h_n(f + k\frac{W}{K}), & \text{si } f \in I_W \\ 0, & \text{ailleurs.} \end{cases}, \tag{10.4}$$

où $h_n(f)$ est le spectre du $n$ième canal non-replié et

$$I_W = \left[f + k\frac{W}{K}, f + (k+1)\frac{W}{K} \right].$$

Afin de représenter adéquatement le canal, on construit une nouvelle matrice canal $\mathbf{H}_s(f)$ ayant la forme suivante :

$$\begin{bmatrix} h_{0,0}(f) & h_{0,1}(f) & \cdots & h_{0,K-1}(f) \\ h_{1,0}(f) & h_{1,1}(f) & \cdots & h_{1,K-1}(f) \\ \vdots & \vdots & \ddots & \vdots \\ h_{N-1,0}(f) & h_{N-1,1}(f) & \cdots & h_{N-1,K-1}(f) \end{bmatrix}. \tag{10.5}$$

On transforme donc un canal vectoriel SIMO en un canal matriciel. Cette transformation permet de tenir compte dans le calcul de la capacité de l'effet du repliement spectral.

La capacité d'un système sous-échantillonné est alors définie par

$$\mathcal{C}_s = \frac{W}{K} \int_{-\frac{W}{2K}}^{\frac{W}{2K}} \log_2 \det \left[\mathbf{I} + \frac{\sigma_x^2}{\sigma_n^2} \mathbf{H}_s(f)^H \mathbf{H}_s(f) \right] df. \tag{10.6}$$

Le comportement de la capacité $\mathcal{C}_s$ dépend directement du comportement des valeurs propres λ_i du produit $\mathbf{H}_s(f)^H \mathbf{H}_s(f)$. Dans le cas idéal, aucune valeur propre ne domine les autres ; nous avons donc suffisamment de sources d'informations distinctes pour reconstruire parfaitement le signal $x(t)$. L'ajout de K convertisseurs permet de compenser pour le repliement spectral qu'induit le sous-échantillonnage.

Nous avons calculé la capacité pour un canal non-sélectif en fréquence avec évanouissements de Rayleigh. On assume un réseau de 4 antennes au récepteur. Le facteur K est le facteur de sous-échantillonnage. La corrélation spatiale est modélisée par

$$\rho_0 = 1, \quad \rho_1 = \rho \quad \rho_2 = \rho^2 \quad \rho_3 = \rho^3$$

où $\rho_{|i-j|} = \rho^{|i-j|}$ est le coefficient de corrélation entre les éléments i et j. Il s'agit du modèle de canal symétrique K-exponentiel.

©LRTS 2005-2006

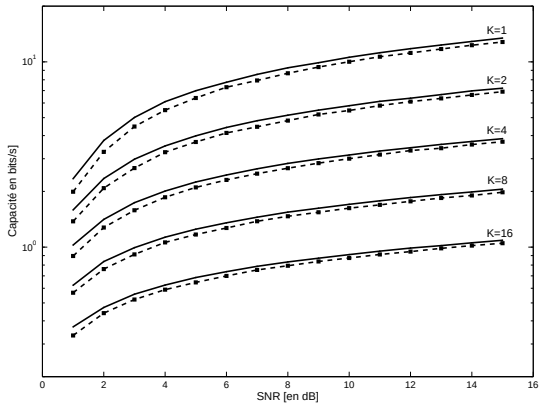


FIG. 10.3: Capacité en fonction du rapport signal-à-bruit. Le trait plein indique un facteur de corrélation de 0 tandis que le trait pointillé indique un facteur de corrélation de 0.9.

La figure 10.3 montre la capacité en bits/s obtenue en fonction du rapport signal à bruit.

En observant la figure 1, on constate que la corrélation spatiale ne joue pas un rôle significatif dans le cas non-sélectif. En effet, peu importe le facteur de sous-échantillonnage K, la corrélation spatiale modifie de manière identique la capacité.

Pour des rapports signal à bruit au delà de 6, une augmentation du facteur de sous-échantillonnage de 2 entraîne une diminution de la capacité du même facteur. On peut envisager qu'en augmentant le nombre de sources d'information par 2, nous pourrons compenser la perte due au repliement spectral.

10.6 Conclusion

Nous avons présenté une brève étude de la capacité. De plus, une nouvelle architecture de récepteur qui exploite le paradigme MIMO va nous permettre de palier la non-idéalité des échantillonneurs parallèle.

Bibliographie

[1] M. I. Kadec, "The exact value of the Paley-Wiener constant," *Dokl. Akad. Nauk SSSR*, pp. 1253-1254, 1964.

[2] R. Gallager, *Information Theory and Reliable Communications*. John Wiley and Sons, Inc., 1968.

[3] G. J. Foschini et M. J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wireless Personnal Communications.*, vol. 6, pp. 311-335, 1998

[4] Nicola Da Dalt, Moritz Hartenec, Christoph Sandner et Andreas Wiesbauer, "On the jitter requirements of the sampling clock for analog-to-digital converters," *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications.*, vol. 49, no. 9, pp. 1354-1360, 2002

Les codes à faible densité de parité

Irina Adjudeanu, *Étudiante au doctorat*
Dr Jean-Yves Chouinard, *Directeur de recherche.*
Dr Paul Fortier, *Co-directeur de recherche.*

Résumé – Nous presentons l'étude des performances d'erreur de trois types de codes LDPC : les codes LDPC construits pseudo-aléatoirement proposés par Gallager, les codes LDPC construits sur la base de la géométrie finie Euclidienne $EG(m, 2^s)$ sur un corps de Galois $CG(2^s)$ et les codes LDPC construits sur la base de la géométrie finie projective $PG(m, 2^s)$ sur un corps de Galois $CG(2^s)$. La performance des codes est analysée pour différents paramètres (longueur du code, taux, poids de la colonne, nombre de bits transmis, nombre d'itérations).

Abstract – We present the error performances of three types of LDPC codes : the pseudo-random LDPC codes proposed by Gallager, the LDPC codes based on the euclidien geometry $EG(m, 2^s)$ over the Galois field $GF(2^s)$ and the LDPC codes based on the projective geometry $PG(m, 2^s)$ over the Galois field $GF(2^s)$. We analyze the performances of these types of codes, as a function of different parameters (length of code, rate, column weight, number of transmitted bits, number of iterations).

11.1 Introduction

Les communications sans fil d'aujourd'hui demandent des débits élevés, de la fiabilité, une efficacité en puissance et en largeur de bande. Les codes LDPC sont des codes qui s'approchent de la limite de Shannon. Il a été démontré que les codes LDPC longs avec un décodage itératif basé sur la propagation de la confiance atteignent une performance d'erreur à une fraction de décibel de la limite du Shannon [1], [2], [3], [4], [5], [6]. Dû à cette caractéristique, concernant le contrôle d'erreurs, les codes LDPC sont en grande compétition avec les codes turbo dans les systèmes de communications numériques qui demandent une fiabilité élevée. En plus, ils ont quelques avantages par rapport aux codes turbo.

Dans ce document on fait une analyse et une comparaison entre les performances des trois types différents de codes LDPC, dans le but de trouver des méthodes pour construire de meilleures codes LDPC.

11.2 Performance des codes LDPC pseudo-aléatoires

Les codes LDPC pseudo-aléatoires sont construits tel que les trois conditions de la définition de codes LDPC donnée par Gallager soient satisfaites [7], [8]. Des analyses avec l'ordinateur

sont nécessaires afin de trouver de tels codes (en particulier pour les codes très longs). Cette construction produit un ensemble de codes aléatoires LDPC et il a été démontré que ceux-ci fournissent de bonnes performances [9].

La construction de la matrice **H** est faite en plusieurs étapes. À chaque étape, une nouvelle colonne est ajoutée à une matrice formée partiellement. La colonne ajoutée est choisie entre plusieurs colonnes selon les conditions à respecter par la matrice de parité d'un code LDPC.

En raison des conditions imposées pendant la construction du code, son graphe de Tanner ne contient pas de cycles d'ordre 4 et alors son périmètre est égal à au moins 6. Cette construction n'est efficace que pour des petites valeurs de γ (3 ou 4). Pour des valeurs plus grandes de γ, les ordinateurs d'aujourd'hui n'arrivent pas à effectuer efficacement les calculs en un temps raisonnable.

Les codes générés pseudo-aléatoirement par ordinateur n'ont pas les mêmes propriétés structurales que les codes de géométrie finie (par exemple la structure cyclique ou quasi-cyclique). En conséquence, l'implémentation matérielle de ces codes est beaucoup plus complexe et ne peut pas être réalisée avec des registres à décalage linéaires.

La construction aléatoire résulte en un ensemble de codes LDPC contenant comme sous-classe les codes LDPC de géométrie finie. Il existe des codes (en particulier les codes aléatoires de grande longueur) qui conduisent à une meilleure performance d'erreur que les codes basés sur la géométrie finie.

Pour cette construction il est très difficile de déterminer la distance minimale du code et pour $\gamma = 3$ ou 4, la limite inférieure $\gamma + 1$ pour la distance minimale peut être très petite.

Pour notre étude, on a choisi en premier un code LDPC pseudo-aléatoire avec les paramètres suivants : la longueur du code $n = 255$, la dimension $k = 170$, le rendement $R = 0.67$, le poids de colonne $\gamma = 3$ et et le poids de ligne $\rho = 9$.

On a fait des analyses des performances de ce type de codes en fonction de différents paramètres :

- la *longueur du code* ($n = 255$, $n = 510$ et $n = 1020$) (Fig. 11.1) en gardant les autres paramètres constants (le rendement du code, le poids de ligne et le poids de colonne, le nombre d'itérations faits pour le décodage SPA et le nombre de mots-codes envoyés). Plus la longueur du code est grande, plus on obtient des meilleures performances, mais ça prend plus de temps pour le décoder et pour créer la matrice **H**.
- *le poids de la colonne* (3 ou 4) (Fig. 11.2), (Fig. 11.3) - plus le poids de la colonne est grand, plus on obtient de mauvaises performances. La distance minimale pour ce type de codes a comme limite inférieure $\gamma + 1$ et donc pour des petites valeurs de γ on obtient des codes avec une petite distance minimale entre les mots-codes et ceci n'est pas avantageux pour le décodage. On doit donc faire un compromis en choisissant la valeur de poids.
- *le nombre maximum d'itérations* dans le décodage SPA (on a des améliorations des performances avec l'augmentation du nombre d'itérations permis). Nous avons fait des simulations pour 10, 30 et 100 itérations (Fig. 11.4).

Les figures 11.1 à 11.4 montrent les résultats des simulations obtenus.

On a essayé de mettre en évidence les effets du décodage SPA sur une image à chaque itération. Pour ce faire, on a construit une image de dimension 90×170, codée avec le code LDPC pseudo-

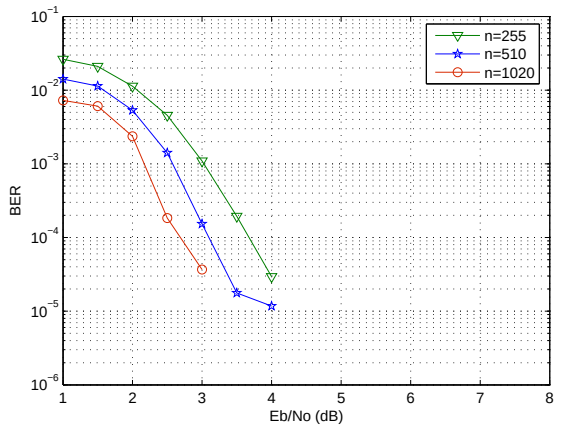


Fig. 11.1: Les probabilités d'erreur par bit des trois codes LDPC pseudo-aléatoires de même rendement ($R = 0.67$), de même poids sur la colonne ($\gamma = 3$), mais de longueurs différentes : $n = 255$, $n = 510$ et $n = 1020$. On transmet 1000 mot-codes qui sont décodés avec l'algorithme log-SPA, après 50 itérations.

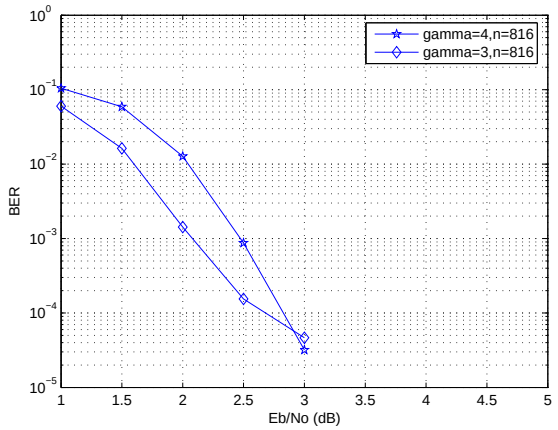


Fig. 11.2: L'influence du poids de la colonne (3 et 4) sur la performance des codes pseudo-aléatoires (simulation avec un code de longueur $n = 816$, rendement $R = 1/2$). On transmet 1000 mots-codes qui sont décodés après 50 itérations de l'algorithme SPA.

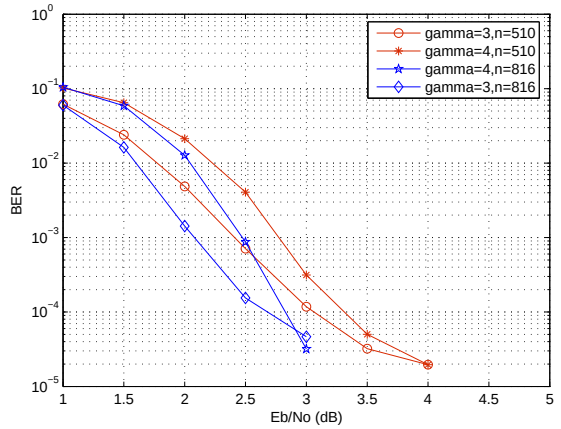


Fig. 11.3: L'influence du poids de la colonne (3 et 4) sur la performance des codes pseudo-aléatoires (comparaison pour deux codes de longueurs différents $n = 816$ et $n = 510$ et rendement $R = 1/2$. On transmets 1000 mots-codes qui sont décodés après 50 itérations de l'algorithme SPA.

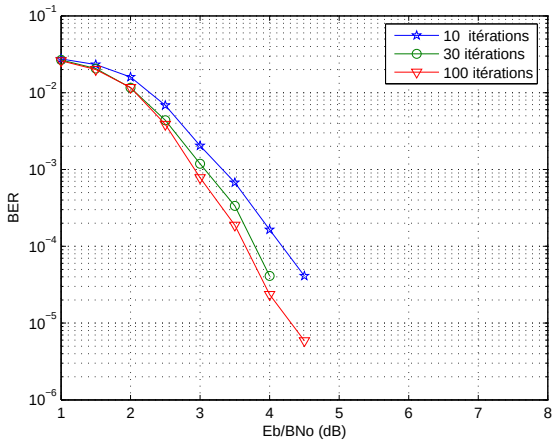


Fig. 11.4: Code LDPC pseudo-aléatoire (255, 170) - Comparaison entre le décodage SPA-log, fait en 10, 30 et 100 itérations.

aléatoire (255,170), i.e. de poids de colonne $\gamma = 3$ et de rendement $R = 0.67$. Cette image est ensuite modulé en BPSK et transmise sur un canal AWGN avec un rapport signal à bruit de

3 dB. À la réception l'image reçue est décodée après 10 itérations du décodage SPA dans la version logarithmique. La figure 11.5 montre les probabilités d'erreur en fonction du rapport signal-à-bruit à chaque itération.

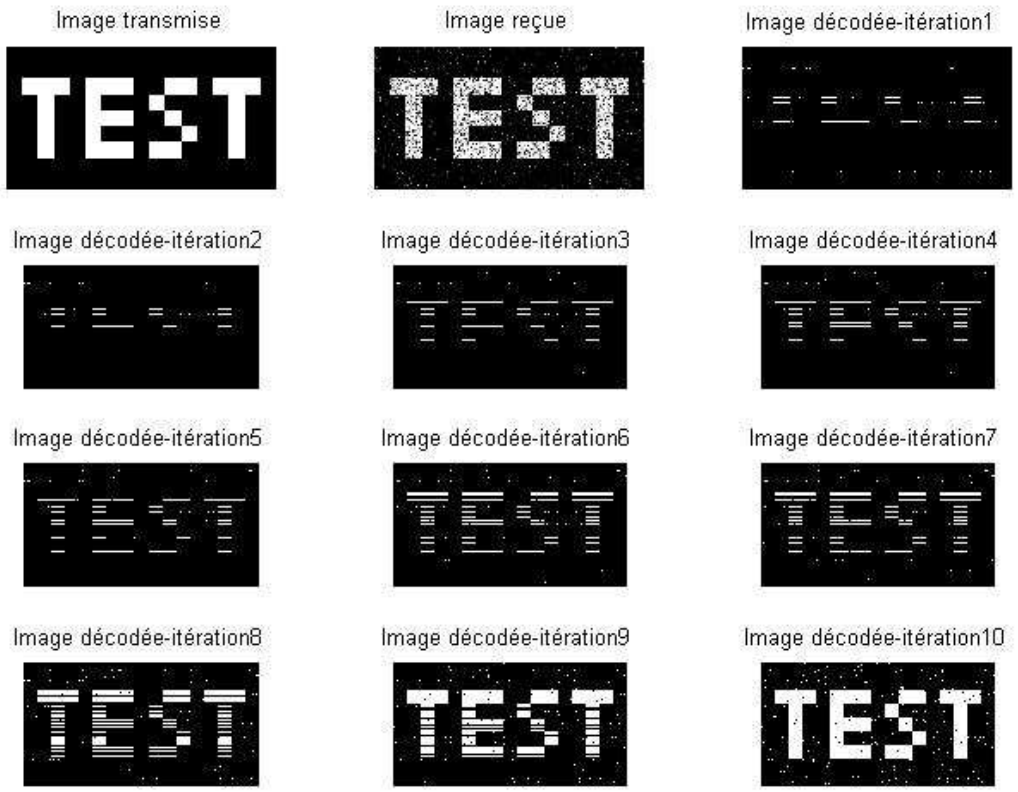


FIG. 11.5: Le décodage SPA-log d'une image codée LDPC - l'évolution du décodage à chaque itération.

11.3 Codes LDPC basés sur la géométrie finie euclidienne

Les codes LDPC basés sur la géométrie finie présentent pour des rendements élevés (i.e. près de l'unité) de très bonnes performances avec l'algorithme de décodage SPA. Aucun plancher d'erreur n'est observé pour des taux d'erreur $\leq 10^{-6}$ (Fig. 11.7).

La géométrie finie $EG(m, 2^s)$ consiste en 2^{ms} points et chaque point est représenté par un m-tuple sur $CG(2^s)$. Par chaque point passent γ lignes. Chaque ligne comprends 2^s points (poids de ligne : $\rho = 2^s$). À partir de cette géométrie finie, on peut construire un code avec la matrice de parité $\mathbf{H}$, ayant ses éléments choisis selon les points et les lignes dans cette géométrie finie.

Pour notre étude on a choisi un code EG-LDPC de type 1 avec $m = 2$ et $s = 4$. Donc on a un code LDPC construit dans la géométrie euclidienne $EG(2, 2^4)$ sur le corps de Galois

$CG(2^4)$. On obtient un code EG-LDPC de type 1, cyclique et bi-dimensionnel $C_{EG}^{(1)}(2,0,s)$ ayant les paramètres suivants :

- longueur : $n = 2^{2\times4} - 1 = 255$
- nombre de bits de parité : $n - k = 3^4 - 1 = 80$
- dimension : $k = 2^{2\times4} - 3^4$=175
- distance minimale : $d_{min} = 2^4 + 1 = 17$
- densité : $r = \frac{2^4}{2^{2\times4}-1} = 0.0627$

Le graphe de Tanner correspondant à ce code a un périmètre égal à 6, ce que veut dire qu'il ne contient pas de cycles courts (d'ordre 4). Le rendement de ce code est $R = k/n = 0.68$. La matrice de parité **H** du code est une matrice régulière et carrée (facile à implémenter en pratique !), de dimensions $(2^{2s} - 1) \times (2^{2s} - 1)$. Le poids de chaque ligne est le même que le poids de chaque colonne ($\gamma = \rho = 2^s$). Dans notre cas, $\gamma = \rho = 2^4 = 16$. Tenant compte que la matrice **H** d'un tel code est carrée, on peut remarquer qu'on ne doit garder en mémoire que la première rangée de **H**, les autres rangées seront ajoutées à l'aide d'un registre à décalage linéaire (par des permutations circulaires de la première rangée). Cela implique une faible complexité du codeur et du décodeur, ce que représente un grand avantage dans l'implémentation pratique.

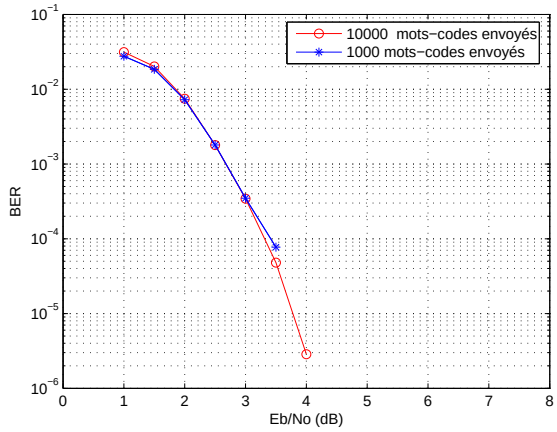


FIG. 11.6: Influence de nombre de mots-codes transmis pour les courbes de performances d'un code EG-LDPC.

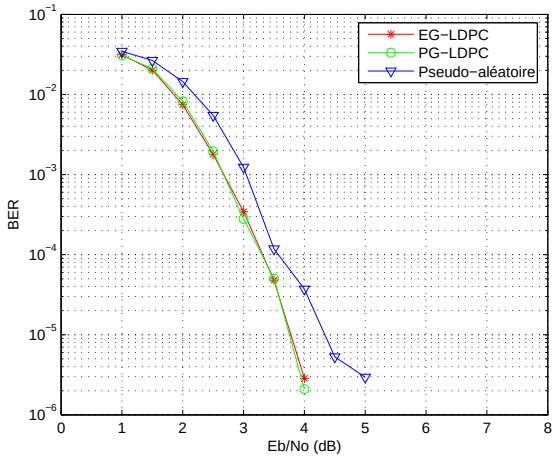


FIG. 11.7: Comparaison entre les performances des trois types de codes LDPC : pseudo-aléatoire, EG-LDPC type I et PG-LDPC type I - Un code LDPC pseudo-aléatoire (255,175) avec $\gamma = 3$, $\rho = 9$, $R = 0.67$, un code EG-LDPC (255,170) et un code PG-LDPC (273,191) ; 10000 mots-codes, SPA-log, 100 itérations.

La figure 11.6 montre pour un code EG-LDPC la différence entre les courbes de performances qu'on obtient avec 1000 et 10000 mots-codes transmis. Avec 1000 mots-codes la courbe de probabilité d'erreur s'arrête à 7.7×10^{-5} pour $E_b/N_0 = 3.5$ dB et pour 10000 mots-codes elle arrive jusqu'à 2.8×10^{-6} pour un rapport signal à bruit de 4 dB.

11.4 Codes LDPC basés sur la géométrie projective

Comme pour la géométrie Euclidienne, la géométrie projective aussi peut être construite à partir d'un corps de Galois [7].

La matrice de contrôle de parité $\mathbf{H}_{PG}^{(1)}$ de ce code est une matrice carrée, qui peut être obtenue en choisissant le vecteur d'incidence d'une ligne dans $PG(2, 2^s)$ et en faisant ses $2^{2s}+2^s$ permutations circulaires pour obtenir les lignes de la matrice.

Pour notre étude, on a choisi un code PG-LDPC de type 1 avec $m = 2$ et $s = 4$. Ce code LDPC est construit avec la géométrie projective $PG(2, 2^4)$ sur le corps de Galois $CG(2^4)$. On obtient un code PG-LDPC de type I, cyclique et bi-dimensionnel $C_{PG}^{(1)}(2, 0, s)$ ayant les paramètres suivants :

- longueur : $n = 2^{2\times4} + 2^4 + 1 = 273$
- nombre de bits de parité : $n - k = 3^4 + 1 = 82$
- dimension : $k = 2^{2\times4} + 2^4 - 3^4 = 191$
- distance minimale : $d_{min} = 2^4 + 2 = 18$
- densité : $r = \frac{2^4+1}{2^{2\times4}+2^4+1} = 0.0623$

11.5 Comparaison entre les trois types de codes

En comparant les codes pseudo-aléatoires avec les codes basés sur les géométries finies euclidienne ou projective (le code EG-LDPC et le code PG-LDPC), pour la même longueur, avec des rendements semblables, 10000 mots-codes transmis et décodage avec l'algorithme SPA, on obtient de meilleures résultats avec les codes basés sur la géométrie finie (voir figure 11.7). On doit préciser que pour les codes pseudo-aléatoires, il est toujours préférable d'imposer un nombre d'itérations beaucoup plus grand (jusqu'à 200 itérations), comparativement au nombre d'itérations nécessaires pour obtenir de bonnes performances avec les codes basés sur les géométries finies EG-LDPC ou PG-LDPC (typiquement 50 itérations sont suffisantes : si on augmente le nombre d'itérations au delà de ce nombre, la performance reste presque constante). Le décodage des codes basés sur la géométrie finie a donc l'avantage de pouvoir être réalisé plus rapidement, en raison d'un plus petit nombre d'itérations nécessaires pour le décodage de chaque mot-code envoyé.

Pour de grandes longueurs des mots-codes, les codes pseudo-aléatoires ont de meilleures performances que les codes basés sur la géométrie finie avec le décodage SPA, mais leur codage est très complexe à cause de leur manque de structure (e.g. ni cyclique, ni quasi-cyclique). Un autre inconvénient des codes pseudo-aléatoires réside dans la difficulté de trouver leurs distances minimales.

11.6 Les structures des cycles dans le graphe de Tanner

Même si les contraintes de la construction des trois types de codes imposent qu'ils n'ont pas de cycles de longueur 4, nous avons construit un programme Matlab pour détecter de manière exhaustive tous les cycles de différentes longueurs dans les graphes des codes. Le programme est un bon outil pour vérifier si les codes sont bien construits (sans cycles de longueur 4) et aussi

pour analyser les autres propriétés du graphe concernant les cycles de longueurs plus grands. On peut vérifier aussi si les codes ainsi construits ont des cycles de longueur 6, 8, 10, etc. Le périmètre du graphe de Tanner, i.e. la longueur du plus petit cycle dans le graphe, doit être aussi grand pour éliminer les cycles de longueurs courtes (en particulier de longueur 4) et obtenir de bonnes performances asymptotiques du code. Cependant il ne doit pas être très grand parce que dans ce cas il résulte en une petite distance minimale du code, ce qui augmente le plancher d'erreur irréductible. On doit donc faire un compromis dans le processus d'élimination de cycles courts.

11.7 Conclusion

Dans la construction des codes LDPC il faut tenir compte d'un ensemble de paramètres qui influencent leur performance. Nous avons montré l'influence de chaque paramètre. On a démontré que pour de courtes longueurs, les codes basés sur les géométries finies peuvent avoir de meilleures performances d'erreur que les codes pseudo-aléatoires. En plus, ils ont aussi des avantages d'implementation pratique, temps de calcul et de mémoire.

Bibliographie

[1] D. MacKay and R. Neal, "Near Shannon Limit Performance of Low Density Parity Check Codes," *Electron. Lett.*, vol. 32(18), pp. 1645–46, 1962.

[2] D. MacKay, "Gallager Codes That Are Better Than Turbo Codes," in *Proc. 36th Allerton Conf. Commun., Control, and Computing*, 1998, monticello, III.

[3] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[4] M. Davey and D. MacKay, "Low Density Parity Check Codes over GF(q)," *IEEE Commun. Lett.*, vol. 2(6), pp. 165–167, 1998.

[5] S. Lin, Y. Kou, and M. Fossorier, "Low Density Parity Check Codes Construction Based on Finite Geometries," in *Proc.GLOBECOM 2000*, 2000, san Francisco, calif., November 27-December 1.

[6] Y. Kou, S. Lin, and M. Fossorier, "Construction of Low Density Parity Check Codes-A Geometric Approach," in *Proc. 2nd Intl. Symp. Turbo Codes and Related Topics*, brest, France, September 4-7.

[7] S. Lin and D. Costello, *Error control coding.* Prentice Hall, 2004.

[8] R. Gallager, "Low Density Parity Check Codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–29, 1962.

[9] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, 1999.

©LRTS 2005-2006

II

Systèmes MIMO

Table des Matières

Sur la faisabilité d'une architecture distribuées pour les communications sans-fil mobile **71**
Schéma de codage spatio-temporel avec diversité de fréquence pour un système MIMO-OFDM **75**
Récepteur MIMO multiusager à traitement multi-couches spatio-temporel **81**

Sur la faisabilité d'une architecture distribuées pour les communications sans-fil mobile

Philippe Leroux, *Étudiant au doctorat.*

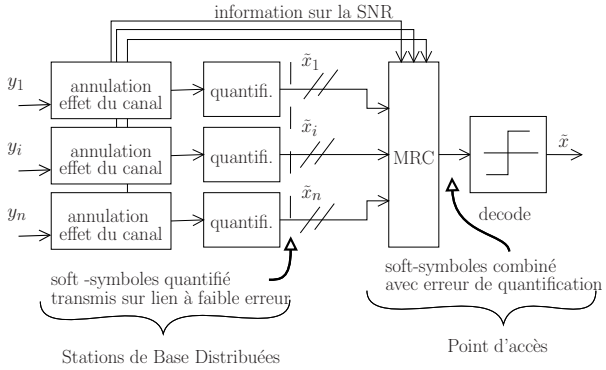
Dr Sébastien Roy, *Directeur de recherche.*

Dr Jean-Yves Chouinard, *Co-directeur de Recherche.*

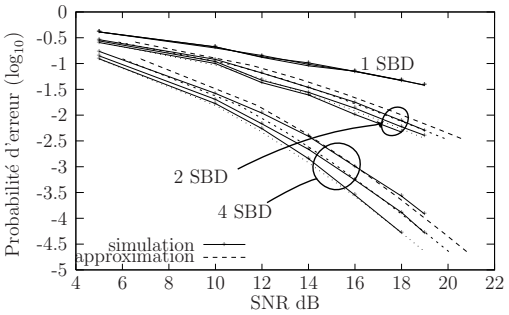
Résumé – L'intérêt de ce travail se porte sur la faisabilité du paradigme de stations de base géographiquement distribuées pour les communications mobiles, permettant des traitements spatio-temporels et démultipliant les degrés de liberté quant à l'allocation des ressources. Dans ce contexte, plusieurs champs connexes sont envisagés afin d'établir une preuve de la faisabilité et de la viabilité d'une telle architecture. On démontre d'abord les gains sur les canaux de transmission "distribués" utilisant des techniques de traitement MIMO. On propose ensuite un algorithme distribué d'allocation des ressources radio pour finir par l'étude de la structure inhérente à une telle architecture et des algorithmes de routage et d'organisation.

Abstract – We are interested here in the study of the feasibility of geographically distributed base stations in mobile communication, allowing space-time processing and offering numerous possibilities in terms of resource allocation. In this context, different aspects are studied for the overall design of the architecture. First, a protocol to gain diversity over distributed channels is proposed. A distributed algorithm is then studied to allocate radio resources. Finally, we survey the possibilities in the network structure comprised of these base stations the feasibility of distributed routing and organization.

Les développements récents en communication sans-fil apportent une multitude de techniques pour augmenter l'efficacité spectrale et la résistance aux évanouissements [1]. Afin de profiter au mieux de ces possibilités, une architecture de station de base distribuée est proposée afin de contrer les effets de "trou de serrure", diminuer les distances de parcours, tout en simplifiant l'électronique embarquée des points d'accès qui devront être peu coûteux afin de faciliter leur déploiement. Compte tenu de l'explosion des possibilités offertes par ce schéma, la question se pose de comment utiliser au mieux les ressources. Justement, la science voit apparaître et se définir un nouveau domaine d'intelligence distribuée [2, 3]. Dans le but d'appliquer des techniques distribuées aux futures générations de systèmes de communication sans-fil, on s'intéresse d'abord à caractériser les canaux de communication dans ce contexte et ensuite de développer des algorithmes efficaces pour leur gestion.



(a) Architecture de diversité par *soft-symboles*.



(b) Effet de la quantification du signal relayé avec une modulation 16-QAM pour 1, 2 et 4 SBD, et des taux de 1,2 et 10.

FIG. 12.1: Architecture de diversité par *soft-symboles* et résultats.

12.1 Caractérisation des Canaux distribués

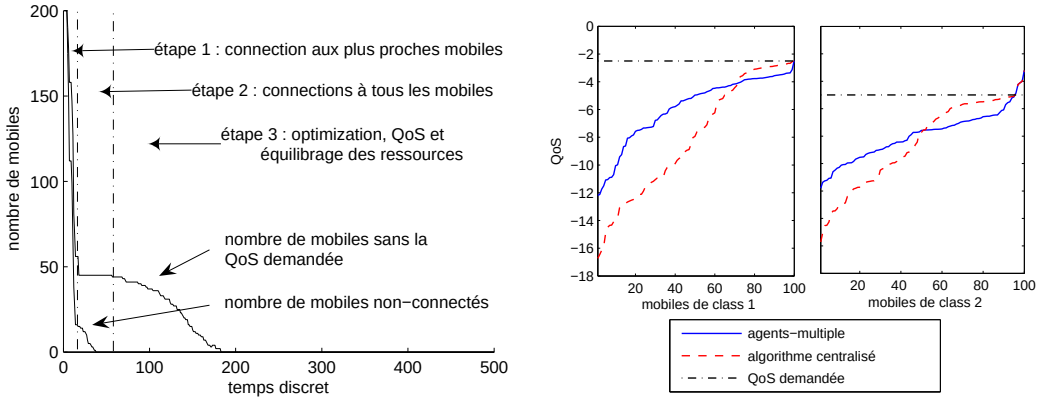
L'architecture de stations de bases distribuées (SBD) consiste en un réseaux de point de relayage (à l'instar de points d'accès), répartis sur l'ensemble de la région couverte. Ces SBD sont reliés entre elles soit par des liens filaires ou sans-fil fixe, voir par RF sur fibre optique. Ce réseau est connecté à des points d'accès pour d'autres réseaux (Internet, téléphone). On s'intéresse d'abord au lien montant. On souhaite exploiter les DBS par des techniques MIMO afin d'augmenter les capacités du système [4].

Une technique de combinaison à ratio maximale est proposée considérant l'hypothèse que la qualité du lien DBS/point d'accès est meilleure que le lien mobile/points d'accès (probabilité d'erreur de transmission significativement plus faible). Cette hypothèse est justifiée par le fait que ce lien est fixe ou câblé et subira peu ou pas d'évanouissement. L'hypothèse contraignante en revanche impose une capacité maximale de transmission dans les liens SBD/points d'accès. Ainsi, les SBD ne peuvent relayer le signal reçu des mobiles parfaitement au point d'accès. On montre par simulation et par une approximation analytique que cette hypothèse n'enlève pas le degré de diversité du traitement MIMO et résulte en une perte de SNR relativement faible.

La figure 12.1(a) illustre le schéma proposé et la figure 12.1(b) donne des résultat de simulation avec les approximations analytiques. On conclut que la technique est viable dans le contexte décrit ci-haut.

12.2 Agents multiples pour allocation des ressources radio

Considérant la même hypothèse de capacité limitée de transmission entre les SBD, on comprend qu'une SBD ne peut relayer qu'un nombre limité des mobiles qu'elle "entend" . De plus l'électronique devant être simplifié pour réduire les coûts, la chaîne de réception RF ne pourrait que démoduler un certain nombre de canaux. La question se pose alors pour les SBD de choisir



(a) Comportement des agents en temps, illustrant la convergence vers un nombre de mobile connecté avec la QoS demandée optimale.

(b) Profile de QoS obtenue en triant sur la QoS reçu par le mobile $P_{\text{tot}}(\dots)$, pour deux classes de mobile. L'algorithme distribué réparti mieux les ressources, la version centralisé essayant de maximiser la somme des QoS reçues

Fig. 12.2: Résultats d'optimisation avec agents multiples

les mobiles à relayer. Ceci avec les contraintes d'assurer la connectivité et autant que possible, la Qualité de Sevice (QoS).

Le problème est combinatoire, et pour M mobile en jeux, B SBD et m connexions (mobile/SBD) possibles par SBD, on a $(C_M^m)^B$ combinaisons possibles (ou C_M^m est le nombre de combinaisons possibles de m parmi M). Un algorithme centralisé pour la gestion des connexions n'est pas souhaitable. Cela génèrerait trop de trafic sur le réseau pour centraliser l'information de l'état du système. De plus, cet état est voué à changer rapidement vu la mobilité des terminaux.

Un algorithme distribué [5] de type colonie d'insectes (*swarm intelligence*) [3, 6] est proposé qui permet d'atteindre une solution optimale. Chaque SBD est considérée comme un agent équipé de senseur qui lui permette de connaître les mobiles dans sa région d'action, ainsi que la QoS demandée et la QoS reçue par chacun au temps présent. La figure 12.2 illustre l'efficacité de la solution proposée

Des études sont en cours pour modéliser le système dans un cadre formel en s'intéressant notamment à la théorie COIN [2] qui semble plus évoluée que la théorie des jeux.

12.3 Réseau *small-world* et partage des ressources

Une fois les connexions mobile/SBD établies, il faut encore que les SDB puissent relayer l'information au point d'accès. De plus, la notion de cellule du paradigme cellulaire disparaît, puisque diverses SBD peuvent relayer la transmission d'un mobile. Certains points d'accès seront nécessairement connectés à un réseau central (Internet par exemple). La question se pose à savoir comment les SBD peuvent relayer l'information au point d'accès optimal, quel genre de trafic cela engendre sur le réseau et comment le balancer de façon optimale, le tout avec des algorithmes

distribués.

La littérature sur les réseaux est très étendue. Développée à l'origine par Rapoport avec les réseaux aléatoires, l'étude des réseaux "petit monde" (*small-world*) est particulièrement d'actualité. L'étude porte son intérêt sur cette structure puisqu'elle semble être inhérente dans tous les réseaux réels (réseaux sociaux, biologique, technologique et d'information) [7].

La structure du réseau des SBD n'échappera pas au principe de connectivité petit monde. Dans ce contexte, plusieurs études dévoilent des résultats encouragents laissant supposer la faisabilité d'algorithmes distribués pour répondre aux questions soulevées plus haut [8].

12.4 Conclusion

Il reste a approfondir plusieurs aspects théorique sur les agents multiples pour l'optimisation de l'allocation des ressources. Toutefois, la preuve de concept est établie. Beaucoup de travaux sont possibles dans le domaine de la caractérisation des canaux de l'architecture distribuée. Les développements en théorie de l'information et en traitement MIMO suggèrent des capacités élevées que pourrait atteindre cette architecture, notamment avec la coopération entre mobiles. Reste à élaborer des architectures de transmission et des protocoles utilisant efficacement ces possibilités. Enfin, le développement de l'architecture du réseau au niveau des stations de bases distribuées est encore à l'état embryonnaire tout en laissant entrevoir des horizons prometteurs.

Bibliographie

[1] J. Laneman, "Cooperative Diversity in Wireless Networks : Algorithms and Architectures," Ph.D. dissertation, Massachusetts Institute of Technology, Sept. 2002.

[2] K. Tumer and D. Wolpert, *Collectives and the Design of Complex Systems.* NY : Springer-Verlag, 2004.

[3] H. Van Dyke Parunak and S. Brueckner, "Stigmergic learning for self-organizing mobile ad-hoc networks (MANET's)," in *Autonomous Agents and Multiagent Systems, 2004. AAMAS 2004. Proceedings of the Third International Joint Conference on*, July 2004, pp. 1324–1325.

[4] P. Leroux, S. Roy, and J.-Y. Chouinard, "The Performance of Soft Macrodiversity Based on Maximal-Ratio Combining in Uncorrelated Rician Fading," in 17th *Annual IEEE International Symposium PIMRC'06*, Sept. 2006.

[5] ——, "An agent system to manage mobile connections in a distributed base station scheme," in 17th *Annual IEEE International Symposium PIMRC'06*, Sept. 2006.

[6] H. V. D. Parunak and S. A. Brueckner, *Methodologies and Software Engineering for Agent Systems.* Springer, 2004, ch. Engineering swarming systems, pp. 341–376.

[7] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, p. 167, 2003. [Online]. Available : http://www.citebase.org/cgi-bin/citations?id=oai:arXiv.org:cond-mat/0303516

[8] J. Kleinberg, "The Small-World Phenomenon : An Algorithmic Perspective," in *Proceedings of the 32nd ACM Symposium on Theory of Computing*, 2000. [Online]. Available : www.cs.cornell.edu/home/kleinber/swn.ps

Schéma de codage spatio-temporel avec diversité de fréquence pour un système MIMO-OFDM

Simon Savary, *Étudiant à la maîtrise*

Huu Tue Huynh, *Directeur de recherche.*

Résumé – Nous présentons un schéma de codage spatio-temporel exploitant la diversité fréquentielle pour un système MIMO-OFDM à large bande. Nous exposons quelques résultats de simulation des performances de ce code.

Abstract – We introduce a space-time coding scheme with frequency diversity for wideband MIMO-OFDM systems. We present some simulated performance results of the proposed scheme.

13.1 Introduction

La demande croissante en téléphonie cellulaire exige l'installation de liens sans fil plus fiables et de meilleurs débits binaires pour supporter cette nouvelle demande. Les systèmes MIMO (*multiple-input, multiple-output*) sont considérés comme d'excellents candidats pour les communications mobiles sans fil de la quatrième génération.

L'exploitation des diversités spatiale, temporelle ou fréquentielle est une voie évidente pour l'amélioration de la fiabilité des liens sans fil, et l'association de la technique de modulation OFDM (*Orthogonal Frequency Division Multiplexing*) et du paradigme MIMO semble prometteuse. La nature multiporteuse de la modulation OFDM permet d ?exploiter la diversité fréquentielle en plus des diversités spatiale et temporelle et a ainsi le potentiel d ?améliorer les performances sur les systèmes à large bande. En exploitant les trois diversités mentionnées, il est théoriquement possible [4] de réaliser un ordre de diversité maximal de $n_t n_r L$, où n_t et n_r sont le nombre d'antennes de transmission et de réception, respectivement, et L est le nombre de parcours effectifs pour le canal sans-fil multiparcours.

Après avoir décrit brièvement les systèmes MIMO-OFDM et le modèle de canal MIMO-OFDM retenu, nous introduirons un nouveau schéma de codage pour les systèmes MIMO-OFDM exploitant la diversité des domaines spatial, temporels et fréquentiels. Quelques résultats de simulation du schéma de codage seront aussi présentés.

13.2 Description du modèle MIMO-OFDM

Nous considèrons un système MIMO-OFDM comportant $n_t = 2$ antennes de transmission et n_r antennes de réception. Une trame OFDM est divisée en N sous-porteuses et est précédée d'un préfixe cyclique de longueur $D \geq L$ symboles, où L est la longueur effectuve du canal MIMO multiparcours. La réponse en fréquence du canal MIMO de longueur L est donnée par

$$\mathbf{H}(k) = \sum_{l=0}^{L-1} \mathbf{H}_l e^{-j2\pi\frac{kl}{N}}, \tag{13.1}$$

où $k \in \{0, \cdots, N-1\}$ et $\mathbf{H}_l$ est la matrice canal pour le l^e parcours. Au récepteur, la relation d'entrée-sortie a la forme

$$\mathbf{R}(k) = \mathbf{H}(k)\mathbf{X}(k) + \mathbf{B}(k), \tag{13.2}$$

où $\mathbf{R}(k)$ et $\mathbf{X}(k)$ sont respectivement deux vecteurs réception et de transmission de longueur n_r associés à la k^e sous-porteuse OFDM. Le vecteur $\mathbf{B}(k)$ est du bruit blanc additif gaussien circulaire avec variance N_0 dont la distribution est notée $\mathcal{CN}(0, N_0)$. La règle de décodage à vraisemblance maximale (ML) est appliquée sur le signal reçu en utilisant la métrique suivante, pour chaque valeur possible de $\mathbf{X}$:

$$\hat{\mathbf{X}}(k) = \arg\min_{\mathbf{X}} \sum_{j=1}^{n_r} \|\mathbf{R}_j(k) - \mathbf{H}(k)\mathbf{X}_j(k)\|^2 . \tag{13.3}$$

13.3 Schémas de codage MIMO-OFDM

Les codes orthogonaux possèdent des caractéristiques importantes, comme le décodage séparé des symboles. Une autre propriété est qu'ils offrent un odre de diversité de $n_t n_r$ dans les systèmes à large bande et jusqu'à $n_t n_r L$ dans les systèmes MIMO-OFDM [4].

Le schéma d'Alamouti

Le schéma d'Alamouti [3] est un code spatio-temporel en bloc simple de plein taux conçu pour les canaux à évanouissements plats. Pour un système MIMO à 2 antennes de transmission et de réception, la matrice code pour ce schéma est

$$\mathbf{X} = \left[\begin{array}{c|c} s_0 & -s_1^* \\ s_1 & s_0^* \end{array} \right], \tag{13.4}$$

où s_i sont les symboles complexes de la constellation choisie et $(\cdot)^*$ est l'opération de conjugaison complexe. Chaque colonne de la matrice (13.4) est appelée un code spatial et chaque ligne, un code temporel. La combinaison au récepteur du signal (13.2) tel que décrit dans [3] donne les symboles estimés $\tilde{s}_0$ and $\tilde{s}_1$:

$$\begin{bmatrix} \tilde{s}_0 \\ \tilde{s}_1 \end{bmatrix} = \|\mathbf{H}\|_F^2 \begin{bmatrix} s_0 \\ s_1 \end{bmatrix} + \mathcal{CN}\left(0, \|\mathbf{H}\|_F^2 N_0\right)_{2\times 1}, \tag{13.5}$$

où $\|\cdot\|^2$ est la norme de Fröbenius. La règle de décision ML est alors la suivante :

Règle de décision 1 *Pour le symbole estimé $\tilde{s}_j$, $j = 0, 1$, choisir s_i si et seulement si :*

$$\left(\|\mathbf{H}\|_F^2 - 1\right)|s_i|^2 + |\tilde{s}_j - s_i|^2 \leq \left(\|\mathbf{H}\|_F^2 - 1\right)|s_k|^2 + |\tilde{s}_j - s_k|^2\,,\ \forall\, i \neq k.$$

Transposition de codes spatio-temporels vers un système MIMO-OFDM

Tout code spatio-temporel peut être transposé directement vers un système MIMO-OFDM, sans toutefois exploiter la diversité de fréquence. L'avantage se réduit donc à l'amélioration du débit binaire, mais aucune diversité supplémentaire n'est apportée. Pour l'exemple du schéma d'Alamouti, sa transposition directe permet un ordre de diversité de $2n_r$, soit le même que sa version pour les canaux à bande étroite. Ceci caractérise la transposition directe de tous les codes spatio-temporels à bande étroite vers les systèmes MIMO-OFDM. Il faut donc trouver de nouveaux codes propres aux canaux à large bande.

13.4 Description du schéma proposé

Nous avons créé un code de taux $R = 1/2$ qui exploite à la fois les diversités spatiale, temporelle et fréquentielle. La matrice code couvre toutefois deux trames OFDM, durant lesquelles $2N$ symboles complexes de la constellation choisie sont transmis. Les $N/2$ symboles transmis dansle premier groupe de $N/2$ sous-porteuses OFDM sont recopiés dans la deuxième moitié (première étape de la figure 13.1). Les symboles dupliqués sont distancés de $N/2$ sous-porteuses, maximisant ainsi la diversité fréquentielle, c'est-à-dire que les sous-porteuses sont maximalement décorrélées.

La diversité spatiale peut être améliorée en échangeant l'information redondante en fréquence de l'étape 1 entre les deux antennes de transmission (étape 2 à la figure 13.1).

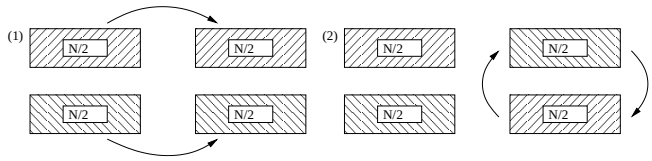


Fig. 13.1: Construction du code pour le schéma proposé. Diversité fréquentielle (étape 1) et diversité spatiale (étape 2). Les étapes sont les mêmes pour la seconde moitié de la matrice code (la deuxième trame OFDM).

La matrice code pour le schéma est la suivante

$$\mathbf{X} = \left[\begin{array}{cc|cc} \mathbf{V}_{0,0} & \mathbf{V}_{N/2,N/2} & -\mathbf{V}^*_{N/2,0} & -\mathbf{V}^*_{0,N/2} \\ \mathbf{V}_{N/2,0} & \mathbf{V}_{0,N/2} & \mathbf{V}^*_{0,0} & \mathbf{V}^*_{N/2,N/2} \end{array}\right], \tag{13.6}$$

avec les vecteurs $\mathbf{V}_{l,m} = \left[X_l^m, X_{l+1}^{m+1}, \ldots, X_{l+N/2-1}^{m+N/2-1}\right]$.

©LRTS 2005-2006

Les équations de combinaison sont les suivantes pour $n_r = 2$. Les détails peuvent être obtenus dans [1, 2].

$$\begin{bmatrix} \tilde{X}_k(k) \\ \tilde{X}_{k+N/2}(k) \end{bmatrix} = \Upsilon(k) \begin{bmatrix} X_k(k) \\ X_{k+N/2}(k) \end{bmatrix} + \check{\mathbf{H}}(k)\check{\mathbf{B}}(k) + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \check{\mathbf{H}}(k+N/2)\check{\mathbf{B}}(k+N/2), \quad (13.7)$$

où $\Upsilon(k) = \|\mathbf{H}(k)\|_F^2 + \|\mathbf{H}(k+N/2)\|_F^2$ and $\check{\mathbf{B}}(k)$ est un vecteur de longueur n_r construit à partir du bruit blanc circulaire symmétrique gaussien sur les sous-porteuses correspondantes.

En comparaison avec la règle de décision 1, la règle de décision pour ce code est donnée par :

Règle de décision 2 *Pour l'estimé $\tilde{X}_k(k)$, $k = 0, \ldots, N/2-1$, choisir X_i si et seulement si*

$$\big(\Upsilon(k)-1\big)|X_i|^2 + \left|\tilde{X}_k(k) - X_i\right|^2 \leq \big(\Upsilon(k)-1\big)|X_j|^2 + \left|\tilde{X}_k(k) - X_j\right|^2, \ \forall\, i \neq j.$$

De la même manière, pour l'estimé $\tilde{X}_{k+N/2}(k)$, $k = 0, \ldots, N/2-1$, choisir X_i si et seulement si

$$\big(\Upsilon(k)-1\big)|X_i|^2 + \left|\tilde{X}_{k+N/2}(k) - X_i\right|^2 \leq \big(\Upsilon(k)-1\big)|X_j|^2 + \left|\tilde{X}_{k+N/2}(k) - X_j\right|^2, \ \forall\, i \neq j.$$

Résultats

La figure 13.2 compare les performances du schéma d'Alamouti transposé directement sur MIMO-OFDM avec ceux du schéma de diversité proposé, pour des configurations de systèmes (2,2) et (2,4). Les paramètres de simulation sont : $L = 4$, $N = 256$, constellation QPSK et un minimum de 100 événements erreur pour la simulation de chaque point de probabilité d'erreur. Pour compenser le taux 1/2 du schéma à l'étude, ses courbes de performances ont été déplacées de 3dB vers la droite. Ainsi les deux schémas peuvent être comparés.

Nous remarquons que la pente des courbes, associée à l'ordre de diversité, est d'environ le double pour le nouveau schéma, ce qui démontre bien le gain de diversité obtenu pas le nouveau code.

13.5 Conclusion

Nous avons proposé un nouveau shéma de codage conçu pour les systèmes MIMO-OFDM. Ce schéma offre de bonnes performances de décodage par rapport à une transposition directe vers MIMO-OFDM d'un code spatio-temporel. Toutefois, bien qu'il exploite les trois types de diversité diiscutés, ce code n'atteint pas l'ordre de diversité maximal théorique de $n_t n_r L$.

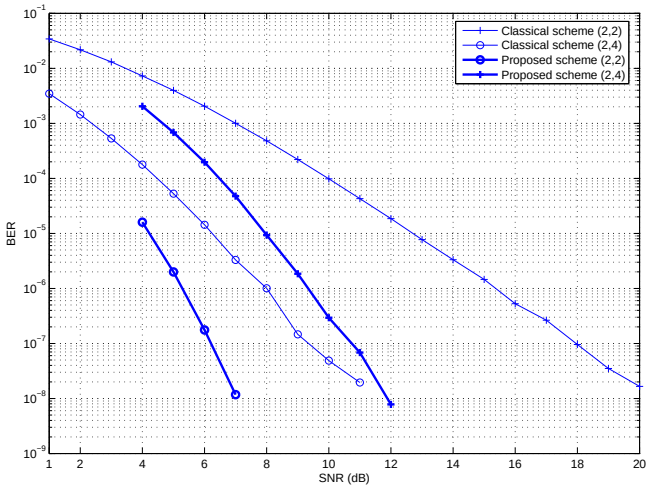


Fig. 13.2: Comparaison des deux schémas de codage. Le schéma proposé est décalé de 3 dB vers la droite pour fins de comparaison.

Bibliographie

[1] S. Savary, H. T. Huynh, J. Y. Chouinard, and S. Roy, "A Space-Frequency-Time Diversity Scheme for MIMO-OFDM Systems," *Canadian Conference on Electrical and Computer Engineering*, pp. 1379-1383, mai 2005.

[2] S. Savary, "Étude des codes spatiaux, temporels et fréquentiels dans les systèmes MIMO-OFDM," *Mémoire de maîtrise*, janvier 2005.

[3] S. M. Alamouti "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, octobre 1998.

[4] H. Bölcskei, "Principles of MIMO-OFDM Wireless Systems," *CRC Handbook on Signal Processing*, M. Ibnkahla, Ed., 2004, à paraître.

©LRTS 2005-2006

Récepteur MIMO multiusager à traitement multi-couches spatio-temporel

Isabelle LaRoche, *Associée de recherche*
Sébastien Roy, *Directeur de recherche.*

Résumé – Les sytèmes de communication sans-fil de prochaine génération nécessitent de nouvelles techniques avancées afin de supporter un nombre continuellement grandissant d'usagers et de services consommant beaucoup de largeur de bande. Les système MIMO (*Multi-Input, Multi-Output*) sont l'une de ces techniques et augmentent le taux binaire sans consommer de largeur de bande additionnelle.

Abstract – Next-generation wireless communication systems require new advanced techniques to support an ever-growing number of users and services consuming a lot of bandwidth. MIMO (*Multi-Input, Multi-Output*) systems are one of these techniques and increase the bitrate without consuming more bandwidth.

14.1 Introduction

Le spectre électromagnétique étant fortement congestionné, on se doit d'utiliser des techniques afin de l'exploiter efficacement. L'emploi de réseaux d'antennes (ou diversité spatiale) à une ou aux deux extrémités d'un lien sans-fil est une technique de plus en plus populaire. Un système MIMO (pour *Multi-Input, Multi-Output*) utilise un réseau d'antennes aux deux extrémités du lien. Il a été montré [1] mathématiquement qu'un tel système peut potentiellement offrir une augmentation d'un ordre de magnitude du taux binaire du lien sans-fil, sans pour autant consommer de largeur de bande additionnelle. Une technique de traitement de signal permettant d'obtenir une grande partie de cette augmentation du taux binaire est le codage spatio-temporel. Nous décrirons une architecture efficace de traitement multi-couches spatio-temporel utilisant un calcul de poids optimaux.

14.2 Système MIMO

La figure 14.1 montre un système MIMO $M \times M$ typique. En utilisant un algorithme multi-couches spatio-temporel [2], le signal de chacune des antennes de transmission est estimé à un endroit du récepteur. Cette estimation se fait souvent par une somme pondérée (filtre spatial),

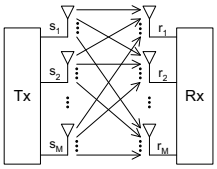


FIG. 14.1: Système MIMO

où le vecteur de poids optimaux peut être choisi selon le critère du zero-forcing (ZF) ou de la minimisation de l'erreur quadratique moyenne (MEQM). L'algorithme utilisé dans le récepteur décrit ici est montré à la figure 14.2. Il s'agit d'une version modifiée de l'algorithme V-Blast original conçu par l'équipe de Bell Labs [2].

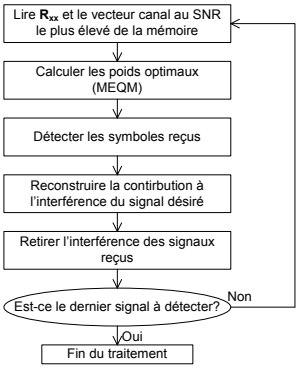


FIG. 14.2: Algorithme de détection V-BLAST modifié

Cet algorithme utilise le critère MEQM pour le calcul des poids. Cette méthode de combinaison des signaux reçus offre une meilleure performance lors de la présence d'interféreurs dans le système. Sous forme vectorielle, les poids optimaux s'expriment comme suit :

$$\mathbf{w} = \alpha \mathbf{R}_{xx}^{-1} \mathbf{c}_0^* \ , \tag{14.1}$$

où α est une constante, $\mathbf{c}_0^*$ est le vecteur canal conjugué de l'usager désiré et $\mathbf{R}_{xx}^{-1}$ est la matrice d'autocorrélation des signaux reçus. Cette matrice s'exprime ainsi :

$$\mathbf{R}_{xx}^{-1} = \sigma^2 \mathbf{I} + \sum_{j=1}^{M} E\left[\mathbf{c}_j^* \mathbf{c}_j^T\right] \ , \tag{14.2}$$

où σ^2 est la puissance du bruit, $\mathbf{I}$ est la matrice identité, $\mathbf{c}_j^*$ est le vecteur canal conjugué du $j^{ième}$ interféreur et $\mathbf{c}_j^T$ est le vecteur canal transposé du $j^{ième}$ interféreur.

14.3 Simulation Matlab

Le récepteur MIMO décrit ci-dessous a été simulé sous le logiciel Matlab. La figure 14.3 montre les résultats d'une simulation Monte Carlo d'un système à quatres antennes de transmission et de réception (4,4), ainsi que des résultats présentés dans [3] pour un système similaire. On peut voir

que l'allure de la courbe est similaire. La performance légèrement meilleure du système simulé dans ce projet s'explique par la différence dans le choix du signal à détecter. En effet, dans le cas de l'algorithme V-Blast original sans ordonnancement, les signaux sont détectés selon un ordre arbitraire tandis que dans le système simulé ici les signaux sont détectés selon leur puissance, ce qui améliore la performance du système.

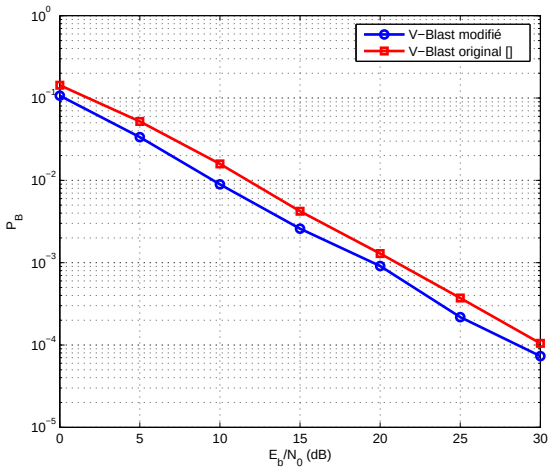


Fig. 14.3: Probabilité d'erreur par bit du récepteur d'un système (4,4)

14.4 Description matérielle

Une description matérielle du récepteur décrit brièvement ci-dessus a été composée en langage VHDL. La figure 14.4 montre l'architecture complète du système. Le bloc d'estimation du canal n'a pas été conçu dans le cadre du projet de maitrise décrit dans cette section, mais est inclus pour une meilleure compréhension du système global.

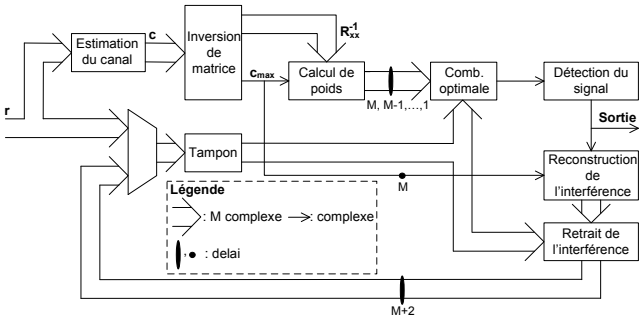


Fig. 14.4: Architecture du récepteur

Ce système a été conçu en visant les puces FPGA de la compagnie Xilinx et a été simulé sous le logiciel Modelsim. En utilisant l'outil *Link for Modelsim* de Matlab, il a été possible d'exécuter une co-simulation du récepteur modélisé sous Matlab et de celui conçu en VHDL à partir des

mêmes signaux d'entrée. De type Monte Carlo, cette co-simulation a produit une courbe de probabilité d'erreur par bit montrée sur la figure 14.5. On peut voir que la simulation produite par Modelsim correspond parfaitement à celle produite par Matlab. Ces résultats montrent que le récepteur réalisé dans le cadre de ce projet est fidèle à celui modélisé sous Matlab.

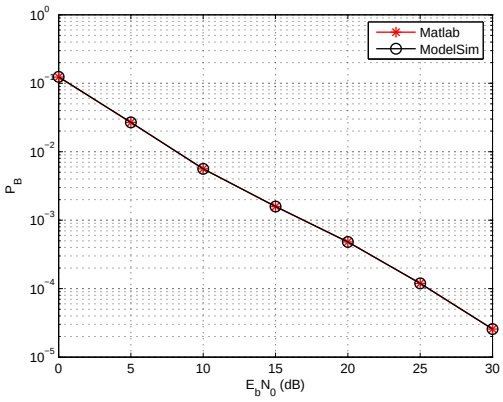


FIG. 14.5: Probabilité d'erreur par bit du récepteur d'un système (4,4) (co-simulation Matlab et Modelsim)

Le récepteur a été synthétisé à l'aide de l'outil XST de Xilinx. Une analyse des résultats obtenus a montré qu'il serait avantageux d'opter pour une puce Virtex-4 XC4VLX200 puisque celle-ci offrait les meilleures performances en terme de consommation d'espace et de fréquence. La fréquence maximale atteinte a été de 52.854 MHz. Le traitement d'une couche par le récepteur prend $3M + E + 4$ cycles d'horloges, tandis que le traitement complet des M couches en prend $3M + M(E + 3) + 1$.

14.5 Conclusion

Dans un premier temps, nous avons décrit les bases théoriques du récepteur MIMO conçu ainsi que l'algorithme de détection multi-couches utilisé. Ensuite, nous avons montré les résultats obtenus lors d'une simulation Monte Carlo du récepteur sous le logiciel Matlab. Nous avons montré que notre récepteur performait mieux qu'un récepteur idéal sans ordannancement. Finalement, nous avons présenté la description matérielle du récepteur ainsi que des résultats d'implantation et de simulation sous Modelsim.

Bibliographie

[1] G. J. Foschini and M.J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wireless Personal Communications*, vol. 6, no. 9, pp. 311–335, 1998.

[2] G. J. Foschini, "Layered Space-Time Architecture for Wireless Communication in a Fading Environment When Using Multi-Element Antennas," *Bell Labs Technical Journal*, pp. 41–595, 1996.

[3] B. Vucetic and J. Yuan, "Space-Time Coding," *Wiley*, 2003.

III

VLSI

Table des Matières

Réalisation d'un algorithme de réception MIMO avec étude architecturale et virgule fixe **87**
Implantation FPGA de l'algorithme de chiffrement à courbes elliptiques **93**
Aspects matériels d'un réseau d'antennes intelligent dédié au *Wi-Fi* **99**
Un architecture régulière de circuit d'inversion de matrice pour le traitement MIMO **103**
FPGA implementation of a digital communication chain **107**

Réalisation d'un algorithme de réception MIMO avec étude architecturale et virgule fixe

Taofik Saïdi, *Étudiant au doctorat.*
Dr Sébastien Roy, *Co-Directeur de recherche.*
Dr Olivier Sentieys, *Co-directrice de Recherche.*

Résumé – Dans le cadre des communications sans fil, la disposition de réseaux d'antennes à chaque extrémité du lien (MIMO : Multiple Input Multiple Output) optimise l'efficacité spectrale de par la transmission simultanée et indépendante de signaux, et ce en exploitant la même bande de fréquences. La complexité des algorithmes qu'implique les traitements MIMO nécessite des architectures matérielles performantes afin d'effectuer le traitement en temps réel entre autres. Dans le cadre de ce projet de recherche, nous nous intéressons à la définition optimale et concrète de ces ressources matérielles de par l'implantation d'un système MIMO performant avec un accès multiple. Un prototype basé sur l'utilisation de la technologie WCDMA (Wideband Code Division Multiple Access) a été réalisé, démontrant ainsi la faisabilité de tels systèmes. Les performances de l'implantation (ASIC, FPGA) sont étudiées suivant certains critères tels que la consommation de puissance et le codage en virgule fixe.

Abstract – In mobile communications, multiple element array antennas at both ends of the wireless link (MIMO : Multiple Input Multiple Output) improve spectral efficiency through independent and simultaneous multi-antenna transmissions without increasing the available radio spectrum. The significant complexity of MIMO techniques requires the design of efficient architectures in order to execute the algorithms in real time and in accordance with others criteria. The aim of this project is the design of optimal and practical integrated solution with the implementation of an efficient MIMO system in a multiple access network. A prototype based on WCDMA (Wideband Code Division Multiple Access) technology is implemented, illustrating the feasibility of such systems. The performances of the design (ASIC, FPGA) are studied according to criteria such as power consumption and fixed-point coding.

15.1 Contexte

La demande croissante en terme de débits de données exigée par de nouveaux services multimédia (internet sans fil, visioconférence, télévision numérique pour la téléphonie mobile) et d'une meilleure qualité de service pour les communications sans fil nécessite de proposer de nouvelles techniques pour augmenter la capacité du canal de transmission sans fil. Les techniques

actuelles associées à des modulations et des codages adaptés mettant en œuvre un lien point à point permettent d'approcher la limite théorique de Shannon. Cependant l'efficacité spectrale acquise de par ce système ne satisfait pas aux contraintes de performances présentes et futures.

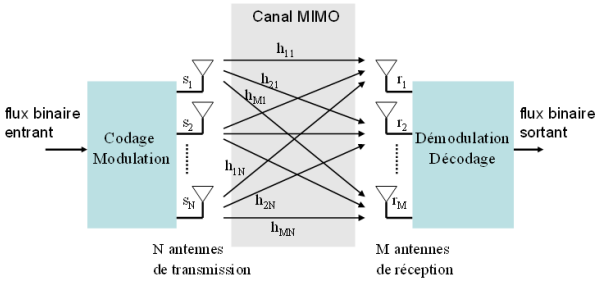


Fig. 15.1: Schéma général d'un système de transmission sans fil MIMO.

La technique des antennes multiples, plus connue sous le terme anglais MIMO (Multiple Input Multiple Output), répond potentionnellement à ces contraintes. De récentes recherches en théorie de l'information [1, 2] ont montré que la capacité des systèmes multi-antennes augmente linéairement avec le nombre d'antennes, dépassant considérablement la limite théorique de Shannon en apparence et ceci sans consommer de ressources radio supplémentaires. Ces systèmes (cf. figure 15.1) permettent ainsi d'augmenter le débit usager et de combattre efficacement les évanouissements et les interférences en exploitant la diversité produite par le canal MIMO (constitué de sous-canaux), améliorant ainsi la qualité du lien sans fil.

L'apport pour les communications numériques sans fil des systèmes MIMO est considérable en terme de débit et ceci sans accroissement de la largeur de bande. L'introduction de cette technique pour les futures normes de communication constituent le thème de travail de nombreux groupes de travail (WiMAX, 3GPP), souhaitant l'accès à un débit dépassant les 300 Mbps ! Cependant, si les algorithmes et l'architecture radiologicielle sont à présent clairement définis, les ressources matérielles devant supporter ces nouvelles applications sont autrement complexes et constituent un défi dans la définition de circuits intégrés performants.

En effet la réalisation matérielle de ces systèmes nécessite la multiplication des antennes et donc des chaînes d'amplification radio-fréquences (RF) qui constituent des parties critiques au vu de leur intégration dans des systèmes embarqués, typiquement les terminaux de téléphonie mobile. A cela s'ajoute l'accroissement de la complexité du système en bande de base due à l'implantation des traitements spatio-temporels exigeant une puissance de calcul considérable. A date, il existe peu de réalisations matérielles [3, 4, 5, 6] pour ces systèmes en raison d'une part de la jeunesse des systèmes MIMO, d'autre part du temps nécessaire aux cycles de développement et de la normalisation en cours des systèmes multi-antennes.

Un intérêt manifeste porte sur la définition d'une architecture performante (puissance de calcul importante, surface silicium occupée faible, consommation d'énergie réduite), suffisamment flexible pour pouvoir supporter des traitements aussi divers que les techniques d'accès OFDM et WCDMA (ou la combinaison des deux : MC-DS-CDMA) et le codage spatio-temporel (en

bloc, en treillis, par couches [7]), reconfigurable à tout instant pour adapter dynamiquement les traitements suivant les conditions de transmission.

15.2 Prototype MIMO-WCDMA

Description

La diversité de transmission sur la voie descendante (MISO : plusieurs antennes émettrices pour la station de base, une antenne réceptrice pour la station mobile) est déjà présente dans la norme UMTS [1]. Dans le cas où deux antennes sont positionnées à l'émission, la technique d'Alamouti [8] est appliquée. Celle-ci fournit un gain en diversité d'ordre 2 et donc améliore la qualité du signal, mais le débit usager n'est pas augmenté. Afin d'obtenir un gain en diversité et en débit, la technique HSDPA [2] [9] a été proposée afin d'accroître le débit de données pour la voie descendante (station de base vers station mobile). Le système se compose de 4 antennes émettrices et 4 antennes réceptrices (configuration inférieure possible). Cette technique substitue deux caractéristiques importantes de la norme UTRAN [3], débit variable et contrôle de puissance, par une technique de codage et de modulation adaptée (AMC [4]) aux variations du canal MIMO.

Pour la voie montante (station mobile vers station de base), la technologie HSUPA [5] [10] est proposée. Cette technique est en cours d'études et une première ébauche propose un système suivant un codage spatio-temporel relativement simple, basé sur l'orthogonalité des codes appliqués à l'émission.

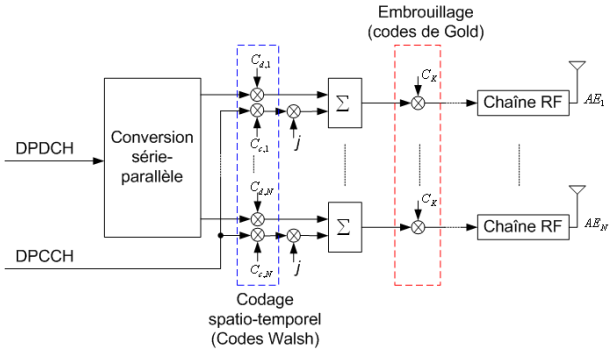


Fig. 15.2: Schéma de transmission pour N antennes émettrices, appliqué par la technique HSUPA.

La figure 15.2 illustre la technique de transmission pour N antennes émettrices. Le prototype développé au sein du laboratoire met en oeuvre cette technique. Initialement le flux de données

[1] Universal Mobile Telecommunications System
[2] High Speed Downlink Packet Access
[3] UMTS Terrestrial Radio Access Network
[4] Adaptative Modulation and Coding
[5] High Speed Uplink Packet Access

©LRTS 2005-2006

usagers (DPDCH [6]) est dissocié en N flux distincts qui sont codés (ou modulés) indépendamment. Le même canal de contrôle (DPCCH [7]), constitué en partie de symboles *pilot*, est associé à chacun de ces flux, pour l'estimation de la réponse impulsionnelle du canal MIMO en réception. Les codes de Walsh appliqués aux N branches sont *orthogonaux* entre eux. Ils permettent ainsi de distinguer au récepteur les différentes sources d'informations pour un usager et donc de faciliter le processus de réception. Un deuxième niveau de codage est appliqué (code d'embrouillage : codes de Gold) pour différencier les usagers sur la voie montante. Les N séquences binaires distinctes sont émises simultanément et indépendamment (multiplexage spatial), via les N antennes émettrices (AE_i).

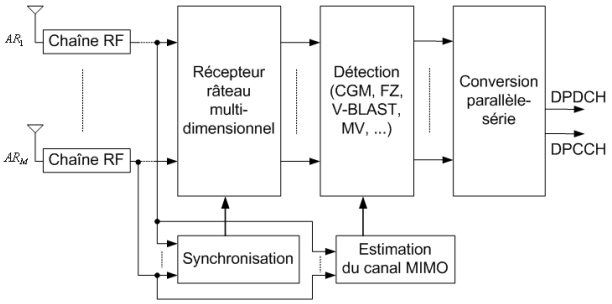


Fig. 15.3: Synoptique du récepteur MIMO.

L'architecture du récepteur est illustrée par la figure 15.3. Les signaux transmis sont perturbés par le canal MIMO large bande et reçus au récepteur, constitué de M antennes réceptrices (AR_i). Les composantes essentielles du récepteur MIMO portent sur un module de synchronisation temporelle, un récepteur RAKE multi-dimensionnel, un module d'estimation du canal MIMO et un circuit de décodage des symboles. Ensuite, le flux initialement codé et transmis est reconstitué.

Le module de synchronisation temporelle identifie les retards des signaux transmis. Il transmet ces informations au récepteur RAKE qui se synchronise et effectue l'intégration des échantillons pour fournir en sortie les statistiques sur les symboles transmis. L'estimation du canal MIMO est réalisée en parallèle. Le module de décodage prend en entrée celle-ci afin de compenser les perturbations du canal MIMO et supprimer les interférences.

Résultats d'implantation

Dans [11, 12], nous présentons le système MIMO-WCDMA développé pour une configuration 2×2. Le tableau 15.1 fournit la complexité en *slices* (entité de base du FPGA) des blocs principaux. Le module RAKE multi-dimensionnel occupe 80 % des ressources d'un des deux FPGA et constitue donc la partie la plus complexe.

Ce prototype met en valeur la complexité matérielle en traitement de base qui croît linéairement avec la configuration MIMO appliquée. La puissance de calcul nécessaire devient excessive et les ressources matérielles nombreuses. Pour un terminal mobile la consommation d'énergie constitue

[6]Dedicated Physical Data CHannel
[7]Dedicated Physical Control CHannel

	nombre de *slices*
Filtre RCSE	620 (4%)
Module de recherche	2230 (15%)
Finger	1447 (10%)

Tab. 15.1: Résultats d'implantation des principaux modules du système SISO-WCDMA pour le FPGA Virtex 3000E.

un critère important et cette complexité croissante n'aide en rien cette contrainte. De plus, les chaînes RF et la couche réseau représentent également des barrières à lever. En conséquence, il est nécessaire de revisiter les méthodes de conception de circuits capables d'intégrer des systèmes MIMO performants.

15.3 Perspectives

Les traitements spatio-temporels nécessitent une puissance de calcul croîssant suivant le nombre d'antennes disposées de part et d'autre, et donc la définition de circuits VLSI performants. Le prototype MIMO-WCDMA développé est en cours d'intégration au sein des stations de base *SignalMaster*. Ces démonstrateurs permettront de confronter les traitements spatio-temporels en environnement réel afin d'évaluer les performances du système développé tant au niveau signal qu'au niveau matériel.

De plus, du prototype réalisé et de l'étude en virgule fixe et architecturale seront extraits les critères de conception afin de définir les capacités d'une architecture reconfigurable performante (en termes de vitesse, de surface et d'énergie dissipée) supportant les multiples traitements induits par les systèmes MIMO. La conception d'une telle architecture constitue sans aucun doute un point crucial dans le déploiement futur des systèmes de communications mobiles 4G.

Bibliographie

[1] G. Foschini and M. Gans, "On limits of wireless communications in a fading environnement when using multiple antennas," *Wireless Personal Communications*, vol. 6, pp. 311–335, march 1998.

[2] I. Telatar, "Capacity of multi-antenna gaussian channels," *European Transactions on Telecommunications*, vol. 10, pp. 585–595, Nov./Dec. 1999.

[3] P. Murphy, F. Lou, A. Sabharwal, and P. Frantz, "An FPGA Based Rapid Prototyping Platform for MIMO Systems," in *Asilomar Conference on Signals, Systems, and Computers*, (Pacific Groove, CA), November 2003.

[4] S. Häene, D. Perels, D. S. Baum, M. Borgmann, A. Burg, N. Felber, W. Fichtner, and H. Bölcskei, "Implementation aspects of a real-time multi-terminal MIMO-OFDM testbed," in *IEEE Radio and Wireless Conference (RAWCON)*, september 2004.

©LRTS 2005-2006

[5] A. B. A. Adjoudani, E. Beck and G. Djuknic, "Prototype experience for mimo blast over third generation wireless system," *Journal on Selected Areas in Communication*, vol. 21, pp. 440–451, April 2003.

[6] D. Garrett, L. Davis, S. T. Brink, B. Hochwald, and G. Knagge, "Silicon complexity for maximum likelihood mimo detection using spherical decoding," *Signal processing theory to implementation, Elsevier Science*, vol. 39, pp. 1544–1552, September 2004.

[7] B. Vucetic and J. Yuan, *Space-Time Coding*. Wiley, 2003.

[8] S. Alamouti, "A simple diversity for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 1451–1458, October 1998.

[9] G. T. R. WG1, "High speed downlink packet access : Physical layer aspects," Rapport technique 25.858, v5.0.0, 2002.

[10] J. Fonollosa, M. Heikkilä, K. Majonen, X. Mestre, A. Pagès, E. Tiirola, A. Wiesel, and J. Ylitalo, "Implementation of relevant algorithms," Rapport technique IST-2000-30148 I-METRA D3.2,v1.0, 2002.

[11] L. Bélanger, S. Roy, T. Saïdi and O. Sentieys, "Prototyping a MIMO W-CDMA system using a system-level approach," in *Global Signal Processing conference*, (Santa-Clara, CA), september 2004.

[12] T. Saïdi, O. Sentieys, and S. Roy, "Prototype mimo temps réel pour l'umts," November 2005.

Implantation FPGA de l'algorithme de chiffrement à courbes elliptiques

Louis Dupont, *Étudiant à la maîtrise*
Sébastien Roy, *Directeur de recherche.*
Jean-Yves Chouinard, *Co-Directeur de recherche.*

Résumé – Nous présentons une implantation FPGA d'un cryptosystème à courbes elliptiques. De tels systèmes deviennent de plus en plus populaires, ceux-ci offrant le plus haut niveau de sécurité par bit parmi les cryptosystèmes communément utilisés. Le cryptosystème a été conçu en exploitant la représentation w-NAF de la clef privée. Les unités arithmétiques sur $GF(2^N)$ ont également été fortement parallélisées.

Abstract – We present a FPGA implementation of an elliptic curve cryptosystem. Such systems are becoming increasingly popular as they provide the highest strength per bit of any cryptosystem commonly used today. The cryptosystem was built exploiting the w-NAF representation of the private key as well as parallelism through the $GF(2^N)$ arithmetic units.

16.1 Introduction

Le chiffrement d'une communication sur un canal quelconque pose un problème de taille. Un émetteur doit en effet transmettre au récepteur une information lui permettant de décoder une communication chiffrée. Le canal d'information n'étant souvent pas physiquement sécurisé, cette information préliminaire doit être transmise sans que les interlocuteurs n'aient à se soucier qu'un autre acteur puisse intercepter cette information.

Différents algorithmes ont été développés afin de rendre possible cet échange préliminaire. Parmi les algorithmes communément utilisés, la cryptographie à courbe elliptique [7] permet de maximiser la sécurité d'une communication avec un minimum d'échange préliminaire d'information.

La cryptographie à courbe elliptique repose sur l'addition de deux points sur cette courbe. Géométriquement, cette opération revient à trouver le troisième point d'intersection entre la courbe elliptique et la droite joignant ces deux points, suivi d'une réflexion selon l'axe vertical tel qu'illustré à la figure 16.1.

La multiplication scalaire kP est définie comme l'addition du point P avec lui-même k fois. Cette opération est relativement lourde au niveau logiciel. Le développement d'un coprocesseur spécialisé pour cette opération devient alors pertinent.

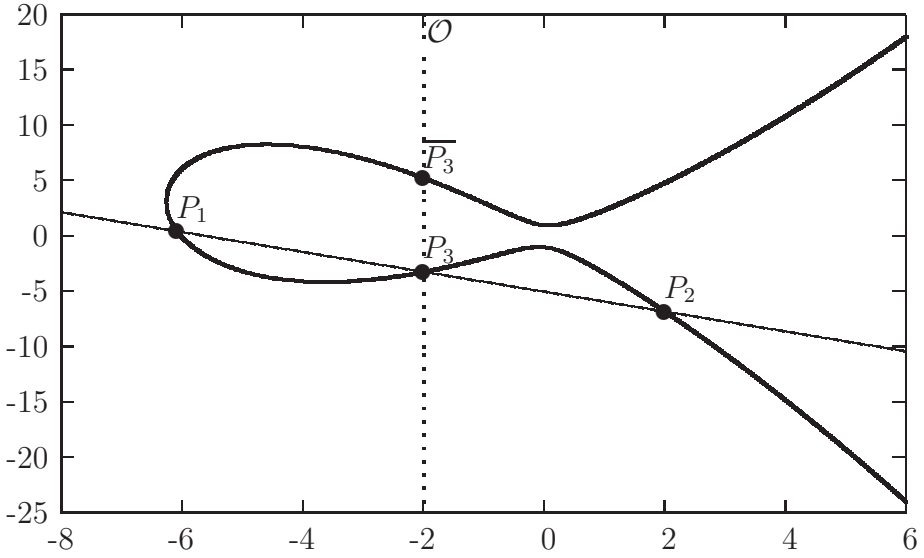


Fig. 16.1: Interprétation géométrique de l'opération d'addition de deux points distincts sur une courbe elliptique ($P_1 + P_2 = \overline{P_3}$)

16.2 Processeur cryptographique

Le circuit a été décomposé en ses différentes unités fonctionnelles reliées entre elles par un bus trois-états de façon analogue à un processeur complexe traditionnel tel qu'illustré à la figure 16.2. La largeur du bus est fixée par la taille des coordonnées des points sur la courbe elliptique. Trois des unités sont dédiées à des fonctions spécifiques ayant trait à l'arithmétique sur l'extension du corps de Galois $GF(2^N)$.

Génération d'entiers aléatoires en représentation w-NAF

La multiplication scalaire peut être allégée en décomposant le scalaire en puissance de 2 (représentation binaire). L'opération s'apparente alors à une multiplication traditionnelle. La charge de calcul peut encore être allégée en représentant le scalaire sous une forme alternative.

La représentation w-NAF minimise le nombre de chiffres différents de zéro dans la représentation du scalaire, minimisant la charge de calcul. Ce dernier est alors représenté en respectant :

$$\begin{aligned} k &= \sum_{i=0}^{n} k_i 2^i \mid k_i \,\epsilon\, \{0, \pm(2j+1 | 0 \leq j \leq 2^{w-2}-1)\} \,, \\ \sum_{l=1}^{w-1} k_i k_{i+l} &= 0. \end{aligned} \tag{16.1}$$

La conversion d'un scalaire vers sa représentation w-NAF s'avère difficile, particulièrement d'un point de vue matériel. Heureusement, dans la plupart des schémas cryptographiques tels

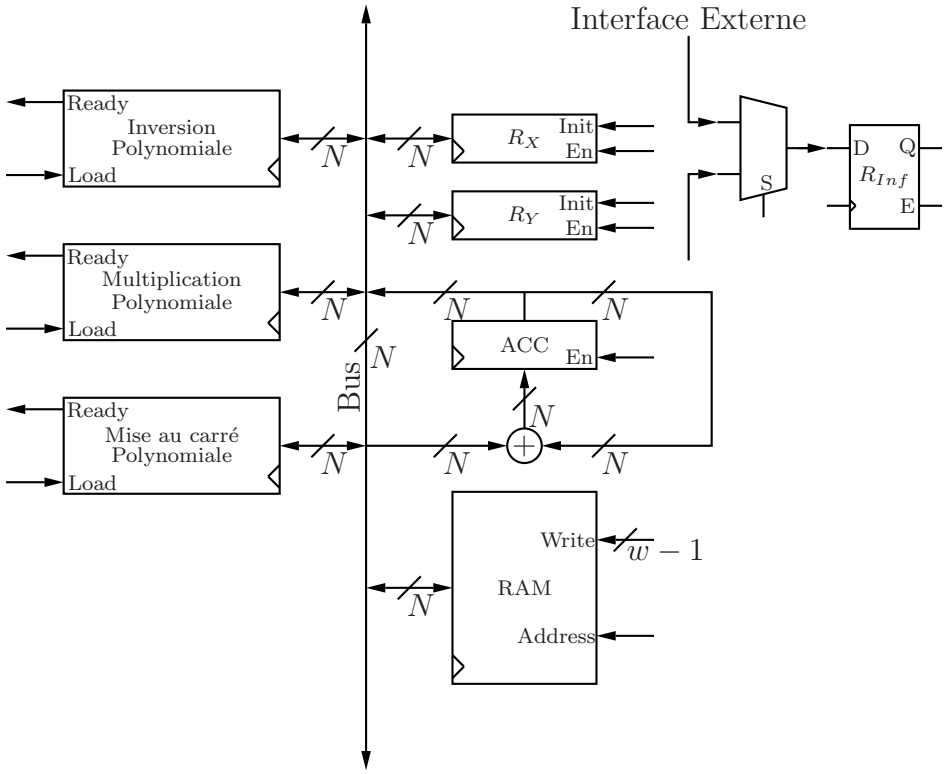


Fig. 16.2: Schéma du processeur

que l'échange de clef Diffie-Hellman [6], cette conversion n'est pas nécessaire puisque le scalaire est invariablement généré aléatoirement.

Nous avons proposé une méthode permettant de générer un scalaire directement dans sa représentation w-NAF. La méthode repose sur la transformation suivante appliquée à la sortie d'un générateur de bits aléatoires, en commençant par le bit le moins significatif :

$$\left\{ \begin{array}{r} \underbrace{s\,(m_{w-3}\,...\,m_1\,m_0)\,1}_{w \text{ bits}} \\ 0 \end{array} \right\} \xrightarrow{T_1} \left\{ \begin{array}{r} \underbrace{(0\,...\,0\,0)\,K}_{w \text{ chiffres}} \\ 0 \end{array} \right\},$$

où M représente la magnitude de K et s son signe. Si s est 1, alors K est négatif. La magnitude de K est donnée par $2M + 1$.

Si le chiffre le plus significatif différent de zéro est négatif suite à cette première transformation, on concatène un autre chiffre prenant la valeur 1 à gauche de la représentation.

Nous avons démontré que bien que la combinaison de ces deux transformations ne génère pas la représentation w-NAF de l'entier en entrée, les valeurs représentées par l'ensemble de sortie constituent une permutation des valeurs représentées par l'ensemble d'entrée, préservant le caractère aléatoire de la quantité transformée. De plus, l'implantation matérielle de cette transformation s'est révélée particulièrement efficace [1].

©LRTS 2005-2006

16.3 Unités arithmétiques sur GF(2^N)

La courbe elliptique a été représentée sur l'extension du corps de Galois $GF(2^N)$. Trois unités spécialisées pour l'arithmétique sur type de corps ont été développées. Les unités ont été fortement parallélisées en prenant soin de ne pas affecter le chemin critique du circuit.

Le chemin critique a été généré par l'unité d'inversion. Cette dernière doit en effet comparer les degrés de deux polynômes dont les coefficients sont définis sur $GF(2^N)$. Une structure récursive (voir figure 16.3), dont le chemin critique croit avec le logarithme de l'extension du corps de Galois, a été développée à cet effet.

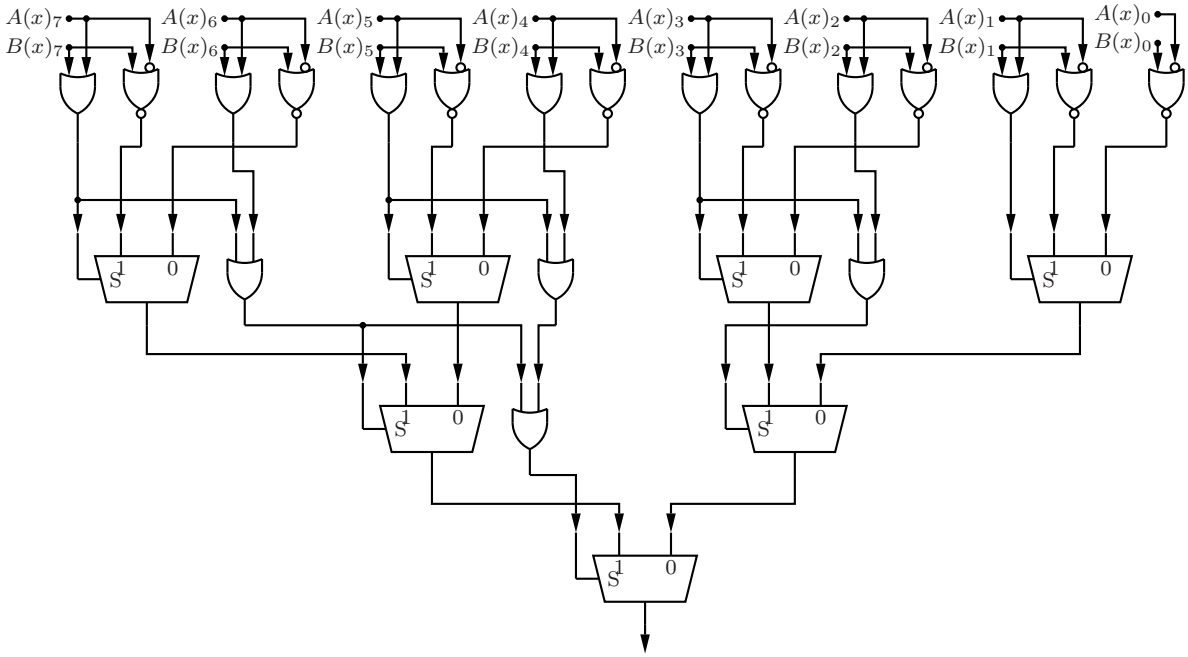


Fig. 16.3: Architecture récursive de comparaison du degré de deux polynômes ($GF(2^8)$)

L'extension choisie du corps de Galois $GF(2^N)$ étant généralement très grande en cryptographie, l'existence d'une unité dont le chemin critique croirait linéairement avec N pourrait fortement diminuer la fréquence d'opération du circuit dans son ensemble.

16.4 Conclusion

Le processeur développé a été comparé avec différents résultats trouvés dans la littérature en choisissant le temps de calcul associé à la multiplication scalaire comme métrique. Le circuit a été implanté sur deux FPGAs Altera et s'est comparé avantageusement aux résultats fournis dans la littérature, même pour une plus grande extension du corps de Galois $GF(2^N)$ tel que démontré au tableau 16.1.

Quelques pistes de recherche ont émergé de ces travaux. Il est en autre d'avis de cet auteur que les performances du circuit pourraient être considérablement améliorées en représentant les points sur la courbe elliptique sous forme projective [8].

Tab. 16.1: Temps de calcul associé à la multiplication scalaire

Publication	FPGA	N	**Temps de calcul (ms)**
	Altera EP1M350F780C5	163	0.9368
	Altera EP1S80B956C6	163	0.9279
Ernst et al., 2001 [3]	Xilinx XC4085XLA	155	1.29
Leung et al., 2000 [4]	Xilinx XCV300-4	155	6.8
Mentens et al., 2004 [5]	Xilinx XCV800-4-HQ240	160	3.801

Bibliographie

[1] Louis Dupont, Sébastien Roy et Jean-Yves Chouinard : A hardware architecture for the generation of w-NAF random integers. *In Proceedings of the 3rd International IEEE Northeast Workshop on Circuits and Systems Conference (NEWCAS '05)*, June 2005.

[2] Louis Dupont, Sébastien Roy et Jean-Yves Chouinard : A FPGA implementation of an elliptic curve cryptosystem. *In Proceedings of IEEE International Symposium on Cicuits and Systems (ISCAS'2006)*, May 2006.

[3] M. Ernst, S. Klupsch, O. Hauck et S. A. Huss : Rapid Prototyping for Hardware Accelerated Elliptic Curve Public-Key Cryptosystems. *In RSP '01 : Proceedings of the 12th International Workshop on Rapid System Prototyping*, page 24, Washington, DC, USA, 2001. IEEE Computer Society.

[4] K. H. Leung, K. W. Ma, W. K. Wong et P. H. W. Leong : FPGA implementation of a Microcoded Elliptic Curve Cryptographic Processor. *In FCCM '00 : Proceedings of the 2000 IEEE Symposium on Field-Programmable Custom Computing Machines*, page 68, Washington, DC, USA, 2000. IEEE Computer Society.

[5] Nele Mentens, Siddika Berna Ors et Bart Preneel : An FPGA implementation of an elliptic curve processor $GF(2^m)$. *In GLSVLSI '04 : Proceedings of the 14th ACM Great Lakes symposium on VLSI*, pages 454–457, New York, NY, USA, 2004. ACM Press.

[6] Diffie, Whitfield et Martin E. Hellman : New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, novembre 1976.

[7] Victor S. Miller : Use of Elliptic Curves in Cryptography. *In CRYPTO '85 : Advances in Cryptology*, pages 417–426, London, UK, 1986. Springer-Verlag.

[8] Julio López et Ricardo Dahab : Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$. *In SAC '98 : Proceedings of the Selected Areas in Cryptography*, pages 201–212, London, UK, 1999. Springer-Verlag.

©LRTS 2005-2006

Aspects matériels d'un réseau d'antennes intelligent dédié au *Wi-Fi*

Louis Dupont, *Professionnel de recherche*
Sébastien Roy, *Responsable de projet*

Résumé – Dans le cadre du projet de point d'accès pour réseaux sans fil avec grand réseau d'antennes et sélection de sous-ensembles, une architecture matérielle reposant sur le codesign matériel/logiciel est élaborée. L'architecture vise spécialement le standard *802.11b* exploitant un réseau d'antennes.

Abstract – In the context of the Wi-Fi access point with large antenna network and subset selection project, a hardware architecture based on hardware/software co-design is developped. The architure targets the *802.11b* standard in the context of an antenna network.

17.1 Analyse des spécifications de la couche physique pour les systèmes *802.11b*

De l'étude de la norme *802.11b* [1] s'est dégagé un découplage des différentes unités constituant la chaîne de communication tel qu'illustrées à la figure 17.1.

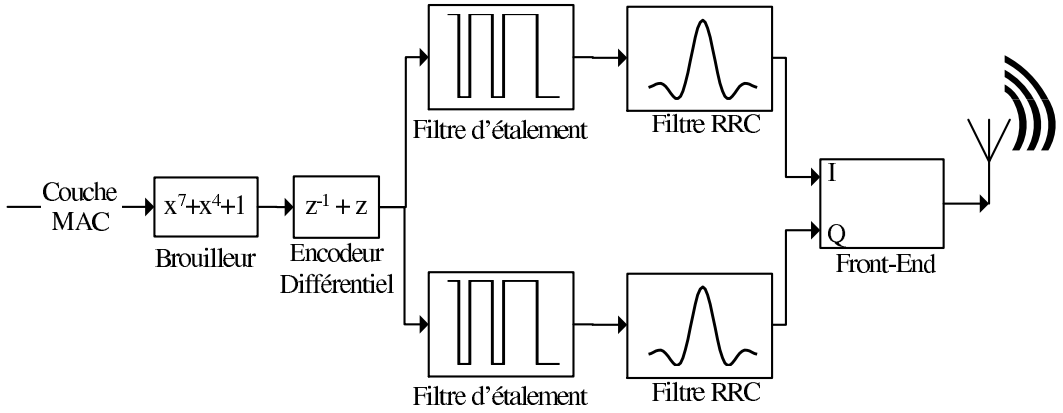


Fig. 17.1: Chaîne de communication

La norme demeure floue sur certains aspects. Entre autres, un état initial est spécifié pour le brouilleur. Paradoxalement, la norme spécifie que le débrouilleur s'autosynchronise avec le brouilleur, peu importe l'état initial de ce dernier, ouvrant la porte à différentes interprétations

de la norme.

Cette ambiguïté ne pose pas de problème dans les systèmes classiques. Toutefois, si l'interprétation de la norme est cohérente entre les différents intervenants du marché, cette information pourrait être exploitée à travers le traitement spatio-temporel requis dans le cadre du projet.

Une première interprétation de la norme s'est dégagée de l'analyse des signaux transmis par un point d'accès commercial (Linksys WRT54G). L'état du brouilleur est initialisé lors de la transmission de chaque paquet à la valeur spécifiée par la norme.

L'analyse exhaustive de tous les types de points d'accès commerciaux afin de confirmer ou d'infirmer un consensus sur l'interprétation de la norme peut sembler pratiquement impossible. Heureusement, les intervenants du marché utilisent un ensemble limité de *chipsets* gérant la couche physique restreignant l'analyse à quelques fabricants.

Cette analyse sera vraisemblablement effectuée au début juillet afin de pouvoir préciser une stratégie spatio-temporelle le plus rapidement possible.

17.2 Équipement de prototypage

Le coeur du système repose sur une plateforme *Virtex-II PRO*. Toutefois, de telles plateformes ne disposent pas d'équipement permettant de transmettre ou de recevoir un signal radio. Cet équipement étant développé parallèlement par un spécialiste des circuits radio (Mario Leblanc), une alternative a été choisie afin de pouvoir valider le fonctionnement des autres éléments du point d'accès en attendant l'étape d'intégration avec la circuiterie radio.

Le laboratoire de radiocommunications et de traitement du signal a récemment fait l'acquisition de plusieurs front-ends *Quad dual band RF transceivers* (développés par Comlab Inc. pour le laboratoire et commercialisés par Lyrtech) permettant de contrôler la phase et l'amplitude (bande de base) d'un signal radio transmis dans n'importe quelle bande de fréquences utilisée en *Wi-Fi*. De plus, ce système permet à la fois de transmettre et de recevoir des signaux sur quatre antennes simultanément, permettant de vérifier le bon fonctionnement de plusieurs aspects du système relatifs au traitement spatio-temporel.

Les limites de la plateforme *Virtex-II PRO* ne s'arrêtent pas à la circuiterie radio. Les signaux en bande de base doivent être générés de même que numérisés, nécessitant deux convertisseurs numériques à analogique de même qu'analogique-numérique pour chaque antenne.

Il a été établi que ces convertisseurs seront montés sur un circuit imprimé dont la conception a été confiée à Steve Légaré (étudiant à la maîtrise). En attendant l'étape d'intégration de la plateforme *Virtex-II PRO* avec ce circuit imprimé, les plateformes Lyrtech *VHS-DAC/ADC* seront utilisées.

Ces deux plateformes combinées disposent en effet de huit convertisseurs analogique-numérique de même que numérique-analogique permettant d'accéder aux signaux en bande de base associés à chacune des quatre antennes. De plus, ces plateformes disposent de FPGAs qui permettront d'effecteur un étage de pré-traitement lié à la couche physique, en plus de multiplexer l'accès à chacune des antennes. Finalement, Lyrtech prévoit fournir la logique nécessaire pour configurer les front-ends permettant au circuit d'alterner entre réception et transmission.

L'accès électrique direct aux FPGAs est certainement le talon d'Achille des plateformes de

Lyrtech. Les deux plateformes ne disposent que d'un seul connecteur. Les caractéristiques de ces derniers étant relativement exotiques, un circuit imprimé permettant de disposer des signaux sur un support physique plus conventionnel a été conçu. La fabrication de ce circuit est actuellement en soumission.

17.3 Architecture matérielle du point d'accès

Le noyau du système repose sur un FPGA Xilinx *Virtex-II Pro*, lui-même disposant de deux processeurs *PowerPC 405* embarqués permettant de déléguer une bonne partie du traitement à une couche logicielle. Une chaîne de transmission a été conçue de façon à être accédée par l'étage de traitement logiciel à la manière d'un périphérique adressable.

Une version préliminaire de la chaîne de transmission a été testée de bout en bout avec succès. Un paquet de type Beacon annonçant un réseau sans fil a été émis par la chaîne de transmission pour être capté par une carte *Wi-Fi* commerciale, validant du même coup notre maîtrise de la couche physique *802.11b*. Cette version préliminaire utilisait les convertisseurs numérique-analogique d'une plateforme Altera spécialisée pour le traitement de signal.

La chaîne de transmission a été portée vers la plateforme Lyrtech tout en élaborant la mécanique permettant à cette dernière de collaborer avec l'étage logiciel. La dernière version de la chaîne de transmission possède ainsi une interface maîtresse sur le bus, lui permettant d'aller récupérer des données placées dans une tierce mémoire par la partie logicielle (accès DMA). La chaîne de transmission interrompt également le processeur une fois le paquet envoyé sur le canal sans-fil.

Cette seconde version de la chaîne de transmission a été testée avec succès en simulation. Les tests finaux seront effectués après réception du circuit imprimé mentionné à la section 17.2. Une fois les tests effectués, l'architecture de la chaîne sera à nouveau raffinée afin que cette dernière s'attribue une partie du traitement de la couche MAC tel que le calcul des codes de redondance cyclique.

Une chaîne de réception a également été développée et testée avec succès en simulation. Une interface doit maintenant être développée afin de pouvoir accéder à cette dernière à partir de l'étage logiciel suivi de raffinements analogues à ceux ayant conduit à l'aboutissement de la chaîne de transmission.

Le traitement spatio-temporel sera ensuite découplé avec pour objectif d'en attribuer une partie à l'étage logiciel. Des périphériques dédiés à accélérer le traitement logiciel seront ensuite élaborés en fonction du découplage choisi.

17.4 Perspectives

La stratégie spatio-temporelle se précise de plus en plus, emmenant certaines avenues de recherche, spécialement en ce qui concerne le mécanisme de récupération de l'horloge des symboles.

La conception matérielle d'un point d'accès fonctionnant à une antenne est quant à elle pratiquement terminée. Certains livrables fournis par des partenaires commerciaux devraient permettre l'intégration des chaînes de transmission et de réception, offrant un support matériel au développement logiciel.

©LRTS 2005-2006

Les aspects liés au codesign matériel/logiciel, tout spécifiquement la compréhension de la mécanique régissant le système de bus *CoreConnect* [2], de même que les mécanismes d'interruption sont maintenant maîtrisés. À partir de cet état de l'art, il est maintenant possible de concevoir des périphériques exploitant au mieux ces mécanismes.

Bibliographie

[1] IEEE : Computer society LAN MAN standards committee. wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE Std. 802.11-1999, 1999.

[2] IBM : The coreconnect bus architecture, 1999. `http://www.chips.ibm.com/products/coreconnect/docs/crcon_wp.pdf`.

Un architecture régulière de circuit d'inversion de matrice pour le traitement MIMO

Isabelle LaRoche, *Étudiante à la maîtrise*

Sébastien Roy, *Directeur de recherche.*

Résumé – Un algorithme et une architecture d'inversion de matrice pour une implantation matérielle efficace sont présentés. Basée sur la formule de Sherman-Morrison, l'architecture proposée est caractérisée par des unités de traitement construites à partir de réseaux réguliers connectés localement et par un traitement itératif simple. Elle constitue une solution idéale au traitement de réseaux d'antennes avec le critère MEQM (Minimisation de l'erreur quadratique moyenne), mais elle peut aussi être généralisée à plusieurs autres applications moyennant de légères modifications.

Abstract – A novel circuit architecture and algorithm is presented for the efficient implementation of a matrix inversion unit. Based on the Sherman-Morrison formula, the proposed architecture is characterized by regular, locally-connected arrays of processing units and simple iterative processing. While it constitutes an ideal solution for antenna array MMSE (minimum mean-square error) processing, it can also be generalized to many other applications with little effort.

18.1 Introduction

Le récepteur MIMO multi-couches décrit dans une autre section utilise la combinaison par minimisation de l'erreur quadratique moyenne (MEQM) pour calculer les poids à appliquer aux antennes de réception. Cette technique nécessite l'inverse de la matrice d'autocorrélation, $\mathbf{R_{xx}^{-1}}$, dans le calcul des poids. Le but du projet global dans lequel ce projet de maitrise s'insère étant d'avoir un récepteur entier sur une seule puce, il faut donc trouver un moyen efficace d'inverser la matrice $\mathbf{R_{xx}}$ sur la puce. Cette section traite d'un algorithme approximatif d'inversion de matrice très bien adapté à l'implantation matérielle. Dans un premier temps, l'algorithme choisi et ses performances dans la simulation du récepteur sous Matlab sont décrits. Dans un deuxième temps, la réalisation en VHDL de cet algorithme est présentée.

18.2 Algorithme d'inversion de matrice

Comme nous l'avons mentionné précédemment, le calcul des poids optimaux selon le critère MEQM nécessite l'inversion de la matrice d'autocorrélation $\mathbf{R}_{xx}^{-1}$. L'implantation sur puce d'un algorithme d'inversion de matrice n'est pas une tâche facile. L'algorithme retenu dans le projet décrit utilise la formule de Sherman-Morrison [2]. Cette formule, qui est un cas spécial du lemme d'inversion de matrice, permet le calcul aisé de l'inverse d'une matrice ayant subit une légère modification si l'inverse de la matrice originale est connu. Toutefois, la modification doit avoir la forme suivante :

$$\mathbf{u} \otimes \mathbf{v} = \mathbf{u}\mathbf{v}^{\mathbf{H}},$$

où $\mathbf{u}$ et $\mathbf{v}$ sont des vecteurs et $\otimes$ dénote le produit externe. Puisque ce produit donne nécessairement une matrice ayant une seule valeur propre non nulle, on dit qu'il s'agit d'une *mise à jour de rang 1*. À partir de l'inverse de la matrice originale et des modifications qui lui ont été apportées, on peut trouver l'inverse de la matrice modifiée comme suit :

$$(\mathbf{A^{-1}} + \mathbf{u} \otimes \mathbf{v})^{-1} = \mathbf{A^{-1}} - \frac{(\mathbf{A^{-1}u}) \otimes (\mathbf{v} \cdot \mathbf{A^{-1}})}{1 + \mathbf{v} \cdot \mathbf{A^{-1}u}}. \tag{18.1}$$

Elle s'applique très bien au problème de l'inversion de la matrice d'autocorrélation $\mathbf{R_{xx}}$ puisque celle-ci se définit comme étant la somme d'une matrice identité et de la somme des produits des vecteurs canaux par leur conjugué (formule 14.2). Comme ces derniers constituent des mises à jour de rang 1, l'application de (18.1) est naturelle. En utilisant une notation différente, on a :

$$\mathbf{R}_i^{-1} = (\mathbf{R}_{i-1} + \mathbf{c}_i\mathbf{c}_i^H)^{-1} = \mathbf{R_{i-1}^{-1}} - \frac{(\mathbf{R_{i-1}^{-1}}\mathbf{c}_i\mathbf{c}_i^H\mathbf{R_{i-1}^{-1}})}{1 + \mathbf{c}_i^H\mathbf{R}_{i-1}^{-1}\mathbf{c}_i}, \tag{18.2}$$

où $\mathbf{R}_i = \sigma^2\mathbf{I} + \sum_{k=1}^{i} \mathbf{c}_k\mathbf{c}_k^H$, tel que $\mathbf{R}_M = \mathbf{R}_{xx}$, et $\mathbf{R}_0 = \sigma^2\mathbf{I}$.

En microélectronique, l'implantation de l'opération de division est très couteuse en temps d'exécution et en espace. Il est donc intéressant de contourner le problème en éliminant la division présente dans la formule. En introduisant un facteur d'échelle approprié, la division devient une multiplication. L'équation 18.2 devient alors :

$$\begin{aligned} \mathscr{R}_i^{-1} &= (\alpha_{i-1} + \mathbf{c}_i^H\mathscr{R}_{i-1}^{-1}\mathbf{c}_i)\left(\mathscr{R}_{i-1} + \frac{\mathbf{c}_i\mathbf{c}_i^H}{\alpha_{i-1}}\right)^{-1} \\ &= \mathscr{R}_{i-1}^{-1}(\alpha_{i-1} + \mathbf{c}_i^H\mathscr{R}_{i-1}^{-1}\mathbf{c}_i) - \\ &\quad (\mathscr{R}_{i-1}^{-1}\mathbf{c}_i\mathbf{c}_i^H\mathscr{R}_{i-1}^{-1}), \end{aligned} \tag{18.3}$$

où $\mathscr{R}_i^{-1} = \alpha_i\mathbf{R}_i^{-1}$ et le facteur d'échelle α est exprimé comme suit :

$$\alpha_{i+1} = \alpha_i(\alpha_i + \mathbf{c}_{i+1}^H\mathscr{R}_i^{-1}\mathbf{c}_{i+1}), \tag{18.4}$$

avec $\alpha_0 = 1$.

18.3 Simulation Matlab

Une simulation de l'algorithme a été faite sous Matlab pour montrer sa performance à l'intérieur du récepteur MIMO. La figure 18.1 montre les probabilités d'erreur pour les deux versions de la formule Sherman-Morrison ainsi que pour la fonction d'inversion de Matlab. Dans un premier temps, on remarque que les deux versions de la formule donnent exactement les mêmes résultats. Il est donc évident que la version modifiée est équivalente à la version originale. Dans un deuxième temps, on remarque que les récepteurs utilisant les formules de Sherman-Morrison offrent une meilleure probabilité d'erreur par bit que celui utilisant l'inversion par Matlab. L'amélioration moyenne d'environ 3 dB s'explique par la plus grande robustesse des méthodes itératives par rapport aux méthodes classiques d'inversion telle que celle employée par Matlab [1].

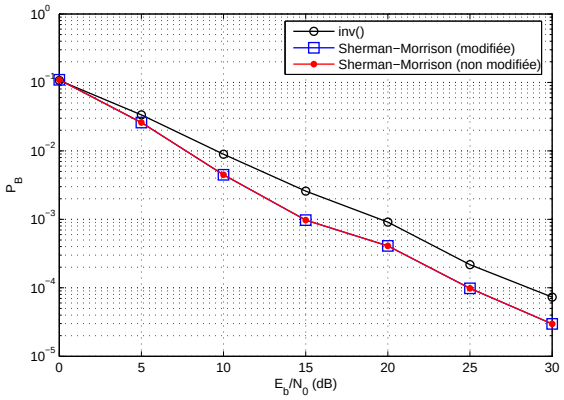


Fig. 18.1: Probabilité d'erreur par bit du récepteur d'un système (4,4)

18.4 Description matérielle

Le circuit ayant été conçu est montré à la figure 18.2. Ce circuit utilise principalement des réseaux systoliques pour effectuer les opérations de l'équation 18.3. Une simulation du circuit sous Modelsim a montré sa faisabilité après quelques améliorations du contrôle du débordement. La fréquence maximale obtenue lors d'une synthèse du circuit avec le logiciel ISE de Xilinx a été de 108.3 MHz. De plus, une seule inversion de matrice nécessite $4M^2$ coup d'horloge, en exploitant $M^2 + M$ cellules de traitement simples. Un temps d'exécution linéaire est possible en utilisant du pipelinage entre les itérations et entre les inversions.

18.5 Conclusion

Dans un premier temps, nous avons présenté la formule de Sherman-Morrison pour l'inversion de matrice ainsi que les modifications que nous y avons apportées. Ensuite, nous avons montré les résultats d'une simulation Monte Carlo faite sous le logiciel Matlab. Finalement nous avons décrit la structure du circuit conçu en VHDL.

©LRTS 2005-2006

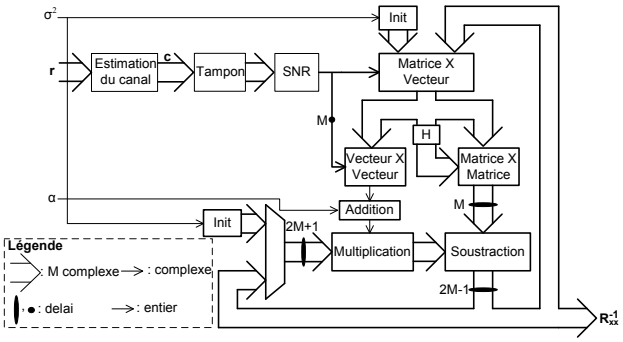


Fig. 18.2: Architecture de l'inverseur de matrice

Bibliographie

[1] T.J. Shepherd and J.G. McWhirter, "Systolic Adaptive Beamforming," *Radar Array Processing*, 1993.

[2] E.W. Weisstein, "Sherman-Morrison Formula," *From MathWorld–A Wolfram Web Resource*, http ://mathworld.wolfram.com/Sherman-MorrisonFormula.html.

FPGA implementation of a digital communication chain

Minh-Quang Nguyen, *Étudiant à la maîtrise.*
Paul Fortier, *Directeur de recherche.*

Résumé – Nous présentons l'application d'une simple mais complète chaîne de communications numériques sur un système de développement FPGA. L'application comporte les éléments suivants : modulateur, démodulateur, canal, estimateur de canal, compteur de taux d'erreurs binaires (BER). Le générateur de bruit gaussien blanc additif (AWGN) est basé sur la combinaison de la méthode de Box-Muller et du théorème de la limite centrale. Le canal de Rayleigh et l'estimateur de canal sont basés respectivement sur la méthode de Young et Beaulieu et la méthode d'interpolation par sinus cardinal. Leurs performances sont vérifiées en comparant les simulations numériques avec l'opération réelle sur le matériel.

Abstract – We present an implementation of a simple but complete digital communication chain on an FPGA development system. The implementation has the following elements : modulator, demodulator, channel, channel estimator and bit error rate (BER) counter. The additive white Gaussian noise (AWGN) generator is based on the combination of the Box-Muller method and the Central Limit Theorem. The Rayleigh channel and channel estimator are based on Young and Beaulieu's method and the sinc interpolator method, respectively. Their performances are verified by comparisons between computer simulations and true hardware operation.

19.1 Introduction

We present the implementation of a communication chain on an FPGA development board. The selected FPGA development board is provided by the Canadian Microelectronics Corporation and manufactured by Altera Corporation. The implementation of the system is coded using Very high speed integrated circuit Hardware Description Language (VHDL) and some IP cores written in the proprietary Altera Hardware Description Language (AHDL), which is a high level and modular language used by Altera.

The system consists of a modulator, a demodulator, a channel and a channel estimator. The modulator and the demodulator are implemented with BPSK, QPSK, 16-QAM and 64-QAM modulation schemes. The channel is either pure AWGN or Rayleigh fading using the algorithm developed in [1, 2]. The channel estimator estimates the Rayleigh fading coefficients.

Using a Stratix FPGA device from Altera as target, the design flow associated with the Altera Quartus II software is shown in Figure 19.1 [3]. However, we have adapted the Altera design flow to fit our design goals. This modified design flow was applied throughout the design.

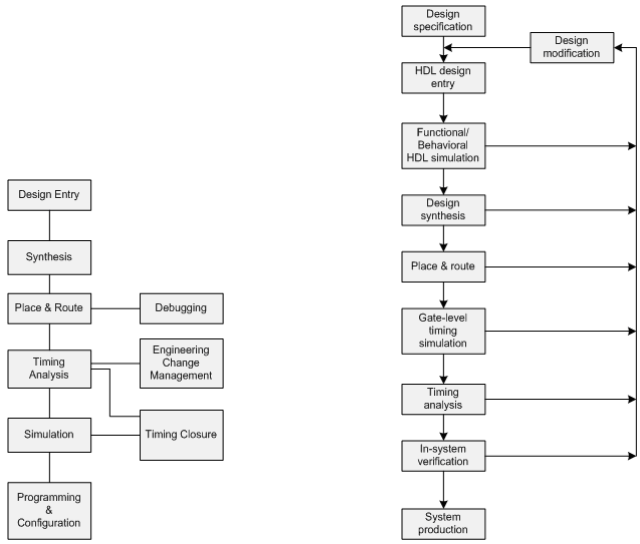


Fig. 19.1: Altera Quartus II software design flow and modified flow.

19.2 Implementation of the AWGN channel

The implementation of the AWGN channel uses the mixed method (Box-Muller and Central Limit Theorem) described in [1]. The parameters of the Box-Muller AWGN generators are shown in Table 19.1 [1].

B	K	m	δ	m'	δ'
6	5	7	0.467	7	0.5

Tab. 19.1: Parameters of the Box-Muller AWGN generator

The architecture of the AWGN generator is illustrated in Figure 19.2.

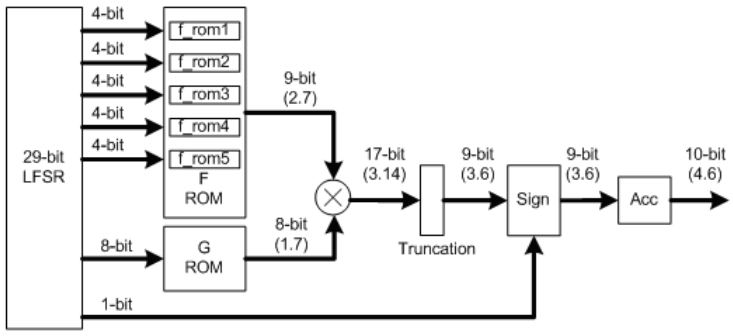


Fig. 19.2: Architecture of the AWGN generator.

Table 19.2 shows the output statistics of the generator.

Figure 19.3 shows the normalized density of the generator (10-bit precision) obtained with 2.10^9 samples and the ideal Gaussian (Normal) density.

Parameters	Implemented (fixed point 4.6)	Ideal (fixed point 4.6)
Mean	-0.3792	0
Standard deviation	63.43	64
Maximum	511	511
Minimum	-512	-512

TAB. 19.2: Output statistics of the AWGN generator.

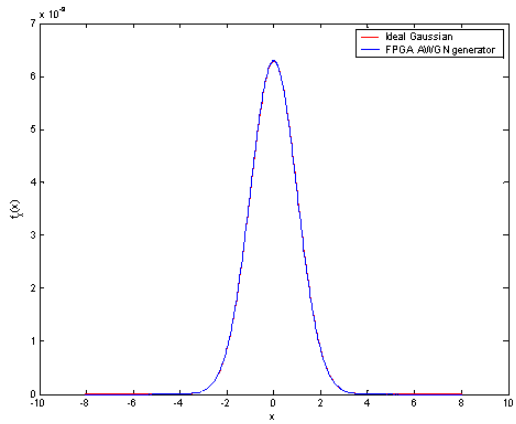


FIG. 19.3: Normalized density of the AWGN generator.

The interface of the AWGN channel component is shown in Figure 19.4 and the implementation results are shown in Table 19.3

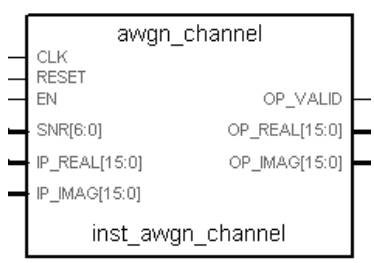


FIG. 19.4: AWGN channel interface.

Logic cells	Memory bits	DSP block 9-bit	Maximum clock (MHz)
730	2048	0	147.02

TAB. 19.3: Implementation results of the AWGN channel.

Since the accumulator is used to accumulate four independent Box-Muller variables to generate a single sample output, the real output rate of the AWGN generator is equal to one-fourth the maximum frequency of the implementation. Thus, the generator can produce random Gaussian noise outputs at 36.76 MHz.

©LRTS 2005-2006

19.3 Implementation of the Rayleigh fading channel

The implementation of the Rayleigh fading channel uses the IDFT method that was proposed in [2]. Figure 19.5 shows the architecture of the Rayleigh random variable generator.

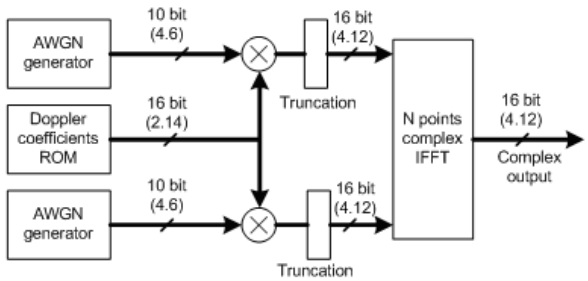


Fig. 19.5: Architecture of the Rayleigh fading generator.

We assume a mobile moving at a speed of 120 km/h and a carrier frequency of 900 MHz. Thus, the maximum Doppler frequency is 100 Hz. The number of IDFT points is chosen according to the required accuracy of the correlation among the generated samples. The parameters of the generator are shown in Table 19.4.

Parameters	Value
Maximum Doppler frequency	100 Hz
Sampling frequency	4000 Hz
Doppler filter coefficients precision	16-bit fixed point [2.14]

Tab. 19.4: Parameters of the Rayleigh fading generator.

Figure 19.6 shows the output signal envelope (first 500 samples), and histogram of the generator obtained with 6.4×10^5 samples.

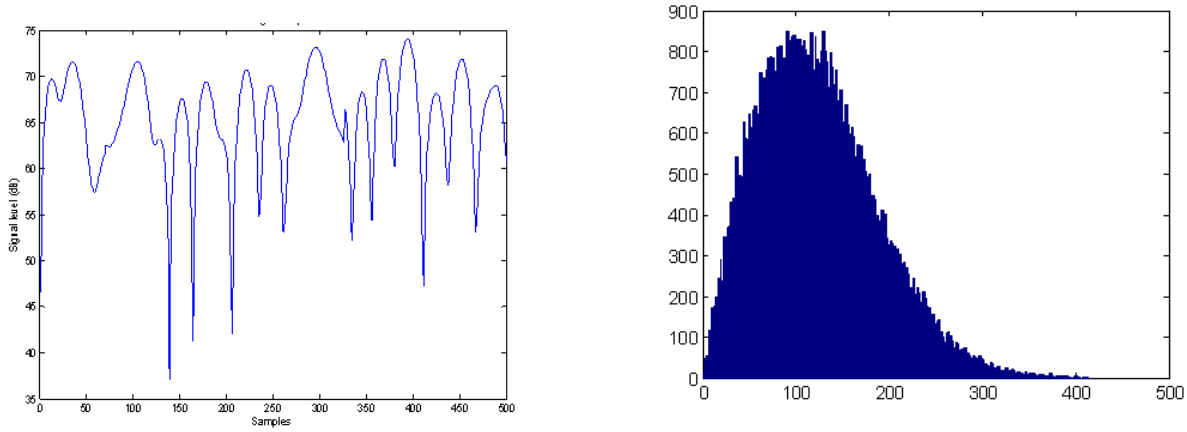


Fig. 19.6: Output signal envelope and histogram of the Rayleigh fading generator.

The output autocorrelation of the Rayleigh fading generator is compared with the theoretical

zeroth order Bessel function of the first kind and a Matlab simulation for IFFT lengths N equal to 256 and 1024 in Figure 19.7.

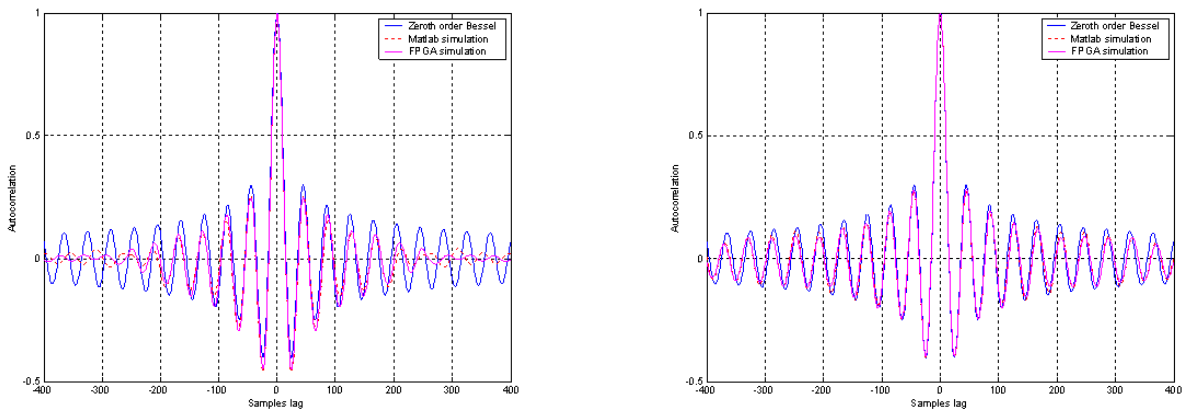


FIG. 19.7: Output autocorrelation for the Rayleigh generator ($N = 256$ and $N = 1024$).

In this figure, we can see that the output autocorrelation function of the Rayleigh fading generator is very close to the ideal theoretical function. Since the output signal is finite in time, the observation window is finite. Thus, the simulated autocorrelation tends towards the ideal autocorrelation function when the observation time tends to infinity (i.e. the IFFT length tends to infinity). Hence, we must choose the IFFT length suitable to the system requirements. Table 19.5 shows the implementation results of the Rayleigh fading generator with IFFT length of 256 and 1024 [6].

IFFT length	Logic cells	Memory bits	DSP block 9-bit	Maximum clock (MHz)
256	1860	18848	14	149.14
1024	1912	58784	14	148.30

TAB. 19.5: Implementation results of the Rayleigh fading generator.

19.4 Implementation of the Rayleigh fading channel estimator

The channel estimator is divided in two main sections which correspond to successive phases. The first phase performs an estimation of the fading coefficients using the method proposed in [4]. The second phase performs compensation for the received signals in order to obtain an estimate of the transmitted signals. The pilot-symbol-aided-modulation (PSAM) sounding technique is used to estimate and compensate for the Rayleigh fading channels. In our estimator design, we use a Rayleigh fading channel length of 256 samples in order to reduce the complexity of the system. Thus, the K and L parameters [4] are 8 and 20, respectively. Figure 19.8 shows the estimation results of the Rayleigh fading estimator with BPSK modulation and channel characteristics as shown in Table 19.4 with a rectangular window applied to the interpolation coefficients.

©LRTS 2005-2006

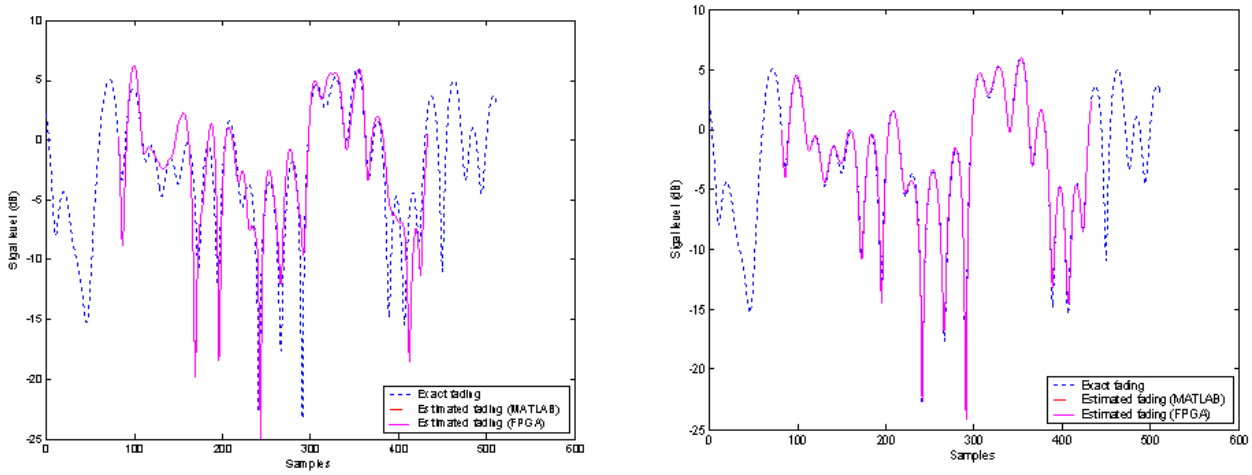


Fig. 19.8: Channel fading estimation results for the BPSK scheme.

19.5 Implementation results of the digital communication chain

System verification

We present the verification of the whole system using either the Altera SignalTap II logic analyzer [3] tool or the "hardware-in-the loop" environment. The SignalTap II logic analyzer is the embedded logic analyzer which allows the capture of signal activities from internal FPGA nodes while the system under test is running. Internal memory resources are required in order to save samples when the logic analyzer is triggered and the test is streamed data off chip via the JTAG port. The device under test includes addition components such as the data pattern generator and the BER counter as shown in Figure 19.9

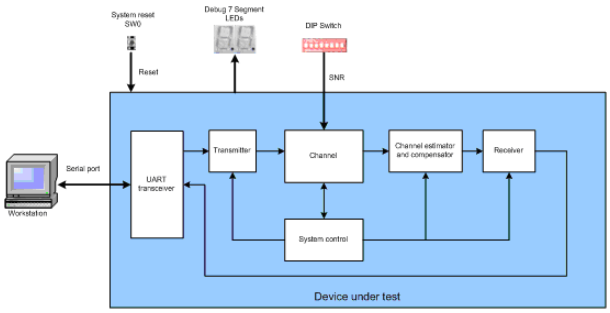
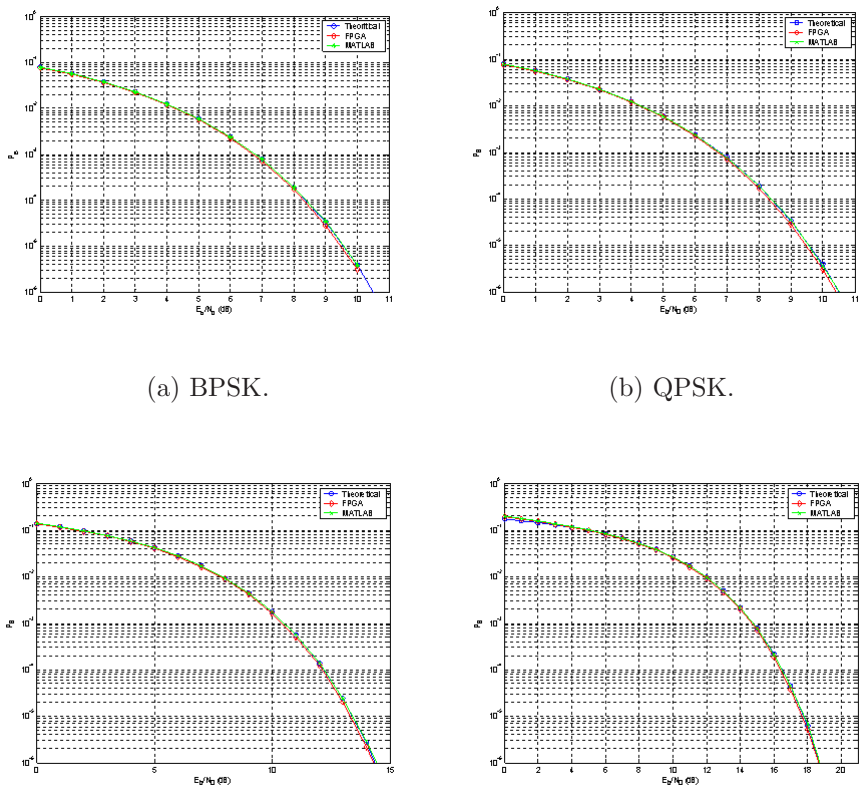


Fig. 19.9: Device under test with hardware-in-the-loop simulation environment.

AWGN channel

Here, we will take a look at the implementation results for BPSK, QPSK, 16-QAM and 64-QAM over the AWGN channel. The implementation results consist of the performance of the system, the resource usage and the maximum operation frequency, as well as the maximum data rate. Figure 19.10 shows the bit error probability as a function of the signal-to-noise ratio for BPSK, QPSK, 16-QAM and 64-QAM modulations over an AWGN channel. Table 19.6 and 19.7 show the performance and resource usage of the systems over AWGN channel.



(a) BPSK.

(b) QPSK.

(c) 16-QAM.

(d) 64-QAM.

FIG. 19.10: Performances of the system over an AWGN channel.

Modulation	Maximum frequency (MHz)	Maximum Data Rate (Mbps)
BPSK	139.61	34.9
QPSK	141.38	70.69
16-QAM	141.38	141.38
64-QAM	122.41	183.61

TAB. 19.6: Performances of the systems over an AWGN channel.

©LRTS 2005-2006

Modulation	Logic cells	Memory bits	DSP blocks 9-bit
BPSK	368	2048	3
QPSK	742	2048	6
16-QAM	772	2048	6
64-QAM	810	2048	6

Tab. 19.7: Total resource usage of the systems over an AWGN channel.

Rayleigh fading channel

In this section, we will take a look at the implementation results for BPSK, QPSK, 16-QAM and 64-QAM over a Rayleigh fading channel. Figure 19.11 shows the bit error probability as a function of the signal-to-noise ratio for BPSK, QPSK, 16-QAM and 64-QAM modulations over a Rayleigh fading channel using either the rectangular window or the Hamming window applied to the interpolation coefficients.

In this figure, we can see the differences between the perfect estimation curves and the Matlab/FPGA curves. As compared with the case of perfect estimation, the Matlab simulation results are degraded by about 2.5 dB.

Since the interpolation coefficients are applicable for both the rectangular and the Hamming windows, we need only to change the content of the interpolation coefficients ROM. Therefore, the implementation results of the systems over a Rayleigh fading channel for BPSK, QPSK, 16-QAM and 64-QAM in both cases are the same. Tables 19.8 and 19.9 summarize the implementation results of the systems.

Modulation	Maximum frequency (MHz)	Maximum Data Rate (Mbps)
BPSK	102.77	14.68
QPSK	92.52	26.43
16-QAM	90.88	51.93
64-QAM	88.50	75.86

Tab. 19.8: Performances of the systems over an Rayleigh fading channel.

Modulation	Logic cells	Memory bits	DSP blocks 9-bit
BPSK	6182	33632	78
QPSK	7963	33632	94
16-QAM	8080	33632	94
64-QAM	8125	33632	94

Tab. 19.9: Total resource usage of the systems over an Rayleigh fading channel.

19.6 Conclusion

We have implemented a digital communication chain using baseband BPSK, QPSK, 16-QAM and 64-QAM modulations over an AWGN channel and a Rayleigh fading channel. These imple-

mentations used less resource, and a simple architecture with respect to a straight forward implementation while maintaining the performances of the systems. The verification of the systems was done using either the integrated tool from Altera, namely the SignalTap II logic analyzer, or the "hardware-in-the-loop" environment. The implementations use no more than 10 percent of the available logic cells, 1 percent of the embedded memory and 53 percent of the embedded DSP elements of the Stratix EP1S80B956C6 device. A block-based implementation approach was employed, i.e. each of the components in our systems were coded as a distinct HDL entity in order to easily manage and integrate the components. This modular, component-based approach provides flexibility, allowing for easy design adjustments and re-use in future designs. We tested the systems using the SignalTap II logic analyzer tool and the "hardware-in-the-loop" environment. The performances of the systems with the Hamming window are superior to the performances using the rectangular window in both Matlab simulations and FPGA implementations. The results obtained show that the performances of the implemented digital communication chain are very close to the computer simulation results in the AWGN channel but not quite as close to the computer simulation results in a Rayleigh fading channel due to the use of integer arithmetic in the implementation.

Bibliographie

[1] A. Ghazel, E. Bouillon, J. L. Danger, G. Gulak, and H. Laamari, "Design and performance analysis of high speed AWGN communication channel emulator," in PACRIM, 2001.

[2] D. J. Young and N. C. Beaulieu, "The Generation of Correlated Rayleigh Random Variates by Inverse Discrete Fourier Transform," *IEEE Transaction on Communications*, vol. 48, pp. 1114–1127, 2000.

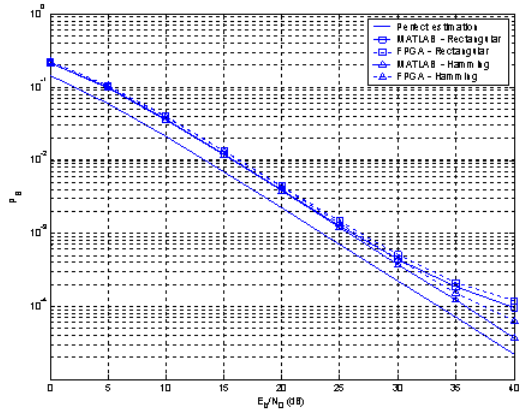
[3] Altera, *Introduction to Quartus II.* Altera Corporation, 2003

[4] X. Tang, M. S. Alouini, and A. J. Goldsmith, "Effect of Channel Estimation Error on M-QAM BER Performance in Rayleigh Fading," *IEEE Transaction on Communications*, vol. 47, pp. 1856–1864, 1999.

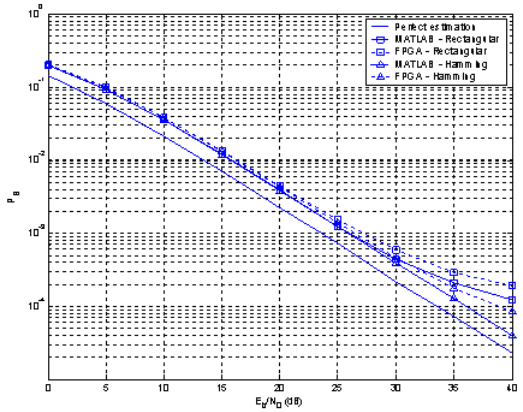
[5] J. J. Ossana, "A Model for Mobile Radio Fading due to Building Reflections : Theoretical and Experimental Fading Waveform Power Spectra," *Bell Systems Technical Journal*, vol. 43, pp. 2935–2971, 1964.

[6] Altera, *FFT MegaCore Function User Guide.* Altera Corporation, 2002

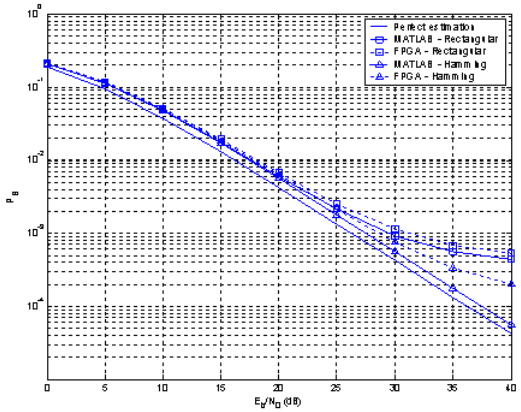
©LRTS 2005-2006



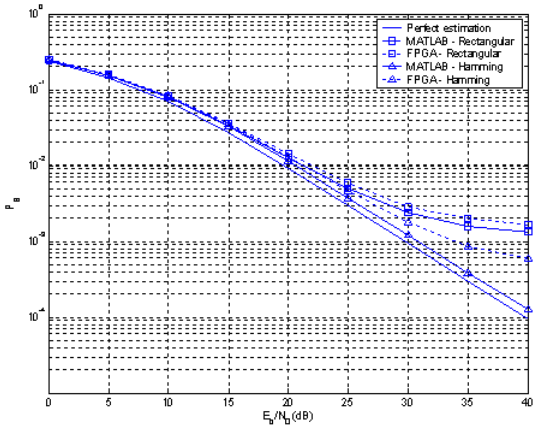
(a) BPSK.



(b) QPSK.



(c) 16-QAM.



(d) 64-QAM.

FIG. 19.11: Performances of the system over an Rayleigh fading channel.

IV

Fusion de données

Table des Matières

Utilisation des réseaux de Kohonen dans le processus de classification 119

Representing fuzzy membership functions into random set formalism 125

Vérification des protocoles de communication et d'agrégation en fusion d'informations 133

Identification de l'impact de la fusion de l'information de la STANAG 1241 sous différents cadres de raisonnement 139

Adaptive combination rule for the evidence theory . . 143

General Measure of Uncertainty in Fuzzy Evidence Theory 151

Calcul d'incidence généralisé modifié 157

Scope of Contribution to Maritime Surveillance 165

Utilisation des réseaux de Kohonen dans le processus de classification

Miroslava Ivanova, *Étudiante au maîtrise*
Dominic Grenier, *Directeur de recherche.*
Eloi Bossé, *Co-directeur de recherche.*

Résumé – On présent ici une étude sur l'utilisation des réseaux de Kohonen dans l'élaboration d'un système à classificateurs multiples utilisant la boîte à outils SOM de Matlab. La première étape consiste à la construction d'un système qui utilise la technique de quantification de vecteur d'apprentissage, un réseau compétitif à classification supervisée. Ensuite, un réseau à organisation autonome classification non supervisée sera intégré. La construction du système et les résultats des simulations sont présentés.

Abstract – We present a study over the place of Kohonen networks in the construction of multiple classifier system by using Matlab SOM toolbox. In the construction of the simulated system Learning Vector Quantization technique is applied which is competitive network for supervised classification and unsupervised SOM classification. We show the construction of that system and the simulation results obtained by test experiments.

20.1 Introduction

Un système de classification utilisant les réseaux de Kohonen dans le bloc d'entraînement sera présenté. Le schéma du processus est présenté à la figure 20.1. La première étape d'entraînement est effectuée par un réseau à organisation autonome "Self Organizing Map (SOM)" et donne un réseau entraîné. Ce résultat est envoyé à l'entrée du module de quantification de vecteur d'apprentissage "Learning Vector Quantization (LVQ)" qui effectue un raffinement de la solution. Après cette procédure, l'étape d'entraînement est considérée terminée. Ensuite, le test avec le classificateurs k-plus proches voisins est effectué. Le test k-plus proches voisins utilise la distance Euclidienne pour la mesure de distance entre deux vecteurs. La construction du classificateur multiple utilise Dempster-Shafer [1] pour pondérer les résultats et extraire le résultat final.

20.2 Réseaux à organisation autonome

Les réseaux SOM à dispositif de Kohonen ont été inventé par Teuvo Kohonen [2][3]. Ils fournissent une manière de représenter des données multidimensionnelles dans un espace à dimension

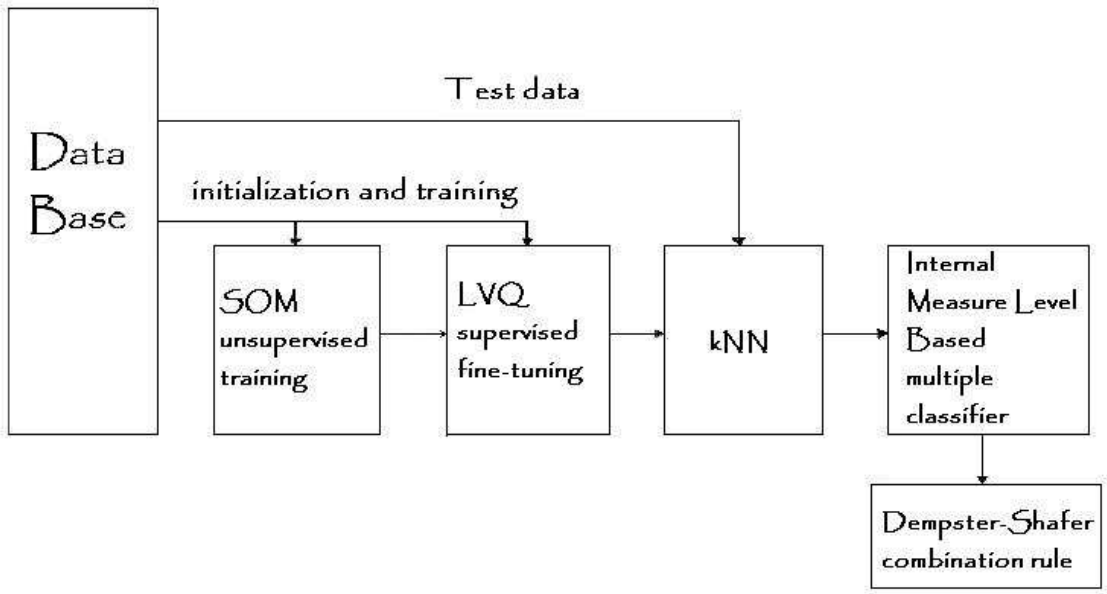


FIG. 20.1: Schéma du processus

réduite, habituellement à une ou deux dimensions. Ce processus, de réduire la dimensionnalité des vecteurs, est essentiellement une technique de compression des données connue sous le nom de quantification de vecteurs. En outre, la technique de Kohonen crée un réseau qui sauvegarde l'information de manière à ce que tous les rapports topologiques de l'ensemble des données d'entrées soient maintenus. Un des aspects les plus intéressants des SOMs est qu'ils apprennent à classifier les données sans supervision. Le réseau est créé d'un treillis de nœuds, qui est entièrement relié à la couche d'entrée. Chaque nœud a une position topologique spécifique et contient un vecteur de poids de la même dimension que les vecteurs d'entrée. Il n'y a aucun raccordement latéral entre les nœuds dans le treillis. Le SOM n'a pas besoin de connaître la valeur de sortie désirée, ce qui diffère avec plusieurs autres types de réseaux. Au lieu de cela, lorsque les poids des nœuds concordent avec le vecteur d'entrée, ce secteur du treillis est optimisé afin de ressembler plus étroitement aux données pour une classe à laquelle le vecteur appartient.

De façon plus formelle, nous pouvons dire que le SOM définit la topologie de l'espace de données d'entrée $\mathbb{R}^n$ sur vecteurs bi-dimensionnels de nœuds. Le vecteur paramétrique de référence $m_i \in \mathbb{R}^n$ est associé à chaque nœud i. La réponse est la meilleure association produite à partir de la comparaison du vecteur d'entrée $\mathbb{R}^n$ et de m_i. Habituellement, le SOM est défini comme une projection non-linéaire de la fonction de densité de probabilité des données d'entrée multi-dimensionnelles sur un affichage bi-dimensionnels [4]. Si $x \in \mathbb{R}^n$ est le vecteur des données d'entrée, il est comparé à tous les m_i dans la métrique choisie, si la distance euclidienne est utilisée, la plus petite valeur définie le nœud avec la meilleure correspondance, signifié par l'indice c :

$$c = \arg\min_i \{\|x - m_i\|\} \tag{20.1}$$

Selon les valeurs du paramètre m_i, x est tracé sur le nœud c. Les nœuds réagissant à la même entrée sont ceux topographiquement proches jusqu'à une certaine distance. Nous pouvons déclarer

que les valeurs utiles de m_i peuvent être vues comme des limites de convergence du processus d'apprentissage et que les valeurs initiales de $m_i(0)$ peuvent être aléatoires :

$$m_i(t+1) = m_i(t) + h_{ci}(t)[x(t) - m_i(t)] \tag{20.2}$$

là où t est la coordonnée de temps discret et un nombre entier. $h_{ci}(t)$ est le noyau du voisinage, c'est une fonction définie au-dessus des points de treillis. Habituellement,

$$h_{ci}(t) = h(\|r_c - r_i\|, t) \tag{20.3}$$

où $r_c \in \mathbb{R}^2$ et $r_i \in \mathbb{R}^2$ sont les vecteurs de rayon des nœuds du vecteur c et i. Avec l'augmentation de $\|r_c - r_i\|$, $h_{ci} \to 0$.

Deux définitions de $h_{ci}()$ peuvent être présentées. La première est reliée à un ensemble de vecteurs autour du nœud c dénoté par N_c par lequel $h_{ci} = \alpha(t)$ si $i \in N_c$ et que $h_{ci} = 0$ si $i \notin N_c$. Ainsi que $\alpha(t)$ est une fonction monotonique décroissante en temps. Une autre définition peut être définie en termes de la fonction gaussienne

$$h_{ci} = \alpha(t).\exp(-\frac{\|r_c - r_i\|^2}{2\sigma^2(t)}) \tag{20.4}$$

où le paramètre $\sigma(t)$ définit la largeur du pas. $\alpha(t)$ et $\sigma(t)$ sont deux fonctions monotoniques décroissantes en temps et leurs définitions exactes ne sont pas critiques.

20.3 Quantification de vecteur d'apprentissage

Les LVQ sont des réseaux concurrentiels pour la classification dirigée [3] [2]. Chaque vecteur interne est assigné à une des classes de sortie. Chaque classe peut avoir un ou plusieurs vecteurs internes. Un inconnu est classifié en trouvant le vecteur interne le plus proche et en assignant l'inconnu à la classe correspondant au vecteur interne. Par conséquent, LVQ est une dérivée de règle du plus proche voisin. Il y a plusieurs variantes de LVQ, les plus communes sont LVQ1, LVQ2.1 et LVQ3. Dans notre travail nous employons LVQ1 et LVQ3.

Ce réseau emploie des règles d'étude dirigées. La quantification de vecteur d'apprentissage classifie ses données d'entrée dans les classes de sortie. Essentiellement, il détermine un espace de n dimensions dans un espace de m dimensions. Les réseaux peuvent être formés pour classifier des entrées tout en préservant la topologie inhérente de l'ensemble d'apprentissage.

LVQ1

La description de la méthode exige l'hypothèse qu'un certain nombre de vecteurs de paramètres libres m_i, appelés vecteurs internes, sont utilisés pour approximer les nombreux domains du vecteur d'entrée x par leurs valeurs à quantifier et sont placés dans l'espace d'entrée. Habituellement, à chaque classe plusieurs vecteurs internes sont assignés, alors x appartient à la classe à laquelle m_i est le plus proche. Le m_i le plus proche de x est déterminé par la distance euclidienne, le résultat est dénoté par m_c. Alors, on obtient un apprentissage qui montre comment les valeurs

©LRTS 2005-2006

de m_i minimisent les erreurs de fausse classification en utilisant la classification du plus proche-voisin. Dans ce but, $x(t)$ est défini comme échantillon d'entrée et $m_i(t)$ représente l'ordre de m_i dans le temps du domaine discret. Les équations suivantes définissent le processus LVQ1 de base :

$$m_c(t+1) = m_c(t) + \alpha(t)[x(t) - m_c(t)] \tag{20.5}$$

si x et m_c appartiennent à la même classe :

$$m_c(t+1) = m_c(t) - \alpha(t)[x(t) - m_c(t)] \tag{20.6}$$

si x et m_c appartiennent à des classes différentes :

$$m_i(t+1) = m_i(t) \tag{20.7}$$

pour $i \neq c$. Dans les équations ci-dessus, $0 < \alpha(t) < 1$ et $\alpha(t)$ peut être une fonction constante ou à décroissance monotonique en fonction du temps [5]. Dans [2], il est recommandé que α soit au commencement inférieur à 0.1. Le procédé LVQ3 est semblable mais dans ce cas-ci, les deux vecteurs internes les plus proches sont mis-à-jour simultanément. L'un d'entre eux appartient nécessairement à la classe recherchée et l'autre à une fausse classe. Il y a une région définie dans le plan grâce à ces deux vecteurs internes et le vecteur à classifier devrait tomber dans cette région.

20.4 LVQ-SOM

Dans son livre [2], Kohonen propose une combinaison de LVQ avec SOM non-supervisée. Les prototypes obtenus à partir de SOM avec la classe *a posteriori* assignée sont employées pour initialiser les prototypes de LVQ. Comme alternatif, Kohonen propose une modification de LVQ2.1 à LVQ-SOM où tout le voisinage des prototypes respectif sont mis-à-jour à chaque étape récursive. Avec ces méthodes le problème des optimums locaux dans la formation de LVQ est partiellement résolu.

LVQ et SOM peuvent aussi avoir une combinaison considérée équation d'apprentissage de base de SOM non-supervisée (20.2). Si chaque échantillon $x(t)$ d'entraînement appartient à une classe particulière et les $m_i(t)$ ont été assigné à leurs classes respectives, l'arrangement de l'apprentissage supervisé peut être utilisé. Si $x(t)$ et $m_i(t)$ appartiennent à la même classe, $h_{ci}(t)$ devrait être choisi. S'ils appartiennent à différentes classes le signe de $h_{ci}(t)$ devraient être réfuté. Dans la combinaison de LVQ-SOM, cette règle des signes est appliquée à chaque $m_i(t)$ dans le voisinage du gagnant. La première méthode exécute classification en utilisant un réseau de SOM pour l'entraînement grossier et puis, les vecteurs internes de SOM sont raffinés en utilisant l'algorithme LVQ3. Les entrées des deux réseaux sont des vecteurs de mesures invariantes. La seconde technique effectue la classification en utilisant SOM et un réseau de LVQ, tous les deux fonctionnant en tandem. D'abord le réseau de SOM est entraîné en utilisant les vecteurs de mesures invariantes. Puis, le réseau de LVQ est employé pour déterminer les coordonnées du neurone gagnant du réseau de SOM, en utilisant les entrées en mode de rappel.

20.5 Simulations et Conclusion

Nous avons présenté un système des classificateurs multiples en combinaison de LVQ-SOM dans le processus de entraînement. Ces deux types de réseaux de Kohonen sont présentement en cours de d'exploration. Les simulations seront effectuées sur le système entier pour déterminer sa capacité et les potentiels de chacune de ses parties. Jusqu'à maintenant, l'évaluation de chacune des parties du système a été effectué. Les meilleurs résultats sont présentement obtenus lorsque le système est utilisé seulement avec la technique de SOM. Nous travaillons maintenant sur l'intégration de LVQ dans le processus. L'effort principal est concentré sur la combinaison de l'arrangement de LVQ-SOM et de sa réalisation pratique pour la simulation.

La table 20.1 présente les résultats des séries d'essais ont été effectuées pour déterminer quelques paramètres comme le ratio optimal du rapport de base de données pour l'entraînement et pour les tests, la valeur k à utiliser dans l'algorithme des k-plus proches voisins, la dimension du réseau et nombre d'itérations pour l'apprentissage.

TAB. 20.1: Paramètres choisis après les essais

paramètre	valeur choisie
dimension du réseau	250
rapport de base de données	0.5
itérations pour l'entraînement	30

Les simulations sont effectuées avec la base de données d'IR_SHIP contenant 2545 images infrarouges caractérisées par 11 paramètres et représentant 8 classes des bateaux. Des résultats ont été obtenu en utilisant les réseaux SOM, le classificateur de kNN et la règle de combinaison de Dempster-Shafer. Les résultats sont présentés dans la table (20.2). Actuellement nous travaillons sur l'intégration de la technique de LVQ dans le processus de apprentissage. Le but de ce travail est d'obtenir le pourcentage de la bonne classification supérieure de 98%.

TAB. 20.2: Pourcentage de la bonne classification

Etap de procesus	Taux d'identification en %
SOM training	82.5952
SOM test	77.5392
kNN training	82.5952
kNN test	77.5392
kNN with DS training	80.7936
kNN with DS test	77.4688
kNN only training	100.00
kNN only test	88.2432

©LRTS 2005-2006

Bibliographie

[1] A. Dempster, "Upper and lower probabilities induced by multivalued mapping," *The Annals of Mathematical Statistics*, vol. 38, pp. 325–339, April 1967.

[2] T. Kohonen, *Self-Organizing Maps.* Berlin : Springer-Verlag, 2001.

[3] T. Kohonen, *Self-Organization and Associative memory.* Berlin : Springer-Verlag, 1984.

[4] T. Kohonen, J. Hynninen, J. Kangas, J. Laaksonen, and K. Torkkola, "The self organising map program package," tech. rep., Helsinki University of Technology Laboratory of Computer and Information Science Rakentajanaukio 2 C, SF-02150 Espoo, Helsinki, Finland, apr 1995. version 3.1.

[5] T. Kohonen, J. Hynninen, J. Kangas, J. Laaksonen, and K. Torkkola, "Learning vector quantization program package," tech. rep., Helsinki University of Technology Laboratory of Computer and Information Science Rakentajanaukio 2 C, SF-02150 Espoo, Helsinki, Finland, apr 1995. version 3.1.

Representing fuzzy membership functions into random set formalism

Mihai Cristian Florea, *M.Sc. Student*
Dr Dominic Grenier, *Advisor.*
Dr Anne-Laure Jousselme, *Co-advisor.*

Résumé – Nous proposons de modéliser l'information en provenance de la théorie des sous-ensembles flous dans la théorie des ensembles aléatoires. La transformation directe génère un nombre très grand d'éléments focaux qui habituellement ne peut pas être traité dans les systèmes de fusion. Nous construisons un ensemble aléatoire approximé pour réduire le nombre d'éléments focaux généré par une FMF. Cette approximation est réalisée avant le processus de fusion et le temps de calcul est réduit considérablement. La qualité de l'approximation est quantifiée par une distance entre deux ensembles aléatoires. Ainsi, on peut combiner des informations, en utilisant la règle de Dempster, sans avoir une explosion de l'algorithme.

Abstract – In this paper we propose to model information coming from fuzzy set theory into random set theory. The direct transformation of the fuzzy membership functions (FMF) creates a large number of focal elements often unmanageable in a fusion process. We propose a way to reduce the number of focal elements generated by a FMF by constructing an approximated random set. Since this approximation is made before the combination process, the computation time is considerably reduced. The quality of the approximation is quantified using a distance between two random sets. Thus, we can combine information, using Dempster's rule, without an algorithm explosion.

21.1 Introduction

Theories like fuzzy set theory, evidence theory, possibility theory were developed to cope with different aspects of uncertainty, for which probability theory was not so appropriate. In information fusion applications, we need to combine information coming from multiple and various sources and random set theory has been seen as an unified framework capable to represent all aspects of uncertainty.

Fuzzy set theory is naturally designed to model human language descriptions. For example, an expert can affirm "*the target is small*" or "*the target has a quite low speed*", information especially well represented by fuzzy membership functions (FMF). In this paper, we will present how to transform information originally represented in fuzzy set theory into random set theory. According to the cardinality of the frame of discernment, the random set representation of a FMF can involve a huge number of focal elements, and thus it will be impossible to have a

computationally tractable fusion process. To avoid the algorithm explosion due to the Dempster's combination rule, in [1] the authors proposed to truncate the results of each fusion step and to keep only a reasonable number of focal elements. In this paper, we propose to approximate the information before inserting it into the fusion process. Since the number of focal elements for an information coming from a FMF is very large, using an approximation before the fusion step, is a better solution than a truncation after the combination step and the algorithm complexity is reduced even more.

Section 21.2 briefly introduce the random set theory and the fuzzy set theory. Section 21.3 proposes three techniques of approximation to transform FMF into random sets. The quality of approximation is quantified using a distance between two random sets. In Section 21.4 we study the performances of the approximations through Monte-Carlo simulations. Section 21.5 presents the conclusion.

21.2 Theoretical basics

Consider $\Theta = \{\theta_1, \theta_2, \ldots, \theta_N\}$ to be the frame of discernment containing N exclusive and exhaustive objects or hypotheses.

The random set concept has been introduced in the early 70's [2, 3] as a generalization of the random variable concept : random sets are random elements whose values are sets, whereas random variables are random elements whose values are numbers. Hence, roughly speaking, random set theory may be viewed as a generalization of random variables and vectors.

Fuzzy set theory was developed by Zadeh [4] to model vague information such as human language descriptions ("*small, large, quick, young*"), concepts that cannot be defined by an interval with strict limits. A fuzzy set is thus a set whose boundaries are not precise, not well defined, *i.e. fuzzy*. It is a more general concept of the classical set : the membership of an element to a fuzzy set is not described by a Boolean function (as for a crisp set), but by a value in the $[0, 1]$ interval, or even in some arbitrary interval $[a, b]$. The theory of fuzzy sets is thus a generalization of the classical theory of sets.

Random set representation for FMFs

In [5], a formal connexion between random sets and fuzzy sets is proposed, fuzzy sets being considered as equivalence classes of random sets, "one-point coverages" of random sets. In [6] is stated that the FMF μ is the contour function of the random set.

In practice, the α-cut representation of a fuzzy set is used to construct the corresponding random set. Let $\underline{A} \subseteq \Theta$ be a fuzzy set defined by the membership function $\mu_{\underline{A}}$. An α-cut of $\underline{A}$ is a crisp set A_α, subset of Θ, such that :

$$A_\alpha = \{\theta | \mu_{\underline{A}}(\theta) \geq \alpha\} \tag{21.1}$$

Hence, $\underline{A}$ can be represented by the entire (infinite) stack of α-cuts $(A_\alpha, \forall \alpha \in [0, 1])$.

Suppose the fuzzy set is defined on a **discrete** domain Θ and let $0 = \alpha_0 < \alpha_1 < \alpha_2 < \cdots < \alpha_M \leq 1$ be the distinct values of the membership function $\mu_{\underline{A}}$. There are less distinct membership values α_i than elements in Θ ($M \leq \text{card}(\Theta)$). Then, the random set representation of this discrete

fuzzy set can be defined not by an infinity of α-levels (as in the continuous case) but by only M α-levels. This representation, with only M focal elements, exactly defines $\underline{A}$ in the random set representation :

$$A_i = \{\theta \mid \mu_{\underline{A}}(\theta) \geq \alpha_i\} \qquad \text{and} \qquad m_i = \frac{\alpha_i - \alpha_{i-1}}{\alpha_M} \qquad \forall i \ , \ 1 \leq i \leq M \tag{21.2}$$

with $\mathcal{X} = \{(A_i, m_i) \mid \forall i, 1 \leq i \leq M\}$.

However, M is often too large and we need to restrict the number of focal elements to only $M_0 \ll M$ so that Dempster's rule of combination can be applied without an algorithm explosion (*i.e.* using a reasonable computation time). Next section presents how to approximate the random sets.

21.3 Approximation of FMFs in the random set formalism

Three approximation techniques of FMFs

The fusion process using Dempster's rule is often computationally highly expensive because the transformations of the FMFs into random sets models involve too many focal elements. To avoid this problem, an approximation of the random set is needed. In [7] the k-l-x approximation method is presented. Here, we propose three new approximation methods.

Consider the optimal transformation based on the α-levels described by Equation (21.2) and let $0 = \alpha'_0 < \alpha'_1 < \alpha'_2 < \cdots < \alpha'_{M_0} < \max\{\mu_{\underline{A}}(\theta)\} = \alpha_M$ be a new set of α-levels, different from the optimal one ($0 = \alpha_0 < \alpha_1 < \alpha_2 < \cdots < \alpha_M \leq 1$), such that $M_0 < M$ (or even $M_0 \ll M$). If exists a α-interval $[\alpha'_{i-1}, \alpha'_i[$ such that no membership degree can be found inside of it, α'_i can be eliminated from the set of α-levels. Thus, we can consider, without loss of generality that

$$\exists \theta | \mu(\theta) \in [\alpha'_{i-1}, \alpha'_i[, \forall i \in \{1, 2, \ldots, M_0\}$$

which means that for every α-interval $[\alpha'_{i-1}, \alpha'_i[$ there exist at least one θ such that its membership degree is inside the α-interval. The random set built from the fuzzy set $\mu_{\underline{A}}$ using the non-optimal set of α-levels can be computed by $B_{M_0+1} = \{\theta \mid \mu_{\underline{A}}(\theta) = \alpha_M\}$, $m_{M_0+1} = (\alpha_M - \alpha'_{M_0})/\alpha_M$ and :

$$B_i = \{\theta \mid \mu_{\underline{A}}(\theta) \geq \alpha'_{i-1}\} \qquad \text{and} \qquad m'_i = \frac{\alpha'_i - \alpha'_{i-1}}{\alpha_M} \qquad \forall i \ , \ 1 \leq i \leq M_0 \tag{21.3}$$

The random set $\tilde{\mathcal{X}} = \{(B_i, m'_i) \mid \forall i, 1 \leq i \leq M_0 + 1\}$ is the approximation of the random set $\mathcal{X}$ obtained using Equation (21.2). The maximum number of focal elements of the random set $\tilde{\mathcal{X}}$ is $M_0 + 1$.

Let consider a discrete FMF $\mu_{\underline{A}}$ and the same set of α-levels ($0 = \alpha'_0 < \alpha'_1 < \alpha'_2 < \cdots < \alpha'_{M_0} < \max\{\mu_{\underline{A}}(\theta)\} = \alpha_M$). Let also consider the following notations :

$$\begin{cases} a_0 = 0 \quad \text{and} \quad b_0 = 0 \\ a_{M_0+1} = b_{M_0+1} = \alpha_M \quad \text{and} \\ a_i = \max\{\mu_{\underline{A}}(\theta) \mid \alpha'_{i-1} \leq \mu_{\underline{A}}(\theta) < \alpha'_i\} \quad \forall i, 1 \leq i \leq M_0 \\ b_i = \min\{\mu_{\underline{A}}(\theta) \mid \alpha'_i \leq \mu_{\underline{A}}(\theta) < \alpha'_{i+1}\} \quad \forall i, 1 \leq i \leq M_0 \end{cases} \tag{21.4}$$

©LRTS 2005-2006

Two new approximations can be made in the random set formalism :

$$C_i = \{\theta \mid \mu_{\underline{A}}(\theta) \geq \alpha'_{i-1}\} \qquad \text{and} \qquad m''_i = \frac{a_i - a_{i-1}}{a_{M_0+1}} \qquad \forall i\ ,\ 1 \leq i \leq M_0 + 1 \tag{21.5}$$

$$D_i = \{\theta \mid \mu_{\underline{A}}(\theta) \geq \alpha'_{i-1}\} \qquad \text{and} \qquad m'''_i = \frac{b_i - b_{i-1}}{b_{M_0+1}} \qquad \forall i\ ,\ 1 \leq i \leq M_0 + 1 \tag{21.6}$$

It is obvious that when $M = M_0 + 1$ and $\alpha'_i = \alpha_i, \forall i, 1 \leq i \leq M$, the three approximations methods are identical to Equation (21.2).

Evaluation of the approximation

To compare differences between an approximated random set and the optimal random set obtained from a FMF we propose to use a distance between two random sets, especially the one proposed by Jousselme *et. al.* in [8] for the Dempster-Shafer theory that can easily be transposed to the random set theory. This distance takes values in the interval $[0, 1]$. The minimum distance is obtained between two identical random sets. The maximum distance is obtain for two random sets having each one only one possible realization and the intersection of the two realizations is the empty set.

By using one of the approximation methods presented in Section 21.3, the fusion process become computationally tractable. To study the performances of the approximations, we have to compare them under the same hypotheses. Thus, we can impose for the approximations the following parameters :

1. the same number of focal elements of the approximation (or a maximum number of focal elements). Two subclasses can also be derived :
   (a) the same level set (*i.e.* the set of α-cuts)
   (b) the same α-step which is defined for a constant difference between two consecutive α-levels. Thus, the level set is constructed as :

   $$\alpha'_i = i * \alpha\text{-step} \qquad \forall i, 0 \leq i \leq \left\lceil \frac{\max \mu_{\underline{A}}(\theta)}{\alpha\text{-step}} \right\rceil - 1 = M_0$$

   The maximum number of focal elements is then $\min(M_0 + 1, M)$.

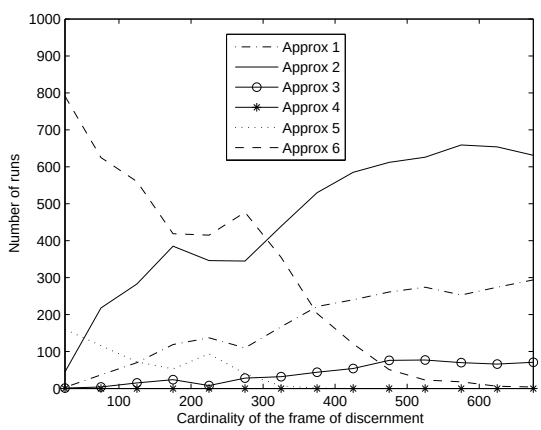
   In this situation, the best approximation is the one that minimize the distance between the approximated random set and the random set obtained without approximation.
2. the maximum ratio between the distance from the approximation to the optimal transformation and the maximum distance obtained from the optimal approximation to the ignorance. In this situation, the best approximation is the one for which the number of focal elements is minimum.

21.4 Approximations' comparison using Monte-Carlo simulations

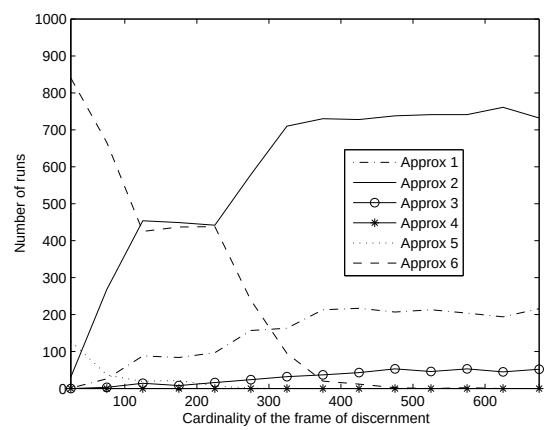
In this section we use Monte-Carlo simulations to compare the three approximation techniques presented in the section 21.3 (and denoted as Approx. 1, 2 and 3) and the k-l-x algorithm from [7] in which we considered three normalization methods : the eliminated mass is transfered to the ignorance (Approx 4), the eliminated mass is transfered to the ignorance and also is redistributed to the other focal elements (Approx 5) and the eliminated mass is redistributed to the other focal elements (Approx 6). The parameters for the k-l-x algorithm are as follows : $k = 0$, $l = 6, 10$ and $x = 0.1$. For this comparison we used the first performance criterion, imposing the maximum number of focal elements.

Here are the steps we used to generate the Monte-Carlo simulation :

1. we generate randomly discrete FMFs over a frame of discernment having $25 - 675$ elements.
2. we compute the direct transformation of the discrete FMF to the random sets formalism.
3. we generate a set of α-levels and we compute the first three approximations.
4. we approximate the random set obtained without approximation, using the k-l-x approximations.
5. we compute the distance between each approximation and the random set obtained without any approximation.
6. we choose the approximation method which has the smallest distance to the random set obtained without any approximation.



(a) 6 focal elements imposed to the approximated RS



(b) 10 focal elements imposed to the approximated RS

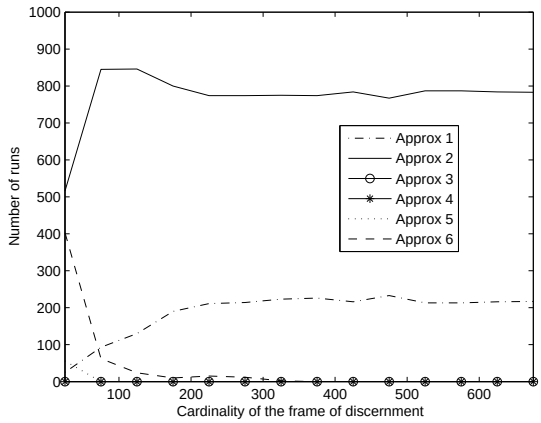
FIG. 21.1: Monte-Carlo simulations for 1000 runs. Best chosen approximation according to the cardinality of the frame of discernment when a random level-set is used for Approx 1, 2 and 3.

Figure 21.1 shows the results of the Monte-Carlo simulations for 1000 runs. For this simulation we generated randomly the α-set for each run. We remark that Approx 6 is the best approximation from the 6 approximations studied here, when the cardinality of the frame of discernment is small (less than 300). From this figure we can conclude two things :

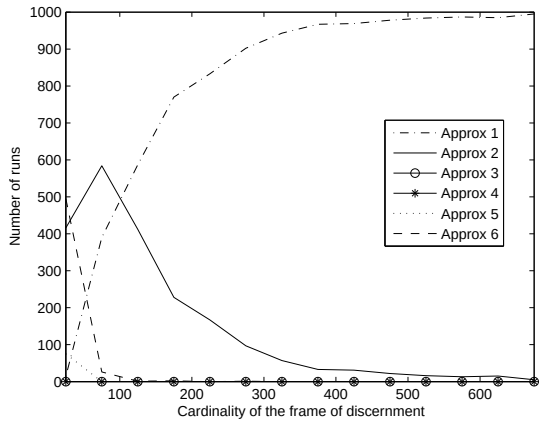
1. More the frame of discernment is larger, more the Approx 2 becomes the best approximation.
2. More the number of focal elements used to make the approximation is large, more the Approx 2 becomes the best approximation.

When the cardinality of the frame of discernment is grater than 400, Approx 2 becomes a better approximation for the majority of the situations, even when the α-levels are choosen randomly.

When the equi-distant α-levels (constant α-step) are used for the simulation (see Figure 21.2), we can remark than the k-l-x approximations are not as good as the approximations proposed in Section 21.3. When we impose 6 focal elements to the approximation, Approx 2 is the best approximation, and when we impose 10 focal elements, Approx 1 is the best approximation.



(a) 6 focal elements imposed to the approximated RS



(b) 10 focal elements imposed to the approximated RS

FIG. 21.2: Monte-Carlo simulations for 1000 runs. Best chosen approximation according to the cardinality of the frame of discernment when a constant α-step is used for Approx 1, 2 and 3.

21.5 Conclusion

In this paper, we present a method to transform a fuzzy membership function from the fuzzy set theory to the random set formalism. A direct transformation leads to a high number of focal elements when the frame of discernment is very large and this random set representation becomes unmanageable in a fusion process because of the explosion of the computation time. To reduce this number of focal elements and avoid the explosion of the algorithm, we proposed to approxi-

mate the fuzzy information before inserting it into the fusion process and three approximation techniques were presented. We used a distance between two random sets to quantify the quality of the approximation. A comparison between these techniques and the k-l-x approximation method was realized through Monte-Carlo simulations. We determined some criterion of use for the approximation techniques.

Bibliographie

[1] P. Valin and M. Boily, "Truncated Dempster-Shafer Optimization and Benchmarking," in *Sensor Fusion : Architectures, Algorithms, and Application*, S. Aerosense, Ed., Orlando, FL, Apr. 2000.

[2] D. G. Kendall, "Foundations of a Theory of Random Sets," in *Stochastic Geometry*, E. F. Hardings and D. Kendall, Eds. J. Wiley - London, 1974, pp. 322–376.

[3] G. Matheron, *Random Sets and Integral Geometry*. J. Wiley, 1975.

[4] L. A. Zadeh, "Fuzzy Sets," *Information and control*, vol. 8, pp. 338–353, 1965.

[5] I. Goodman, "Fuzzy Sets as Equivalence Classes of Random Sets," in *Fuzzy Sets and Possibility Theory*, R. R. Yager, Ed. Pergamon Press, Oxford, 1982, pp. 327–342.

[6] D. Dubois and H. Prade, "Consonant approximations of belief functions," *International Journal of Approximate Reasoning*, vol. 4, pp. 419–449, 1990.

[7] B. Tessem, "Approximations for efficient computation in the theory of evidence," *Artificial Intelligence*, vol. 61, no. 2, pp. 315–329, June 1993.

[8] A.-L. Jousselme, D. Grenier, and E. Bossé, "A new distance between two bodies of evidence," *Information Fusion*, vol. 2, no. 2, pp. 91–101, June 2001.

©LRTS 2005-2006

Vérification des protocoles de communication et d'agrégation en fusion d'informations

Gilles Ibrahim Wassi, *Étudiant au doctorat*
Dominic Grenier, *Directeur de recherche*
Anne-Laure Jousselme, *Co-directrice de recherche*
Patrick Maupin, *Scientifique de la défense (RDDC-Valcartier)*

Résumé – Nous présentons le modèle de représentation des systèmes distribués ou multiagents, sous forme de systèmes interprétés, proposé par R. Fagin, J. Halpern, Y. Moses et M. Vardi. Nous montrons sur un exemple d'application comment ce modèle peut être utilisé pour modéliser les systèmes de fusion d'informations, pour développer des protocoles de communication ou d'agrégation basés sur la connaissance que les agents du système possèdent à propos de l'état actuel du monde et pour vérifier ces protocoles.

Abstract – We present the model of representation of distributed or multi-agent systems by interpreted systems proposed by R. Fagin, J. Halpern, Y. Moses and M. Vardi. We show on an example how this model can be used to model the information fusion systems, to develop communication or aggregation protocols based on the knowledge that the agents of the system have on the current state of the world and to check these protocols.

22.1 Introduction

Le modèle de représentation des systèmes distribués ou multiagents sous forme de systèmes interprétés proposé par R. Fagin, J. Halpern, Y. Moses et M. Vardi dans [1] (cadre FHMV) est un modèle qui permet de représenter les systèmes multiagents sous forme de structures de Kripke. Basé sur la logique modale épistémique [2, 3] et la théorie des mondes possibles [1], le cadre FHMV permet de raisonner à la fois à propos de l'incertitude et à propos de la connaissance.

Dans les systèmes de fusion d'informations, on est souvent appelé à développer des protocoles de communication et d'agrégation. Ces protocoles doivent être vérifiés avant de les implémenter en pratique. L'intérêt du cadre FHMV est justement qu'il permet d'une part de modéliser formellement les systèmes de fusion d'informations (réseau de capteurs ayant par exemple pour tâche l'identification ou le pistage de cibles) et d'autre part de développer des protocoles de communication ou d'agrégation, basés sur la connaissance des agents et non sur la vérité à laquelle les agents n'ont pas accès, et de vérifier ces protocoles. La vérification peut se faire automatiquement

en utilisant les logiciels de “model checking” [4].

Après une brève description des différents composants du cadre FHMV, nous expliquons comment on assigne de la connaissance aux agents et comment l'incertitude peut y être représentée. Enfin sur un exemple que nous modélisons en utilisant le cadre FHMV, nous montrons comment développer un protocole basé sur la connaissance des agents et vérifier ce protocole.

22.2 Cadre FHMV

Chaque système multiagent est composé d'un certain nombre d'agents. Les agents peuvent être des individus, des senseurs, des composants d'un système, etc. La modélisation des systèmes multiagents en utilisant le cadre FHMV repose sur une notion fondamentale : l'*état local* d'un agent à un instant donné. En effet, chaque agent d'un système multiagent se trouve dans un état particulier à chaque instant. Cet état particulier est appelé l'état local de l'agent. L'état local, noté ℓ_i, d'un agent i regroupe toute l'information à propos du système, à laquelle l'agent i a accès. Mais il peut y avoir aussi de l'information à propos du système à laquelle aucun agent n'a accès mais qui est importante. Pour cela, on définit un autre acteur dans le système : l'*environnement*. L'état local ℓ_e de l'environnement regroupe toute l'information utile à laquelle aucun des autres agents n'a accès. On définit ensuite l'*état global* d'un système multiagent, formé de n agents, comme étant le $(n+1)$-uplet ayant la forme $(\ell_e, \ell_1, \ldots, \ell_n)$ où ℓ_e est l'état local de l'environnement et ℓ_i est l'état local de l'agent i, $i = 1, \ldots, n$. L'état global décrit l'état du système à un instant donné. Soient $\boldsymbol{L}_e$ l'ensemble des états locaux possibles de l'environnement et $\boldsymbol{L}_i$ l'ensemble des états locaux possibles de l'agent i, pour $i = 1, \ldots, n$. L'ensemble $\mathcal{G} \subseteq \boldsymbol{L}_e \times \boldsymbol{L}_1 \times \ldots \times \boldsymbol{L}_n$ est l'ensemble des états globaux possibles du système.

Pour tenir compte de l'évolution temporelle des systèmes, on définit l'*exécution*. Une exécution $r : \mathbb{N} \to \mathcal{G}$, sur $\mathcal{G}$, est une fonction du domaine temporel vers l'ensemble des états globaux $\mathcal{G}$. Le temps est défini de manière discrète par des nombres naturels. Donc $r(0)$ décrit l'état global initial du système dans l'exécution r, $r(1)$ l'état global suivant dans l'exécution r et ainsi de suite. On peut avoir plusieurs exécutions possibles dans un système. Formellement, on définit dans le cadre FHMV un *système* $\mathcal{R}$ sur l'ensemble $\mathcal{G}$ comme un ensemble non vide d'exécutions sur $\mathcal{G}$. Un système est donc formé par l'ensemble des éxécutions qu'il peut avoir. La paire (r, m), constituée de l'exécution $r \in \mathcal{R}$ et du temps $m \in \mathbb{N}$, est appelée un *point* du système $\mathcal{R}$. Si $r(m) = (\ell_e, \ell_1, \ldots, \ell_n)$, avec $r_e(m) = \ell_e$ et $r_i(m) = \ell_i$, $i = 1, \ldots, n$, alors $r_i(m)$ est l'état local de l'agent i au point (r, m) et $r_e(m)$ est l'état de l'environnement au point (r, m).

Typiquement, un système change d'état global suite aux *actions* exécutées par les agents et l'environnement. Chaque agent i dispose d'un ensemble $\mathbf{ACT}_i$ non vide d'actions possibles qu'il peut exécuter. L'environnement dispose également d'un ensemble $\mathbf{ACT}_e$ non vide d'actions possibles. L'*action nulle* Λ, qui correspond à l'action de ne rien faire, est incluse dans $\mathbf{ACT}_i$ et $\mathbf{ACT}_e$. Dans le cadre FHMV, les actions sont exécutées dans les *rounds*. Un round est la période entre deux temps discrets consécutifs. Les notions de point, de round et d'exécution sont illustrées graphiquement sur la figure (22.1) dans lequel on considère un seul agent et l'environnement.

Chaque agent suit un *protocole* pour déterminer les actions à exécuter. Intuitivement, le protocole d'un agent décrit les actions qu'il peut prendre quand il est dans un état local donné. Formellement, un protocole $P_i : \boldsymbol{L}_i \to 2^{\mathbf{ACT}_i} - \{\emptyset\}$ pour un agent i est une fonction de l'en-

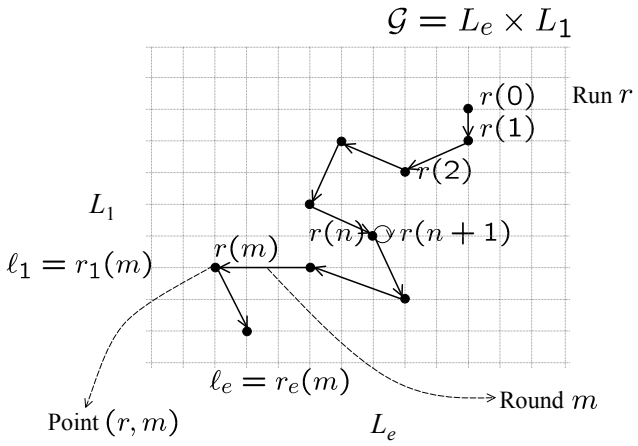


FIG. 22.1: Points, rounds et exécutions dans un système [5]

semble des états locaux $\boldsymbol{L}_i$ de l'agent i vers l'ensemble non vide des actions $\mathbf{ACT}_i$ que l'agent i peut exécuter. L'environnement suit également un protocole $P_e : \boldsymbol{L}_e \rightarrow 2^{\mathbf{ACT}_e} - \{\emptyset\}$. Notons qu'un protocole est une fonction des états locaux de chaque agent et non des états globaux du système. En effet, chaque agent a uniquement accès à l'information contenue dans sont état local. Il ne peut exécuter des actions basées sur de l'information à laquelle il n'a pas accès. Le n-uplet $(P_1, P_2, \ldots, P_n)$ formé des protocoles de tous les n agents est appelé un *protocole conjoint* P.

Pour déterminer le comportement général du système, il faut déterminer dans quel *contexte* le protocole conjoint est exécuté. En effet, le comportement d'un même système peut être différent selon le contexte dans lequel il s'exécute. Dans le cadre FHMV, on définit le contexte γ, dans lequel évolue un système, par le uplet $(P_e, \mathcal{G}_0, \tau, \Psi)$ où P_e est le protocole de l'environnement, $\mathcal{G}_0 \subseteq \mathcal{G}$ est formé des états globaux initiaux possibles du système, τ est une fonction de transition et Ψ est une *condition d'admissibilité* sur les exécutions. Formellement Ψ est un ensemble d'exécutions et $r \in \Psi$ si l'exécution r satisfait la condition Ψ. La condition d'admissibilité Ψ indique quelles sont les exécutions acceptables. Elle peut être caractérisée par une formule dans la logique temporelle [6, 7]. Si toutes les exécutions du système sont acceptables, on utilise la tautologie $\top$ comme condition d'admissibilité Ψ.

22.3 Modélisation de la connaissance et de l'incertitude dans le cadre FHMV

Pour modéliser la connaissance et raisonner à son propos dans le cadre FHMV, on utilise les systèmes interprétés. Un *système interprété* $\mathcal{I}$ est formé de la paire $(\mathcal{R}, \pi)$ où $\mathcal{R}$ est un système sur l'ensemble des états globaux $\mathcal{G}$ et π est une interprétation pour les propositions primitives, contenues dans Φ (Φ est l'ensemble des propositions primitives qui caractérisent les états globaux du système $\mathcal{R}$), sur $\mathcal{G}$. L'interprétation π assigne des valeurs de vérité aux propositions primitives dans les états globaux du système $\mathcal{R}$. Donc, pour toute proposition primitive $p \in \Phi$ et pour tout état global $\ell \in \mathcal{G}$, on a $\pi(\ell)(p) \in \{Vrai, Faux\}$. On construit ensuite la structure de Kripke, associée au système interprété $\mathcal{I} = (\mathcal{R}, \pi)$, qui a la forme $M_{\mathcal{I}} = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ où S est l'ensemble des points du système $\mathcal{R}$ et les $\mathcal{K}_i$ sont des relations binaires sur S pour chaque agent

i, $i = 1, \ldots, n$. Si $\ell = (\ell_e, \ell_1, \ldots, \ell_n)$ et $\ell' = (\ell'_e, \ell'_1, \ldots, \ell'_n)$ sont deux états globaux de $\mathcal{R}$, on dit que ℓ et ℓ' sont indistinguables à l'agent i, noté $\ell \sim_i \ell'$, si l'agent i possède le même état local dans ℓ et ℓ', soit $\ell_i = \ell'_i$. On étend la relation $\sim_i$ aux points du système $\mathcal{R}$. Deux points (r, m) et (r', m') sont indistinguables à l'agent i, noté $(r, m) \sim_i (r', m')$, si $r_i(m) = r'_i(m')$. Dans la structure de Kripke $M_{\mathcal{I}}$, la relation binaire $\mathcal{K}_i$ est définie par $\sim_i$ sur les points du système. Si l'agent se trouve à un point du système, il considère possibles tous les points dans lesquels il a le même état local. On dit qu'un agent i connait un fait φ, noté $K_i\varphi$, à un point (r, m) du système si le fait φ est vrai à tous les points que l'agent i considère possibles lorsqu'il est à (r, m).

Il y a plusieurs manières de représenter l'incertitude dans les systèmes interprétés. D'abord, le modèle des mondes possibles peut être utilisé pour quantifier l'incertitude de l'agent. L'incertitude de l'agent dépend donc du nombre d'états globaux ou de points du système qu'il considère possibles. Plus ce nombre est grand, plus son incertitude à propos de l'état réel des choses est grande et inversément. Une deuxième manière de représenter l'incertitude en utilisant le cadre FHMV est d'intégrer au cadre l'une des approches numériques utilisées pour représenter l'incertitude. Si on utilise la théorie des probabilités par exemple, on ajoutera dans la structure de Kripke $M_{\mathcal{I}} = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ associée au système interprété $\mathcal{I} = (\mathcal{R}, \pi)$, une assignation de probabilité $\mathcal{P}$. L'assignation de probabilité $\mathcal{P}$ assigne, à chaque agent i, $i = 1, \ldots, n$, et à chaque point (r, m) du système interprété, un espace probabilistique $\mathcal{P}(i, r, m) = (S_{i,r,m}, \mathcal{F}_{i,r,m}, \mu_{i,r,m})$ où $S_{i,r,m}$ est l'ensemble de tous les points que l'agent i considère possibles au point (r, m), $\mathcal{F}_{i,r,m}$ est une algèbre sur $S_{i,r,m}$ et $\mu_{i,r,m} : \mathcal{F}_{i,r,m} \to [0, 1]$ est une mesure de probabilité. On construit ainsi dans le cadre FHMV une nouvelle structure de Kripke $M_{\mathcal{I}_P} = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$ qui permet de modéliser à la fois la connaissance et l'incertitude et de raisonner à leur propos.

22.4 Exemple d'application

Soit le problème suivant :

> *On considère un robot qui se déplace dans un environnement où il y 8 positions alignées p possibles, soit $p \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Pour déterminer sa position, le robot dispose d'un senseur. La lecture du senseur n'est toutefois pas précise. Ainsi si le robot se trouve à la position p, le senseur lit une valeur positive ou nulle $v \in \{p-1, p, p+1\}$. Le robot est déposé à la position $p = 0$. Le but du robot est de s'arrêter quand il arrivera dans à $p \in \{2, 3, 4\}$ (zone $\{2, 3, 4\}$). Si le robot ne s'arrête pas, il continue d'avancer de manière inconditionnelle d'une position à chaque fois (le robot ne le sait pas) jusqu'à la position $p = 7$.*

Dans ce problème, le robot est le seul agent du système. Son état local ℓ_1 est la lecture v du senseur, soit $\ell_1 = v$. L'ensemble des états locaux possibles du robot est $\boldsymbol{L}_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. L'état local de l'environnement ℓ_e est la position exacte p du robot et l'ensemble des états locaux possibles de l'environnement est donc $\boldsymbol{L}_e = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Un état global du système est donc de la forme (ℓ_e, ℓ_1) où $\ell_e \in \boldsymbol{L}_e$ et $\ell_1 \in \boldsymbol{L}_1$. On peut remarquer que l'ensemble des états globaux du système est $\mathcal{G} = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2), (2,3), (3,2),$-$(3,3), (3,4), (4,3), (4,4), (4,5), (5,4), (5,5), (5,6), (6,5), (6,6), (6,7), (7,6), (7,7), (7,8)\}$. On considère $\Phi = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7\}$ l'ensemble des propositions primitives du système

où φ_i signifie que "*le robot est à la position* $p = i$". La fonction d'interprétation π est définie de manière naturelle. Ainsi on a $\pi((\ell_e, \ell_1))(\varphi_i) = Vrai$ si et seulement si $i = \ell_e$.

L'ensemble des actions du robot est $\mathbf{ACT}_1 = \{Stop, \Lambda\}$ (Λ est l'action nulle) et celui des actions de l'environnement est $\mathbf{ACT}_e = \{AvanceRobot, \Lambda\}$. Le but du robot est de s'arrêter dès qu'il sait que $p \in \{2, 3, 4\}$. S'il ne le sait pas, alors il ne fait rien. Donc le protocole P_1 du robot peut être décrit par :

P_1 : Si $K_1(\varphi_2 \vee \varphi_3 \vee \varphi_4)$ est vraie alors *Stop* ; sinon Λ.

L'environnement quant à lui doit avancer le robot d'une position à chaque fois, tant que le robot ne s'arrête pas de lui-même, jusqu'à la position $p = 7$. Son protocole P_e peut être décrit par :

P_e : Si le robot exécute l'action *Stop* ou si $p = 7$ alors Λ ; sinon *AvanceRobot*.

Nous venons de modéliser le problème d'une manière très simple en utilisant le cadre FHMV. Nous avons aussi développé un protocole pour le robot en se basant uniquement sur la connaissance qu'il a de sa position et non sur sa position réelle. Ce protocole apparaît très simple. C'est justement l'un des attraits du cadre FHMV qui permet de faire des descriptions de haut-niveau des systèmes et des protocoles. Maintenant on peut vérifier le protocole P_1 en se posant la question suivante : Est-ce que ce protocole permet au robot de s'arrêter chaque fois qu'il passe dans la zone $\{2, 3, 4\}$? Pour répondre à cette question, nous utilisons le diagramme de transitions du système, illustré à la figure (22.2), qui montre toutes les exécutions possibles dans le système. Une de ces exécutions, notons r, est encadrée en rouge où on a $r(0) = (0, 0)$, $r(1) = (1, 1)$, $r(2) = (2, 2)$, $r(3) = (3, 4)$, $r(4) = (4, 5)$, $r(5) = (5, 5)$, $r(6) = (6, 6)$ et $r(7) = (7, 7)$.

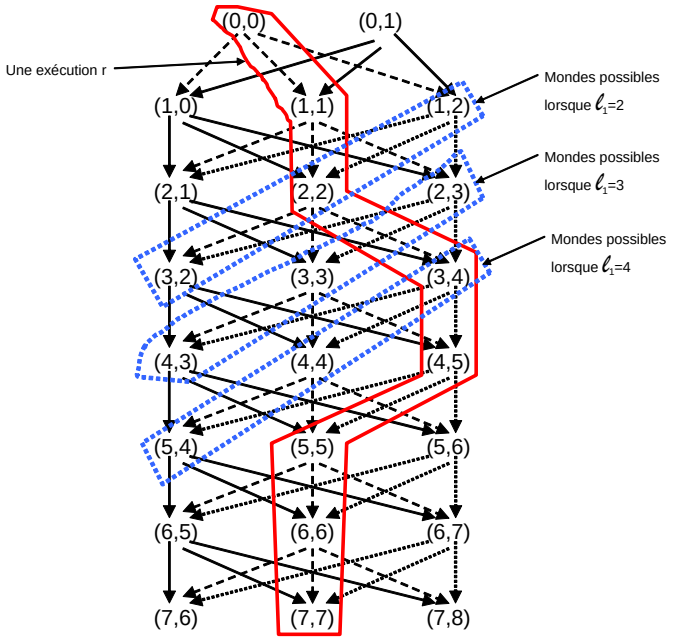


FIG. 22.2: Diagramme de transitions

En observant le diagramme de transitions du système, on constate que $K_1(\varphi_2 \vee \varphi_3 \vee \varphi_4)$ est vraie seulement quand $\ell_1 = 3$. En effet, quand $\ell_1 = 3$, le robot considère possibles seulement les états globaux $(2, 3)$, $(3, 3)$ et $(4, 3)$. Or, dans chacun de ces trois états globaux $\varphi_2 \vee \varphi_3 \vee \varphi_4$ est

vraie. Donc en suivant le protocole P_1, le robot ne s'arrêtera de lui-même (exécute l'action *Stop*) que si son senseur lit la valeur 3. On peut remarquer que la reponse à la question précédemment posée est donc ***non***. En effet, il y a des exécutions dans lesquelles le robot passera dans la zone $\{2, 3, 4\}$ sans s'arrêter. Ce sont les exécutions n'ayant aucun point où l'état global du système est $(2, 3)$, $(3, 3)$ ou $(4, 3)$. Une de ces exécutions est l'exécution r. Il faut donc développer un autre protocole pour le robot si le but est qu'il s'arrête obligatoirement dès qu'il passe dans la zone $\{2, 3, 4\}$. Le cadre FHMV permet donc de vérifier si les protocoles que nous avons développés repondent à certaines spécifications désirées.

22.5 Conclusion

Nous avons montré sur un exemple simple comment utiliser le cadre FHMV pour modéliser un système, développer des protocoles et vérifier ces protocoles. Le but de notre travail de recherche est d'appliquer cette méthode dans les systèmes de fusion d'informations plus complexes où interviennent plusieurs agents. Dans ces systèmes multiagents, les connaissances individuelles ne sont plus les seules notions de connaissance présentes. Les notions de connaissance de groupe d'agents apparaissent aussi. Les protocoles à développer sont donc beaucoup plus complexes. Par exemple, dans un réseau de capteurs effectuant des tâches de pistage de cibles ou d'identification, il faut développer des protocoles de communication, de routage et d'agrégation qui minimisent l'énergie consommée dans le réseau et optimisent l'utilisation de la bande passante. Puisque les espaces d'états (le nombre d'états globaux) de ces systèmes sont grands, nous envisageons d'utiliser la technique de model checking, une technique de vérification entièrement automatique, pour vérifier les protocoles développés.

Bibliographie

[1] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi, *Reasoning about Knowledge*. MIT Press, 2002.

[2] J. Y. Halpern, *Reasoning about Uncertainty*. MIT Press, 2003.

[3] W. van der Hoek and R. Verbrugge, "Epistemic logic : A survey," *Game Theory and Applications*, vol. 8, pp. 53–94, 2002.

[4] J. Edmund M. Clarke, O. Grumberg, and D. A. Peled, *Model Checking*. MIT Press, 1999.

[5] P. Maupin and A.-L. Jousselme, "A general algebraic structure for situation analysis," in *Proceedings of the 7th International Conference on Information Fusion 2005*, 2005.

[6] Y. Kesten, A. Pnueli, and L. Raviv, "Algorithmic verification of linear temporal logic specifications," in *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, vol. 1443, pp. 1–16, Springer Berlin / Heidelberg, 1998.

[7] E. A. Emerson and J. Srinivasan, "Branching time temporal logic," *Lecture Notes In Computer Science*, vol. 354, pp. 123–172, 1988.

Identification de l'impact de la fusion de l'information de la STANAG 1241 sous différents cadres de raisonnement

Pascal Djiknavorian, *Étudiant à la maîtrise*
Dominic Grenier, *Directeur de recherche.*
Pierre Valin, *Co-Directeur de recherche.*

Résumé – Mon mémoire portera sur une analyse comportementale comparative entre diverses théories de fusion de données. Il consistera plus exactement en l'identification de l'impact de la fusion de l'information de la STANAG 1241 sous différents cadres de raisonnement. Il faudra donc établir une base de simulation pour divers cadres de raisonnement, puis comparer et analyser leur performances dans le cadre de l'Accord de standardisation de l'OTAN 1241.

Abstract – My master's thesis will be about a behavioral comparative analysis between theories in data fusion. More specifically, it will be about the identification of the impact of information fusion of the STANAG 1241 within various frame of reference. We will then have to establish a basis for simulation within various frames of reference and then compare and analyse their performances within the NATO Standardization Agreement 1241.

23.1 Introduction à mon sujet de mémoire

Dans les domaines où des décisions critiques sont régulièrement prises à un rythme où l'humain ne peut arriver à concilier toutes les informations disponibles afin de prendre la meilleure décision suivant ses objectifs et critères de décision : ce sont des implémentations informatique et électronique de modèles mathématiques avancés de prise de décisions qui donnent des recommandations aux responsables de la prise de décision.

Domaine en effervescence où de nouvelles théories et règles de conciliation de l'information disponible voient régulièrement le jour, la fusion de données connait présentement plusieurs cadres de raisonnement et règles de combinaison de l'information sous incertitude dans l'objectif d'identification d'objets. Présentement, la théorie de l'évidence de Demspter remaniée par Shafer [2] est présentement utilisée dans différent domaines pour différents usages. Plus récemment, un nouveau cadre développé par Smarandache et Dezert [1] suscite l'intérêt de différents acteurs impliqués dans les processus de décision utilisant, ou intéressé à utiliser, les différents outils offerts dans le cadre de théories de la décision.

Chaque théorie et règle de combinaison d'information possède des avantages et désavantages, tant du point de vue théorique que pratique. Le problème est que beaucoup de théories récentes

ont très peu été utilisées à ce jour. Par conséquent, elles ont un comportement et des performances pratiques peu connues, sinon totalement inconnues. L'objectif du travail sur lequel portera mon mémoire sera d'expérimenter avec ces diverses théories dans le but de permettre de comparer le comportement et les performances en conditions d'exécution pratique ; les comparaisons théoriques ont, elles, déjà été réalisés par différents acteurs en fusion de données. On peut retrouver de telles comparaisons théoriques dans des articles tel que celui-ci [3].

La théorie de Dezert-Smarandache (DSmT)

Définitions

- *Cadre de discernement* (Θ) : $\Theta = \{\theta_1, \theta_2, \ldots \theta_n\}$. Cet ensemble inclut tout les objets possibles.
- *Ensemble de puissance* $\left(2^{\Theta}\right)$: représente l'ensemble de tous les ensembles d'objets possibles du cadre de discernement Θ. Il inclut l'ensemble vide, mais exclut les intersections. Avec le cadre de discernement défini ci-haut, nous obtenons l'ensemble de puissance $2^{\Theta} = \{\emptyset, \{\theta_1\}, \{\theta_2\}, \ldots \{\theta_n\}, \{\theta_1, \theta_2\}, \ldots \{\theta_1, \theta_2, \ldots \theta_n\}, \ldots, \Theta\}$.
- *Ensemble d'hyperpuissance* $\left(D^{\Theta}\right)$: représente l'ensemble de tous les ensembles d'objets possibles du cadre de discernement Θ avec les intersections. Il inclut également l'ensemble vide. Avec le cadre de discernement définit ainsi : $\Theta = \{\theta_1, \theta_2\}$, nous obtenons l'ensemble d'hyperpuissance $D^{\Theta} = \{\emptyset, \{\theta_1\}, \{\theta_2\}, \{\theta_1 \cap \theta_2\}, \{\theta_1 \cup \theta_2\}\}$.
- *Croyance* (Bel(A)) : est une évaluation du niveau minimal de certitude, de confiance, que peut avoir un ensemble.
- *Plausibilité* (Pl(A)) : est une évaluation du niveau maximal de certitude, de confiance, que peut avoir un ensemble.
- *Contrainte* : est un ensemble que l'on considère impossible à obtenir.
- *Basic belief assignement* (bba) : $m \ : 2^{\Theta} \rightarrow [0, 1]$, donc la masse donnée à un ensemble $A \subseteq \Theta$ suit $m(A) \in [0, 1]$.
- *Noyau de* Θ ($\mathcal{K}$) : est l'ensemble de tous les éléments focaux de Θ, où un élément focal est un sous-ensemble A de Θ tel que $m(A) > 0$.

Les règles de combinaison de la DSmT

La DSmT fonctionne avec des ensemble d'hyperpuissance. Ainsi, la DSmT est en mesure de fonctionner correctement avec des intersections. De plus, la DSmT règle le problème de redistribution de masses conflictuelles survenant sous la théorie de Dempster-Shafer. La DSmT comporte deux règles de combinaison, la version classique ainsi que la version hybride. La règle de combinaison hybride de la DSmT permet la gestion et le fonctionnement malgré divers types de contraintes, ce que la version classique n'est pas en mesure de faire.

- Règle de combinaison classique (DSmC)

$$m(C) = \sum_{A \cap B = C} m_1(A)\, m_2(B) \qquad A, B \in D^{\Theta}, \forall C \in D^{\Theta} \tag{23.1}$$

- Règle de combinaison hybride (DSmH)

$$m_{M(\Theta)}(A) = \phi(A)\left[S_1(A) + S_2(A) + S_3(A)\right] \tag{23.2}$$

$$S_1(A) = \sum_{X_1 \cap X_2 = A} m_1(X_1)\, m_2(X_2) \qquad \forall X_1, X_2 \in D^{\Theta} \tag{23.3}$$

$$S_2(A) = \sum_{\substack{[(u(X_1) \cup u(X_2)) = A] \vee \\ [((u(X_1) \cup u(X_2)) \in \emptyset) \wedge (A = I_t)]}} m_1(X_1)\, m_2(X_2) \qquad \forall X_1, X_2 \in \emptyset \tag{23.4}$$

$$S_3(A) = \sum_{X_1 \cup X_2 = A} m_1(X_1)\, m_2(X_2) \qquad \forall X_1, X_2 \in D^{\Theta} \quad \text{and} \quad X_1 \cap X_2 \in \emptyset \tag{23.5}$$

Notez que $\phi(A)$ de l'équation (23.2) est une fonction binaire donnant 0 pour les ensembles vide ou impossibles, autrement il nous donne 1. Dans l'équation (23.4), $u(X)$ représente l'union de tous les objets de l'ensemble X. L'équation (23.5) nous dit que c'est l'union de tous les objets des ensembles X_1 et X_2, lorsque ce n'est pas vide. Finalement, également à partir de l'équation (23.4), I_t représente l'ignorance totale ou l'union de tous les objets inclus dans le cadre de discernement.

Afin de mieux comprendre la DSmH, nous proposons de voir cette règle de combinaison comme une procédure. La table 23.1 nous montre une telle procédure détaillant clairement comment on peut calculer la DSmH. Évidemment, c'est équivalent à l'équation mathématique, par contre, cette façon de voir la combinaison en permet une meilleure compréhension ainsi qu'une implémentation plus aisée.

Tab. 23.1: Procédure à appliquer à chaque pair d'ensemble (X_1, X_2) tant que le produit de leur masse n'est pas donné à un ensemble

Étape S1 $(\theta_1 \cap \theta_2)$	Si $(\theta_1 \cap \theta_2)$ est une contrainte, alors continuer à l'étape S3, autrement, la masse $m_1(X_1)\, m_2(X_2)$ est ajoutée à la masse $A = (\theta_1 \cap \theta_2)$.
Étape S3 $(\theta_1 \cup \theta_2)$	Si $(\theta_1 \cup \theta_2)$ est une contrainte, alors continuer à l'étape S2, autrement, la masse $m_1(X_1)\, m_2(X_2)$ est ajoutée à la masse $A = (\theta_1 \cup \theta_2)$.
Étape S2 $(u(X_1) \cup u(X_2))$	Si $(u(X_1) \cup u(X_2))$ est une contrainte, alors ajouter sa masse à I_t, autrement, la masse $m_1(X_1)\, m_2(X_2)$ est ajoutée à la masse $A = (u(X_1) \cup u(X_2))$.

Le *NATO Standardization Agreement* (STANAG) 1241

Le processus d'identification par combinaison d'informations (PICI) est une combinaison d'informations de sources d'informations multiples et distribués. Son but est de concilier l'information disponible au sein de l'environnement et de support d'identification aux officiers pour l'identification d'objets ami, ennemi, ou neutre. Le PICI utilise l'information des ESM (electronic support measures), traces radars, comportements d'objet, ainsi que de systèmes d'identification d'ami et

©LRTS 2005-2006

d'ennemi (IFF) afin d'établir la catégories d'appartenance d'un objet. L'appartenance d'un objet se fait par la nomenclature définit dans le cadre du STANAG 1241 : ami, considéré ami, neutre, suspect, ou ennemi.

23.2 Survol d'un chapitre produit pour la 2e édition de *Advances and Applications of DSmT for Information Fusion* [1]

Ce chapitre, co-réalisé avec Dominic Grenier et reprennant les travaux de Marie-Line Gagnon [4] sur l'implémentation informatique de la règle de combinaison hybride de la théorie de Dezert-Smarandache, s'intitule : *Reducing DSmT hybrid rule complexity throught optimisation of the calculation algorithm.* Il porte principalement sur la présentation de la méthode empruntée pour l'optimisation du calcul de la règle de combinaison hybride. Cette règle de combinaison est considérée comme étant l'une des plus complexes au niveau du calcul et exigeantes au niveau des ressources mnémoniques.

Nos résultats sont concluants au point de vue de la possibilité de l'implémentation de cette règle de combinaison. Par contre, la priorité de la conception était principalement porté au niveau du calcul optimal du résultat de la combinaison. Nous avons ainsi pu déceler que le noeud de travail du système se situe maintenant au niveau de l'algorithme de tri nécessaire pour le calcul de la combinaison. La prochaine étape consisterait donc à optimiser cette partie qui peut devenir problématique en terme de temps de calcul pour des combinaisons de grands ensembles d'informations.

Outre le potentiel problème d'optimisation de l'algorithme de tri, l'implémentation de la règle de combinaison hybride est fonctionnelle pour un calcul dynamique et nous donne, entre autre, les résultats suivants :

- le temps d'exécution varie exponentiellement en fonction de l'évolution du cardinal du cadre de discernement, allant de 3 à 9,
- le temps d'exécution varie exponentiellement en fonction de l'évolution du nombre de sources d'informations, allant de 3 à 9,
- le temps d'exécution varie linéairement en fonction de l'évolution du cardinal du noyau, (ie. : du nombre de masses non nulles), allant de 3 à 9,
- la mémoire requise par Matlab pour l'exécution des tests sur le temps d'exécution ne dépasse pas 10 MB.

Bibliographie

[1] F. Smarandache, J. Dezert (ed.), *Advances and Applications of DSmT for Information Fusion.* American Research Press, 2004.

[2] G. Shafer, *A Mathematical Theory of Evidence.* Princeton University Press, 1976.

[3] F. Smarandache, *Unification of Fusion Theories*, ArXiv Computer Science e-prints, arXiv :cs/0409040, 2004.

[4] M.-L. Gagnon, D. Grenier, *Rapport : Fusion de données, été 2005.*, Université Laval, 2005.

Adaptive combination rule for the evidence theory

Mihai Cristian Florea, *Ph.D Student*
Dr Dominic Grenier, *Advisor.*
Dr Anne-Laure Jousselme, *Co-advisor.*

Résumé – La théorie de l'evidence avec la règle de combinaison de Dempster est un outil très puissant pour le raisonnement sous incertitude. Depuis que Zadeh a montré avec son exemple que la règle de Dempster produit des résultats contre-intuitifs quand des informations contradictoires sont combinées, différentes règles alternatives ont été définies. Dans le but de prendre en compte de manière automatique la fiabilité des sources d'informations, nous proposons une nouvelle classe de règles adaptatives mélangeant les règles conjonctive et disjonctive. Nous présentons quelques propriétés intéressantes et un cas particulier : la règle adaptative avec des coefficients symétriques. Le comportement de la règle proposée est illustré sur deux exemples.

Abstract – Evidence theory with Dempster's rule of combination is a powerful tool for the reasoning under uncertainty. Since Zadeh proved with an example that Dempster's rule of combination provides counter-intuitive results when combining conflictual information, different alternative combination rules have been defined. In the aim of automatically accounting for the reliability of the sources of information, we propose a new class of adaptive combination rules as a mixing of the conjunctive and the disjunctive combination rules. We present some interesting properties and a particular case : an adaptive rule with symmetric weighting functions. The behaviour of the proposed rule is illustrated on two examples.

24.1 Introduction

The Dempster-Shafer theory (DST) [1, 2], or evidence theory, is one of the mathematical tools developed for reasoning under uncertainty. One of its strengths is that it can cope with imprecise or uncertain information or a mixing of both. Moreover, combination rules are defined in the DST setting which allow to combine different pieces of information. The oldest combination rule, proposed by Dempster's [3] is commonly used in data fusion applications. However, Dempster's rule has been often criticized based on its occasionally unexpected behaviour. In particular, Zadeh proved through a simple example [4] that Dempster's rule provides counter-intuitive results when combining highly conflictual information.

To cope with this problem, some authors proposed (1) to better model the information before the combination step [5, 6, 7, 8], (2) new more flexible theories in order to cope with an unknown and unpredictable reality - such the Transferable Belief Model of Smets and Kennes [9] or the

Dezert-Smarandache Theory (DSmT) [10] and (3) new combination rules such as Yager's rule [11], Dubois and Prade's rule [12] and Inagaki's rule [13].

In this paper, we consider that the sources of information are independent and can be homogeneous or heterogeneous. A piece of information is defined on a frame of discernment containing an exclusive and exhaustive list of hypotheses. Consequently, we consider that the conflict is due to the unreliability of some sources. Moreover, instead of modifying the initial BPA to account for the reliability, we adopt the approach of an automatic combination rule based on the mixing of the two conjunctive and disjunctive operators.

In Section 24.2 we briefly review the evidence theory framework. We introduce in Section 24.3 a class of adaptive combination rules as a mixing of the conjunctive and disjunctive combination rules. We also restrict to a particular case of a symmetric adaptive combination rule. We then illustrate in Section 24.4 some properties of the proposed adaptive rule on two examples. Section 24.5 ends with the conclusions.

24.2 Dempster-Shafer's evidence theory

Evidence theory has been first introduced by Dempster in 1967 in his work on upper and lower probabilities [1] and formalized in 1976 by Shafer in his book *A Mathematical Theory of Evidence* [2]. This theory is often described as an extension of probability theory as it lies on the power set of the universe of discourse (frame of discernment) instead of the universe itself.

Let Θ be the frame of discernment, containing N exclusive and exhaustive objects or hypotheses. A BPA is a mapping $m : 2^\Theta \to [0,1]$ that must satisfy the following conditions : (1) $m(\varnothing) = 0$ and (2)$\sum_{A\subseteq\Theta} m(A) = 1$, where $0 \leq m(A) \leq 1, \forall A \in 2^\Theta$. $m(A)$ is called the *mass* of A and represents the degree of belief that someone strictly assigns to A. A subset A with a non-null mass is called a *focal element* of m. Let $\mathcal{F}$ designate the set of all focal elements of m.

The disjunctive rule (p) and the conjunctive rule (q) are :

$$p(A) = \sum_{B\cup C=A} m_1(B)m_2(C) \qquad q(A) = \sum_{B\cap C=A} m_1(B)m_2(C) \qquad \forall A \subseteq \Theta \tag{24.1}$$

$k = q(\varnothing)$ is called the *weight of conflict* (or simply *conflict*) between m_1 and m_2, and is equal to the mass of the empty set after the conjunctive combination and before any normalization. If k is close to 0, the BPAs are not in conflict, while if k is close to 1, the BPAs are in conflict.

Dempster's rule of combination is defined by $(m_1 \oplus m_2)(\varnothing) = 0$ and :

$$(m_1 \oplus m_2)(A) = \frac{1}{1-k} \sum_{B\cap C=A} m_1(B)m_2(C) \qquad , \forall A \subset \Theta, A \neq \varnothing \tag{24.2}$$

When $k = 1$, Dempster's rule of combination is not defined.

New combination rules in the DST were defined as alternatives to Dempster's rule such as Yager [11] who proposed to re-assign the mass of the empty set to the ignorance, Dubois and Prade [12] who introduced the disjunctive operator to account for the reliability of the sources, or Inagaki [13] who presented a general class of rules. In the next section we propose a new class of adaptive rules which are a mixing between the disjunctive and the conjunctive rules, following an equivalent idea as Dubois and Prade developed in [12], [14].

24.3 Adaptive combination rule in evidence theory

In [14], the authors propose for the possibility theory a class of adaptive combination rules which mixes any disjunctive rule with any conjunctive rule. We extend here this idea and propose a new class of combination rules for the evidence theory, where the mixing between p and q is done through two *weighting coefficients* α and β which are functions of the conflict k between the two BPAs m_1 and m_2.

Let m_1 and m_2 be two BPAs defined on the same frame of discernment Θ. The adaptive combination rule (ACR) between m_1 and m_2 is defined by :

$$(m_1 \diamond m_2)(A) = \alpha(k)p(A) + \beta(k)q(A) \qquad , \forall A \subseteq \Theta, A \neq \varnothing \tag{24.3}$$

and $(m_1 \diamond m_2)(\varnothing) = 0$. Here, p and q are the disjunctive and conjunctive rules and α and β are functions of the conflict $k = q(\varnothing)$ from $[0,1]$ to $[0,+\infty[$.

Because $(m_1 \diamond m_2)$ is a BPA, $\alpha(k)$ and $\beta(k)$ must satisfy the condition : $\sum_{A\subseteq\Theta}(m_1 \diamond m_2)(A) = 1$. It follows that

$$\alpha(k)\sum_{A\subseteq\Theta} p(A) + \beta(k)\sum_{A\subseteq\Theta} q(A) = 1 \qquad \Longleftrightarrow \qquad \alpha(k) + (1-k)\beta(k) = 1 \quad , \forall k \in [0,1] \tag{24.4}$$

Then, the ACR may be expressed according only to the function β as follows :

$$(m_1 \diamond m_2)(A) = [1-(1-k)\beta(k)]p(A) + \beta(k)q(A) \qquad , \forall A \subseteq \Theta, A \neq \varnothing \tag{24.5}$$

and $(m_1 \diamond m_2)(\varnothing) = 0$ where β is any function such that $\beta : [0,1] \to [0,+\infty[$.

Here are some properties of the general formulation of the ACR :

1. The disjunctive and Dempster's combination rules are special cases of Equation (24.3) for $\alpha(k) = 1$ and $\beta(k) = 0$ and for $\alpha(k) = 0$ and $\beta(k) = 1/(1-q(\varnothing))$ respectively, $\forall k \in [0,1]$.
2. The class of ACR $\diamond$ can be written under Inagaki's general class of combination rules.
3. Written under Inagaki's form, the class of ACR $\diamond$ extends Inagaki's general class since in this case, the weighting coefficients $w(A)$ can be negative.
4. The combination of m_1 and m_2 using the $\diamond$ operator leads to a **partial positive reinforcement** of the belief for the focal elements common to both m_1 and m_2.
5. The ACR is insensitive to the non-exhaustivity of the frames of discernment.
6. The ACR preserves the neutral impact of the vacuous belief ($m_0(\Theta) = 1$) in the fusion process, that is $m \diamond m_0 = m$.

Particular case of the ACR

In the general case, α and β are functions of k with no particular constraint. However, a desirable behaviour of the ACR is that it should act more like the disjunctive rule p whenever k is close to 1 (*i. e.* at least one source is unreliable), while it should act more like the conjunctive rule q, if k is close to 0 (*i. e.* both sources are reliable). This amounts to add three conditions on the general formulation and leads thus to :

©LRTS 2005-2006

(C1) α is an increasing function with $\alpha(0) = 0$ and $\alpha(1) = 1$;

(C2) β is a decreasing function with $\beta(0) = 1$ and $\beta(1) = 0$.

(C3) $\alpha(k) = 1 - (1 - k)\beta(k)$

In particular, when $k = 0$ the sources are in total agreement and $(m_1 \diamond m_2)(A) = p(A), \forall A \subseteq \Theta$, the conjunction represents the combined evidence, while when $k = 1$ the sources are in total conflict and $(m_1 \diamond m_2)(A) = q(A), \forall A \subseteq \Theta$, the disjunction is the best choice considering that one of them is wrong.

Note that the three conditions above are dependent and (C1) can be removed, since it is a consequence of the (C2) and (C3). The particular case of the adaptive combination rule can be stated as Equation (24.5), $\forall A \subseteq \Theta, A \neq \varnothing$ and $m(\varnothing) = 0$, where β is any decreasing function such that $\beta : [0, 1] \to [0, 1]$ and $\beta(0) = 1$ and $\beta(1) = 0$.

ACR with symmetric weighting functions

The behaviours at the extremum values ($k = 0$ and $k = 1$) are easily interpretable. Indeed, whenever $k = 0$, the sources are in total agreement and thus can be considered as both reliable, so the only basic rule to be used in this case must be the conjunctive rule q, implying then $\alpha(0) = 0$ and $\beta(0) = 1$. Whenever $k = 1$, the sources are in total disagreement and thus it can be considered that at least one of them is unreliable, so the caution is required so that the only basic to be used in this case must be the disjunctive rule p, implying then $\alpha(1) = 1$ and $\beta(1) = 0$.

However, if $k = 0$ means "total agreement" and $k = 1$ means "total disagreement", what does $k = 0.5$ mean ? A suitable interpretation to $k = 0.5$ is the one of a total ignorance about the agreement between both sources. Because we cannot decide if the sources are in conflict or not, we do not know either if the rule must be more conjunctive or more disjunctive. Facing this uncertainty and without any additional information a sober choice is to give an equal weight to both basic rule in this case. Hence, $\alpha(0.5) = \beta(0.5)$, which leads to the ACR with symmetric weightings for p and q about $k = 0.5$ called SACR, which is unique and is defined by :

$$(m_1 \diamond m_2)(A) = \frac{k}{1 - k + k^2} p(A) + \frac{1 - k}{1 - k + k^2} q(A) \tag{24.6}$$

$\forall A \subseteq \Theta, A \neq \varnothing$ and $(m_1 \diamond m_2)(\varnothing) = 0$.

Evidence combination and updating

Two main schemes can be considered when combining pieces of information : (1) combining scheme, where evidences represent different opinion about the same event, (2) updating scheme, where evidences represent sequential opinions about an dynamic event. In the first case, the time is not implied and we are concerned by the aggregated evidence among the different sources, while in the second case, the time is crucial since the dynamic of the situation must be considered and that different pieces of information can be provided by the same source at different time steps.

Figure 24.1 shows a sequential fusion process using the ACR as combination rule. Because of the non-associativity of the ACR, this scheme better suits to the combination of streaming data.

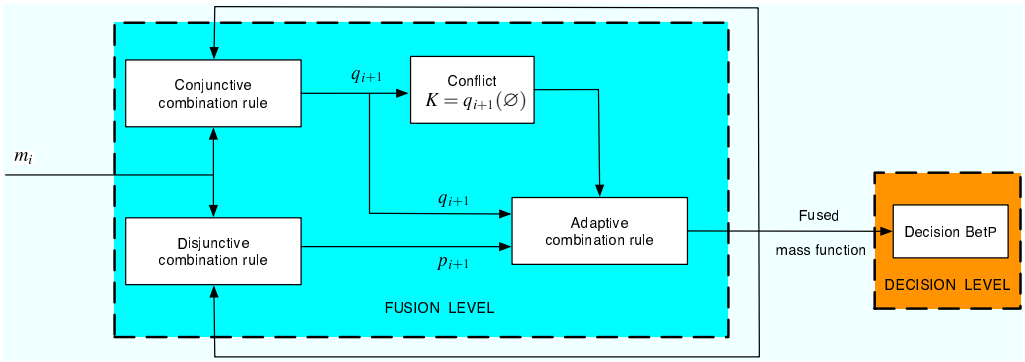


FIG. 24.1: Adaptive combination rule in a sequential fusion process.

Although in a combination scheme the associativity property is crucial since we do not want the order of combination to change the aggregate information among the sources, this property becomes however less desirable since as pointed out by Yager for instance [15, 16], in some applications of belief updating the last piece of information should be assigned a higher weight and a quasi-associative rule is preferred.

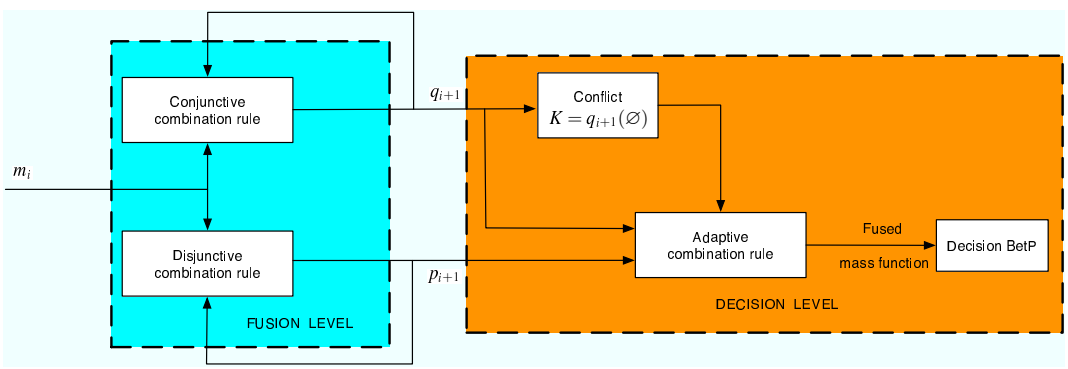


FIG. 24.2: Quasi-associative adaptive combination rule in a sequential fusion process.

The ACR is not associative. However, based on the commutativity and associativity properties of the conjunctive and the disjunctive combination rules p and q, a quasi-associative ACR can be defined from Equation (24.5). Instead of $(m_1 \diamond m_2)(A)$, $p(A)$ and $q(A)$ are rather propagated, as illustrated in Figure 24.2. Whenever associativity is required, a quasi-associative ACR can be defined which is insensible to the order of combination of the pieces of information.

24.4 Examples

Example 1 *m_1 and m_2 are two BPAs defined over $\Theta = \{\theta_1, \theta_2, \theta_3\}$ as follows :*

$m_1(\theta_1) = 0.3$	$m_2(\theta_1) = 0.4$
$m_1(\theta_3) = 0.3$	$m_2(\theta_3) = 0.2$
$m_1(\{\theta_1, \theta_3\}) = 0.2$	$m_2(\{\theta_2, \theta_3\}) = 0.4$
$m_1(\{\theta_1, \theta_2\}) = 0.2$	

©LRTS 2005-2006

Let BetP_1 and BetP_2 be the corresponding pignistic probability distributions (the BetP function is defined in [17] as a decision criterion) of m_1 and m_2 respectively. We have then before combination :

$$\begin{array}{ll} \mathrm{BetP}_1(\theta_1) = 0.5 & \mathrm{BetP}_2(\theta_1) = 0.4 \\ \mathrm{BetP}_1(\theta_2) = 0.1 & \mathrm{BetP}_2(\theta_2) = 0.2 \\ \mathrm{BetP}_1(\theta_3) = 0.4 & \mathrm{BetP}_2(\theta_3) = 0.4 \end{array}$$

Hence, Source #1 is in favour of θ_1, while Source #2 is equally in favour of θ_1 and θ_3. We thus expect that after combination θ_1 will be identified. The pignistic distributions after combination using Dubois and Prade's rule (BetP_*) and the symmetric adaptive rule ($\mathrm{BetP}_\diamond$) are as follows :

$$\begin{array}{ll} \mathrm{BetP}_*(\theta_1) = 0.4233 & \mathrm{BetP}_\diamond(\theta_1) = 0.4210 \\ \mathrm{BetP}_*(\theta_2) = 0.1334 & \mathrm{BetP}_\diamond(\theta_2) = 0.1586 \\ \mathrm{BetP}_*(\theta_3) = 0.4433 & \mathrm{BetP}_\diamond(\theta_3) = 0.4204 \end{array}$$

On one hand, Dubois and Prade's rule followed by a maximum of pignistic probability decision criterion gives θ_3 as solution, which seems contrary to our intuition before combination. On the other hand, because of a higher positive reinforcement, the SACR gives θ_1 as solution which is the expected solution.

TAB. 24.1: Example 1 : Combining m_1 and m_2

Focal elements	Conjunctive rule q	Disjunctive rule p	Dempster rule Inagaki rule	Yager	DP rule	SACR
$\varnothing$	0.34	0	0	0	0	0
θ_1	0.28	0.12	0.4242	0.28	0.28	0.2909
θ_2	0.08	0	0.1212	0.08	0.08	0.0681
θ_3	0.30	0.06	0.4546	0.30	0.30	0.2816
$\{\theta_1, \theta_2\}$	0	0.08	0	0	0	0.0351
$\{\theta_1, \theta_3\}$	0	0.30	0	0	0.18	0.1315
$\{\theta_2, \theta_3\}$	0	0.12	0	0	0	0.0525
$\Theta = \{\theta_1, \theta_2, \theta_3\}$	0	0.32	0	0.34	0.16	0.1403
Decision (BetP)	$\varnothing$	θ_1	θ_3	θ_3	θ_3	θ_1

Table 24.1 shows the results of the different combination rules using this example. Dempster's rule, Yager's rule or Dubois and Prade's rule associated with the pignistic probability decision criterion all provide singleton θ_3 as the solution. The disjunctive rule and the SACR are the only combination rules which provide θ_1 as a solution.

Example 2 *Let m_3, m_4 and m_5 be three BPAs defined as follows :*

$$\begin{array}{c|c|c} m_3(\theta_1) = 0.5 & m_4(\theta_1) = 0.5 & m_5(\theta_2) = 0.5 \\ m_3(\theta_2) = 0.5 & m_4(\theta_3) = 0.5 & m_5(\theta_3) = 0.5 \end{array}$$

In this example, three pieces of information must be combined, contrary to the other example. Because of the symmetry, our intuition says that the three singletons θ_1, θ_2 and θ_3 should be

equally probable after the combination. Most of the combination rules are not associative, for which the order of combination is important and the last piece of information to be fused will be more important than the others. Consequently, Singletons θ_2 and θ_3 are chosen by the non-associative combination rules. Considering the three pieces of information as expert opinions for example, we should use an associative or a quasi-associative rule in order to obtain an aggregate opinion of these three sources. The quasi-associative ACR is reduced in this case to the disjunctive combination rule (since the global conflict k equals 1) :

$$m(\{\theta_1, \theta_2\}) = m(\{\theta_1, \theta_3\}) = m(\{\theta_2, \theta_3\}) = m(\{\theta_1, \theta_2, \theta_3\}) = 0.25$$

which is equivalent to a decision between Singletons θ_1, θ_2 and θ_3 and suits our intuition. Dempster's rule is not defined in this example since $k = 1$ and thus cannot be used. Using Yager's rule, Dubois and Prade's rule and the conjunctive rule, we have to chose between Singletons θ_2 and θ_3 only.

24.5 Conclusions

In this paper we have defined a new class of combination rules for evidence theory. This new class of rules is developed to cope with the problem of combining conflictual information, a case where Dempster's classical rule of combination fails to provide intuitive results. The interpretation given to the weight of conflict between two BPAs is then directly linked to the relative reliability of the sources : If the conflict is low, then both sources are reliable, and if the conflict is high, then at least one source is reliable. Depending on the conflict, the proposed class of adaptive rules acts more like a conjunctive rule (low conflict) or more like a disjunctive rule (high conflict). Under its general formulation, the ACR satisfies a set of important properties, among them : the partial positive reinforcement, the insensitivity to the heterogeneity of the sources and the preservation of the neutral impact of the vacuous belief. We also presented a special case of the ACR obtained by imposing a symmetry about $k = 0.5$.

Like many other combination rules recently proposed in the framework of evidence theory, the ACR is not associative, that makes it more suitable for updating evidence. However, because the ACR lies on two associative operators, namely the disjunction and the conjunction, it is possible to define a quasi-associative rule which can then be used for combining evidences.

Bibliographie

[1] A. Dempster, "Upper and Lower Probablilities Induced by Multivalued Mapping," *Ann. Math. Statist.*, vol. 38, pp. 325–339, 1967.

[2] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[3] A. Dempster, "A generalization of bayesian inference," *Journal of the Royal Statistical Society : Series B*, vol. 30, pp. 205 – 245, 1968.

[4] L. A. Zadeh, "Review of Shafer's Mathematical Theory of Evidence," *AI Magazine*, vol. 5, pp. 81 – 83, 1984.

©LRTS 2005-2006

[5] F. Voorbraak, "On the justification of Dempster's rule of combination," *Artificial Intelligence*, vol. 48, pp. 171–197, 1991.

[6] F. Janez and A. Appriou, "Theory of evidence and non-exhaustive frames of discernment : Plausibilities correction methods," *Int. J. of Approx. Reasoning*, vol. 18 (1/2), pp. 1–19, 1998.

[7] R. Haenni, "Are alternatives to Dempster's rule of combination real alternatives ? Comments on "About the belief combination and the conflict management problem"—Lefevre et al.," *Information Fusion*, vol. 3, pp. 237–239, 2002.

[8] W. Liu and J. Hong, "Reinvestigating Dempster's idea on evidence combination," *Knowledge and Inf. Syst.*, vol. 2, pp. 223–241, 2000.

[9] P. Smets and R. Kennes, "The Transferable Belief Model," *Artificial Intelligence*, vol. 66, pp. 191–234, 1994.

[10] F. Smarandache and J. Dezert, eds., *Applications and Advances of DSmT for Information Fusion*. Am. Res. Press, Rehoboth, 2004.

[11] R. R. Yager, "On the Dempster-Shafer framework and new combination rules," *Information Science*, vol. 41, pp. 93–138, 1987.

[12] D. Dubois and H. Prade, "Representation and combination of uncertainty with belief functions and possibility measures," *Computational Intelligence*, vol. 4, pp. 244–264, 1988.

[13] T. Inagaki, "Interdependence between safety-control policy and multiple-sensor schemes via Dempster-Shafer theory," *IEEE Trans. on reliability*, vol. 40, no. 2, pp. 182 – 188, 1991.

[14] D. Dubois and H. Prade, "La fusion d'informations imprécises," *Traitement du Signal*, vol. 11, no. 6, pp. 447–458, 1994.

[15] R. R. Yager, "Quasi-Associative Operations in the Combination of Evidence," *Kybernetes*, vol. 16, pp. 37 – 41, 1987.

[16] R. R. Yager, "On the Dempster-Shafer framework and new combination rules," *Information Sciences*, vol. 41, pp. 93 – 137, 1987.

[17] P. Smets, "Constructing the pignistic probability function in a context of uncertainty," *Uncertainty in Artificial Intelligence*, vol. 5, pp. 29–39, 1990.

[18] P. Smets, "Belief Functions : The Disjunctive Rule of Combination and the Generalized Bayesian Theorem," *International Journal of Approximate Reasoning*, vol. 9, pp. 1 – 35, 1993.

General Measure of Uncertainty in Fuzzy Evidence Theory

Chunsheng Liu, *Chercheur post-doctoral*
Dominic Grenier, *Directeur de recherche.*

Résumé – Le travail présenté ici consiste à trouver une mesure dans la théorie de l'évidence floue, incluant toutes formes d'incertitudes. Notre proposons un algorithme pour calculer AU(Bel) qui réduit la complexité du calcul de l'algorithme MRW de A. Meyerowitz *et al.* . Afin de surmonter les imperfections de MRW (*compliqué, peu sensible, distinction difficile entre la discorde et la nonspécificité*), une mesure alternative à AU pour quantifier l'ambiguïté des fonctions de croyance est proposée ; elle se note AM. Une nouvelle mesure, appelée mesure généralisée GM, est proposée ; elle inclut toutes formes d'incertitudes.

Abstract – Our objective is to find a measure in fuzzy evidence theory, which includes all kinds of uncertainty. We propose an algorithm to calculate AU(Bel) which reduces the computing complexity of the MRW algorithm as proposed by A. Meyerowitz *et al.* . In order to overcome the shortcomings (*complicated, insensitive, difficult to distinguish two kinds of uncertainty*) an alternative measure to AU for quantifying ambiguity of belief functions is proposed ; she is noted AM. A new measure, called General Measure (GM) is proposed, and it includes all kinds of uncertainty.

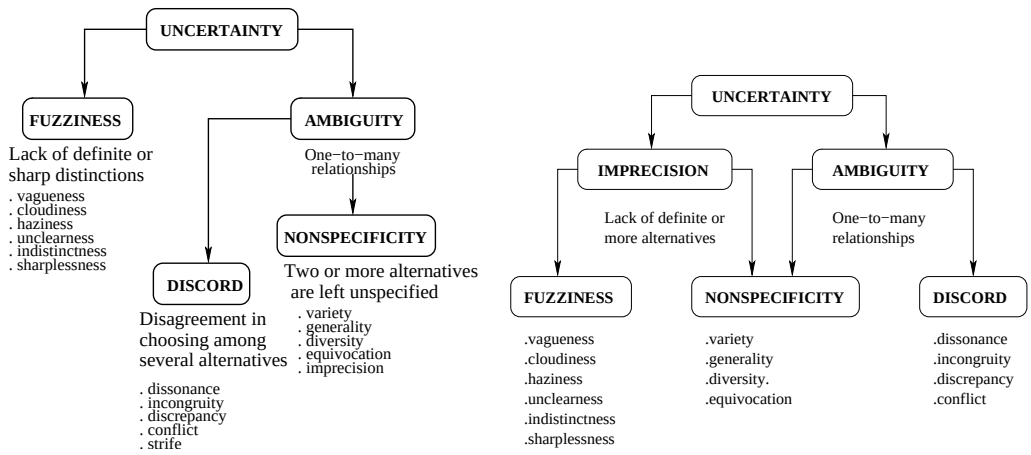
25.1 Introduction

Figure 25.1(a) depicts the typology of uncertainty proposed by Klir and Yuan [1] and our typology of uncertainty [2]. In both of these two typology, uncertainty includes *fuzziness*, *discord* and *nonspecificity*. Our aim is to look for a measure of uncertainty which includes all these three types of uncertainty.

Many measures were proposed by many authors. These measures are divided two parts : one is for fuzziness and nonspecifity in fuzzy set theory ; the other part is discord and nonspecificity in Dempster-Shafer theory. An aggregate uncertainty (AU) was proposed in [3, 4], which is "currently the only well justified measure of uncertainty for Dempster-Shafer theory", its definition is as follows,

Definition 1 *Let X be a finite frame of discernment, and* Bel *be a belief measure on X. The aggregate uncertainty associated with* Bel *is measured by*

$$\mathrm{AU}(\mathrm{Bel}) = \max_{\mathcal{P}_{\mathrm{Bel}}} \left[-\sum_{x \in X} p_x \log_2 p_x \right] \tag{25.1}$$



(a) Klir's typology of uncertainty (b) Our typology of uncertainty

FIG. 25.1: Typology of Uncertainty

where the maximum is taken over all probability distributions that are consistent with the given belief measure. Thus, $\mathcal{P}_{\text{Bel}}$ *in equation (25.1) consists of all probability distributions* $\langle p_x | x \in X \rangle$ *that satisfy the constraints :*

$$p_x \in [0,1] \quad \forall x \in X \ \textit{and} \ \sum_{x \in X} p_x = 1 \tag{25.2}$$

$$\text{Bel}(A) \leq \sum_{x \in A} p_x \leq 1 - \text{Bel}(\overline{A}) \quad \forall A \subseteq X \tag{25.3}$$

where $\overline{A}$ *is the complement of* A *with respect to* X*.*

However, AU presents three main shortcomings identified by Klir [5] :

(Sh1) High computing complexity ;

(Sh2) Highly insensitive to changes of evidence ;

(Sh3) No clear distinction between the two types of uncertainty (discord and nonspecificity).

25.2 Reducing Algorithm Complexity for Computing Aggregate Uncertainty

Meyerowitz, Richman and Walker proposed an algorithm, the MRW algorithm, for calculating AU(Bel) from a given belief function. But this algorithm has high computing complexity. We propose an alternative algorithm for MRW. The idea of this algorithm is based on the observation that if one restricts a subset to the set of the focal elements included in it, its belief stays unchanged (from definition of a belief), while its size may decrease. So, one may consider only exact unions of focal elements rather than all the subsets. For this reason, we call this algorithm [7], $\mathcal{F}$-algorithm, as $\mathcal{F}$ represents the set of all focal elements of a belief function.

Input : The set of focal elements $\mathcal{F}$ of a belief function Bel and their corresponding basic probability assignments.

Output : AU(Bel), $\langle p_x | x \in \mathcal{C} \rangle$ such that $\mathrm{AU(Bel)} = -\sum_{x \in X} p_x \log_2 p_x$, $p_i \geq 0$, $\sum_{x \in \mathcal{C}} p_x = 1$, and $\mathrm{Bel}(A) \leq \sum_{x \in A} p_x \ \forall \ \varnothing \neq A \subseteq \mathcal{C}$.

Step 1. Initialization AU(Bel) = 0.

Step 2. Compute the belief measures for all elements of $\mathcal{F}$ and their unions. Suppose $|\mathcal{F}| = M$:

$$\begin{aligned}
&\mathrm{Bel}(A_i) = m(A_i) \quad \forall A_i \in \mathcal{F} \\
&\mathrm{Bel}(A_i \cup A_j) = m(A_i) + m(A_j) \quad \forall A_i, A_j \in \mathcal{F} \\
&\vdots \\
&\mathrm{Bel}(A_1 \cup A_2 \cdots \cup A_M) = \sum_{i=1}^{M} m(A_i)
\end{aligned}$$

Step 3. Find a set $A \in 2^{\mathcal{F}}$, such that $\frac{\mathrm{Bel}(A)}{|A|}$ is maximal. If there are more such sets A than one, take the one with maximal cardinality.

Step 4. For $x \in A$, put $p_x = \frac{\mathrm{Bel}(A)}{|A|}$; calculate $\mathrm{AU(Bel)} = \mathrm{AU(Bel)} - \mathrm{Bel}(A) \times \log_2 p_x$.

Step 5. For each focal element $B_i \in \mathcal{F}$, put $S_i = B_i - A \cap B_i$ (set difference).
– If $S_i = \varnothing$, then $\mathcal{F} = \mathcal{F} - \{S_i\}$;
– otherwise put $m(S_i) = m(B_i)$.
For each new focal element S, set $m(S) = \sum_{S_i = S} m(S_i)$ and prune all S_i such that $S = S_i$.

Step 6. If $|\mathcal{F}| > 1$, go to Step 2.

Step 7. If $|\mathcal{F}| = 1$, put $p_x = \frac{m(A)}{|A|}$ and $\mathrm{AU(Bel)} = \mathrm{AU(Bel)} - m(A) \times \log_2 p_x$

Note that in Step 5, we compute belief values directly instead of computing BPA. For each focal element B, let $B' = B \cap (X - A)$.

$$\mathrm{Bel}(B') = \mathrm{Bel}(B' \cup A) - \mathrm{Bel}(A) \tag{25.4}$$

25.3 Measures of Ambiguity

The $\mathcal{F}$-algorithm resolves the computing complexity problem, but it has nothing to do for other two problems (sh2 and sh3). An alterantive uncertainty measure, called AM was defined by [6] to resolve all these shortcomings.

Definition 2 *Let X be a frame of discernment with N elements, $X = \{x_1, x_2, \cdots, x_N\}$, and let m_X be a BPA defined on X. We define :*

$$\mathrm{AM}(m_X) = -\sum_{x \in X} \mathrm{BetP}_m(x) \log_2(\mathrm{BetP}_m(x)) \tag{25.5}$$

where BetP_m *is the pignistic probability distribution of* m_X.

©LRTS 2005-2006

We first proved that this measure AM satisfies the five requirements stated by Klir and Wierman for aggregate uncertainty measures in the theory of evidence (*Probability consistency, Set consistency, The range is* $[0, \log_2 |X|]$, *Subadditivity, Additivity*). Since the uncertainty measure of a body of evidence is not unique, this new measure is one of many such measures which satisfy all these requirements.

25.4 General Uncertainty Measure in the Fuzzy Evidence Theory Framework

Definition 3 *Let X be a finite set. Suppose the elements of the power set $\mathcal{P}(X)$ of X are selected according to the definition of finite random set on X :*

$$m_X : \mathcal{P}(X) \to [0,1] \quad \textit{with} \quad \sum_{\widetilde{A} \subseteq X} m_X(\widetilde{A}) = 1$$

The function m_X is the basic probability assignment (BPA) of a body of evidence but the set A is now defined as a fuzzy set with membership $\mu_{\widetilde{A}}(x_i)$ $\forall$ $x_i \in \widetilde{A}$.

Based on this definition, we know that fuzzy evidence includes all kinds of uncertainty as shown on Figure 25.2.

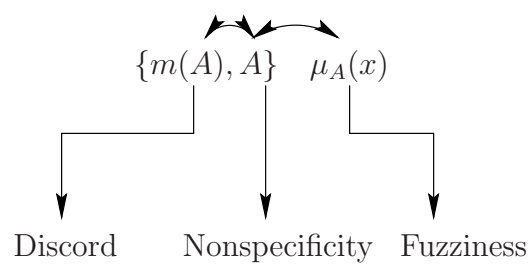


FIG. 25.2: fuzzy evidence

Fuzzy evidence can address all kinds of uncertainty :
1. $m_X(\widetilde{A})$ represents discord,
2. Subset $\widetilde{A}$ containing some elements of a finite given universal set X addresses the nonspecificity,
3. Membership $\mu_{\widetilde{A}}(x)$ of each subset $\widetilde{A}$ represents the fuzziness.

Then we create a new measure [8] able to take into account all kinds of uncertainty.

Definition 4 (GM) *Given a body of evidence $(m_X(A), A)$ on the power set of a finite set X, A is a fuzzy subset of X and with fuzzy membership degree $\mu_A(x_i)$ $\forall$ $x_i \in A$, and $m_X(A)$ is its basic probability assignment with $m_X : \mathcal{P}(X) \mapsto [0,1]$, $m_X(\varnothing) = 0$ and $\sum_{A \subseteq X} m_X(A) = 1$. We define :*

$$\mathrm{GM}(m_X, \mu) = -\sum_{x_i \in X} \left[\mathrm{BetP}(x_i) \log_2 \mathrm{BetP}(x_i) + \overline{\mathrm{BetP}}(x_i) \log_2 \overline{\mathrm{BetP}}(x_i) \right] \tag{25.6}$$

where

$$\mathrm{BetP}(x_i) = \sum_{x_i \in A \subseteq X} \frac{m_X(A)\mu_A(x_i)}{\sum_{x_j \in A} \mu_A(x_j)} \tag{25.7}$$

$$\overline{\mathrm{BetP}}(x_i) = \sum_{x_i \in A \subseteq X} \frac{m_X(A)(1-\mu_A(x_i))}{\sum_{x_j \in A} \mu_A(x_j)} \tag{25.8}$$

GM becomes equivalent to Shannon entropy, or Hartley function, including fuzziness measure. Our fuzzified Dempster-Shafer theory includes fuzzy set theory, Dempster-Shafer theory, crisp set theory, and probability theory. Possibility theory being a bridge between Dempster-Shafer theory and fuzzy set theory, it is also included in the fuzzified D-S theory. So we consider it to be a general method to represent uncertainty.

25.5 Conclusion

1) We give some justifications for reducing the computation of Aggregate Uncertainty measure (AU) to the core of the corresponding belief function, and propose an algorithm to calculate AU(Bel) which reduces the computing complexity of the MRW algorithm as proposed by A. Meyerowitz *et al.* . We prove that this algorithm leads to the same results as Meyerowitz's, and give conditions under which it significantly reduces the computing complexity.

2) In order to overcome the shortcomings (*complicated, insensitive, difficult to distinguish two kinds of uncertainty*) an alternative measure to AU for quantifying ambiguity of belief functions is proposed. This measure, called Ambiguity Measure (AM), besides satisfying all the requirements for general measures, also overcomes some of the shortcomings of AU.

3) A new measure, called General Measure (GM) is proposed, and it includes all kinds of uncertainty. We give the definition of GM, and we show that GM defined on fuzzy evidence theory, will be AM in evidence theory and imprecision measure (including fuzziness and nonspecificity) in fuzzy set theory under some conditions.

Bibliographie

[1] G. J. Klir and B. Yuan, *Fuzzy Sets and Fuzzy Logic : Theory and Applications* Prentice Hall PTR, 1995

[2] C. Liu, *A general measure of uncertainty-based information* Ph. D thesis, Laval University, 2004

[3] Y. Maeda, H. T. Nguyen and H. Ichihashi, "Maximum entropy algorithms for uncertainty measures" *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 1, pp. 69–93, 1993.

[4] D. Harmanec and G. J. Klir, "Measuring total uncertainty in Dempster-Shafer theory" *International Journal of General Systems*, vol. 22, pp. 153–163, 1994.

[5] G. J. Klir and R. M. Smith, "Recent Development in Generalize Information Theory", *International Journal of Fuzzy Systems*, vol. 1, pp. 1–13, 1999

©LRTS 2005-2006

[6] C. Liu, D. Grenier, A.-L. Jousselme, E. Bossé, "Reducing Algorithm Complexity for Computing an Aggregate Uncertainty Measure", *IEEE Trans. on Systems, Man and Cybernetics, Part A*, Marsh 2005. Accepted (# SMCA04-02-0040.R1).

[7] A.-L. Jousselme, C. Liu, D. Grenier and and É. Bossé, "Measuring Ambiguity in the Evidence Theory" *IEEE Transactions on Systems, man, and Cybernetics, Part A : Humans and Systems*, 2005. Accepted.

[8] C. Liu, A.-L. Jousselme, D. Grenier, E. Bossé, "General Uncertainty Measure of a Body of Evidence", *IEEE Trans. on Systems, Man and Cybernetics, Part A*, 2005. submitted.

Calcul d'incidence généralisé modifié

Marc-André Dumas, *Étudiant au 2e cycle*
Dominic Grenier, *Directeur de recherche.*
Anne-Laure Jousselme, *Co-directrice de recherche.*

Résumé – Le calcul d'incidence généralisé est une technique hybride symbolique-numérique qui présente un potentiel intéressant pour la fusion de données, notamment par sa correspondance possible avec la théorie de l'évidence. Nous présentons des modification permettant d'éliminer certaines limitations.

Abstract – Generalized Incidence Calculus is a hybrid symbolic-numeric approach to data fusion that presents many interesting characteristics, in particular a correspondence with the Theory of Evidence. We present modifications that eliminates some of its limitations.

26.1 Introduction

Le calcul d'incidence (Incidence Calculus) a été introduit par Alan Bundy en 1985 [1]. Celui-ci voulait intégrer des mesures numériques aux raisonnements symboliques fréquemment utilisés dans la logique afin d'y intégrer la notion d'incertitude. La plupart des tentatives jusqu'alors consistaient à assigner des valeurs numériques directement aux règles et aux informations afin d'en déterminer la certitude. Généralisé par Weiru Liu [2] afin de s'approcher de la théorie de l'évidence[3], le calcul d'incidence présente un potentiel très intéressant. Après avoir présenté les grandes lignes de cette théorie, nous présentons quelques modifications qui en améliorent les performances.

26.2 Approches numériques et symboliques

Approches numériques

On est porté à attribuer des valeurs numériques lors de la modélisation de l'information incertaine. L'approche numérique est naturellement intéressante, mais comporte un certain nombre de défauts. D'abord, il est généralement difficile de gérer des informations qui ne sont pas indépendantes avec cette approche. Aussi, les approches numériques ne restent pas nécessairement aussi intuitives après quelques combinaisons, principalement puisqu'il devient difficile d'expliquer à un humain la signification d'un chiffre représentant une incertitude. La théorie de l'évidence de Dempster et Shafer est un très bon exemple d'une telle approche numérique.

Approches symboliques

Les approches purement symboliques utilisent des informations précises pour en sortir des conclusions précises. Un exemple bien connu d'une approche symbolique est l'algèbre de Boole.

Les approches symboliques sont attirantes en raison de leur rigueur logique. Ils ont la particularité de laisser des traces de leur raisonnement qui permettent à un humain de comprendre la logique derrière la réponse. La rigueur des approches purement symboliques est aussi leur inconvénient majeur : ils ne peuvent pas représenter et raisonner lorsqu'elles sont en présence de propositions incertaines. Certains efforts ont tout de même été faits pour créer des systèmes logiques symboliques capables de répondre à cette demande[4].

Approches hybrides

Les approches numériques et symboliques ayant chacune leurs avantages, il est normal que l'on soit tenté de les combiner de manière à récupérer leurs meilleures caractéristiques. Plusieurs méthodes sont utilisées pour combiner les deux approches [2], citons notamment la superposition de mesures numériques à des raisonnements symbolique où des mesures de certitude numériques peuvent être calculées à partir des inférences, mais n'influencent pas le raisonnement. Le calcul d'incidence est une technique de ce type.

26.3 Le calcul d'incidence

Alan Bundy a noté que les limitations des méthodes purement numériques au niveau de l'indépendance de l'information compliquaient la combinaison d'informations. En effet, il est nécessaire de conserver la mesure de corrélation entre chacune des propositions du système, ce qui est très difficile lorsque le nombre d'informations est grand. C'est pourquoi Bundy a proposé une solution à base d'ensembles pour permettre de résoudre ce problème de dépendance, le calcul d'incidence[1].

Weiru Liu a apporté certaines améliorations[2] au calcul d'incidence pour lui permettre d'abord de combiner de l'information de la manière de la combinaison de Dempster ce qui a donné le calcul d'incidence généralisé (CIG, *Generalized Incidence Calculus*).

Cette théorie est basé sur le concept d'univers. Posons un ensemble de points $\mathcal{W}$, chaque point étant un univers possible, dans lequel une proposition sera vraie ou fausse. Ces points sont exhaustifs et disjoints. Prenons par exemple quatre univers qui représentent l'univers ensoleillé (w_1), l'univers pluvieux (w_2), l'univers variable (w_3) et l'univers nuageux (w_4). Ces univers sont mutuellement exclusifs puisque que sont des points distincts, totalement indépendants. Un observateur se retrouve dans un, et un seul des univers à la fois. On peut ensuite attribuer à chacun de ces univers la probabilité que ce soit l'univers dans lequel on se trouve.

Définition 26.1 *Une théorie du calcul d'incidence généralisé (Generalized Incidence Calculus Theory, ou GICT) est une modélisation de l'information sous la forme d'un tuplet tel que :*

$$< \mathcal{W}, \mu, \mathcal{P}, \mathcal{A}, i > \tag{26.1}$$

où :

- $\mathcal{W}$ *: L'ensemble fini des univers possibles*
- *Pour tout* $w \in \mathcal{W}$*,* $\mu(w)$ *est la probabilité de* w *et* $\mu(\mathcal{W}) = 1$*, puisque* $\mu(I) = \sum_{w \in I} \mu(w)$
- $\mathcal{P}$ *: Ensemble fini de propositions atomiques. Ex. :*$\{a, b, c\}$*. Chaque proposition atomique peut avoir l'état vrai, faux ou inconnu.*
- $\mathcal{A}$ *: Sous-ensemble de* $\mathcal{L}(\mathcal{P})$ *sur lequel on a de l'information. vrai et faux font toujours partis de cet ensemble. Ex. :* $\{a, b, a \vee b, a \wedge c, vrai, faux\}$
- i *est une fonction qui fait une transformation* $\mathcal{A} \rightarrow 2^{\mathcal{W}}$*.* $i(\phi)$ *est l'ensemble des univers dans* $\mathcal{W}$ *pour lequel* ϕ *a une valeur vraie, i.e.,* $i(\phi) = \{w \in \mathcal{W} \mid w \models \phi\}$*.*

$\mathcal{L}(\mathcal{P})$ et $\mathcal{L}(\mathcal{A})$, utilisé plus loin, nécessitent la définition :

Définition 26.2 *Langage propositionnel* $\mathcal{L}(O)$ *:*
Si O *est un ensemble fini de propositions, son langage propositionnel est formé des éléments suivants :*
- *vrai, faux* $\in \mathcal{L}(O)$
- *si* $q \in O$*, alors* $q \in \mathcal{L}(O)$
- *si* $\phi, \psi \in \mathcal{L}(O)$ *alors* $\neg\phi, \neg\psi, \phi \wedge \psi, \phi \vee \psi, \phi \rightarrow \psi, \psi \rightarrow \phi \in \mathcal{L}(O)$

C'est donc dire que $\mathcal{L}(O)$ *est fermé avec les opérateurs logiques de négation (*$\neg$*), de disjonction (*$\vee$*), de conjonction (*$\wedge$*) et d'implication (*$\rightarrow$*).*

Il est parfois nécessaire de transférer deux GICT de manière à ce qu'ils partagent le même ensemble d'univers.

Définition 26.3 *Transformation des GICT :*
Soient $< \mathcal{W}_1, \mu_1, \mathcal{P}_1, \mathcal{A}_1, i_1 >$ *et* $< \mathcal{W}_2, \mu_2, \mathcal{P}_2, \mathcal{A}_2, i_2 >$*, deux GICT qui peuvent être transformées en :*

$$< \mathcal{W}_3, \mu_3, \mathcal{P}_3, \mathcal{A}_1, i'_1 > \tag{26.2}$$

et

$$< \mathcal{W}_3, \mu_3, \mathcal{P}_3, \mathcal{A}_2, i'_2 > \tag{26.3}$$

où :
- $\mathcal{W}_3 = \mathcal{W}_1 \otimes \mathcal{W}_2 \setminus \mathcal{W}_0$
- $\mathcal{W}_0 = \bigcup_{\phi \wedge \psi \models faux} i_1(\phi) \otimes i_2(\psi)$
- $i'_1(\phi) = (i_1(\phi) \otimes \mathcal{W}_2) \setminus \mathcal{W}_0$*, lorsque* $\phi \in \mathcal{A}_1$
- $i'_2(\phi) = (\mathcal{W}_1 \otimes i_2(\phi)) \setminus \mathcal{W}_0$*, lorsque* $\phi \in \mathcal{A}_2$
- $\mathcal{P}_3 = \mathcal{P}_1 \cup \mathcal{P}_2$

La nouvelle distribution de probabilité sur $\mathcal{W}_3$ *est donnée par :*

$$\mu_3(\langle w_{1i}, w_{2j} \rangle) = \frac{\mu_1(w_{1i})\mu_2(w_{2j})}{1 - \sum_{\langle w_{1m}, w_{2n} \rangle \in \mathcal{W}_0} \mu_1(w_{1m})\mu_2(w_{2n})} \tag{26.4}$$

Une fois que l'on a deux GICT avec le même ensemble $\mathcal{W}$, on peut procéder à la combinaison en tant que telle.

©LRTS 2005-2006

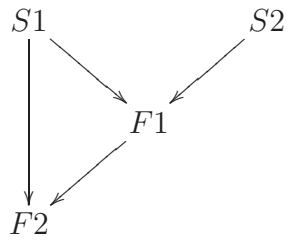


FIG. 26.1: Combinaison des sources S1 et S2 en F1, puis recombinaison de S1.

Règle de combinaison

Définition 26.4 *Règle de combinaison :*
Soient $< \mathcal{W}, \mu, \mathcal{P}, \mathcal{A}_1, i_1 >$ *et* $< \mathcal{W}, \mu, \mathcal{P}, \mathcal{A}_2, i_2 >$*, deux GICT avec un ensemble d'univers commun. Le résultat de la combinaison de ces deux GICT est donné par :*

$$< \mathcal{W} \setminus \mathcal{W}_0, \mu', P, \mathcal{A}, i > \tag{26.5}$$

où :
- $\mathcal{W}_0 = \bigcup\{i_1(\phi) \cap i_2(\psi) \mid \phi \wedge \psi = \mathit{faux}, \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2\}$
- $\mathcal{A} = \{\varphi \mid \varphi = \phi \wedge \psi, \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2, \varphi \neq \mathit{faux}\}$
- $i(\varphi) = \bigcup\{i_1(\phi) \cap i_2(\psi) \mid \phi \wedge \psi \models \varphi, \varphi \in \mathcal{A}, \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2, \phi \wedge \psi \neq \mathit{faux}\} \cup \{\mathit{faux}\}$
- *Pour tout* $w \in \mathcal{W} \setminus \mathcal{W}_0, \mu'(w) = \frac{\mu(w)}{1-\sum_{w' \in \mathcal{W}_0} \mu(w')}$
- $i(\mathit{vrai}) = \mathcal{W} \setminus \mathcal{W}_0$, $i(\mathit{faux}) = \emptyset$

Le CIG comporte toutefois une limitation importante : elle ne peut gérer certains cas, notamment celui de la Figure 26.1. Dans ce cas, l'information provenant de la source S1 est surenforcée si un conflit existe entre S1 et S2. De la même manière que la théorie de l'évidence ne peut combiner des information dépendantes en raison de perte d'informations, le CIG ne peut combiner le cas énoncé en raison d'information perdue en présence de conflit.

26.4 Parallèle avec la théorie de l'évidence

Une caractéristique importante du calcul d'incidence est l'existence de bornes inférieures et supérieures d'incidence, analogues à ce que l'on connaît dans la théorie de l'évidence.

$$i_*(\phi) = \bigcup_{\psi \in \mathcal{L}(\mathcal{A})} \{i(\psi) \mid \psi \models \phi\} \tag{26.6}$$

$$i^*(\phi) = \bigcap_{\psi \in \mathcal{L}(\mathcal{A})} \{i(\psi) \mid \phi \models \psi\} \tag{26.7}$$

Il a été démontré par Liu et Bundy [5] que le calcul d'incidence généralisé est équivalent à la théorie de l'évidence pour la combinaison d'informations DS-indépendantes. Il a d'abord été démontré que : [5]

Théorème 1 (Représentation de l'évidence) *Pour toute structure DS (Θ, Bel), il existe une GICT. Pour tout sous-ensemble A de Θ et sa formule correspondante ϕ_A dans $\mathcal{L}(\mathcal{P})$, Bel(A) dans la théorie de l'évidence est égale à $p_*(\phi_A)$ dans la GICT.*

$$Bel(A) = \mu(i_*(\phi_A)) \tag{26.8}$$

Il en découle que la plausibilité correspond à la probabilité de la borne supérieure de l'incidence :

$$\mathrm{Pl}(A) = \mu(i^*(\phi_A)) \tag{26.9}$$

Il est aussi prouvé que la combinaison est équivalente : [5]

Théorème 2 (Combinaison d'information DS-indépendantes) *Soient (Θ, Bel_1) et (Θ, Bel_2), deux structures DS et Bel_1 et Bel_2 sont obtenues de deux informations DS-indépendantes, et que la combinaison de ceux-ci donne une structure DS (Θ, Bel). De plus, $< \mathcal{W}_1, \mu_1, \mathcal{P}_\Theta, \mathcal{A}_1, i_1 >$ et $< \mathcal{W}_2, \mu_2, \mathcal{P}_\Theta, \mathcal{A}_2, i_2 >$ sont deux GICT produites à partir des deux premières structures DS et que $< \mathcal{W}, \mu, \mathcal{P}_\Theta, \mathcal{A}, i >$ est la GICT combinée, alors (Θ, Bel) est équivalente à $< \mathcal{W}, \mu, \mathcal{P}_\Theta, \mathcal{A}, i >$. Cela veut donc dire que pour tout sous-ensemble A de Θ,*

$$Bel(A) = \mu(i_*(\phi_A)) \tag{26.10}$$

26.5 Modifications

Afin d'enlever certaines limites au CIG, nous en redéfinissons les concepts de manière à éviter la perte d'information lors des combinaisons[6]. Le principal changement apporté se situe au niveau du traitement des univers dans lesquels des contradictions logiques existent. Dans le CIG, ces univers sont éliminés. Ici, nous ne faisons que marquer ces univers d'un drapeaux. Ce marquage évite la perte d'information et permet des combinaisons complètement symboliques. Les opérations numériques sont repoussées à la toute fin du traitement.

Définition 26.5 *Univers :*
Situation dans laquelle on se trouve. Il y a une infinité d'univers, membres de l'ensemble $\mathcal{S}$. La somme des probabilités de chacun des univers est unitaire.

$$\sum_{w \in \mathcal{S}} Prob(w) = 1 \tag{26.11}$$

Définition 26.6 *Contexte initial :*
Un contexte initial $\mathcal{W}$ est l'ensemble des sous-ensembles d'une partition de l'ensemble des univers $\mathcal{S}$ représentant une connaissance. Chaque sous-ensemble de la partition est appelé univers initial.

Définition 26.7 *Contexte combiné :*
Produit cartésien de deux contextes, initiaux ou combinés, tel que :

$$\mathcal{W}_c = \mathcal{W}_a \times \mathcal{W}_b \tag{26.12}$$

Il est à noter que $\mathcal{W}_a \times \mathcal{W}_b$ et $\mathcal{W}_b \times \mathcal{W}_a$ sont équivalents.

©LRTS 2005-2006

Modélisation de l'information

Dans la prochaine définition, le texte en gras mets en évidence les modifications apportées par rapport au CIG.

Définition 26.8 *Modèle d'incidence (MI) :*
Un modèle d'incidence est un tuplet tel que :

$$< \mathcal{W}, \mathcal{W}^F, \mu^0, \mathcal{P}, \mathcal{A}, i > \tag{26.13}$$

où :

- $\mathcal{W}$ *: Contexte du modèle. Il peut s'agir d'un contexte initial ou combiné.* ***Il peut contenir des univers impossibles.***
- $\mathcal{W}^F$ ***: L'ensemble des ensembles d'univers du contexte*** $\mathcal{W}$ ***dans lesquels des contradictions logiques surviennent.***
- μ^0 ***: Fonction de distribution des probabilités sur chacun des contextes initiaux du modèle, même après combinaison.***
- $\mathcal{P}$ *: Ensemble fini de propositions atomiques. Ex. :*$\{a, b, c\}$
- $\mathcal{A}$ *: Sous-ensemble de* $\mathcal{L}(\mathcal{P})$ *sur lequel on a de l'information. vrai et faux font également partis de cet ensemble. Ex. :* $\{a, b, a \vee b, a \wedge c, vrai, faux\}$
- i *:* $i(\phi)$ *est l'ensemble des univers dans* $\mathcal{W}$ *pour lequel* ϕ *a une valeur vraie et auquel on a retiré les univers impossibles* $\mathcal{W}^F$*, i.e.,* $i(\phi) = \{w \in \mathcal{W} \setminus \mathcal{W}^F \mid w \models \phi\}$.

La probabilité d'un ensemble d'univers est donnée par :

$$\mu(w) = \begin{cases} \mu_\cap(w) + \frac{\mu_\cap(w) \cdot \mu(\emptyset)}{1-\mu(\emptyset)} = \frac{\mu_\cap(w)}{1-\mu(\emptyset)} & \forall w \subseteq \mathcal{W} \setminus \mathcal{W}^F \\ 0 & ailleurs \end{cases} \tag{26.14}$$

avec

$$\mu_\cap(w) = \prod_{w_j \in w} \mu^0(w_j) \tag{26.15}$$

$$\mu(\emptyset) = \sum_{w \in \mathcal{W}^F} \mu_\cap(w) \tag{26.16}$$

Combinaison de l'information

Deux informations sous forme de MI se combinent en suivant les étapes décrites ci-après.

Étape 1 : La création d'un contexte commun.

Cette étape optionnelle est nécessaire si les deux MI ont des contextes $\mathcal{W}$ différents. On doit alors modifier les deux MI, disons MI_1 et MI_2 pour leur attribuer un nouveau contexte.

$$\mathcal{W}_3 = \mathcal{W}_1 \times \mathcal{W}_2 \tag{26.17}$$

Puisque les fonctions i_1 et i_2 des MI font référence respectivement à $\mathcal{W}_1$ et $\mathcal{W}_2$, on doit également les modifier pour qu'ils réfèrent au contexte $\mathcal{W}_3$.

$$i'_1(\phi) = i_1(\phi) \times \mathcal{W}_2 \tag{26.18}$$

$$i'_2(\phi) = \mathcal{W}_1 \times i_2(\phi) \tag{26.19}$$

Les fonctions μ^0 seront alors combinées de manière à ce que la transformation d'un univers du contexte initial vers une probabilité reste la même. Cela revient à faire une concaténation de μ_1^0 et μ_2^0 en un μ_3^0. L'on doit aussi ajuster les ensembles en conflit $\mathcal{W}^F$:

$$\mathcal{W}_1^{F'} = \mathcal{W}_1^F \times \mathcal{W}_2 \tag{26.20}$$

$$\mathcal{W}_2^{F'} = \mathcal{W}_1 \times \mathcal{W}_2^F \tag{26.21}$$

Étape 2 : Détection des conflits.

L'ensemble $\mathcal{W}_3^C$ contient les univers dans lesquels des impossibilités logiques surviennent, c'est à dire $\phi \wedge \psi \models$ faux. Cela revient à vérifier si la proposition $\phi \wedge \psi$ est validable.

$$\mathcal{W}_3^C = \bigcup_{\phi \wedge \psi \models \text{faux}} i'_1(\phi) \cap i'_2(\psi) \qquad \forall\ \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2 \tag{26.22}$$

On forme finalement l'ensemble $\mathcal{W}_3^F$ en ajoutant les $\mathcal{W}^F$ des prémisses, ce qui permet de garder les traces des univers impossibles qui étaient déjà détectés lors des combinaisons précédentes.

$$\mathcal{W}_3^F = \mathcal{W}_1^{F'} \cup \mathcal{W}_2^{F'} \cup \mathcal{W}_3^C \tag{26.23}$$

Si une proposition était impossible dans un des deux MI, elle le restera dans le MI combiné.

Étape 3 : Construction des nouveaux axiomes et propositions.

On construit l'ensemble des axiomes $\mathcal{A}_3$ en prenant les axiomes des deux MI combinés et en ajoutant de nouveaux axiomes créés par la conjonction de ceux-ci. Puisque les ensembles $\mathcal{A}_1$ et $\mathcal{A}_2$ comprennent les propositions vrai et faux, l'opération suivante sera suffisante :

$$\mathcal{A}_3 = \{\varphi \mid \varphi = \phi \wedge \psi, \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2, \varphi \not\models \text{faux}\} \cup \{\text{faux}\} \tag{26.24}$$

Le contenu de l'ensemble des propositions $\mathcal{P}_3$ sera le résultat d'une simple union :

$$\mathcal{P}_3 = \mathcal{P}_1 \cup \mathcal{P}_2 \tag{26.25}$$

Étape 4 : Création de nouvelles fonctions d'incidence

On doit finalement créer une fonction d'incidence qui tiendra compte des nouvelles propositions créées grâce à la disjonction.

$$i_3(\varphi) = \bigcup \{i'_1(\phi) \cap i'_2(\psi) \ \mid (\phi \wedge \psi \models \varphi), \phi \in \mathcal{A}_1, \psi \in \mathcal{A}_2, \phi \wedge \psi \not\models \text{faux}\} \setminus \mathcal{W}_3^F \tag{26.26}$$

On est maintenant en mesure de former un MI_3 tel que :

$$< \mathcal{W}_3, \mathcal{W}_3^F, \mu^0, \mathcal{P}_3, \mathcal{A}_3, i_3 > \tag{26.27}$$

©LRTS 2005-2006

26.6 Conclusion

On retrouve dans [6] une démontration de la capacité du calcul d'incidence généralisé modifié (CIGM) à gérer le cas de la Figure 26.1. Puisqu'on peut gérer un tel cas, le CIGM peut être utilisé dans la résolution de problème de bouclage d'information, situation où une information est combinée à plusieurs reprises à la suite d'échange entre des unités de traitement séparées, ce qui peut mener à un surenforcement de l'information bouclée.

Une caractéristique importante de la modification apportée est qu'elle exclut toutes opérations numériques des combinaisons et se concentre sur les opérations symboliques. Cela a comme avantage de réduire le nombre d'opérations à virgule flottante nécessaires pour l'obtention des résultats. De plus, le fait d'avoir des expressions symboliques permet d'effectuer facilement certaines analyses graphiques et algébriques qui sont plus coûteuses sur le plan de temps de calcul avec l'utilisation d'un traitement numérique. Certains outils de calculs peuvent être utilisés, comme le gradient, de manière à déterminer par exemple quelle source est la plus critique dans une identification.

Le calcul d'incidence généralisé modifié (CIGM) présente beaucoup de flexibilité au niveau du type de combinaison possible. Même s'il a été conçu pour la combinaison de Dempster, il a été démontré dans [6] que de légères modifications permettent de créer une combinaison de Yager[7] associative. D'autres modifications permettent au CIGM d'émuler la théorie de Dezert-Smarandache (DSmT)[8].

Bibliographie

[1] A. Bundy, "Incidence calculus : A mechanism for probabilistic reasoning," *J. Autom. Reason.*, vol. 1, no. 3, pp. 263–283, 1985.

[2] W. Liu, *Propositional, Probabilistic and Evidential Reasoning*. Studies in Fuzziness and Soft Computing, Physica-Verlag, 2001.

[3] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[4] P. Maupin, A.-L. Jousselme, and É. Bossé, "Logical and mathematical perspectives in high-level information fusion," Tech. Rep. TR 2002-233, Recherche et développement pour la défense Canada - Valcartier, 2005. en rédaction.

[5] W. Liu and A. Bundy, "A comprehensive comparison between generalized incidence calculus and the Dempster-Shafer theory of evidence," *International Journal of Human-Computer Studies*, vol. 40, no. 6, pp. 1009–1032, 1994.

[6] M.-A. Dumas, "Application du calcul d'incidence à la fusion de données," Master's thesis, Université Laval, 2006.

[7] R. R. Yager, "On the dempster-shafer framework and new combination rules," *Information Sciences*, vol. 41, pp. 93–137, Mar. 1987.

[8] F. Smarandache and J. Dezert, eds., *Advances and Applications of DSmT for Information Fusion*. American Research Press, 2004.

Scope of Contribution to Maritime Surveillance

Melita Hadzagic, *Étudiante au doctorat*
Hannah Michalska, *Directrice de recherche.*
Dominic Grenier, *Co-directeur de recherche.*

Résumé – La marine Canadienne maintient une série de donnés relative à l'activité maritime. Ce regroupement de donnés est mieux connu sous le nom de tableau de la situation maritime (TSM). Sous sa présente forme, le TSM permet l'agglomération de reneseignements provenant de plusieurs agences vers un seul post d'affichage. Par contre, ce dernier n'est doté que d'une capacité limitée en se qui à trait à la fusion des donnés de surveillance, plus précisément : une capacité limitée à integrer les rensegneiments provenant des sources divers. Cette thése vise à améliorer la compréhension de donnés, à l'amélioration des techniques de fusion de donnés et du même fait, à l'amélioration du TSM. Un fondement théorique a été exaustivement préparé et un scenario de test informatisé a été conçu pour appuyer ce dernier. Le présent corps de recherche s'attarde à l'évaluation de deux types d'algorithmes afin d'établir les fondations d'un nouvel "track-to-track" algorithme de fusion.

Abstract – The Canadian Navy maintains a picture of maritime activity known as the Recognized Maritime Picture (RMP). As currently compiled, it is capable of combining data from multiple agencies in one display, but is limited in its ability to effectively fuse surveillance data, i.e. to integrate information coming from dissimilar sources. The contribution of this Thesis aims at better understanding of the data to be fused and enhancement of the data fusion techniques, hence the RMP. An extensive theoretical background research has been carried out and a test scenario which simulates ground truth and fused sensor data has been developed in C++. Current research involves an evaluation of two types of tracking algorithms in order to lay out foundations for a novel track-to track fusion algorithm.

27.1 Introduction

As part of Canada's comprehensive surveillance and awareness of activity in the maritime domain, the Canadian Navy maintains a picture of maritime activity known as the Recognized Maritime Picture (RMP).

The RMP as currently complied, using Global Command and Control System-Maritime (GCCS-M), is capable of combining data from multiple agencies in one display, but is limited in its ability to effectively fuse surveillance data, i.e. to integrate information coming from dissimilar sources.

The information sources may include High Frequency Surface Wave Radar (HFSWR), detection of ships' radars, Automated Identification System (AIS), Aircraft, Uninhabited Aerial Vehicles (UAVs) or space based sensors. Although the combined awareness provided by such a range of information sources is potentially high, their full value cannot be realized without effective fusion.

In addition to the challenges described above, even existig data in the current RMP is under utilized due to the operator overload, inadequate fusion techniques, lack of automation, and poor integration techniques.

The research toward this PhD Thesis involves solving the challenge of integrating new sources which will enhance the RMP, while allowing for more effective use of existing sources. Additionally, a better understanding of the information to be fused, and the use of enhanced fusion techniques, should allow significant improvement of the RMP.

27.2 Toward the RMP Improvement

Background Research

The background research involved :

1. Studying the properties of the information sources used in compiling the RMP, namely the HFSWR and AIS, [1, 2]. The main features of these sensors are briefly summarized below.
   HFSWR :
   – Area of coverage : $200nm \times 200nm$,
   – Continuous tracking,
   – Track accuracy : $\sim 0.25nm$ in range, 0.25 degree in azimuth, and 0.5 knots in velocity.
   AIS :
   – Data that can be transmitted : a) *static*, such as name, ship type, etc. (every 6 minutes and on request), b) *dynamic*, such as position, course over ground, speed over ground, etc. (at variable rate, depending on speed and course alteration), or c) *voyage related*, such as ship draught, hazardous cargo type, destination and ETA, etc. (6 minutes on request and when amended)
   – Different modes of tracking (autonomous and continuous, assigned or polling)
   – Track accuracy : Ship $0-14$knots-$0-86$m, ship $14-23$knots-$43-71$m, ship $0-4$knots and changing course-$0-29$m, ship$>$ 23knots-35m at 23kn.

2. Studying the available information fusion techniques other than probability theory, such as evidence theory, possibility theory and fuzzy set theory [3, 4, 5]. Special emphasis was put on studying the quality of information and available methodologies for incorporating uncertainty, relevance, completeness and reliability in the information fusion process. The results are summarized in [6].

3. Investigation of the tracking algorithm currently used within GCCS-M, namely Maneuvering Target Statistical Tracker (MTST) [7]. Developed in the early 1980', this tracker was chosen as the standard tracker for at-sea targets. For the purpose of its in-depth understanding a detailed mathematical description of MTST is presented in [8].

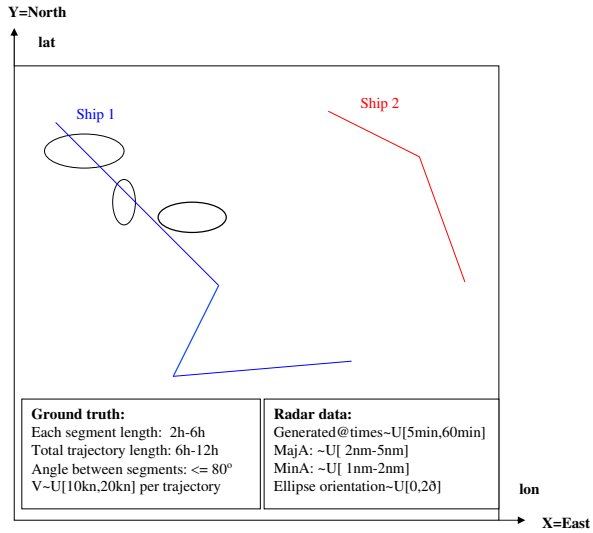


FIG. 27.1: A snapshot of the scenario

Ongoing Research

To lay out foundations for a novel track-to-track fusion algorithm that will lead to improvement of the RMP, an evaluation of the tracking performance of the MTST is proposed. This evaluation includes performance comparison between the MTST and a tracking algorithm which uses a genetic algorithm (GA) to generate the track model [9].

The performance comparison will be carried out in terms of estimation errors (e.g RMSE) and it will be based on a developed scenario. The scenario covers the area of 200nm $\times$ 200nm. It includes simulated ground truth and fused sensor data. The simulated ground truth allows for as many ships present in the surveillance area as determined by input. The software development was done using C++. A snapshot of the scenario is provided in the Figure 27.1.

Tracking Algorithms

MTST

The MTST uses integrated Ornstein-Uhlenbeck (IOU) and random walk (RW) stochastic processes to describe the system motion model.

The formulation of the IOU model used by MTST is given in terms of state vector components :

$$dx(t) = u(t)dt \tag{27.1}$$

$$dy(t) = v(t)dt \tag{27.2}$$

$$du(t) = -\beta u(t) + \sigma dW(t) \tag{27.3}$$

$$dv(t) = -\beta v(t) + \sigma dW(t) \tag{27.4}$$

where $x(t)$ is x-coordinate, $y(t)$ is y-coordinate, $u(t)$ and $v(t)$ are the x and y-components of the velocity of the process, respectively, and $dW(t)$ represents random disturbances described by a white noise (Wiener differential) process, with scale parameter $\sigma > 0$.

©LRTS 2005-2006

The MTST approach involves using RW model as a means to relate the IOU model (via its parameters) to RW parameters. The RW model is defined by

$$E[R_t^2] = \frac{2V^2}{\alpha^2}(e^{-\alpha t} - 1 + \alpha t) \tag{27.5}$$

$$R_t^2 = x_t^2 + y_t^2 \tag{27.6}$$

where V is a constant speed, and all times-on-leg are chosen independently from an exponential distribution with mean value $1/\alpha$. Then, the IOU model can be expressed in terms of RW parameters as :

$$E[x(t)] = 0 \tag{27.7}$$

$$E[y(t)] = 0 \tag{27.8}$$

$$var[x(t)] = E[x(t)^2] = \frac{V^2}{\alpha^2}(e^{-\alpha t} - 1 + \alpha t) \tag{27.9}$$

$$var[y(t)] = E[y(t)^2] = \frac{V^2}{\alpha^2}(e^{-\alpha t} - 1 + \alpha t) \tag{27.10}$$

$$cov[x(t), y(t)] = 0 \tag{27.11}$$

Detailed mathematical description of calculating the track parameters can be found in [7, 8].

GA-based

The GA-based tracking algorithm under investigation is a hybrid optimization algorithm based on GA and simulated annealing algorithm (SAA). In [9] is used as a batch type of algorithm. Different states of the track are represented by chromosomes which are made up from contacts ordered in time. Each gene represents a contact and has two possible values, 0 or 1. Value 1 always represents the beginning of a segment or end of a track. The track is assumed to be consisted of up to three linear segments. The initial state of population is randomly generated, one segment having at least four contacts.

The cost (fitness) function to minimize is given by

$$COST = \sum_{s=1}^{ns} (\frac{\chi^2}{\upsilon})_s \tag{27.12}$$

where

$$\frac{\chi^2}{\upsilon} = \frac{1}{2n-4} \sum_{q=x,y} \sum_{i=1}^{n} \Big(\frac{q_i - (\alpha_q + \beta_q t_i)}{\sigma_{q_i}} \Big)^2 \tag{27.13}$$

and, υ is the number of degrees of freedom, ns is the number of segments, n is the number of contacts in segment, q_i is x or y axis, α_q and β_q are the track parameters calculated analytically, and σ_{q_i} are the values of maximum error projections.

The generation with a lowest cost is selected to form a track. The algorithm ends when the state with the lower cost is same for ten generations in a row. This algorithm needs to be refined in terms of accounting for correlated and heteroscedastic measurements.

27.3 Summary and Future Research

The RMP needs to be improved in terms of dissimilar data fusion. The first proposed step toward its improvement is the evaluation of the MTST, which is currently used in compiling the RMP. The evaluation will include performance comparison with a GA-based tracking algorithm, which is proved to be very successful in ship tracking [9], using a C++ developed designated scenario and Monte-Carlo simulations. The evaluation will allow to choose better performing tracking algorithm, to improve its shortcomings by taking into account the nature of dissimilar data, and hence lay ot foundations for improved track-to track fusion.

Bibliographie

[1] A.M, Ponsford "Surveillance of the 200nm Exclusive Economic Zone (EZZ) Using HFSWR," *Proceednings of the* 7th *ICCRTS*, 2002.

[2] Association of AIS and radar data, MCA tech. report prepared by SML Technologies Ltd.,UK, December 2002.

[3] G. Shafer, *A mathematical theory of evidence*. Princeton University Press, 1976.

[4] A. Motro and P. Smets, editors *Uncertainty Management in Information Systems : from needs to solutions*. Kluwer Academic Publishers, 1997.

[5] G.J. Klir and T.A. Folger, *Fuzzy Sets, Uncertainty and Information*. NJ, Prentice Hall, 1988.

[6] E. Lefebvre, M. Hadzagic, É. Bossé, "On Quality of Information in Multi-Source Fusion Environments," *to appear in NATO ASI book*, 2006.

[7] Over-The-Horizon/Detection Classification and Targeting (OTH/DC&T) System Level Specification Ship Tracking Algorithm, tech.report, Tiburon Systems, Inc., San Hose, CA, 1991.

[8] M. Hadzagic, "Mathematical description of the MTST," report, McGill University, Laval University, Lockheed-Martin Canada, 2006, version 1.0.

[9] E. Lefebvre, C. Helleur, "Automated Association of Track Information from Sensor Sources with Non-Sensor Information in the Context of Maritime Surveillance," *Proc. of Intl. Conference of Information Fusion*, 2004.

©LRTS 2005-2006

V

Antennes et Radar

Table des Matières

Réseaux d'antennes en ondes millimétriques. **173**
Calibrage des réseaux d'antennes par réseaux de neurones artificiels **181**
Emploi du signal XM comme source d'opportunité d'un système non coopératif pour la détection passive cohérente **191**
Simulation de la section efficace radar sur une trajectoire **195**

Réseaux d'antennes en ondes millimétriques.

Jean-Sébastien Néron, *Candidat au doctorat*
Dr Gilles-Y. Delisle, *Directeur de recherche*
Dr Dominic Grenier, *Codirecteur de recherche*

Résumé – Ce sommaire présente l'état d'avancement des travaux de conception et réalisation de composants microruban pour utilisation en bande EHF (36 GHz) et fonctionnant sur une largeur de bande d'au moins 400 MHz. Les éléments présentés sont un coupleur hybride, un coupleur 0 dB, une interconnexion verticale à couplage électromagnétique, une matrice de Butler 8 × 8 et un dipôle planaire à BALUN intégré. Les références aux publications détaillant explicitement les étapes de conception, simulations et les mesures sont données.

Abstract – This paper summarizes design as well as measurements results of microstrip components operating over a bandwidth of at least 400 MHz at EHF band (36 GHz). The devices described are a quadrature hybrid, a 0 dB coupler, a vertical interconnection using electromagnetic coupling, an 8×8 Butler matrix, and a printed dipole with integrated BALUN. References to the complete design, simulations, and measurement details are also provided.

28.1 Introduction

Depuis la parution du dernier rapport annuel du LRTS, plusieurs travaux ont eu lieu en électronique micro-ondes au laboratoire afin entre autres de réaliser une antenne réseau à faisceaux multiples en bande EHF (Extremely High Frequency), bande pour laquelle les fréquences excèdent 30 GHz. Afin d'obtenir une telle réalisation (voir figure 28.2), une multitude de composants s'avèrent nécessaires et les résultats des dernières conceptions sont ici présentés en condensé. Dans un premier temps, il sera question de dispositifs micro-ondes dont un coupleur hybride, un coupleur 0 dB, une interconnexion verticale à couplage électromagnétique. Ensuite, un dipôle planaire à BALUN intégré et une matrice de Butler 8×8 utilisant ces composants seront présentés.

28.2 Sélection du substrat

Les divers dispositifs microruban dont il est question ici ont été conçus et réalisés sur un assemblage de lignes microruban à couches doubles illustré à la figure 28.1. Le substrat utilisé est le RT/Duroid 5880 du fabricant Rogers d'une épaisseur de 0.254 mm. Celui-ci a été sélectionné parce qu'il a une permittivité faible ($\epsilon_r = 2.2$), ce qui favorise le rayonnement des antennes, et aussi pour ses faibles pertes diélectriques ($\tan\delta = 0.0009$) qui font en sorte que l'efficacité du circuit est meilleure. Les couches métalliques (Cond, Cond2 et Slot/Gnd) sont en cuivre d'une épaisseur de 35 μm et comme on peut le voir sur la figure, les lignes microruban supérieures et inférieures partagent le même plan de masse. La fabrication du circuit imprimé a été faite selon le procédé photo lithographique classique et l'assemblage multicouche repose sur un film de liaison Rogers RO3001 pressé à chaud.

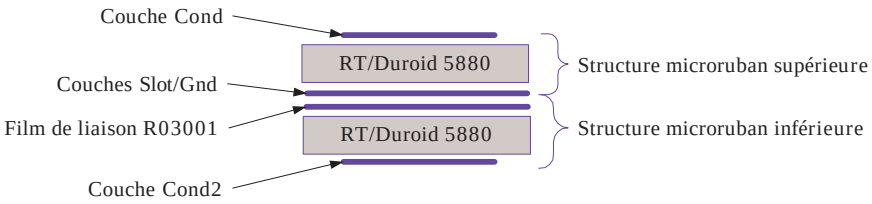


FIG. 28.1: Structure microruban à couches doubles utilisée pour la réalisation des composants.

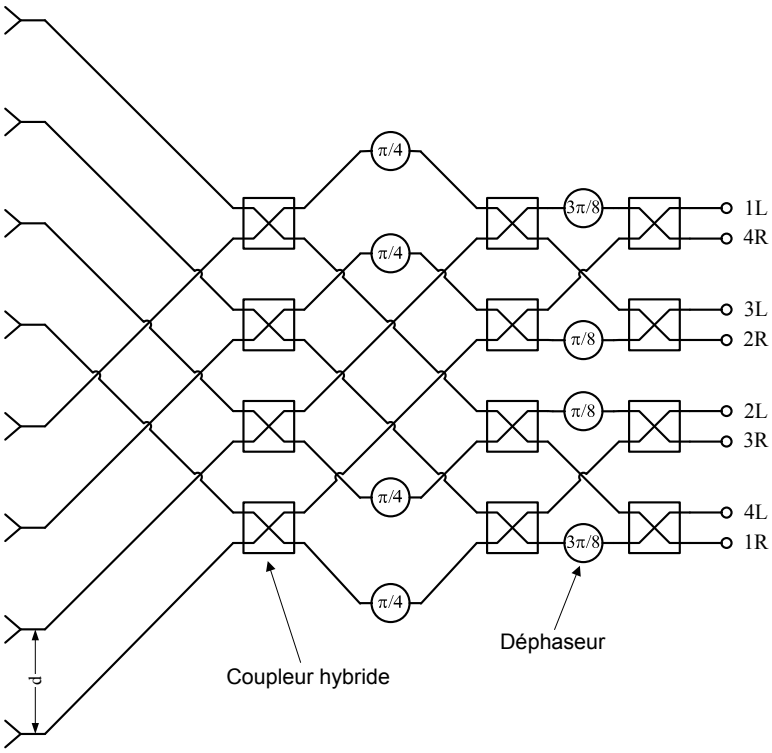


FIG. 28.2: Schéma d'une antenne réseau linéaire à espacement constant reliée à une matrice de Butler 8×8.

28.3 Coupleur hybride

La figure 28.3 montre le coupleur hybride à branches tel qu'il a été réalisé pour utilisation à 36 GHz. Son fonctionnement est tel que si on applique un signal à un de ses accès, on retrouve le même signal réparti entre les accès du côté opposé, l'accès le plus éloigné accusant un retard de 90 degrés sur celui le plus rapproché. Par exemple, si on applique un signal à l'accès 1, le signal à l'accès 2 est celui en phase (I) tandis que celui de l'accès 3 est en quadrature (Q) et donc déphasé de 90 degrés par rapport au signal de l'accès 2 c'est-à-dire

$$\angle I - \angle Q = \frac{\pi}{2} + b_p, \tag{28.1}$$

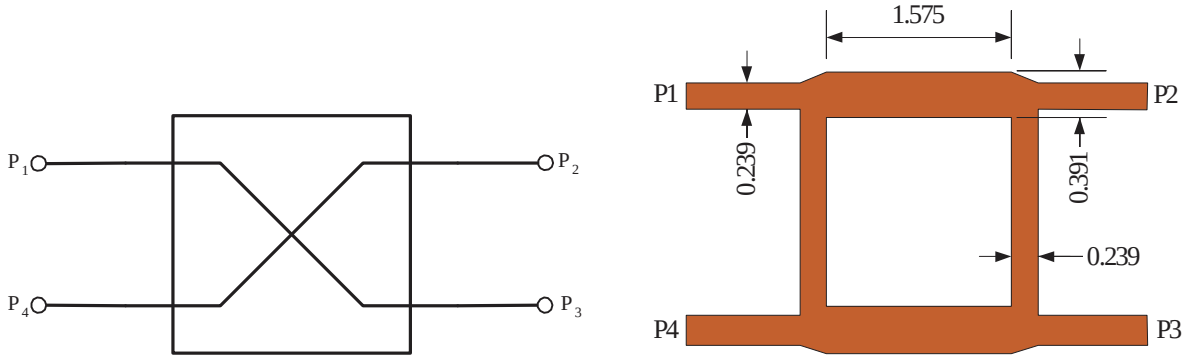
où b_p est la balance de phase. Le ratio des puissances de sortie est la balance de gain b_g :

$$\left|\frac{Q}{I}\right|^2 = b_g. \tag{28.2}$$

Idéalement, $b_p = 0$ et $b_g = 1$, ce qui est très difficile à atteindre expérimentalement. Puisqu'une partie du signal appliqué à l'entrée est dissipée, des pertes d'insertion sont en jeu et nous pouvons les calculer comme suit :

$$IL = -10 \log \left(|I|^2 + |Q|^2\right) \quad \text{dB}. \tag{28.3}$$

L'isolation entre les accès adjacents du coupleur est $1/\rho$ et Γ est le coefficient de réflexion aux 4 accès. En théorie l'isolation est infinie ($\rho = 0$) et l'adaptation est parfaite ($\Gamma = 0$). L'analyse approfondie ainsi que les détails de conception de ce coupleur sont donnés en [1] et en [2] respectivement. On retrouve au tableau 28.1 un sommaire des principales caractéristiques mesurées de ce coupleur.



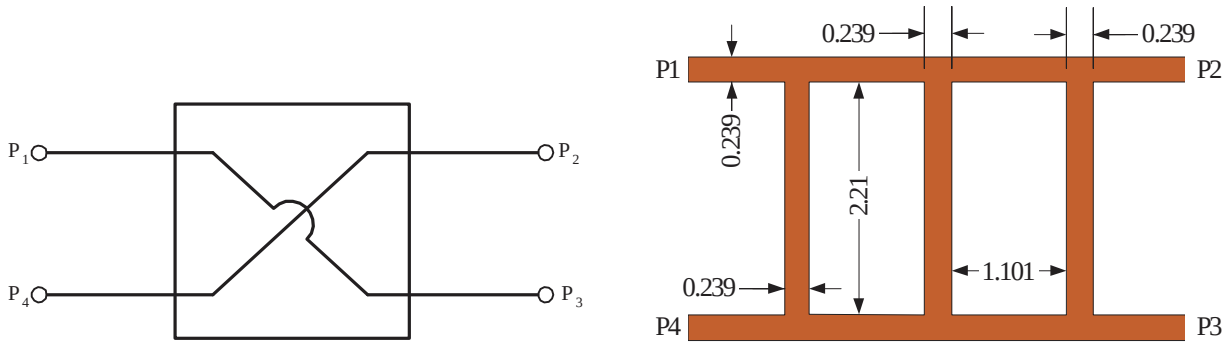
(a) Représentation (b) Conception microruban

FIG. 28.3: Coupleur hybride tel que réalisé (dimensions en mm).

28.4 Coupleur 0 dB

Lors de la fabrication d'un circuit imprimé, lorsque vient le temps croiser deux lignes sans qu'il y ait de transmission de signal entre les deux parcours, une des deux traces est passée sur une

autre couche à l'endroit où se fait le croisement et le tour est joué. À plus hautes fréquences, la transition d'une couche à l'autre se fait au détriment des pertes d'insertion et la nécessité d'avoir une couche supplémentaire complique considérablement la conception. Le coupleur 0 dB apparaît donc comme une solution fort à propos puisqu'il permet de faire ce croisement sur une seule couche. La figure 28.4 montre un coupleur 0 dB à branches et son modèle équivalent. La



(a) Représentation (b) Conception microruban

FIG. 28.4: Coupleur 0 dB tel que réalisé (dimensions en mm).

transition d'un signal de l'accès 1 à l'accès 3 ainsi que de l'accès 2 à l'accès 4 devrait se faire de façon complètement indépendante lorsque l'isolation est très élevée. De plus, les pertes que subit le signal devraient être minimales, ce qui peut difficilement être atteint avec le type de structure dont il est question ici.

Le tableau 28.1 regroupe les principaux paramètres obtenus expérimentalement. Comme on peut le constater à l'inspection de ce dernier, les pertes d'insertion sont minimes et l'isolation est relativement bonne, ce qui nous permet d'affirmer qu'effectivement les 2 parcours sont découplés.

28.5 Interconnexion verticale à couplage électromagnétique

Le passage des signaux d'une couche à l'autre d'un circuit imprimé se fait généralement à l'aide de vias. Ce type de branchement introduit une discontinuité du signal qui a des effets non négligeables surtout lorsque les fréquences en jeu sont élevées. L'introduction de vias dans la fabrication d'un circuit introduit une étape supplémentaire faisant du même coût grimper les coûts. De plus, les tolérances mécaniques du procédé de fabrication font en sorte que la répétivité de la transition peut varier d'un item à l'autre. Afin de contourner les effets indésirables des vias, un branchement par couplage électromagnétique a été conçu et réalisé. La figure 28.5 montre le principe qui repose sur une ouverture rectangulaire pratiquée dans le plan de masse afin d'acheminer l'énergie d'une couche à l'autre.

La modélisation d'une telle structure doit inévitablement passer par les méthodes numériques telles que la méthode des moments pour bien caractériser l'interaction entre les couches. En ce qui concerne le coefficient de transmission $s_{21} = s_{12}$, les simulations se sont révélées assez fidèles aux résultats des mesures pour la plage de fréquences comprise entre 35.8 et 36.2 GHz (voir

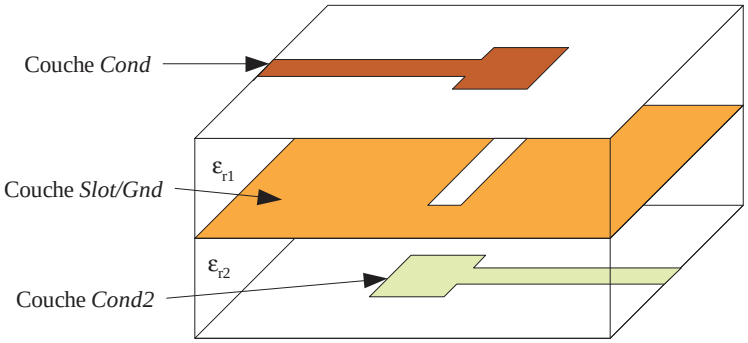
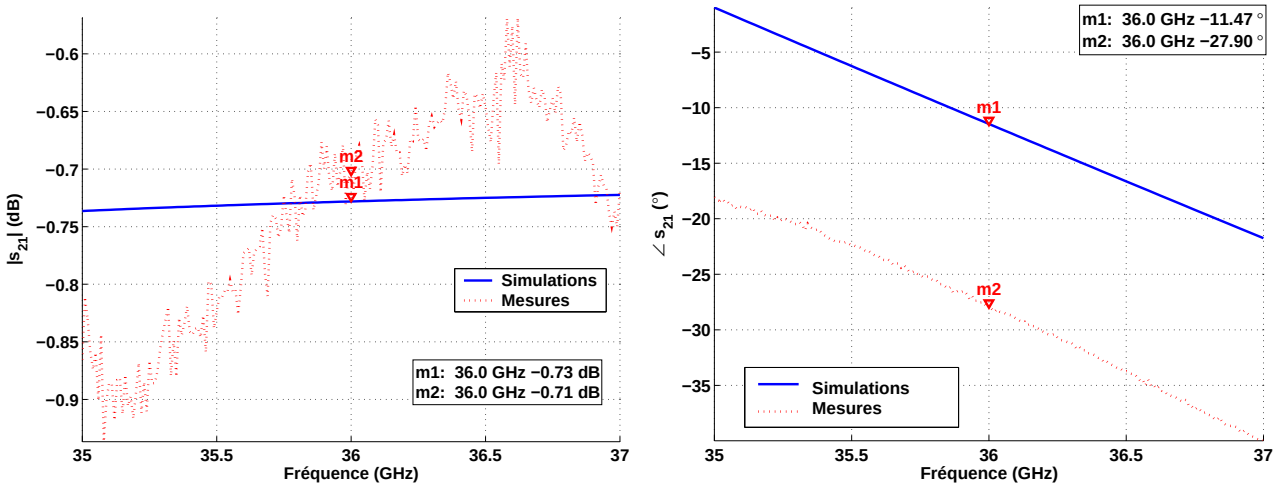


FIG. 28.5: Interconnexion verticale à couplage électromagnétique.

figure 28.6). Il faut cependant noter qu'un déphasage supplémentaire d'environ seize degrés a été obtenu expérimentalement, ce qui n'est pas surprenant compte tenu de toutes les sources d'erreur possibles. Parmi celles-ci, on peut dénombrer la variabilité de l'assemblage multicouche et la surexposition du cuivre faisant en sorte que les dimensions du circuit tel qu'il a été fabriqué diffèrent de leur valeur originale.



(a) Module (dB) (b) Angle (degrés)

FIG. 28.6: Coefficient de transmission simulé et mesuré de l'interconnexion verticale.

28.6 Dipôle planaire à BALUN intégré

Ce type d'antenne [3] est fort intéressant, car il a un rayonnement longitudinal (réponse maximale dans le plan du circuit imprimé) et aussi une largeur de bande relativement grande. La figure 28.7 montre la topologie du circuit et donne ses principales dimensions. Les détails de conception ainsi que les mesures de cet élément rayonnant sont donnés dans [4].

À l'inspection des diagrammes de rayonnement reproduits ici à la figure 28.8, on peut remar-

©LRTS 2005-2006

quer une bonne correspondance entre ceux obtenus des simulations par la méthode FDTD et ceux mesurés. Le diagramme obtenu dans le plan E est un peu plus étroit que lors des simulations. Toujours dans le même plan, on peut aussi percevoir un affaiblissement de la réponse pour les angles autour de -65 ° qui est causé par une interférence destructive provenant du BALUN.

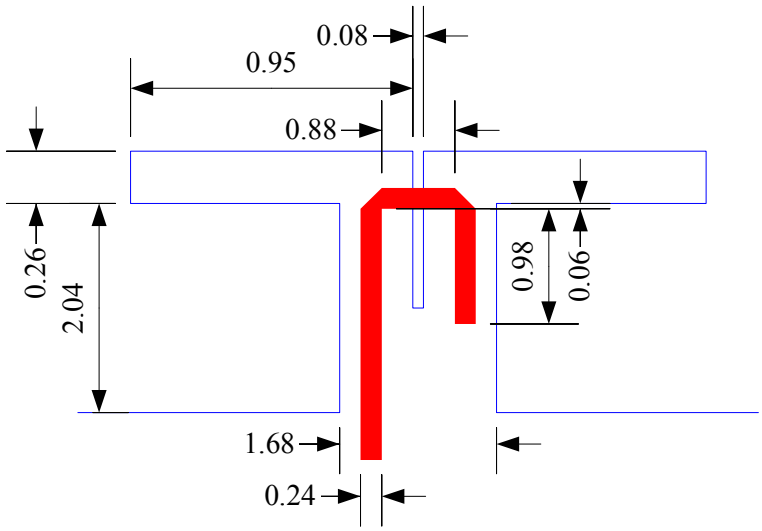
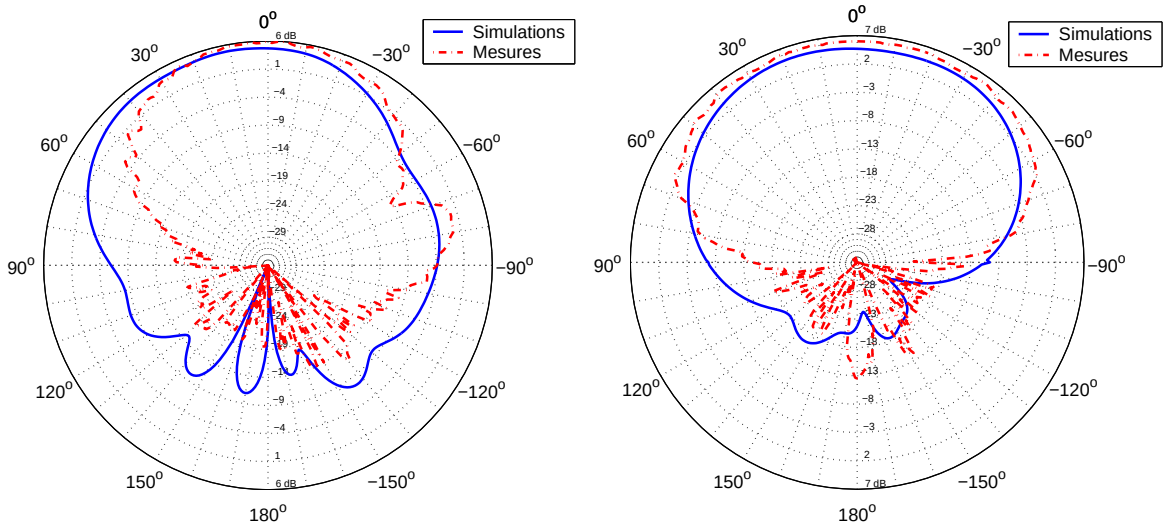


FIG. 28.7: Dipôle planaire à BALUN intégré tel que réalisé (dimensions en mm).

28.7 Matrice de Butler 8×8

Pour couronner cette étape de réalisation de composants microruban, une matrice de Butler 8×8 [5] a été réalisée à l'aide des composants décrits précédemment. La figure 28.2 montre le circuit nécessaire afin de réaliser ce réseau de formation de faisceaux. Comme on peut le voir sur cette figure, 16 croisements de lignes sont nécessaires et plusieurs composants doivent coexister sur un même circuit imprimé. Une des solutions employées afin de minimiser le nombre de croisement et aussi de diminuer la densité des composants a été de répartir le circuit sur 2 couches. Le passage d'une couche à l'autre se fait par le biais de l'interconnexion verticale à couplage électromagnétique décrite précédemment. Les croisements restants se font à l'aide du coupleur 0 dB aussi décrit plus tôt. Enfin, les divers déphasages sont réalisés à l'aide de longueurs fixes de lignes de microruban calculées afin de faire en sorte que le délai introduit à 36 GHz corresponde au déphasage voulu.

La matrice a d'abord été testée isolément à l'aide de l'analyseur de réseaux HP 8722ES du laboratoire. À partir de la matrice de diffusion ainsi obtenue, le facteur de réseau a été calculé et les principaux paramètres (gain, direction du faisceau, niveau des lobes secondaires) de chacun des faisceaux ont été extraits. Cette même matrice de Butler a aussi été réalisée et intégrée à un réseau linéaire de dipôles tels que conçus précédemment. Les diagrammes de rayonnement ont été mesurés en chambre anéchoïque et de ces derniers les principaux paramètres ont été obtenus. Encore une fois, les détails de la conception et les résultats sont rapportés en détail dans [2, 4].



(a) Plan E (b) Plan H

FIG. 28.8: Diagrammes de rayonnement du dipôle planaire à BALUN intégré à 36 GHz.

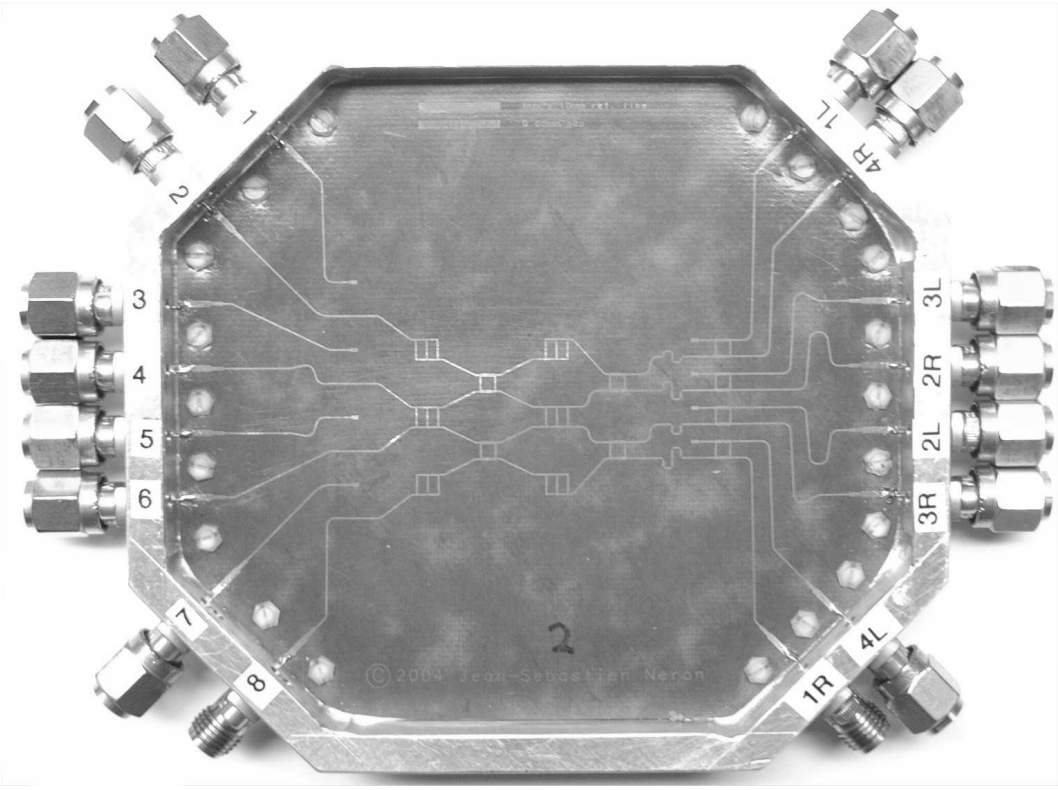


FIG. 28.9: Matrice de Butler 8×8 telle que réalisée et assemblée sur un support d'aluminium.

Description	Paramètre	Valeur	Unité
Coupleur hybride			
Isolation min.	$1/\rho$	10.7	dB
Pertes d'insertion max.	IL	0.8	dB
Balance de phase	$\|b_p\|$	< 2.3	$\circ$
Balance de gain	b_g	< 1.1	dB
Coupleur 0 dB			
Isolation min.	s_{21}, s_{43}	18	dB
Pertes d'insertion max.	s_{31}, s_{42}	0.6	dB
Interconnexion verticale			
Pertes d'insertion max.	s_{21}	0.75	dB
Dipôle planaire à BALUN intégré			
Gain		6.1	dBi
Largeur de bande (TOS$<$ 2)		6.3	GHz

TAB. 28.1: Performance mesurée pour les composants microruban (35.8 GHz $\leq f \leq$ 36.2 GHz).

28.8 Conclusion

La réalisation d'une antenne à faisceaux multiples en bande EHF utilisant les lignes microruban a été démontrée et nous a permis du même coup de mettre en pratique des concepts novateurs tels que l'interconnexion verticale à couplage électromagnétique. Les tolérances de fabrication du circuit imprimé ont fait en sorte que les mesures ont parfois été déviées des prédictions mais le fonctionnement général a été démontré avec succès. Une analyse de sensibilité s'impose pour mieux comprendre l'effet des multiples erreurs de fabrication : nous y travaillons présentement et les résultats seront rapportés sous peu.

Bibliographie

[1] D. M. Pozar, *Microwave engineering.* Wiley, 2nd ed., 1998.

[2] J.-S. Néron and G.-Y. Delisle, "Microstrip EHF Butler Matrix Design and Realization," *ETRI Journal*, vol. 27, pp. 788–797, Dec. 2005.

[3] B. Edward and D. Rees, "A broadband printed dipole with integrated balun," *Microwave Journal*, vol. 30, pp. 339–344, May 1987.

[4] J.-S. Néron and G.-Y. Delisle, "Multiple Beam Array Realization at EHF Band," in 13th *International Conference on Telecommunications Proceedings*, (Funchal, Madeira Island, Portugal), May 2006.

[5] J. L. Butler, "Digital, matrix and intermediate-frequency scanning," in *Microwave Scanning antennas* (R. Hansen, ed.), vol. 3, ch. 3, pp. 217–288, New York : Academic press, 1966.

Calibrage des réseaux d'antennes par réseaux de neurones artificiels

Hugo Bertrand, *Étudiant au doctorat*
Dominic Grenier, *Directeur de recherche*
Sébastien Roy, *Codirecteur de recherche*

Résumé – Nous présentons les travaux de recherche portant sur le calibrage des réseaux d'antennes par le biais de réseaux de neurones artificiels. Il est bien connu que pour effectuer de l'estimation de direction d'arrivée (DOA) avec précision en utilisant des algorithmes tel MUSIC (MUltiple SIgnals Classification), les données d'un réseau d'antennes doivent être calibrées afin de respecter le modèle théorique sur lequel repose ces algorihtmes de DOA. Nous présentons ici des mesures expérimentales obtenues avec un réseau d'antennes linéaire et nous proposons une nouvelle technique de calibrage basée sur les réseaux de neurones artificiels entraînés à partir des vecteurs directifs expérimentaux et théoriques. Dasn ce contexte, la performance d'un type de réseaux de neurones - réseau de neurones linéaire adaptatif - est évaluée. Puis, cette perfomance est comparée à une autre méthode de calibrage, démontrant ainsi que la technique proposée fonctionne bien tout en étant simple à implanter.

Abstract – We present the research works based on the antenna array calibration topic by using artificial neural networks. It is well known that to perform accurate Direction of Arrival (DOA) estimation using algorithms like MUSIC (MUltiple SIgnals Classification), antenna array data must be calibrated to match the theoretical model upon wich DOA algorithms are based. This paper presents experimental measurements obtained with a linear antenna array and proposes a novel calibration technique based on artificial neural networks trained with experimental and theoretical steering vectors. In this context, the performance of a type of neural network - ADAptive LInear Neuron (ADALINE) network - is assessed and then compared with another calibration technique, thus demonstrating that the proposed technique works well while being very simple to implement.

29.1 Introduction

Depuis les deux dernières décennies, nous avonc connu une incroyable explosion de la demande pour les systèmes de télécommunications sans fil causée par une augmentation du nombre d'utilisateurs ainsi que de la largeur de bande utilisée par chacun d'eux. Cela engendre aujourd'hui des problèmes d'efficacité spectrale et de capacité qui limitent grandement la continuité de cette croissance. Il est généralement admis que les solutions à ces problèmes résident dans les techniques de traitement spatio-temporel qui impliquent l'utilisation de réseaux d'antennes à une ou aux

deux extrémité du lien sans fil.

Les travaux présentés utilisent principalement deux classes d'algorithmes de traitement spatio-temporel : la formation de voies (beamforming) et l'estimation de directions d'arrivée (DOA). Même si l'utilisation commune de ces algorithmes a démontré son potentiel pour règler le problème de capacité théoriquement (l'estimation de DOA dans la liaison montante peut être utlisée pour effectuer de la formation de voies précise dans la liaison descendante permettant une réutilisation de la fréquence porteuse par discimination spatiale [1]), les réalisations pratiques ne sont malheureusement pas aussi simples à cause du comportement non idéal du réseau d'antennes. Cette disparité entre le modèle théorique et les mesures expérimentales provient de plusieurs causes. Premièrement, le débalancement de gain et de phase entre les parties en phase (I) et en quadrature (Q) de chaque antenne et les erreurs CC de l'électronique des sous-systèmes I/Q engendrent une divergence par rapport au modèle statistique du signal sur lequel repose les algorithmes de traitement [2, 3]. En effet, ces algorithmes sont construits en fonction de différentes hypothèses, telles que les propriétés idéales de variables aléatoires gaussiennes complexes [4]. Une autre différence entre la théorie et la pratique est due aux erreurs de gain et de phase entre les canaux, i.e. les variations entre les sous-systèmes associés à chacune des antennes du réseau. La troisième source d'erreur provient des effets du couplage mutuel entre les antennes, tandis que la quatrième source est l'incertitude sur la position exacte des antennes l'une par rapport à l'autre. Finalement, la dispersion causée par la structure de l'antenne et les objets environnants constitue la cinquième souce d'erreur.

Toutes ces perturbations ont pour effet d'affecter la structure spécifique de la matrice de covariance des données. De plus, les vecteurs de balayage théoriques peuvent se retrouver à l'extérieur du sous-espace signal expérimental. Ces effets impliquent une mauvaise performance des algorithmes de traitement du signal [5].

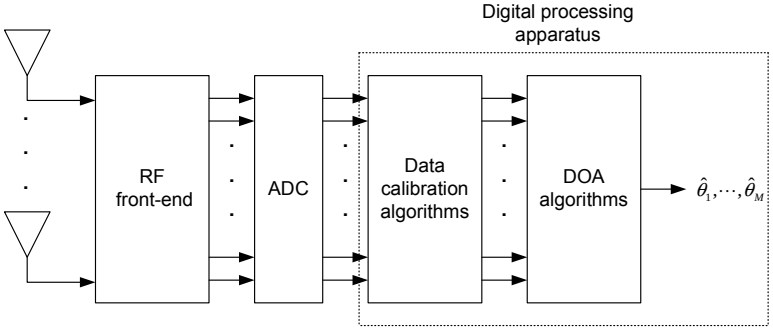


FIG. 29.1: Une représentation schématique d'un réseau d'antennes performant de l'estimation de DOA

La solution à tous ces problèmes est une certaine procédure de calibrage des données afin qu'elles respectent le modèle théorique ou encore, de façon équivalente, le calibrage de l'ensemble des vecteurs directifs expérimentaux afin qu'ils respectent celui formé par les vecteurs de balayage théoriques. La Figure 29.1 montre une représentation schématique d'un réseau d'antennes utilisé pour effectuer de l'estimation de DOA pour M sources.

On retrouve dans la littérature plusieurs contributions à propos du calibrage des réseaux

d'antennes. La majorité sont seulement basées sur des simulations, qui ne peuvent à elles seules tracer un portrait complet de cette problématique essentiellement expérimentale. Ces travaux peuvent être collectivement regroupés en trois approches. Premièrement, certains auteurs [6] tentent de contourner le problème de calibrage en construisant une nouvelle matrice de covariance possédant une structure Toeplitz. La seconde classe est celle appelée *auto calibrage*, car elle ne nécessite pas la connaissance des directions des sources servant à la procédure de calibrage. Finalement, la dernière approche est appelée *calibrage supervisé* et implique la connaissance exacte de la position des sources servant au calibrage. Pour de plus amples détails sur chacune de ces approches, consulter [7].

Pour notre approche du problème, nous imaginons un système cellulaire avec plusieurs points d'accès/stations de base qui peuvent communiquer entre elles et s'échanger une certaine séquence d'entraînement connue qui, combinée à la connaissance a priori de la position de chacune ce ces stations, permettraient le calibrage supervisé.Le réseau GSM décrit dans [8] avec ses 16 stations de base supporte davantage le concept d'entraînement supervisé.

Dans ce contexte, le concept de calibrage supervisé a été investigué et on a trouvé que les réseaux de neurones artificiels constituent un outil algorithmique puissant pour ce type de situation. On se bornera ici à présenter les résultats obtenus avec un réseau de neurones linéaire d'une seule couche, entraîné avec les vecteurs directifs expérimentaux et théoriques par un algorithme de faible complexité basé sur l'optimisation des moindres carrées. Cette simplicité permet à l'algorithme proposé d'être un candidat idéal pour une implantation en temps réel. Il est à préciser qu'une comparaison de la performance de différents types de réseaux de neurones a été effectuée dans [9].

29.2 Le modèle du réseau d'antennes

Dans le cas idéal, la sortie du réseau de N antennes linéairement et uniformément espacées est une matrice $\mathbf{X}$ composée de K vecteurs gaussiens complexes $\mathbf{x}_k$ indépendants et identiquement distribués, de moyenne nulle et de matrice de covariance $\mathbf{R}$.

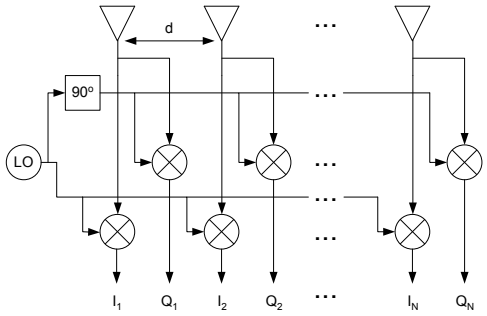


Fig. 29.2: Un réseau d'antennes linéaire

Chacun de ces vecteurs peut être exprimé par

$$\begin{aligned}\mathbf{x}_k &= [(I_1 + jQ_1)\ (I_2 + jQ_2)\ \cdots\ (I_N + jQ_N)]^T \\ &= \sum_{i=1}^{M} \alpha_i(k)\mathbf{a}(\theta_i) + \boldsymbol{\eta}_k, \end{aligned} \tag{29.1}$$

où $\alpha_i(k)$ sont des variables aléatoires gaussiennes complexes de moyenne nulle et de variance σ_i^2 reliée à la puissance reçue de la i^{ieme} source, $\mathbf{a}(\theta_i)$ sont les vecteurs directifs associés avec la i^{ieme} source et $\boldsymbol{\eta}_k$ sont des vecteurs de bruit additif gaussien de moyenne nulle et de variance σ_η^2.

Le vecteur directif de la i^{ieme} source est donné théoriquement par

$$\mathbf{a}(\theta_i) = \frac{1}{\sqrt{N}} \left[1\ e^{j\varphi_i}\ e^{j2\varphi_i}\ \cdots\ e^{j(N-1)\varphi_i}\right]^T, \tag{29.2}$$

où φ_i est le délai électrique entre les signaux de chaque antenne dû à la distance entre les antennes d, la position de la i^{ieme} source θ_i et sa longueur d'onde λ_i, et est exprimé par

$$\varphi_i = \frac{2\pi d}{\lambda_i} \sin(\theta_i). \tag{29.3}$$

La matrice de données peut être exprimée par

$$\mathbf{X} = [\mathbf{x}_1\ \mathbf{x}_2\ \cdots\ \mathbf{x}_K]. \tag{29.4}$$

Dans la situation idéale, la matrice de covariance $\mathbf{R}$ est Toeplitz hermitienne et peut être exprimée par

$$\mathbf{R} \approx \mathbf{X}\mathbf{X}^H. \tag{29.5}$$

On peut effectuer sa décomposition propre ainsi :

$$\begin{aligned}\mathbf{R} &= \sum_{i=1}^{M} \lambda_i \mathbf{v}_i \mathbf{v}_i^H + \sum_{i=M+1}^{N} \lambda_i \mathbf{v}_i \mathbf{v}_i^H \\ &= \mathbf{V}_s \boldsymbol{\Lambda}_s \mathbf{V}_s^H + \sigma_\eta^2 \mathbf{I}, \end{aligned} \tag{29.6}$$

où $\{\lambda_i\}$ sont les N valeurs propres en ordre décroissant, associées aux vecteurs propres $\{\mathbf{v}_i\}$. Les M premiers vecteurs propres constituent le sous-espace signal et les autres forment le sous-espace bruit.

On sait que les M premiers vecteurs propres engendrent le même sous-espace que les M vecteurs directifs $\mathbf{a}(\theta_1)$ à $\mathbf{a}(\theta_M)$ et que les autres vecteurs propres définissent un sous-espace perpendiculaire aux vecteurs directifs.

Cette structure est exploitée par les algorithmes de DOA classiques. Par exemple, MUSIC (MUltiple SIgnals Classification) [10] est basé sur la distance euclidienne entre tous les vecteurs directifs possibles et le sous-espace signal. Malheureusement, losque des données expérimentales non calibrées sont utilisées avec cet algorithme, cela donne des résultats erronés (comme on peut le voir à la Figure 29.8). Cela est dû au fait que les vecteurs directifs théoriques $\mathbf{a}(\theta_i)$ ne se trouvent plus exactement dans le sous-espace signal. Ainsi, nous devons procéder au calibrage des vecteurs directifs expérimentaux $\hat{\mathbf{a}}_e(\theta_i)$ afin qu'ils respectent le modèle théorique sur lequel repose les algorithmes de DOA.

29.3 L'algorithme proposé

L'originalité de l'approche proposée repose sur l'utilisation de réseaux de neurones artificiels [9]. Nous avons trouvé qu'un réseau de neurones linéaire (Figure 29.3) entraîné avec L paires de

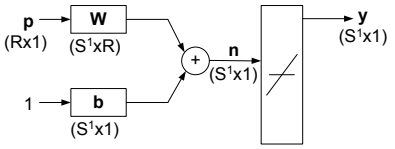


Fig. 29.3: Un réseau de neurones linéaire

vecteurs "entrée du réseau" et "sortie désirée" formés des parties réelles et imaginaires des vecteurs directifs expérimentaux et théoriques donnaient d'excellents résultats, même si l'algorithme d'apprentissage est simple et que le nombre de neurones est petit. Le processus d'apprentissage ajuste les valeurs des poids et biais du réseau afin de minimiser une approximation de l'erreur quadratique moyenne entre les vecteurs de sortie du réseau $\mathbf{y}(k)$ ($\mathbf{a}_{cal}(k)$) et les vecteurs cible $\mathbf{t}(k)$ ($\mathbf{a}(k)$) pour les vecteurs d'entrée $\mathbf{p}(k)$ ($\hat{\mathbf{a}}_e(k)$), i.e.

$$\text{MSE} = F(\mathbf{e}) \approx \frac{1}{L}\sum_{k=1}^{L}\sum_{i=1}^{2N}(e_i(k))^2 = \frac{1}{L}\sum_{k=1}^{L}\mathbf{e}(k)^T\mathbf{e}(k), \tag{29.7}$$

with $\mathbf{e}(k) = \mathbf{t}(k) - \mathbf{y}(k)$. Cette indice de performance F est de forme quadratique ce qui nous assure de la convergence du processus d'entraînement vers un minimum global, ce qui est confirmé par les résultats expérimentaux.

29.4 Montage et résultats expérimentaux

La Figure 29.4 présente le réseau d'antennes expérimental comprenant 8 antennes cornet fonctionnant dans la bande X (8-12GHz), voir [9] pour les détails sur les composantes. Bien que le design de ce montage ait été fait aussi rigoureusement que possible, il présente toutes les imperfections discutées précédemment.

Le débalancement I/Q peut être observé via la figure de Lissajou (Figure 29.7), puis les variations de gain et de phase entre les antennes sont illustrées à la Figure 29.5.

La Figure 29.6 montre l'impact sur les signaux de la méthode de calibrage proposée à la section précédente : les variations de gain et de phase entre les antennes sont corrigées, mais il a été observé que le débalancement I/Q est encore présent : même après le calibrage, la figure de Lissajou est toujours une ellipse et non un cercle.

Finalement, la Figure 29.8 montre l'impact combiné de toutes ces perturbations sur la performance des algorithmes de DOA en présentant un pseudospectre avant et après calibrage pour une source située à 0 degré.

On explique ici la procédure de calibrage. Des mesures ont été prises avec une source en bande X à tous les demis degrés sur une plage de -20 and 20 degrés. Pour chacune de ces mesures, le vecteur propre principal de la matrice de covariance spatial a été utilisé comme vecteur directif

©LRTS 2005-2006

FIG. 29.4: Le réseau d'antennes

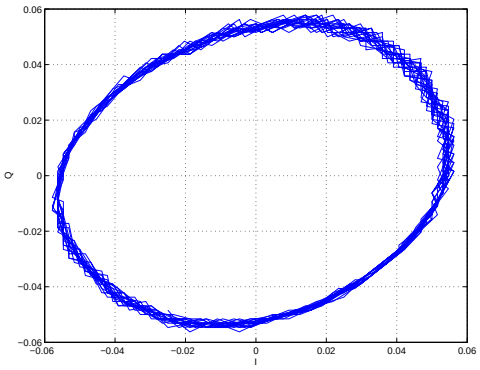


FIG. 29.7: Figure de Lissajou des signaux en phase (I) et en quadrature (Q)

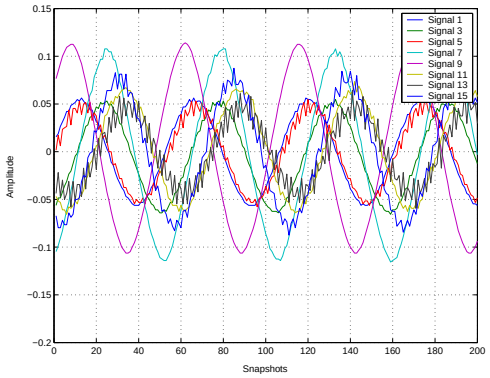


FIG. 29.5: Les 8 signaux en phase non calibrés lorsqu'une source est située à 0 degré.

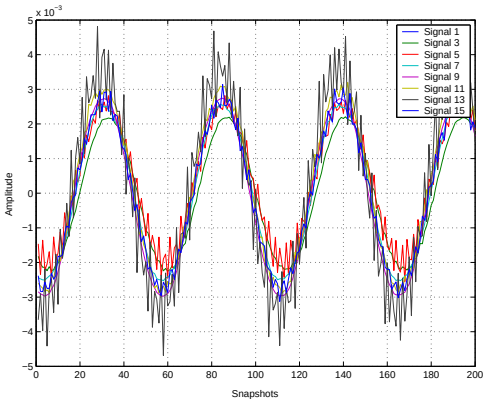


FIG. 29.6: Les 8 signaux en phase calibrés lorsqu'une source est située à 0 degré.

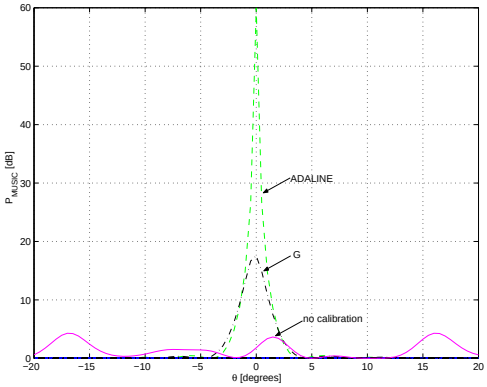


FIG. 29.8: Pseudospectre obtenu par l'algorithme MUSIC avec les données calibrées et non calibrées pour une source à 0 degré

expérimental, tandis que celui théorique a été créé en se basant sur la position mesurée (et non estimée) de la source émettrice. Cette opération a fourni l'ensemble d'entraînement entrée/sortie du réseau de neurones.

La Figure 29.8 présente l'excellent résultat du calibrage pour une source à 0 degré en utilisant tout l'ensemble d'entraînement. On peut réaliser que la meilleure performance a été réalisée avec le réseau de neurones linéraire (voir [7] pour une présentation de l'algorithme de comparaison utilisant la matrice de calibrage $\hat{\mathbf{G}}$).

Pour comparer la performance de ces techniques lorsque le DOA ne fait pas partie de l'ensemble d'entraînement, nous avons calculé l'angle moyen $\theta_{average}$ entre le vecteur calibré $\mathbf{a}_{cal}$ et celui théorique $\mathbf{a}$ pour différentes tailles L de l'ensemble d'entraînement

$$\theta_{average} = \frac{1}{L}\sum_{i=1}^{L} \arccos\left(\frac{\left\|\mathbf{a}^H(i)\mathbf{a}_{cal}(i)\right\|}{\left\|\mathbf{a}^H(i)\right\|\left\|\mathbf{a}_{cal}(i)\right\|}\right). \tag{29.8}$$

Ces résultats sont présentés à la Figure 29.9. Nous pouvons conclure que la performance de ces algorithmes se dégrade à mesure que la taille de l'ensemble d'entraînement diminue (comme

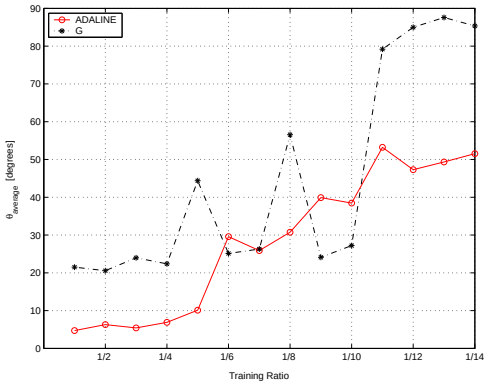


FIG. 29.9: Angle entre les vecteurs directifs calibrés et théoriques pour différentes tailles de l'ensemble d'entraînement

c'est le cas habituellement) et que le meilleur compromis entre la performance et la facilité d'implantation provient de la méthode basée sur les réseaux de neurones.

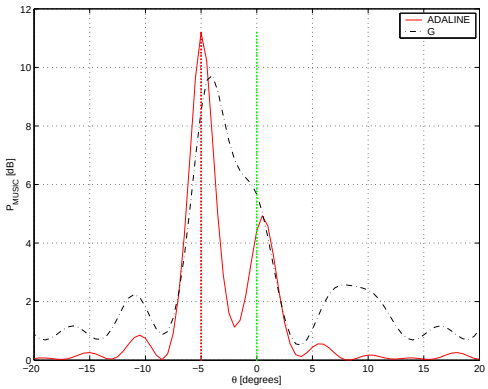


FIG. 29.10: Pseudospectre obtenu par l'algorithme MUSIC avec les données calibrées pour deux sources non corrélées situées à -5 and 0 degrés

Pour démontrer la capacité de généralisation du réseau de neurones, il a été utilisé pour calibrer de nouvelles mesures expérimentales obtenues à partir de deux sources. Les résultats d'une expérience typique obtenus avec des réseaux de neurones comparés à ceux provenant de la méthode de la matrice de calibrage $\hat{\mathbf{G}}$ sont présentés à la Figure 29.10. La technique basée sur les réseaux de neurones généralise bien et donne de meilleurs résulats que la matrice $\mathbf{G}$ tout en étant du même ordre de complexité.

29.5 Conclusion

Une méthode originale de calibrage basée sur les réseaux de neurones a été présentée, entraînée par les vecteurs directifs expérimentaux et théoriques. Nous avons trouvé qu'un réseau de neurones linéaire donne de meilleurs résultats - ou très similaires - en moyenne que toutes les autres

méthodes de calibrage tout en étant simple d'implantation. Après plusieurs essais expérimentaux, il semble que cette méthode converge toujours vers le minimum global.

Bibliographie

[1] P. Petrus, A. Chemali, D. Depierre, and L. Yun, "Method and appartus for estimating downlink beamforming weights in a communications system," US Patent 6,839,574 B2, 2005.

[2] A. Sinsky and P. Wang, "Error analysis of a quadrature coherant detector processor," *IEEE Transactions on Aerospace and Electronics Systems*, vol. 10, pp. 880–883, Nov. 1974.

[3] N. Barber, "Narrow band-pass filter using modulation," *Wireless Engineer*, pp. 132–134, May 1947.

[4] N. Goodman, "Statistical analysis based on a certain multivariate complex gaussian distribution," *Ann. Mathematical Statistics*, vol. 34, pp. 152–177, 1963.

[5] H. Park and S. Bang, "Model based antenna array calibration for digital beamforming systems," in *Vehicular Technology Conference Proceedings*, vol. 2, pp. 867–870, IEEE, Apr. 2003.

[6] Y.-M. Chen, J.-H. Lee, C.-C. Yeh, and J. Mar, "Bearing estimation without calibration for randomly perturbeted arrays," *IEEE Transactions on Signal Processing*, vol. 39, pp. 194–197, Jan. 1991.

[7] H. Bertrand, D. Grenier, and S. Roy, "Experimental antenna array calibration with ADAptive LInear NEuron (ADALINE) network," accepted for oral presentation at VTC spring 2006.

[8] K. Pensel, H. Aroudaki, and J. Nossek, "Calibration of smart antennas in a GSM network," in *Workshop on Signal Processing Advances in Wireless Communications*, pp. 354–357, IEEE, May 1999.

[9] H. Bertrand, D. Grenier, and S. Roy, "Experimental antenna array calibration with artificial neural networks," submitted for publication.

[10] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, pp. 276–280, Mar. 1986.

©LRTS 2005-2006

Emploi du signal XM comme source d'opportunité d'un système non coopératif pour la détection passive cohérente

Louis-Philippe Gill, *Étudiant au doctorat.*
Dr Dominic Grenier, *Directeur de recherche.*
Dr Jean-Yves Chouinard, *Co-directeur de recherche.*

Résumé – L'emploi du signal XM comme source d'un système radar passif est envisagé. Par l'analyse de la fonction d'ambiguïté du signal et l'élaboration d'une simulation adéquate, le sytème est étudié. L'utilisation d'un procédé imitant l'algorithme CLEAN est envisagée pour résoudre les problèmes liés à l'écho noyé dans le signal direct.

Abstract – The use of XM Radio Satellite signal as a source by a passive radar system is considered. By the analysis of the ambibuity function and the development of an adequate simulation, the sytem is studied. The use of a process imitating CLEAN algorithm is planned to solve the problems related to the echo drowned in direct path signal.

30.1 Introduction

La détection passive cohérente (PCL) est à l'origine de la dernière résurgence en date du bistatisme dans le domaine radar. Caractérisé par un récepteur utilisant le signal d'une source indépendante (souvent destiné à d'autres fins), le radar PCL reçoit, captés par deux antennes différentes, le signal direct et l'écho afin d'établir une cohérence et ainsi pouvoir extraire des informations sur la cible. Les difficultés de localisation du récepteur, puisque aucun signal n'est émis à partir de celui-ci contrairement à un système radar monostatique, sont un exemple d'avantages qu'offre un tel système. Comme source non-coopérative pour un système radar passif (une source dont la fonction n'est pas la détection mais dont l'emploi peut y être dédié), le système satellite radio numérique de XM est un candidat intéressant. Sa couverture, par ses deux satellites géostationnaires offre une puissance au sol supérieure à celle que pourrait offrir, par exemple, le système GPS ou GLONASS [1].

Pour cette étude, on effectue d'abord, par sa fonction d'ambiguïté, l'analyse du signal satellite de radio numérique XM et de son potentiel de détection. Par la suite, on expose les détails visant à élaborer une simulation viable et on suggére une méthode permettant d'extraire l'information contenue dans l'écho radar d'une cible.

30.2 Le signal XM

XM Satellite Radio Inc. est un service de radio satellite numérique dont le signal provient de deux satellites géostationnaires (Rock et Roll) couvrant les États-Unis et débordant aux frontières canadiennes et mexicaines. Chacun d'eux émet un signal sur deux porteuses d'une puissance rayonnée effective (ERP) de 68.5 dBW. Diffusé en bande S (de 2332.5 à 2345.0 GHz) et modulé en QPSK, le signal est émis à un taux de transmission de 3.28 Mbits/sec. Les satellites en orbite à 35786 km d'altitude sont respectivement positionnés à des longitudes de 85 et 115 degrés Ouest [2].

30.3 La fonction d'ambiguité

Afin de vérifier la performance de ce signal, une simulation du signal XM est codée et la fonction d'ambiguïté résultante est étudiée. Le signal XM est simulé par une série de symboles QPSK générés aléatoirement puis traités par un filtre à cosinus surélevé. En variant le nombre de symboles constituant la séquence, il est possible d'observer l'impact de la longueur de la séquence de cohérence (le nombre de symbole pouvant frapper une cible sans que les points de diffusion caractérisant la réflexion sur cette même cible ne varient) sur le potentiel de détection du signal. L'échantillonnage se fait à une fréquence de 32 échantillons par symbole (16 échantillons par bit).

Les figures 30.1 et 30.2 présentent la fonction d'ambiguité en coupe à $\tau = 0$ et à $f_d = 0$ respectivement pour 1000 et 5000 symboles de cohérence. Comme les symboles constituant le signal XM sont générés aléatoirement, quelques variations se présentent d'une simulation à l'autre sur la fonction d'ambiguïté. Une étude par simulation montecarlo est de mise afin de fixer des valeurs moyennes aux caractéristique de la fonction d'ambiguïté.

Les différents rapports d'amplitude des lobes secondaires et des " nulls " ainsi que leur position nous renseignent sur la capacité de discernement (résolution) que le signal offre pour plusieurs cibles. Ainsi, indépendamment de la longueur de la séquence de cohérence, le délai minimal permettant une détection de deux cibles distinctes est de 1.525e-7 seconde. De plus, le domaine fréquentiel est influencé par la longueur de la séquence de cohérence. La résolution doppler est donc conséquente du nombre de symboles qui constitue la séquence.

30.4 Problématique et solution envisagée

Pour tout système bistatique, et tout particulièrement les systèmes de détection passive, le principal problème, outre la puissance limitée des échos à détecter, est la détection d'échos noyés dans le signal en trajet direct. Bien que le traitement spatial permet d'empêcher la présence du signal dans le lobe principal de l'antenne réceptrice, la présence de celui-ci ne pourra être illiminée dans les lobes secondaires. Il est donc essentiel de permettre une extraction de l'information provenant de l'écho dans le signal direct dont l'amplitude est inévitablement supérieure à ce même écho.

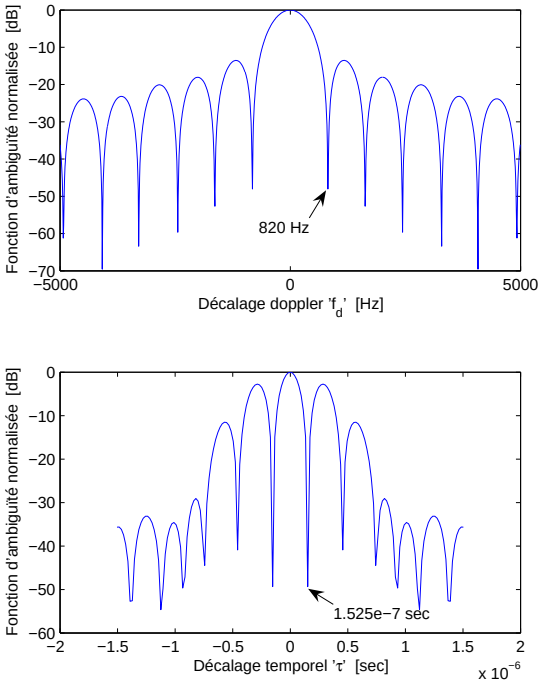


FIG. 30.1: Coupes de la fonction d'ambiguïté pour 1000 symboles de cohérence

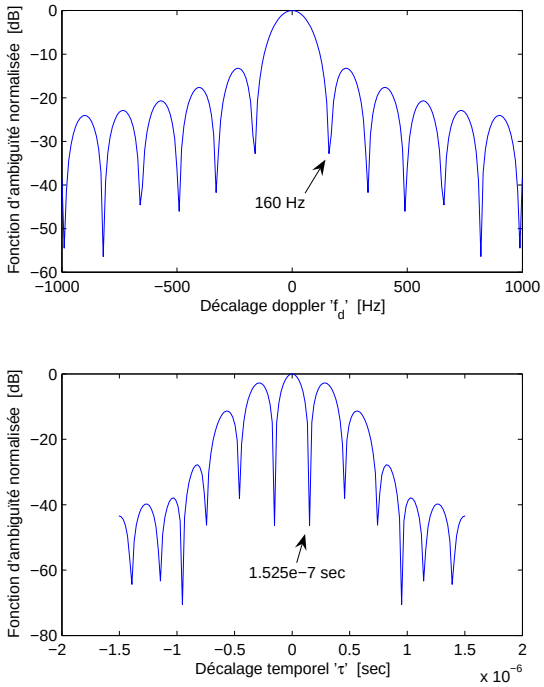


FIG. 30.2: Coupes de la fonction d'ambiguïté pour 5000 symboles de cohérence

Simulation

La performance du signal XM étant fortement tributaire du nombre de symbole de cohérence frappant la cible, il faut savoir identifier avec soin le comportement de la cible lorsqu'illuminée. Sur ce, puisqu'il n'existe aucun modèle, nous devons vérifier l'influence de l'atmosphère sur le comportement d'un signal satellite en bande S la traversant (les fluctuations d'amplitude, les variations de phase, l'atténuation et le délai) ainsi que le comportement d'une cible en mode bistatique (les variations du ou des points de diffusion en fonction du temps d'illumination).

La figure 30.3 présente le schéma bloc d'une simulation du cas d'une réception de n échos noyés dans le signal en trajet direct. Chaque échos ayant un délai (τ_{cible}) et un décalage doppler

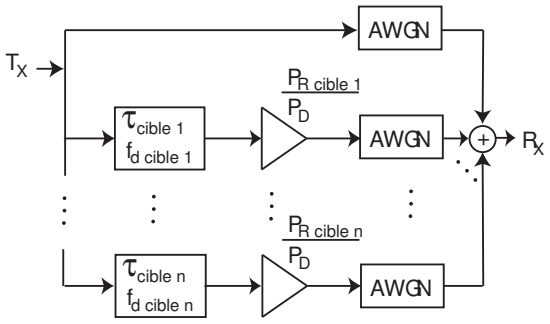


FIG. 30.3: Schéma bloc de la simulation

($f_{d\,cible}$) qui lui est propre. L'amplitude de l'écho se définit à partir du ratio de la puissance de l'écho d'une cible ($P_{R\,cible}$) sur la puissance du signal en trajet direct (P_D)[3] :

$$\frac{P_{R\,cible}}{P_D} = \frac{\sigma_B L}{4\pi \left(R_T R_R\right)^2} \tag{30.1}$$

où R_T et R_R sont les distances respectives émetteur-cible et récepteur-cible, σ_B est la section efficace radar bistatique de la cible et L est la distance entre l'émetteur et le récepteur.

Méthode envisagée

Pour le récepteur, on tente d'appliquer un principe d'extraction de l'écho similaire à l'algorithme CLEAN [4] utilisé en astronomie. Puisqu'au récepteur le message en trajet direct est connu, il est possible de reconstituer parfaitement ce signal et de le soustraire au signal reçu. Idéalement, il ne devrait avoir que l'écho et le bruit résultant de ce traitement. La détection est ensuite effectuée en utilisant un traitement temps-fréquence par des filtres adaptées.

Le principal obstacle pour cette méthode est l'évaluation adéquate de l'amplitude du signal à soustraire à la séquence principale. La soustraction d'un écho d'amplitude surévaluée contribuera à dénaturer la séquence principale tandis que la soustraction d'un écho d'amplitude sous-évaluée entrainera l'ajout de bruit dans le signal. La nécessité d'extraire justement les informations reliées au signal direct ainsi qu'à une certaine cible (dans l'optique d'appliquer cette méthode dans le but de différentier plusieurs cibles présentes dans la même séquence reçue) est vitale.

30.5 Conclusion

La détection radar passive par l'emploi du signal satellitaire XM est étudiée. La fonction d'ambiguïté permet d'analyser les caractéristiques propres au signal et de vérifier son potentiel quant à son emploi comme source d'un système radar passif. Par contre, les difficultés inhérentes à un tel procédé sont importantes. Outre la puissance reçue, l'action interférente du signal direct sur la réception de l'écho radar, source de l'information à obtenir, limite le potentiel de détection d'un tel système. L'emploi d'un traitement, similaire à CLEAN pour permettre l'extraction de ou des échos présents dans le signal reçu, permmetra d'obtenir l'information menant à la détection.

Bibliographie

[1] B. Mojarrabi et al., "Power budget study for passive target detection and imaging using secondary applications of GPS signals in bistatic radar systems," in IEEE International Geoscience and Remote Sensing Symposium, 2002.

[2] Federal Communications Commission, "In the Matter of XM Radio Inc. for Minor Modification of License to Construct, Launch and Operate a Geostationary Satellite Digital Audio Radio Service System," Washington D.C., 2001.

[3] N. J. Willis, "Bistatic Radar," Norwood, Artech House, 1991.

[4] B. D. Steinberg et al., "Microwave Imaging Techniques," John Wiley & Sons, 1991.

Simulation de la section efficace radar sur une trajectoire

Frédéric Côté, *Étudiant*
Dominic Grenier, *Co-directeur de recherche.*
Xavier Maldague, *Co-directeur de recherche.*

Résumé – Dans un contexte d'étude d'algorithme de traitement radar, la section efficace radar (SER) est souvent requise pour simuler le signal reçu à l'antenne. À haute fréquence, cette SER peut être avantageusement calculée à partir d'une cible représentée par un ensemble de facettes. L'objectif de ce travail a été d'investiguer trois méthodes analytiques pour modéliser la SER des facettes d'une cible afin d'obtenir une SER globale précise pour la simulation d'un radar se déplaçant vers une cible. Les méthodes de modélisation étudiées ont utilisé l'optique physique (OP), l'optique physique modifiée pour le champ proche et la théorie physique de diffraction (TPD) modifiée avec le concept de la méthode des courants équivalents (MCE). Les méthodes ont été validées avec des cas simples. La méthode basée sur l'OP modifiée pour le champ proche a donné le meilleur rapport précision / vitesse de calcul.

Abstract – Within the framework of radar processing studies, the radar cross section (RCS) is often required to simulate the signal received at an antenna. At high frequency, this RCS can be advantageously computed from a target modeled as a set of facets. The aim of this work was to investigate three analytic methods to model facets RCS of a target to obtain accurate global RCS values for the simulation of a radar moving toward a target. The studied analytic methods used the physical optics (PO), a refined physical optics formulation adapted to near field and the physical theory of diffraction modified with the concept of the equivalent current method (PTDECM). These methods were validated with some simple cases. The near-field refined PO approach gave the best ratio accuracy / computer efficiency.

31.1 Introduction

Dans un contexte d'engagement terminal missile-cible, on a besoin de trouver la position, l'orientation et la dimension d'une cible afin de mieux prédire la géométrie terminale de rencontre. Une approche possible pour trouver ces paramètres est l'utilisation de techniques d'imagerie ISAR à haute résolution. L'évaluation de ces techniques d'imagerie requiert des signatures radar très réalistes et celles-ci peuvent être simulées par ordinateur.

Pour simuler des signatures réalistes, on a besoin de la section efficace radar (SER) précise de la cible pour une géométrie donnée. À haute fréquence, cette SER peut être avantageusement

calculée à partir d'une cible représentée par un ensemble de facettes. L'objectif de ce travail est d'investiguer trois méthodes analytiques pour modéliser la SER des facettes d'une cible afin d'obtenir une SER globale précise pour la simulation d'un radar se déplaçant vers une cible.

Dans ce chapitre, on présente une brève description des méthodes analytiques utilisées pour modéliser la SER des facettes. Ensuite, on présente quelques résultats obtenues et finalement, on donne l'orientation des travaux futurs.

31.2 Méthodes de calcul de SER

La SER d'un objet est définie par l'équation suivante :

$$\sigma = 4\pi r^2 \frac{|\mathbf{E}_s|^2}{|\mathbf{E}_i|^2}$$

où r est la distance radar-cible, $\mathbf{E}_s$ est le champ rayonné et $\mathbf{E}_i$ est le champ incident. Le calcul de la SER est en fait un calcul de $\mathbf{E}_s$ car toutes les autres variables sont connues. Cette section donne l'idée principale pour le calcul de $\mathbf{E}_s$ selon les divers théories.

Optique physique

Le champ rayonné $\mathbf{E}_s$ par une facette peut être calculé à partir de la densité de courant circulant sur la surface de la facette. Selon la théorie de l'optique physique, cette densité de courant $\mathbf{J}$ est simplement proportionnel à l'intensité du champ magnétique incident $\mathbf{H}_i$ illuminant directement la facette [2]. Mathématiquement, on a donc :

$$\mathbf{J} = \begin{cases} 2\hat{\mathbf{n}} \times \mathbf{H}_i & \text{pour la surface illuminée} \\ 0 & \text{pour la surface ombragée} \end{cases}$$

Ces courants sont supposés uniformes sur la surface de la facette et dans le cas d'une surface polygonale plane, le champ rayonné peut être calculé sans l'utilisation d'intégration. Cette technique est très rapide.

Optique physique modifiée pour le champ proche

Lorsque l'on calcule le champ rayonné $\mathbf{E}_s$ sur une facette avec l'optique physique, il faut évaluer la fonction de Green définie par $\frac{e^{-jk|\mathbf{r}-\mathbf{r}'|}}{|\mathbf{r}-\mathbf{r}'|}$. Cette fonction dépend principalement de la distance entre la facette et le point d'observation ($|\mathbf{r}-\mathbf{r}'|$) (fig. 31.1).

Dans le champ lointain, cette distance est approximée par :

$$|\mathbf{r}-\mathbf{r}'| \approx r - \mathbf{r}' \cdot \hat{k}_s$$

et cette approximation devient imprécise à mesure que l'on se rapproche de la cible. La méthode implémentée a pour objectif de conserver une estimation précise de la distance facette - point d'observation lorsque le point d'observation (le radar) se rapproche de la cible [3]. La nouvelle formulation de la fonction de Green permet aussi l'utilisation d'une solution efficace pour résoudre l'intégrale de surface dans le calcul du champ rayonné.

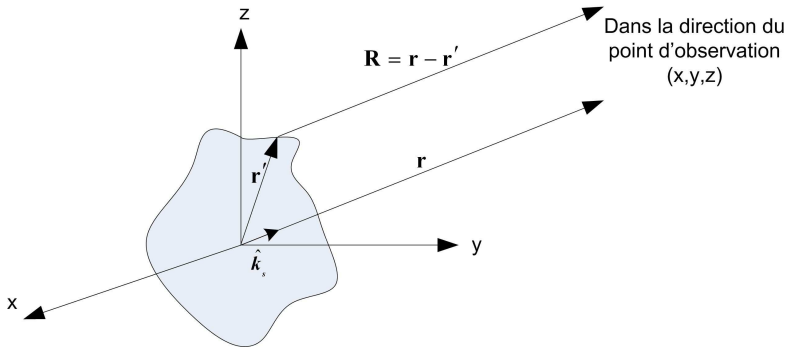


FIG. 31.1: Distance facette - point d'observation

Théorie physique de la diffraction

Avec la TPD, le champ rayonné total $\mathbf{E}^T$ est construit en additionnant un champ rayonné de frange $\mathbf{E}^{fr}$ au champ rayonné donné par l'optique physique $\mathbf{E}^{PO}$. Ce champ de frange est déterminé à partir de courants électriques et magnétiques fictifs ou équivalents circulant le long des arêtes de la cible.

$$\mathbf{E}^T = \mathbf{E}^{fr} + \mathbf{E}^{PO}$$

Le champ de frange ou de diffraction est calculé en utilisant la méthode des courants équivalents. On utilise la définition des courants équivalents proposés par Knott et Senior [1] et dans cette définition de courants, on utilise les coefficients de la théorie physique de diffraction [4]. De cette façon, le champ diffracté par les arêtes sont compatibles avec l'approche de l'optique physique.

31.3 Exemples de SER obtenue

Deux exemples de résultats sont montrés pour une plaque et un radar qui se déplace vers un cylindre.

La figure 31.2 illustre la SER obtenue pour une plaque de $3\lambda \times 3\lambda$. Ces SER sont comparées à une SER obtenues avec la méthode des moments. De plus, les résultats données par l'OP et la PTD sont similaires aux courbes données dans Knott [2].

La géométrie de simulation de la SER sur une trajectoire est illustrée à la figure 31.3 dans le cas où la cible est un cylindre. Les géométrie de rencontre sont variées 1) en changeant l'angle entre l'axe du cylindre et la ligne de trajectoire et 2) en changeant la distance minimum entre la trajectoire et le cylindre.

La figure 31.3 montre un résultat obtenu pour la simulation d'une SER dynamique avec un cylindre. Dans cette géométrie, l'angle entre l'axe du cylindre et la ligne de trajectoire est de 30° et la distance minimum entre la trajectoire et le cylindre est de 10 m. Les courbes ont des formes semblables mais il faudrait ajouter un facteur d'atténuation avec la distance pour corriger le décalage entre les courbes.

©LRTS 2005-2006

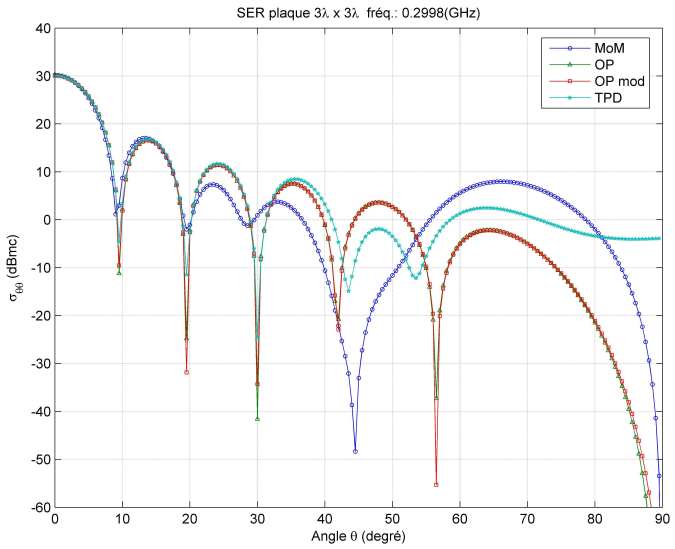


FIG. 31.2: SER d'une plaque de $3\lambda \times 3\lambda$

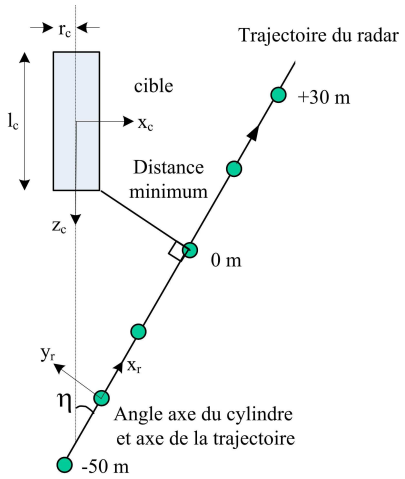


FIG. 31.3: Géométrie de simulation de SER sur une trajectoire

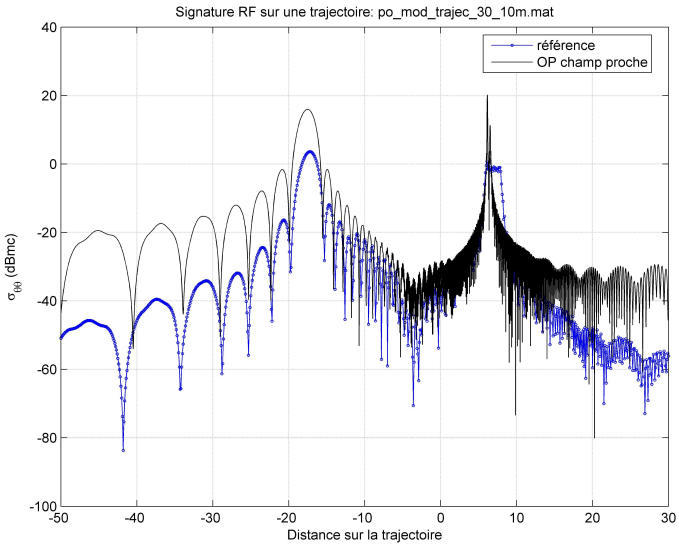


FIG. 31.4: SER obtenue avec un cylindre (angle = 30° et miss = 10 m

31.4 Travaux futurs

Les travaux relatifs à ce projet sont terminés et la rédaction du rapport final est en cours. Ce projet a été supporté par le RDDC Valcartier.

Bibliographie

[1] E.F. Knott and T.B.A. Senior. Comparison of three high-frequency diffraction techniques. *Proceedings of the IEEE*, 62(11) :1468–1474, nov 1974.

[2] E.F. Knott, J.F. Shaffer, and M.T Tuley. *Radar Cross Section*. SciTech Publishing, Raleigh, NC, 2 edition, 2004. 611.

[3] S. R. Legault. Refining physical optics for near-field computations. *Electronics Letters*, 40(1) :71–72, jan 2004.

[4] N.N. Youssef. Radar cross section of complex targets. *IEEE Transactions on Antennas and Propagation*, 77(5) :722–734, mai 1989.

©LRTS 2005-2006

Personnel du laboratoire

Professeurs

- Jean-Yves Chouinard
- Paul Fortier
- Dominic Grenier
- Sébastien Roy

Professeurs associés

- Éloi Bossé (RDDC-Valcartier)
- Gilles Y. Delisle (Institut international des télécommunications, Montréal)
- Charles Despins (PROMPT-Québec)
- Huü Tué Huynh (Université Laval)
- Elie Inaty (Université Balamand)
- Anne-Laure Jousselme (RDDC-Valcartier)
- René Le (UQAT)
- Pierre-Martin Tardif (UQAT)
- Xianbin Wang (CRC, Ottawa)

Stagiaires post-doctoraux, associés de recherche

Nom	*Directeur de projet*	*Page*
Jean-François Boudreault	S. Roy	
Louis Dupont	S. Roy	99
Isabelle Laroche	S. Roy	81
Chunsheng Liu	D. Grenier	151
Assia Semmar	J.-Y. Chouinard	

Responsables Informatique

- David-Alexandre Davidson (Dept. de Génie Élec. et de Génie Info.)
- Pierre Gaumond (Dept. de Génie Élec. et de Génie Info.)

Secrétaire

- Ghislaine L'Hébreux (Dept. de Génie Élec. et de Génie Info.)

Ajusteur mécanique

- Marco Béland (Dept. de Génie Élec. et de Génie Info.)

Étudiants de 1er cycle

Nom	*Directeur de projet*
Marie-Line Gagnon	D. Grenier
Frédéric Talbot	S. Roy

©LRTS 2005-2006

Étudiants gradués

Nom	*Niveau*	*Directeur/Co-directeur de projet*	*Page*
Irina ADJUNEAU	Ph.D.	J.-Y. CHOUINARD/P. FORTIER	61
Ahmed AHRICHE	M.Sc.	H. T. HUYNH/P. FORTIER	
Samir ARAB	M.Sc.	P. FORTIER	
Hacène BENREDOUANE	M.Sc.	H. T. HUYNH/P. FORTIER	
Abdellah BERDAI	M.Sc.	H. T. HUYNH/J.-Y. CHOUINARD	47
Hugo BERTRAND	Ph.D.	D. GRENIER/S. ROY	181
Geneviève BOUCHARD	M.Sc.	S. ROY/D. GRENIER	
Frédéric CHAMPAGNE	M.Sc.	L. A. RUSCH/J.-Y. CHOUINARD	
Abdellah CHEHRI	Ph.D.	P. FORTIER/P.-M. TARDIF	39
Frédéric CÔTÉ	M.Sc.	D. GRENIER/X. MALDAGUE	195
Benoit COURNOYER	M.Sc.	S. ROY	
Pascal DJIKNAVORIAN	M.Sc.	D. GRENIER/P. VALIN	139
Éric DUBÉ	M.Sc.	S. ROY	
Patrick DUBOIS	M.Sc.	J. GENEST/S. ROY	
Marc-André DUMAS	M.Sc.	D. GRENIER/A.-L. JOUSSELME	157
Maxime DUMAS	M.Sc.	J.-Y. CHOUINARD/S. ROY	
Louis DUPONT	M.Sc.	S. ROY/J.-Y. CHOUINARD	93
Mihai Cristian FLOREA	M.Sc.	D. GRENIER/A.-L. JOUSSELME	125
	Ph.D.	D. GRENIER/A.-L. JOUSSELME	143
Louis-Philippe GILL	Ph.D.	D. GRENIER/J.-Y. CHOUINARD	191
Pham Viet HA	Ph.D.	J.-Y. CHOUINARD	
Melita HADZAGIC	Ph.D.	H. MICHALSKA/D. GRENIER	165
Zhiyong HE	Ph.D.	P. FORTIER/S. ROY	21,25,29
Gregory HUCHET	Ph.D.	J.-Y. CHOUINARD	
Miroslava IVANOVA	M.Sc.	D. GRENIER/É. BOSSÉ	119
Isabelle LAROCHE	M.Sc.	S. ROY	103
Steve LÉGARÉ	M.Sc.	S. ROY	
Philippe LEROUX	Ph.D.	S. ROY/J.-Y. CHOUINARD	71
Jennifer MARTIN	M.Sc.	D. GRENIER	
Simon MATHIEU	Ph.D.	S. ROY/J.-Y. CHOUINARD	55
Manani MOUTAIROU	Ph.D.	G. Y. DELISLE/D. GRENIER	
Minh-Quang NGUYEN	M.Sc.	P. FORTIER	107
	Ph.D.	P. FORTIER/S. ROY	
Jean-Sébastien NÉRON	Ph.D.	G. Y. DELISLE/D. GRENIER	173
Edem NOFODJIE	Ph.D.	D. GRENIER	
Rachelle OUEDRAOGO	Ph.D.	S. ROY/L. A. RUSCH	
Tran Cao QUYEN	Ph.D.	P. FORTIER	
Robert RAAD	Ph.D.	P. FORTIER/E. INATY	3
Taofik SAÏDI	Ph.D.	S. ROY/O. SENTIEYS	87

Nom	*Niveau*	*Directeur/Co-directeur de projet*	*Page*
Simon Savary	M.Sc.	H. T. Huynh	75
	Ph.D.	J.-Y. Chouinard	17
Limeng Song	M.Sc.	J.-Y. Chouinard/S. Roy	
Michel Thériault	M.Sc.	L. A. Rusch/P. Fortier	9
	Ph.D.	S. Roy/L. A. Rusch	
Carolle Thon-Adjalin	M.Sc.	P. Fortier	
James Veilleux	M.Sc.	P. Fortier/S. Roy	
Gilles Ibrahim Wassi	Ph.D.	A.-L. Jousselme/P. Maupin/D. Grenier	133
Rujiang Wang	Ph.D.	G. Y. Delisle	35
Xin Yuan	M.Sc.	P. Fortier/P.-M. Tardif	

Courrier électronique

Le laboratoire dispose d'une boîte aux lettres électroniques avec l'adresse suivante :

`lrts@gel.ulval.ca`

Tous les membres du laboratoire ont une adresse électronique pour les rejoindre à l'Université Laval. Cependant, pour les étudiants, cette adresse électronique ne peut être divulguée que si l'étudiant l'a spécifiquement autorisé. Pour obtenir l'adresse électronique (et autres informations comme le poste téléphonique, le numéro de FAX et le bureau), il suffit de se rendre sur le site web de l'Université Laval, sous l'onglet "Chercher" soit à l'adresse

`http://www.ulaval.ca/Al/cherch.html`

On tape alors le nom de l'étudiant ou de l'employé dans la case appropriée.

Ce rapport, ainsi que plusieurs autres renseignements sur la vie du laboratoire (anciens rapports, activités de recherche, photos, site wiki), sont disponibles sur le site web à l'adresse

`http://lrts.gel.ulaval.ca/`

©LRTS 2005-2006

Publications 2001-2006

Articles publiés ou acceptés dans des revues avec comité de lecture

[1] X. Wang, Y. Wu, and J.-Y. Chouinard, "A New Position Location System using DTV Transmitter Identification Watermark Signals," *EURASIP Journal on Applied Signal Processing*, 2006. Accepté pour publication en juillet 2005.

[2] T. Kurt, A. Yongacoglu, and J.-Y. Chouinard, "OFDM and Externally Modulated Multimode Fibers in Radio over Fiber Systems," *IEEE Transactions on Wireless Communications*, 2006. Accepté pour publication en octobre 2004.

[3] X. Wang and Y. Wu and J.-Y. Chouinard and H.-C. Wu, "On the Design and Performance Analysis of Multi-Symbol Encapsulated OFDM Systems," *IEEE Transactions on Vehicular Technology*, vol. 55, pp. 990–1002, mai 2006.

[4] X. Wang and Y. Wu and J.-Y. Chouinard, "Robust Data Transmission using the Transmitter Identication Sequences in ATSC DTV Signals," *IEEE Transactions on Consumer Electronics*, vol. 51, pp. 41–47, février 2005.

[5] I.C. Sikaneta and J.-Y. Chouinard, "SAR-GMTI with eigen-decomposition of the multichannel covariance matrix," *European Journal of Signal Processing*, vol. 84, pp. 1501–1535, septembre 2004. Numéro spécial sur les "New trends and findings in antenna array processing for radar". The Signal Processing Best Paper Award 2004 (EURASIP).

[6] Y. Tong and T. Yeap and J.-Y. Chouinard, "Implementation of a Turbo Decoder with Log-MAP Based Iterative Decoding," *IEEE Transactions on Instrumentation and Measurement*, vol. 53, pp. 1268–1278, août 2004.

[7] B. Abdel-Aziz and J.-Y. Chouinard, "On Perceptual Quality of Watermarked Images - An Experimental Approach," *Digital Watermarking, Second International Workshop, IWDW 2003, Seoul, Korea, October 2003, Revised Papers, Lecture Notes in Computer Science, Springer-Verlag*, vol. 2939, pp. 277–288, 2004.

[8] X. Wang and Y. Wu and J.-Y. Chouinard and S. Lu and B. Caron, "A Channel Characterization Technique Using Frequency Domain Pilot Domain Correlation Method for DVB-T Systems," *IEEE Transactions on Consumer Electronics*, vol. 49, pp. 949–957, novembre 2003.

[9] A. Bergeron and J.-Y. Chouinard and Y. Wu, "NTSC In-Band Data Broadcasting using Orthogonal Frequency Division Multiplexing," *IEEE Transactions on Broadcasting*, vol. 47, pp. 325–339, décembre 2001.

[10] R. Raad, E. Inaty, P. Fortier, and H. M. H. Shalaby, "Optical S-Aloha/CDMA systems for multirate applications : Architecture, performance evaluation, and system stability," *IEEE/OSA Journal of Lightwave Technology*, vol. 24, pp. 1968–1977, mai 2006.

[11] E. Inaty, H. M. H. Shalaby, and P. Fortier, "On the cutoff rates of a multi-class OFFH-CDMA system," *IEEE Transactions on Communications*, vol. 53, pp. 323–334, février 2005.

[12] E. Inaty, H. M. H. Shalaby, and P. Fortier, "A new transmitter-receiver architecture for noncoherent multirate OFFH-CDMA system with fixed optimal detection threshold," *IEEE Journal of Lightwave Technology*, vol. 20, pp. 1885–1894, novembre 2002.

©LRTS 2005-2006

[13] M. L. Ammari, P. Fortier, and H. T. Huynh, "Equalizing OFDM : A study using importance sampling," *Revue canadienne de génie électrique et informatique*, vol. 27, pp. 75–81, avril 2002.

[14] E. Inaty, H. M. H. Shalaby, P. Fortier, and L. A. Rusch, "Multirate optical fast frequency hopping CDMA system using power control," *Journal of Lightwave Technology*, vol. 20, pp. 166–177, février 2002.

[15] E. Inaty, P. Fortier, and L. A. Rusch, "SIR performance evaluation of a multirate OFFH-CDMA system," *IEEE Communications Letters*, vol. 5, pp. 224–226, mai 2001.

[16] P. Valin, F. Rhéaume, C. Tremblay, D. Grenier, A.-L. Jousselme, and E. Bossé, "Comparative implementation of two fusion schemes for multiple complementary flir imagery classifiers," *Journal of Information Fusion*, vol. 7, pp. 197–206, June 2006.

[17] H. Joannis, P. Savoie, and D. Grenier, "Electrical resistance of high moisture chopped alfalfa," *Transactions of ASAE*, Nov. 2005. Accepted (# IET-05548-2004).

[18] C. Liu, D. Grenier, A.-L. Jousselme, and E. Bossé, "Reducing algorithm complexity for computing an aggregate uncertainty measure," *IEEE Trans. on Systems, Man and Cybernetics, Part A*, Nov. 2005. Accepted (# SMCA04-02-0040.R2).

[19] M. Florea, D. Grenier, A.-L. Jousselme, and E. Bossé, "An adaptive combination rule for the evidence theory," *IEEE Trans. on Systems, Man and Cybernetics, Part A*, May 2005. Resubmitted after revision (# SMCA04-08-0259.R1).

[20] A.-L. Jousselme, C. Liu, D. Grenier, and E. Bossé, "Measuring ambiguity in the evidence theory," *IEEE Trans. on Systems, Man and Cybernetics, part A*, Dec. 2004. Accepted (#SMCA03-11-0250).

[21] E. Bossé, P. Valin, A.-C. Boury-Brisset, and D. Grenier, "A priori knowledge exploitation for information fusion," *Journal of Information Fusion*, Nov. 2004. IF04B04 : Accepted, in press.

[22] A.-L. Jousselme, D. Grenier, and H. T. Huynh, "Analyse de la distorsion spectrale d'images radar de surfaces de mer," *Can. Journal on Electr. and Comp. Eng.*, vol. 29, pp. 245–253, oct. 2004.

[23] A.-L. Jousselme, D. Grenier, and E. Bossé, "A new distance between two bodies of evidence," *Journal of Information Fusion*, vol. 2, pp. 91 – 101, June 2001.

[24] J. Caron, D. Grenier, C. Ménard, T. Cliche, and B. Dansereau, "Measuring physical properties of peat substrates in containers to monitor irrigation and aeration needs," *International Peat Journal*, pp. 89–97, Jan. 2001.

[25] Z. He, P. Fortier, and S. Roy, "A class of irregular LDPC codes with low error floor and low encoding complexity," *IEEE Communication Letters*, vol. 10, pp. 372–4, mai 2006.

[26] S. Roy and P. Fortier, "A simple analytical model characterizing fading envelope correlation accross a wideband array," *IEEE Trans. Wireless Comm.*, vol. 3, pp. 1502–1507, sept. 2004.

[27] S. Roy, H. T. Huynh, and P. Fortier, "Compound Doppler spread effects of subscriber motion and scatterer motion," *Int. J. Electron. and Comm.*, vol. 57, pp. 237–246, mars 2003.

[28] Z. He, P. Fortier, and S. Roy, "Design of high-performance low-density parity-check codes using interleaver approach," *Electronic Letters*, vol. 41, pp. 1390–1, déc. 2005.

[29] Z. He, P. Fortier, and S. Roy, "Highly-parallel decoding architectures for convolutional turbo codes," *IEEE Trans. VLSI Systems*, 2006. accepté pour publication le 13 mai 2006.

[30] S. Roy and P. Fortier, "Maximal-ratio combining architectures and performance with channel estimation based on a training sequence," *IEEE Trans. Wireless Comm.*, vol. 3, pp. 1154–64, juil. 2004.

[31] S. Roy and D. D. Falconer, "Multi-User Decision-Feedback Space-Time Processing with Application to Broadband Wireless," *Wireless Personal Communications*, vol. 27, pp. 1–32, oct. 2003.

[32] S. Roy and L. Bélanger, "The Design of an FPGA-Based MIMO Transceiver for Wi-Fi," *DSP Magazine*, vol. 1, mars 2006.

[33] S. Roy and J.-S. Néron, "The impact of estimation error and dwell time on the performance of predetection selection diversity receivers," *Wireless Personal Communications*, vol. 33, pp. 87–108, avr. 2005.

[34] S. Roy and D. D. Falconer, "The matched-filter bound on optimal space–time processing in correlated fading channels," *IEEE Trans. Wireless Comm.*, vol. 3, pp. 2156–69, nov. 2004.

Articles soumis à des revues avec comité de lecture

[1] L. Dupont and S. Roy and J.-Y. Chouinard, "Generation of Random Integers Respecting the wNAF Representation for a Hardware Implementation of Elliptic Curve Cryptography," *IEEE Transactions on Circuits and Systems*, 2005. Soumis pour publication en octobre 2005.

[2] A. Semmar and J.-Y. Chouinard and P.V. Ha, S. Laflèche and X. Wang and Y. Wu, "Digital Broadcasting Television Channel Measurements and Characterization for SIMO Mobile Reception," *IEEE Transactions on Broadcasting*, 2005. Acceptation conditionnelle en décembre 2005.

[3] S. Hinds and P. Galko and J.-Y. Chouinard, "Improvement of Modulation Rate Through a Novel Semiconductor Laser Injection Locking Technique," *IEEE Journal of Lightwave Technology*, 2005. Acceptation conditionnelle en octobre 2005.

[4] R. Raad, E. Inaty, P. Fortier, and H. M. H. Shalaby, "Performance comparison of S-ALOHA and R^3T protocols for multirate OFFH-CDMA systems in optical packet network," *Soumis à Journal of Optical Network*, avril 2006.

[5] H. Bertrand, D. Grenier, and S. Roy, "Experimental antenna array calibration with artificial neural networks," *IEEE Trans. on Aerosp. and Electr. Syst.*, May 2006. Submitted (# TAES-200601846).

[6] C. Liu, A.-L. Jousselme, D. Grenier, and E. Bossé, "General uncertainty measure of a body of evidence," *IEEE Trans. on Systems, Man and Cybernetics, Part A*, Feb 2006. Submitted SMCA06-02-0051.

[7] M. C. Florea, A.-L. Jousselme, D. Grenier, and E. Bossé, "Using fuzzy membership functions and belief functions in data fusion to solve object identification problems," *J. of Advanced Information Fusion*, July 2005. To be submitted soon.

Articles de conférences avec comité de lecture

[1] P. Leroux, S. Roy, and J.-Y. Chouinard, "The Performance of Soft Macrodiversity Based on Maximal-Ratio Combining in Uncorrelated Rician Fading," in *17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06)*, (Helsinki, Finlande), 11 au 14 septembre 2006. Accepté pour présentation.

[2] P. Leroux, S. Roy, and J.-Y. Chouinard, "An Agent System to Manage Mobile connections in a Distributed Base Station Scheme," in *17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06)*, (Helsinki, Finlande), 11 au 14 septembre 2006. Accepté pour présentation.

[3] X. Wang, Y. Wu, G. Gagnon, and J.-Y. Chouinard, "Performance Analysis and Implementation of a New Position Location System Using DTV TxID Watermark," in *IEEE Vehicular Technology Conference (VTC 2006 Fall)*, (Montréal, Canada), IEEE, 25 au 28 septembre 2006. Accepté pour présentation.

[4] S. Watson, J.-Y. Chouinard, and M. Bouchard, "Performance of an orthogonal diversity combining detector for spread-spectrum signals," in *Conférence canadienne de génie électrique et informatique 2006 (CCGÉI 2006)*, (Ottawa, Canada), 7 au 10 mai 2006.

[5] L. Dupont, S. Roy, and J.-Y. Chouinard, "A FPGA Implementation of an Elliptic Curve Cryptosystem," in *2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, (Île de Kos, Grèce), 21 au 24 mai 2006.

[6] X. Wang, Y. Wu, K. Yi, B. Tian, and J.-Y. Chouinard, "A Fast Synchronization Technique for DVB-H System Using In-band Pilots and Cyclic Prefix," in *IEEE International Conference on Consumer Electronics (ICCE'2006)*, (Las Vegas, États-Unis), pp. 407–408, 7 au 11 janvier 2006. Article 9.2-1.

[7] M. Dumas, L. Bélanger, S. Roy, and J.-Y. Chouinard, "Development of a SCA 3.1 compliant W-CDMA waveform on DSP/FPGA specialized hardware," in *2005 Software Defined Radio Technical Conference (SDR'05)*, (Orange County, Californie, États-Unis), 14 au 18 novembre 2005.

[8] S. Mathieu, S. Roy, and J.-Y. Chouinard, "De la performance des systèmes MIMO sous-échantillonnés," in *2005 Canadian Workshop on Information Theory (CWIT 2005)*, (Montréal, Canada), pp. 402–405, 5 au 8 juin 2005.

[9] F. Mathieu and J.-Y. Chouinard, "Codes fréquence-temps en treillis dans une application multi-usagers en transmission montante," in *2005 Canadian Workshop on Information Theory (CWIT 2005)*, (Montréal, Canada), pp. 272–275, 5 au 8 juin 2005.

[10] X. Wang, Y. Wu, B. Caron, and J.-Y. Chouinard, "A New Position Location System using ATSC TxID Signals," in *IEEE 61st Semiannual Vehicular Technology Conference (VTC 2005 Spring)*, (Stockholm, Suède), IEEE, 29 mai au 1er juin 2005.

[11] X. Wang, Y. Wu, and J.-Y. Chouinard, "System Design and Implementation of Multiple-Symbol Encapsulated OFDM," in *IEEE 61st Semiannual Vehicular Technology Conference (VTC 2005 Spring)*, (Stockholm, Suède), IEEE, 29 mai au 1er juin 2005.

[12] S. Savary and J.-Y. Chouinard, "A Space-Time Diversity Scheme for MIMO-OFDM Systems," in *18e Conférence canadienne de génie électrique et informatique (CCGÉI 2005)*, (Saskatoon, Canada), 1er au 4 mai 2005.

[13] P. Ha, J.-Y. Chouinard, S. Lu, and A. Semmar, "Channel Characterization and Antenna Diversity in a 6 MHz DVB-T Channel," in *18e Conférence canadienne de génie électrique et informatique (CCGÉI 2005)*, (Saskatoon, Canada), 1er au 4 mai 2005.

[14] F. Mathieu and J.-Y. Chouinard, "Frequency-Time Codes for OFDMA Uplink Applications," in *18e Conférence canadienne de génie électrique et informatique (CCGÉI 2005)*, (Saskatoon, Canada), 1er au 4 mai 2005.

[15] X. Wang, Y. Wu, B. Caron, and J.-Y. Chouinard, "Transmitter Identification in Distributed Transmission Network and Its Application in Position Location and a New Data Transmission Scheme," in *2005 National Association of Broadcasters Conference (NAB2005)*, (Las Vegas, États-Unis), pp. 511–520, NAB, 16 au 21 avril 2005.

[16] A. Semmar, P. Ha, S. Lu, J.-Y. Chouinard, S. Laflèche, Y. Wu, and X. Wang, "On Spatial Diversity for Mobile Reception using ATSC 8-VSB Digital TV Signals," in *2005 National Association of Broadcasters Conference (NAB2005)*, (Las Vegas, États-Unis), NAB, 16 au 21 avril 2005.

[17] J.-Y. Chouinard, X. Wang, and Y. Wu, "MSE-OFDM : A New OFDM Transmission Technique with Improved System Performance," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'2005)*, (Philadelphie, États-Unis), pp. 511–520, IEEE, 19 au 23 mars 2005.

[18] X. Wang, Y. Wu, B. Caron, and J.-Y. Chouinard, "Robust Data Transmission using the Transmitter Identication Sequences in ATSC DTV Signals," in *IEEE International Conference on Consumer Electronics (ICCE'2005)*, (Las Vegas, États-Unis), pp. 421–422, IEEE, 8 au 12 janvier 2005.

[19] I. Sikaneta and J.-Y. Chouinard, "Non-Linear Eigen-Projection for SAR-GMTI in Heterogeneous Terrain," in *First International Conference on Waveform Diversity and Design*, (Edinburgh, Écosse), 8 au 10 novembre 2004.

[20] A. Semmar, P. Ha, J.-Y. Chouinard, S. Laflèche, X. Wang, and Y. Wu, "UHF Wideband Mobile Channel Measurements and Characterization using ATSC Signals and Diversity Antennas," in *54th Annual IEEE Broadcast Symposium*, (Washington D.C., États-Unis), IEEE, 13 au 15 octobre 2004.

[21] X. Wang, Y. Wu, and J.-Y. Chouinard, "Modified Channel Estimation for OFDM Systems with Reduced Complexity," in *7th International Conference on Signal Processing (ICSP 2004)*, (Beijing, Chine), pp. 1747–1751, IEEE, 31 août au 4 septembre 2004.

[22] F. Mathieu, J.-Y. Chouinard, and A. Semmar, "Frequency-Time Block Codes for OFDMA Uplink Applications," in *22nd Biennial Symposium on Communications*, (Kingston, Ontario, Canada), pp. 261–263, 31 mai au 3 juin 2004.

©LRTS 2005-2006

[23] B. Abdel-Aziz, J. Zhao, and J.-Y. Chouinard, "On the Limits of Second Generation Watermarks," in *Canadian Conference on Computer and Robot Vision (CRV2004)*, (London, Ontario, Canada), pp. 209–216, 17 au 19 mai 2004.

[24] T. Kurt, A. Yongacoglu, and J.-Y. Chouinard, "Performance of External Modulators for Wireless Local Area Networks under Multi-Path Fading," in *Conférence canadienne de génie électrique et informatique 2004 (CCGÉI 2004)*, (Niagara Falls, Canada), pp. 277–280, 4 au 7 mai 2004.

[25] A. Semmar, J.-Y. Chouinard, X. Wang, and Y. Wu, "UHF DTV Band Channel Characterization for Mobile Reception," in *Conférence canadienne de génie électrique et informatique 2004 (CCGÉI 2004)*, (Niagara Falls, Canada), pp. 1339–1342, 4 au 7 mai 2004.

[26] S. Lu, A. Semmar, X. Wang, Y. Wu, J.-Y. Chouinard, and P. Fortier, "Implementation and Field Test of a New Channel Estimation Technique for DVB-T System," in *Conférence canadienne de génie électrique et informatique 2004 (CCGÉI 2004)*, (Niagara Falls, Canada), pp. 1343–1346, 4 au 7 mai 2004.

[27] X. Wang, Y. Wu, and J.-Y. Chouinard, "On the Comparison between Conventional OFDM and MSE-OFDM Systems," in *IEEE Globecom'2003*, (San Franscisco, Californie, États-Unis), IEEE, 1er au 5 décembre 2003.

[28] B. Abdel-Aziz and J.-Y. Chouinard, "On Perceptual Quality of Watermarked Images : An Experimental Approach," in *2003 International Workshop on Digital Watermarking (IWDW'2003)*, (Séoul, Corée), pp. 296–307, 20 au 22 octobre 2003.

[29] L. Thibault, D. Taylor, L. Zhang, J.-Y. Chouinard, and R. Boudreau, "Advanced Demodulation Technique for COFDM in Fast Fading Channels," in *2003 International Broadcasting Conference (IBC'2003)*, (Amsterdam, Pays-Bas), pp. 416–422, 11 au 15 septembre 2003.

[30] I. Sikaneta, C. Gierull, and J.-Y. Chouinard, "Metrics for SAR-GMTI Based on Eigen-Decomposition of the Sample Covariance Matrix," in *International Conference on Radar (RADAR 2003)*, (Adelaide, Australie), pp. 442–447, 3 au 5 septembre 2003.

[31] Y. Tong, T. Yeap, and J.-Y. Chouinard, "A VHDL Implementation of Turbo Coding," in *2003 IEEE Instrumentation and Measurement Technology Conference (IMTC'2003)*, (Vail, Colorado, États-Unis), pp. 682–687, IEEE, 20 au 22 mai 2003.

[32] B. Abdel-Aziz and J.-Y. Chouinard, "Performance Analysis of a Content Authentication Semi-Fragile Watermark," in *Congrès canadien en génie électrique et informatique 2003 (CCGÉI 2003)*, (Montréal, Canada), pp. 2055–2058, 4 au 7 mai 2003. Article TF547.

[33] J.-Y. Chouinard, A. Bergeron, Y. Wu, and B. Caron, "An In-Band Multicarrier Digital Broadcasting System using Analog Television Transmitters," in *52nd Annual IEEE Broadcast Symposium*, (Washington D.C., États-Unis), IEEE, 9 au 11 octobre 2002.

[34] I. D. la Tour, G. Bochmann, and J.-Y. Chouinard, "A Secure Authentication Infrastructure for Mobile Communication Services over the Internet," in *6th International Federation for Information Processing (IFIP) Communications and Multimedia conference (CMS'2001)*, (Darmstadt, Allemagne), pp. 405–416, IFIP, 21 au 22 mai 2002.

[35] H. Schöneich, J.-Y. Chouinard, and M. Moher, "Iterative Multiuser Decoding of Narrowband Signals in Fading Channels," in *2001 Canadian Workshop on Information Theory (CWIT'2001)*, (Vancouver, Canada), pp. 126–129, 3 au 6 juin 2001.

[36] A. Chehri, P. Fortier, and P.-M. Tardif, "Frequency-domain analysis of UWB channel propagation in underground mines," in *64th Semi-Annual IEEE Vehicular Technology Conference - Fall*, (Montreal), 25-28 septembre 2006.

[37] L. V. Ninh, T. A. Vu, H. T. Huynh, and P. Fortier, "New cyclic prefix based symbol timing and carrier synchronization for OFDM," in *23rd Biennial Symposium on Communications*, (Kingston, Ontario), pp. 198–203, 29 mai - 1er juin 2006.

[38] A. Chehri, P. Fortier, H. Aniss, and P.-M. Tardif, "UWB spatial fading and small scale characterization in underground mines," in *23rd Biennial Symposium on Communications*, (Kingston, Ontario), pp. 213–218, 29 mai - 1er juin 2006.

[39] R. Raad, E. Inaty, P. Fortier, and H. M. H. Shalaby, "Optical S-ALOHA/CDMA system for multirate applications : System architecture and performance evaluation," in *IEEE Globecom 2005*, (St-Louis), 28 novembre - 2 décembre 2005.

[40] H. Aniss, P.-M. Tardif, R. Ouédraogo, and P. Fortier, "Communications network for underground mines based on the IEEE 802.11 and Docsis standards," in *IEEE Vehicular Technology Conference 2004*, Fall, 26-29 septembre 2004.

[41] J.-J. Beaudoin, G. Tran, P.-M. Tardif, and P. Fortier, "Underground experiments of video transmission over an IEEE 802.11 infrastructure," in *IEEE Vehicular Technology Conference 2004*, Fall, 26-29 septembre 2004.

[42] M. Hamza, H. T. Huynh, and P. Fortier, "Fixed and multiple step power control algorithms for MC-DS-CDMA in indoor and outdoor environments," in *IEEE International Conference on Communications*, (Paris), pp. 2965–2969, 20-24 juin 2004.

[43] E. Inaty, H. M. H. Shalaby, and P. Fortier, "Multi-class/multi-rate overlapped optical FFH-CDMA system : SIR performance evaluation and cutoff rates analysis," in *IEEE International Conference on Communications*, (Paris), pp. 1714–1719, 20-24 juin 2004.

[44] M. Thériault, L. A. Rusch, and P. Fortier, "Effect of RAKE corelations on the performance of hybrid RAKE," in *22nd Biennial Syposium on Communications*, (Kingston, Ontario), 31 mai - 3 juin 2004.

[45] M. Hamza, H. T. Huynh, and P. Fortier, "Performance of orthogonal multicarrier CDMA in indoor and outdoor systems via the characteristic function method," in *2003 Canadian Workshop on Information Theory*, (Waterloo, Ontario), 18-21 mai 2003.

[46] M. L. Ammari, H. T. Huynh, and P. Fortier, "Turbo detection of turbo coded symbols over time varying frequency selective fading channel," in *2002 IEEE Semiannual Vehicular Technology Conference*, (Vancouver), 24-29 septembre 2002.

[47] C. D. Iskander, P. Fortier, and H. T. Huynh, "Fast-converging neural equalizers for broadband QAM microcell systems," in *2002 IEEE Semiannual Vehicular Technology Conference*, (Birmingham, Al), 6-10 mai 2002.

[48] E. Inaty, H. M. H. Shalaby, and P. Fortier, "On the cutoff rate of a variable-bit-rate (VBR OFFH-CDMA system," in *2002 IEEE International Conference on Communications*, (New York), 28 avril - 2 mai 2002.

©LRTS 2005-2006

[49] E. Inaty, M. H. Shalaby, and P. Fortier, "A new transmitter-receiver architecture for non-coherent multirate OFFH-CDMA system with fixed optimal detection threshold," in *IEEE Globecom 2001*, (San Antonio), 25-28 novembre 2001.

[50] M. L. Ammari, P. Fortier, and H. T. Huynh, "Iterative joint Turbo decoding of correlated Rayleigh fading channel," in *2001 Canadian Workshop on Information Theory*, (Vancouver), 3-6 juin 2001.

[51] Y. Ernou and P. Fortier, "A software radio receiver for a seismical data system," in *Canadian Conference in Electrical and Computer Engineering*, (Toronto), 4-16 mai 2001.

[52] H. Bertrand, D. Grenier, and S. Roy, "Experimental antenna array calibration with adaptive linear neuron (adaline) network," in *IEEE VTC2006-Spring*, (Melbourne (Australia)), May 2006. Accepted.

[53] H. Joannis, P. Savoie, and D. Grenier, "Dc resistance of high moisture alfalfa and corn as a function of time, temperature and moisture content," in *ASAE/CSAE Annual International Meeting*, (Tampa (FL)), July 2005.

[54] G. I. Wassi, D. Grenier, C. Despins, and C. Nerguizian, "Radiolocation using fingerprinting technique in an underground mining environment," in *1st Internat. Workshop on Wireless Comm. in Underground and Confined Areas*, (Val-d'Or (CANADA)), pp. pp. 163–166, June 2005.

[55] M. C. Florea, A.-L. Jousselme, and D. Grenier, "Dempster-shafer evidence theory through the years : limitations, practical examples, variants under conflict and a new adaptive combination rule," in *Multisensor Data and Information Processing for Rapid and Robust Situation and Threat Assessment*, (Albena (Bulgaria)), May 2005.

[56] G. Wassi, D. Grenier, C. Nerguizian, and C. Despins, "Indoor location using received signal strengh of ieee 802.11b access point," in *CCECE*, (Saskatoon (SA)), May 2005. 1568952996.

[57] M. Pearson, A. L'Espérance, D. Grenier, and A. Gérard, "Cartography of sound intensity with manual swipping technique," in *Spring Conference on Environmental and Occupational Noise* (A. Society, ed.), (Banff (CANADA)), pp. pp. 178–184, May 2005.

[58] H. Joannis, P. Savoie, and D. Grenier, "Electrical resistance of high moisture chopped alfalfa," in *ASAE/CSAE/SCGR Annual International Meeting*, no. 041142, (Ottawa (ON)), Aug. 2004.

[59] H. Joannis, P. Savoie, and D. Grenier, "Résistivité électrique de la luzerne," in *Demi-journée d'information scientifique sur les fourrages* (C. et CQPF, ed.), (Victoriaville (CANADA)), pp. 10–16, fév. 2004.

[60] H. Dombrowski, D. Grenier, and S. Roy, "Isar imaging with array antenna receiver using autoclean algorithm," in *Can. Conf. on Electr. and Comp. Eng.*, no. 5224, (Niagara Falls (CANADA)), May 2004.

[61] L.-P. Gill and D. Grenier, "Mesures des caractéristiques radar du clinker en bande x pour l'évaluation volumétrique dans les silos," in *Can. Conf. on Electr. and comp. Eng.*, no. 4229, (Niagara Falls (CANADA)), May 2004.

[62] M. Florea, A.-L. Jousselme, D. Grenier, and E. Bossé, "Combining belief functions and fuzzy membership functions," in *SPIE - Sensor Fusion*, vol. 5099, (Orlando (FL)), pp. 113–123, May 2003.

[63] A. M. Osman, P. Savoie, D. Grenier, and R. Thériault, "Parallel-plate capacitance moisture sensor for hay and forage," in *ASAE/CIGR International Meeting*, (Chicago (IL)), p. PN : 021055, July 2002.

[64] M. Florea, D. Grenier, A.-L. Jousselme, and E. Bossé, "Fusion des données imparfaites l'aide des ensembles aléatoires," in *Congrès ACFAS*, (Québec (CANADA)), pp. S–207,www.acfas.ca/congres/congres70/S570.HTM, mai 2002.

[65] A. M. Osman, P. Savoie, D. Grenier, and R. Thériault, "Real-time determination of moisture content in hay and forage using electromagnetic effects," in *NABEC 2002*, (Québec (QC)), June 2002. # 02-016.

[66] F. Rhéaume, A.-L. Jousselme, D. Grenier, E. Bossé, and P. Valin, "New multiple classifier based on dempster-shafer theory of evidence," in *SPIE - Sensor Fusion*, vol. 4729, (Orlando (FL)), pp. 319–328, April 2002.

[67] M. Florea, A.-L. Jousselme, D. Grenier, and E. Bossé, "Unified approach to imperfect data fusion," in *SPIE - Sensor Fusion*, vol. 4731, (Orlando (FL)), pp. 75–85, April 2002.

[68] A.-L. Jousselme, D. Grenier, and E. Bossé, "Analyzing approximation algorithms in the theory of evidence," in *SPIE - Sensor Fusion*, vol. 4731, (Orlando (FL)), pp. 65–74, April 2002.

[69] A.-L. Jousselme, E. Bossé, and D. Grenier, "More results on a metric to measure the performance of evidential reasoning for identity information fusion," in *Fusion 2001 Conf.*, vol. 1, (Montréal (CANADA)), pp. TuB3–3 – TuB3–8, Aug. 2001.

[70] E. Ménard, A.-L. Jousselme, D. Grenier, and E. Bossé, "Application of valuation-based systems to object recognition problem," in *Fusion 2001 Conf.*, vol. 2, (Montréal (CANADA)), pp. FrC2–17 – FrC2–24, Aug. 2001.

[71] A. Osman, P. Savoie, D. Grenier, and R. Thériault, "Dynamic monitoring of crop moisture content in a forage harvester," in *CSAE/SCGR-NABEC Meeting*, (Guelph (CANADA)), July 2001.

[72] E. Ménard, A.-L. Jousselme, and D. Grenier, "Application des systèmes à base de "valuation" aux problèmes de reconnaissance d'objets.," in *Congrès ACFAS*, (Sherbrooke (CANADA)), p. 25, mai 2001.

[73] F. Rhéaume, A.-L. Jousselme, and D. Grenier, "Facteurs de qualité dans la fusion de classificateurs multiples," in *Congrès ACFAS*, (Sherbrooke (CANADA)), p. 25, mai 2001.

[74] S. Roy and P. Fortier, "A closed-form analytical model characterizing fading envelope correlation across a wideband array," in *Pacific Rim Conf. on Comm., Computers and Signal Proc. (PACRIM)*, (Victoria, Colombie-Britannique), août 2003.

[75] L. Dupont, S. Roy, and J.-Y. Chouinard, "A hardware architecture for the generation of wNAF random integers," in *Northeast Workshop on Circuits and Systems (NEWCAS)*, (Québec, Québec), juin 2005.

©LRTS 2005-2006

[76] S. Roy and J.-S. Néron, "A low-cost selection diversity architecture and its performance," in *Queen's Biennial Symposium on Communications (QBSC)*, (Kingston, Canada), juin 2004.

[77] S. Savary, H. T. Huynh, and S. Roy, "A Space-Frequency Diversity Scheme for MIMO-OFDM System," in *Conf. Canadienne en Génie Électri. et Info. (CCGÉI)*, (Saskatoon, Saskatchewan), mai 2005.

[78] I. Laroche and S. Roy, "An efficient regular matrix inversion circuit architecture for MIMO processing," in *IEEE Int. Symp. Circuits and Systems (ISCAS)*, (Kos, Grèce), mai 2006.

[79] J. Veilleux, P. Fortier, and S. Roy, "An FPGA implementation of an adaptive modulation system," in *Northeast Workshop on Circuits and Systems (NEWCAS)*, (Québec, Québec), juin 2005.

[80] S. Roy and P. Fortier, "Analyzing the impact of signature estimation on the output SINR of an adaptive array," in *Queen's Biennial Symposium on Communications (QBSC)*, (Kingston, Canada), juin 2002.

[81] Z. He, S. Roy, and P. Fortier, "Capacity-approaching LDPC codes with low error floors for high-speed digital communications," in *Queen's Biennial Symposium on Communications (QBSC)*, mai 2006.

[82] S. Roy and P. Fortier, "Circuit rapide d'extraction du logarithme," in *Congrès de l'ACFAS*, (Québec, Québec), mai 2002.

[83] S. Roy, "Défis architecturaux dans les transcepteurs MIMO," in *Congrès de l'ACFAS*, (Montréal, Québec), mai 2006.

[84] S. Mathieu, P. Fortier, S. Roy, and H. T. Huynh, "Discrete wavelet modulation for wireless channels," in *Queen's Biennial Symposium on Communications (QBSC)*, (Kingston, Canada), juin 2002.

[85] Z. He, S. Roy, and P. Fortier, "Encoder architecture with throughput over 10 Gbit/sec for quasi-cyclic low density parity check codes," in *IEEE Int. Symp. Circuits and Systems (ISCAS)*, (Kos, Grèce), mai 2006.

[86] Z. He, S. Roy, and P. Fortier, "High-speed and low-power design of parallel turbo codes," in *IEEE Int. Symp. Circuits and Systems (ISCAS)*, (Kobe, Japon), mai 2005.

[87] Z. He, S. Roy, and P. Fortier, "High-Speed Decoder for Short and Long Turbo Codes in Wireless Communication," in *Canadian Workshop on Info. Theory (CWIT)*, (Montréal, Québec), juin 2005.

[88] S. Roy and P. Fortier, "On the Doppler effects of scatterer motion in high-frequency wireless links," in *Queen's Biennial Symposium on Communications (QBSC)*, (Kingston, Canada), juin 2002.

[89] S. Roy, "On the Exact Performance of Zero-Forcing Combining Antenna Arrays," in *Canadian Workshop on Info. Theory (CWIT)*, (Montréal, Québec), juin 2005.

[90] J. Veilleux, P. Fortier, and S. Roy, "On the Performance of a Practical OFDM Adaptive Modulation Scheme Using a Feedback Channel," in *Pacific Rim Conf. on Comm., Computers and Signal Proc. (PACRIM)*, (Victoria, Colombie-Britannique), août 2005.

[91] S. Roy and D. D. Falconer, "Performance des récepteurs à traitement spatio-temporel en présence d'évanouissements corrélés," in *Congrès de l'ACFAS*, (Québec, Québec), mai 2002.

[92] T. Saïdi, S. Roy, and O. Sentieys, "Prototype MIMO 2 X 2 appliqué à la technologie HSUPA," in *Majecstic'2005*, (Rennes, France), nov. 2005.

[93] L. Bélanger, S. Roy, T. Saïdi, and O. Sentieys, "Prototyping a MIMO W-CDMA System using a System-Level Approach," in *Internat. Signal Processing Conf. (ISPC) and Global Signal Processing Expo (GSPx)*, (Santa Clara, États-Unis), sept. 2004.

[94] S. Roy, "Reduced complexity space-time array receiver with subarray selection," in *Pacific Rim Conf. on Comm., Computers and Signal Proc. (PACRIM)*, (Victoria, Colombie-Britannique), août 2003.

[95] J. M. M. da Silva, S. Roy, and P. Fortier, "The impact on the capacity of a GSM / GPRS systen using space-time processing techniques," in *Conf. Canadienne en Génie Électri. et Info. (CCGÉI)*, (Montréal, Québec), mai 2003.

[96] S. Roy, "The MIMO matched-filter bound in correlated dispersive Rician fading," in *Canadian Workshop on Info. Theory (CWIT)*, (Montréal, Québec), juin 2005.

[97] S. Roy, "The performance of maximal-ratio combiners in nakagami fading with imperfect weight estimation," in *Queen's Biennial Symposium on Communications (QBSC)*, (Kingston, Canada), juin 2004.

[98] S. Roy and D. D. Falconer, "The space-time matched-filter bound in correlated LOS and NLOS fading channels," in *IEEE Int. Conf. Comm. (ICC)*, (Paris, France), juin 2004.

Rapports techniques, livres et brevets

[1] S. Roy and J.-Y. Chouinard, *Réseaux d'antennes et systèmes MIMO reconfigurables*, ch. 6, pp. 161–195. collection Réseaux et Télécom, Lavoisier, juillet 2005. Chapitre du traité "Les systèmes radio-mobiles reconfigurables", G. Vivier (éditeur), ISBN 2-7462-1127-0.

[2] A. Bergeron and Y. Wu and J.-Y. Chouinard, "Method and System for Broadcasting a Digital Data Signal Within An Analog TV Signal Using Orthogonal Frequency Division Multiplexing." Brevet américain : US Patent #6,788,349. 7 septembre 2004.

[3] M.-Q. Nguyen, P. Fortier, and S. Roy, "Fundamentals of 4th generation multi-carrier code division multiple access (MC-CDMA)," tech. rep., Université Laval, mars 2006. DRDC-Ottawa, contract W7714-050942.

[4] D. Grenier, "Quality assessment and unified information fusion framework - 1st and 2nd year," tech. rep., Lockheed-Martin Canada, Aug. 2003 and 2004.

[5] R. Thériault, P. Savoie, and D. Grenier, "Optimisation des techniques de récolte et d'entreposage de foin destiné au commerce," rapport technique, CORPAQ 101074, Mars 2004.

[6] J. Caron, D. Grenier, R. Nemati, and T. Cliche, "Développement d'un systême de contrôle de la fertirrigation pour les plantes en contenants basé sur la technologie de la réflectométrie métallique," rapport technique, CORPAQ 4409, juillet 2001.

[7] D. Grenier and M. Lecours, "Fusion of imaging and non-imaging sensors through evidential reasoning," tech. rep., CRSNG-Lockheed-Martin Canada, Jan. 2001.

©LRTS 2005-2006