

# Transmissions acoustiques sous-marines furtives basées sur un étalement de spectre à codes chaotiques

S. Azou et G. Burel

Laboratoire d'Electronique et Systèmes de Télécommunications (UMR CNRS 6165)  
6, avenue Le Gorgeu, CS 93837, 29238 BREST cedex 3, FRANCE

E-mail : {Stephane.Azou, Gilles.Burel}@univ-brest.fr

## Résumé

Nous présentons dans cet article un système original destiné aux communications numériques sécurisées en acoustique sous-marine. La solution proposée, reposant sur des propriétés de systèmes dynamiques chaotiques, permet de se protéger à la fois contre l'interception et la détection par l'utilisateur non-autorisé. La nature chaotique des codes d'étalement utilisés à l'émission permet en effet d'éviter toute périodicité en gardant de bonnes propriétés de corrélation. Deux démodulateurs ont opéré avec succès à la mer (un utilisateur) : le premier, basé sur un traitement RAKE, est proche de solutions conventionnelles ; le second, plus original, repose sur un filtrage de Kalman parallèle pour estimer simultanément symbole et erreur de phase en bande de base.

## 1 Introduction

Depuis près de quinze ans, l'on assiste à une intensification des activités de recherche pour l'application de la théorie du chaos à la transmission de l'information. Cette motivation fait suite à des résultats de Pecora et Caroll à propos des propriétés de synchronisation de deux oscillateurs chaotiques identiques initialisés à des états différents [1]. En conséquence de ses propriétés similaires à celles du bruit, tout en gardant un caractère déterministe, le chaos permet d'assurer conjointement l'étalement du spectre et le cryptage. La discrétion des signaux peut ainsi être réduite en raison de la non-périodicité des codes d'étalement (i.e. Faible Probabilité d'Interception ; FPI) et en raison de la dynamique extrêmement complexe il s'avère difficile pour l'utilisateur non-autorisé d'accéder à l'information portée par le signal intercepté.

De nombreuses variantes de modulateurs chaotiques ont été explorées à ce jour ; citons notamment l'étalement de spectre par séquence directe ou par sauts de fréquence utilisant des séquences chaotiques, le masquage chaotique ou la commutation chaotique. Pour une revue de ces différentes approches, le lecteur pourra se référer à [2, 3]. Les résultats reportés dans la littérature concernent le plus souvent des simulations numériques, intégrant des modèles de canaux plus ou moins réalistes ; les rares investigations menées au plan expérimental ne concernent que le canal radio-fréquence. La nature non-périodique et l'extrême sensibilité aux conditions initiales des oscillateurs chaotiques posent des problèmes nouveaux pour la conception de démodulateurs, surtout lorsqu'il s'agit de mettre en oeuvre l'idée originale de Pecora et Caroll.

Les techniques d'étalement de spectre de type DS-CDMA (Direct-Sequence Code Division Multiple Access) sont devenues très populaires, grâce notamment à l'explosion des applications radio-mobiles (téléphonie, positionnement...). Dans le domaine sous-marin, le DS-CDMA semble aussi la technologie privilégiée pour le déploiement de réseaux acoustiques en eau peu profonde [4, 5]. Jusqu'à présent les systèmes DS-CDMA font un usage intensif de codes d'étalement pseudo-aléatoires comme les séquences de longueur maximale, les séquences de Gold ou de Kasami. Des études récentes montrent que la périodicité de ces codes ainsi que leur mécanismes de construction bien connus peuvent constituer une faille de sécurité [6, 7, 8]. La mise en oeuvre de codes chaotiques est une solution potentielle à ce problème, à condition bien sûr de satisfaire à peu près aux mêmes objectifs que le système DS-CDMA conventionnel, en terme de Taux d'Erreur Bit (TEB), de capacité de canal ou de complexité d'implémentation.

Dans un article récent [10], nous avons évalué la faisabilité de transmissions à étalement de spectre par séquence chaotique directe en ASM, grâce à l'usage d'un simulateur de propagation acoustique. Deux récepteurs ont ainsi été expérimentés : le premier, qui opère à l'aide d'un corrélateur à l'issue de la récupération de porteuse (boucle de Costas) et du verrouillage du retard de code, n'a de différence avec les solutions standards que la nature chaotique de la séquence d'étalement ; le second récepteur emprunte une toute autre approche avec un filtrage de Kalman parallèle pour estimer simultanément code d'étalement et symbole après récupération de porteuse. Ce second récepteur correspond en fait à une solution semi-aveugle au sens que seul le modèle dynamique du code est exploité en réception au lieu d'une réplique locale exacte pour la première approche. L'idée de reconstruction au récepteur de la séquence d'étalement correspond à la synchronisation chaotique explorée par Pecora et Carroll. L'objectif initial de cette opération était de simplifier de façon significative les opérations de synchronisation au récepteur (éviter les boucles à verrouillage de retard). Nous montrons dans [10] que le récepteur à synchronisation chaotique est viable tant que le Rapport-Signal-à-Bruit (RSB) est positif sur simulateur ASM. Des études complémentaires ont été menées pour rendre plus robuste ce type d'approche. Dans l'objectif d'assurer une réelle furtivité des transmissions en ASM petit-fond ( $RSB \ll 0$  dB, présence de trajet-multiple et non-stationnarités), nous avons développés deux autres solutions de récepteurs, qui ont été expérimentées à la mer au cours de l'année 2003 en rade de Brest. L'une des deux approches correspond à un traitement RAKE utilisant un retour de décision symbole, l'autre, opérant au rythme chip, reprend le principe de filtrage Kalman parallèle mais en considérant cette fois la version originale de code d'étalement et en estimant symbole et phase en bande de base. Afin de réaliser un bon compromis performances/coût de calcul, nous utilisons à chaque fois des filtres de Kalman Unscented [13] au lieu du classique filtre de Kalman étendu [12]. Quelques résultats d'essai à la mer du récepteur Kalman parallèle sont reportés dans [11], pour le cas de RSB positifs. Nous montrons dans le présent article quelques résultats complémentaires, pour les récepteurs RAKE et Kalman parallèle, en contexte de transmission furtive (pour un utilisateur).

L'article est organisé comme suit ; Au second paragraphe nous illustrons quelques unes des propriétés attractives du chaos pour la transmission d'information. Le principe de l'étalement de spectre par séquence chaotique directe est présenté au paragraphe 3. Les deux récepteurs mis en oeuvre sont alors évoqués au paragraphe 4 avant d'illustrer leurs fonctionnements à la mer.

## 2 Définition et Propriétés générales des signaux chaotiques

Un oscillateur chaotique est un système dynamique non-linéaire déterministe capable de produire des trajectoires en apparence aléatoire, en raison de son extrême sensibilité aux conditions initiales. Deux trajectoires débutant en des états voisins vont alors diverger exponentiellement (fig.1), à la condition que l'un des exposants de Lyapunov  $\{\lambda_i\}_{i=1,\dots,n}$  soit strictement positif (au moins),  $n$  désignant l'ordre du système. Les exposants de Lyapunov constituent une mesure

du taux de divergence de deux trajectoires initialement voisines. Une autre condition nécessaire pour l'existence de chaos est que l'ordre doit vérifier  $n \geq 1$  pour un système en temps discret ou bien  $n \geq 3$  pour un système en temps continu. Par la suite, nous considérons le cas d'un système en temps discret, régi par l'équation aux différences en dimension un  $x_{k+1} = f(x_k)$ , où  $x_k \in \mathbb{R}$  désigne l'état du système à l'itération  $k$  et où  $f(\cdot)$  est une fonction non-linéaire.

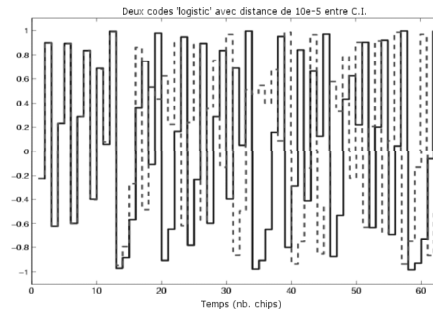


FIG. 1 – Deux séquences chaotiques générées par l'application *logistic* pour des conditions initiales voisines ( $\epsilon = 10^{-5}$ )

Grâce au chaos, il est possible de générer des séquences  $\{x_k\}_{k=1,\dots,L}$  de dynamique complexe à partir de systèmes très simples, ce qui est un avantage du point de vue de l'implémentation et du coût de calcul. Aussi, les propriétés de corrélation sont tout à fait compatibles avec une application aux communications numériques de type CDMA. Considérons par exemple l'application *logistic* :

$$x_{k+1} = f(x_k) = rx_k(1 - x_k) \quad (1)$$

L'évolution de l'exposant de Lyapunov en fonction du paramètre  $r$ , influant sur la dynamique du système est indiquée à la figure 2. Nous observons que seules certaines valeurs de  $r$  engendrent le chaos ( $\lambda_1 > 0$ ) ; pour la suite, nous prendrons  $r = 4$  pour bénéficier de séquences chaotiques centrées, avec de bonnes propriétés de corrélation. Asymptotiquement (i.e.  $L \rightarrow \infty$ ), les séquences obtenues sont alors idéales, puisque

$$R_x(d) = E\{x_k \cdot x_{k-d}\} = \frac{1}{2} \delta_d \quad (2)$$

où  $\delta_d$  désigne la fonction de Dirac discrète.

Lorsque les séquences sont tronquées, cette bonne propriété est perdue mais de très bonnes performances sont tout de même réalisées, comme l'indiquent les simulations de Monte Carlo de la figure 3 ( $L = 63$ , 100 expériences).

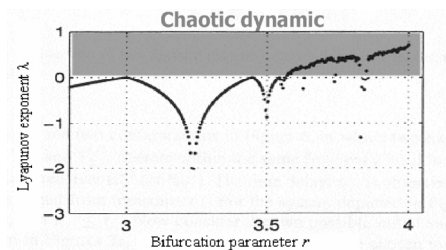


FIG. 2 – Influence du paramètre  $r$  sur la dynamique de l'application *logistic*

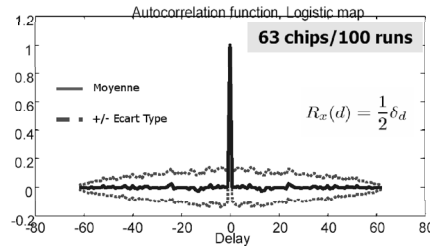


FIG. 3 – Autocorrélation de séquences *logistic* de longueur 63

### 3 Émetteur à étalement de spectre par séquence chaotique directe

Le principe de l'émetteur à étalement de spectre chaotique mis en oeuvre est indiqué à la figure 4; l'information est encodée en BPSK (ou DPSK) avant étalement de spectre par séquence chaotique directe au rythme chip  $F_c \gg F_b$ , où  $F_b$  désigne la fréquence symbole. La nature chaotique de la séquence d'étalement permet d'éviter toute périodicité, qui serait incompatible avec l'objectif de discrétion absolue.

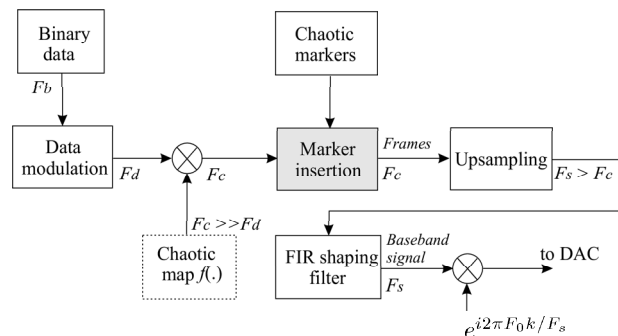


FIG. 4 – Émetteur à étalement de spectre par séquence chaotique directe

Le gain de traitement  $W = F_c/F_b$  est un paramètre-clé du système, habituellement ajusté en fonction de contraintes telles que Taux d'Erreur Bit (TEB), débit, bande passante du canal ou discrétion des signaux (niveau de densité spectrale de puissance). Ce dernier critère étant jugé primordial dans l'application étudiée, seules de grandes valeurs de gain de traitement seront utilisées ( $L > 63$ ). Après étalement de spectre, le signal est structuré en trames, avec marqueurs chaotiques (i.e. symboles pilotes) en préambule afin de faciliter la synchronisation et l'initialisation des divers estimateurs mis en oeuvre au récepteur. Enfin, après suréchantillonnage, le signal est filtré passe-bas (racine de cosinus surélevé) puis transposé en fréquence via porteuse sinusoïdale.

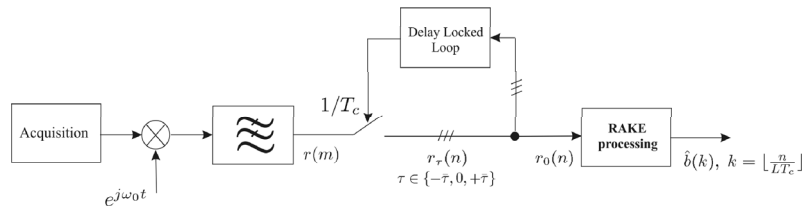


FIG. 5 – Structure du récepteur RAKE

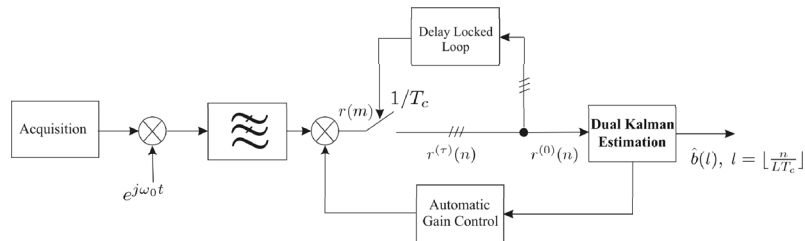


FIG. 6 – Structure du récepteur Kalman parallèle

## 4 Les deux solutions de démodulateur envisagées

Le premier récepteur développé, de structure assez conventionnelle (figure 5), repose sur un traitement RAKE pour combattre les échos présents sur le canal. Avant démodulation, le signal, issu de l'étape d'acquisition, est transposé en bande de base puis filtré passe-bas (racine de cosinus surélevé) ; Un sous-échantillonnage au rythme chip, piloté par une boucle à verrouillage de retard, est ensuite opéré.

La structure globale du second récepteur est similaire (figure 6), mais avec en plus une boucle de contrôle automatique de gain. Cette fonction, jugée non essentielle pour le premier récepteur, peut y être rajoutée afin d'améliorer les performances. Le second récepteur repose sur un filtrage de Kalman parallèle, une fois le verrouillage du retard symbole assuré, pour estimer simultanément le code (dans l'objectif de contrôle de gain uniquement), le symbole et l'erreur de phase de la porteuse. Les estimations au sein de ce démodulateur sont cadencées à la fréquence chip au lieu du rythme symbole pour la solution RAKE. De par la nature non-linéaire des signaux mis en oeuvre, nous avons choisi d'implémenter ce deuxième récepteur à l'aide de filtres *Unscented Kalman* [13], une alternative récente au classique filtre de Kalman étendu [12], jugé moins robuste et plus délicat à implémenter.

Le démodulateur est détaillé à la figure 7. Celui-ci va, en parallèle et au rythme chip, estimer le code d'étalement, le symbole d'information et l'erreur de phase de la porteuse. A un instant donné  $n$  chacun des trois filtres exploite les estimations passées (instant  $n - 1$ ) des autres filtres en tant que paramètres. Le signal reçu  $r(n)$  est modélisé comme suit :

$$r(n) = b.c_n.e^{j\phi_n} + w_n \quad (3)$$

où  $b = \pm 1$  est le symbole transmis,  $c_n \in [-1, +1]$  est le code d'étalement associé (de type *logistic*, par exemple),  $\phi_n \in [0, 2\pi]$  est l'erreur de phase de la porteuse (la transposition en bande de base se fait à fréquence fixe) et  $w_n \in \mathbb{C}$  un bruit blanc gaussien complexe de variance  $R_w$ , modélisant les imperfections du canal de transmission.

Ce modèle ne prend donc pas explicitement en compte le problème de trajet multiple ; malgré

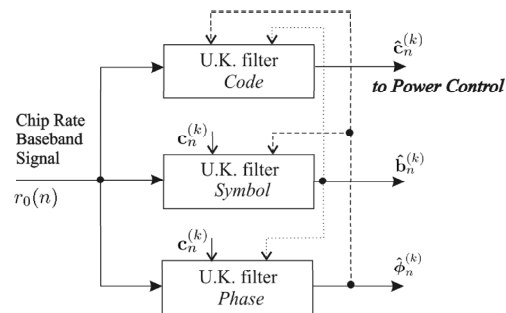


FIG. 7 – Démodulateur à filtrage de Kalman parallèle du Code/Symbole/Phase

cette simplicité apparente, nous constaterons que le démodulateur est en mesure de bien fonctionner tant qu'il existe un trajet d'énergie dominante par rapport aux répliques retardées. Le terme  $w_n$  reflète donc à la fois le bruit rencontré sur le canal et la propagation par trajet multiple (les échos sont alors considérés comme sources de bruit).

## 5 Quelques résultats d'essai à la mer

Nous illustrons ci-après les performances des deux récepteurs précédents sur une expérimentation à la mer effectuée en rade de Brest en juillet 2003, avec une distance relative émetteur-récepteur d'environ 6 km. Le code d'étalement mis en oeuvre était de type logistic, avec un gain de traitement de 127 et une fréquence chip valant 4410 Hz. Le RSB estimé en entrée du récepteur (bande de Nyquist), d'environ -6.5 dB, satisfait a priori à l'objectif de discrétion. Une représentation du signal enregistré dans le plan temps-fréquence nous permet de vérifier que la transmission est effectivement noyée dans le bruit de fond (figure 8). En raison du caractère non-périodique du code d'étalement, cette dernière condition peut être considérée comme suffisante pour garantir la bonne discrétion des signaux (très faible probabilité d'interception).

L'estimation de canal, obtenue au moyen du traitement RAKE au rythme symbole, est illustrée à la figure 9. Ne sont représentés ici que les trajets sélectionnés au seuil de 3 dB d'atténuation par rapport au trajet le plus énergétique. Les échos s'étalent sur une dizaine de temps chip, soit 2.2 ms environ ; un trajet énergétiquement dominant ressort assez bien. Au seuil de sélection choisi, un bruit de fond significatif est pris en compte dans l'estimation symbole mais un TEB nul est tout de même atteint pour la trame de 200 bits transmise. La constellation (figure 10) témoigne en effet d'une réception correcte de l'information.

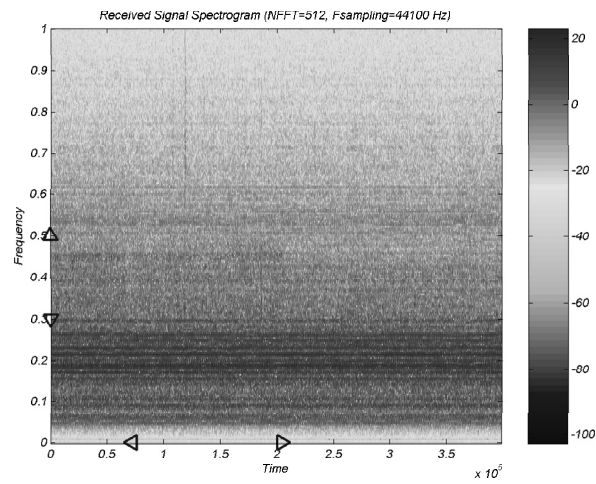


FIG. 8 – Représentation temps-fréquence du signal reçu ; les symboles  $\{\triangleleft, \triangleright\}$  marquent le début et la fin de la transmission respectivement, alors que  $\{\triangle, \nabla\}$  délimitent la bande passante

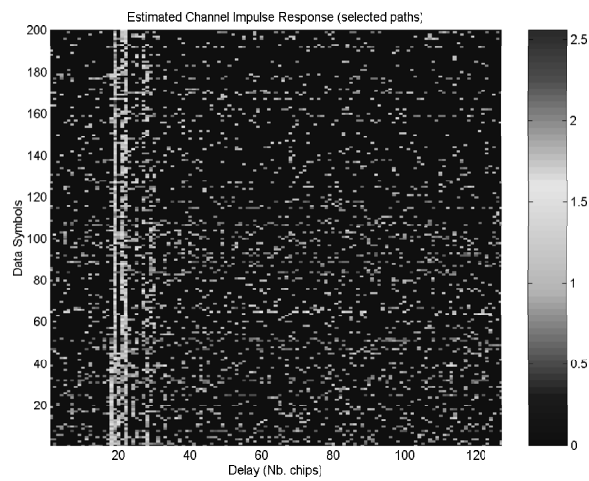


FIG. 9 – Estimation de canal au rythme symbole lors du traitement RAKE (trajets sélectionnés)

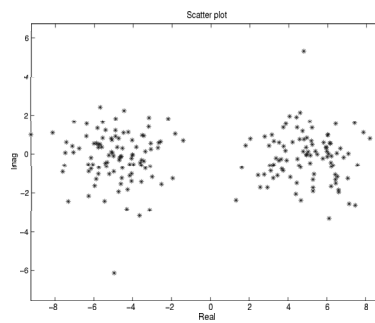


FIG. 10 – Constellation à l'issue du traitement RAKE

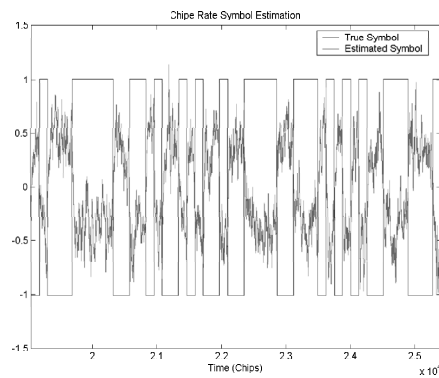


FIG. 11 – Estimation de symbole au rythme chip par le démodulateur Kalman parallèle

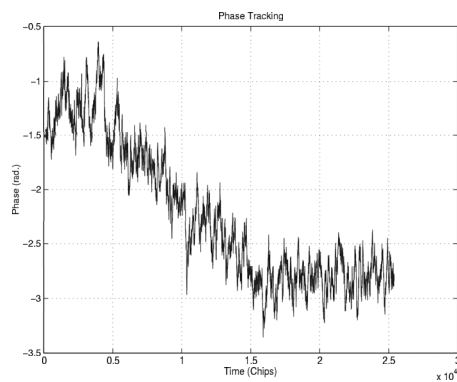


FIG. 12 – Estimation de l'erreur de phase au rythme chip par le démodulateur Kalman parallèle

Le récepteur Kalman parallèle fonctionne lui aussi très bien sur cet essai. L'estimation au rythme chip des symboles transmis est montrée à la figure 11, pour une partie de trame. L'impact des trajets multiple peut être observé sur cette figure : nous rappelons en effet que le modèle mis

en oeuvre dans le récepteur ne prend pas explicitement en compte ce phénomène de propagation. Les transitions au changement de symbole ainsi que l'estimation globale sur une durée symbole restent tout de même bonnes ; un TEB nul est obtenu pour la trame entière (200 bits). L'erreur de phase porteuse, compensée au rythme chip, laisse apparaître des fluctuations assez rapide.

## 6 Conclusions

Grâce aux propriétés de systèmes dynamiques chaotiques, un système de communications numériques furtives a été développé. Par séquence chaotique directe, nous réalisons à la fois l'étalement de spectre et le cryptage de l'information. Diverses solutions de récepteurs ont été étudiées, parmi lesquelles un traitement RAKE avec retour de décision symbole et un filtrage Kalman simultané sur le symbole et la phase, à la fréquence chip. La chaîne de transmission complète a été testée à la mer, en rade de Brest, au cours de l'année 2003. Ces essais ont permis de vérifier le bon comportement des récepteurs dans des conditions variables (géométrie du canal, portée, RSB, gain de traitement etc.). La furtivité des signaux a bien été atteinte à de nombreuses reprises ; la longueur des codes d'étalement étant infinie, le RSB négatif de quelques dB peut être jugé comme condition suffisante pour réaliser cet objectif.

**Remerciements** Ce travail a été effectué pour le compte du Ministère de la Défense (contrat DGA-CELAR 0159915/00-470-15-35). Les auteurs tiennent à remercier G. Lapierre, C. Pistre et L. Le Duff du Groupe d'Etudes Sous-Marines de l'Atlantique (GESMA, Brest, France) pour leurs conseils et pour la gestion des ressources matérielles lors des essais en mer.

## Références

- [1] L. Pecora, T. Carroll, " Synchronization in chaotic systems ", *Phys. Rev. Lett.*, Vol. 64, pp. 821-823, 1990.
- [2] M. Hasler " Synchronization of chaotic systems and transmission of information ", *Int. J. Bifurcation and Chaos*, Vol. 8, No 4, pp 647-659, 1998.
- [3] T. Yang, "A Survey of Chaotic Secure Communication Systems", *International Journal of Computational Cognition* (<http://www.YangSky.com/yangijcc.htm>), Volume 2, Number 2, June 2004.
- [4] E. M. Sozer, M. Stojanovic, J. G. Proakis, " Underwater Acoustic Networks ", *IEEE J. Oceanic Eng.*, Vol. 25, No 1, 2000.
- [5] L. Freitag, M. Stojanovic, S. Singh, M. Johnson, " Analysis of Channel Effects on Direct-Sequence and Frequency-Hopped Spread-Spectrum Acoustic Communication ", *IEEE J. Oceanic Eng.*, Vol. 26, No. 4, Oct. 2001.
- [6] G. Burel, C. Boudier, " Blind estimation of the pseudo-random sequence of a direct-sequence spread spectrum signal ", *IEEE 21st Century Military Communications Conference (IEEE-MILCOM'2000)*, October 22-25, 2000, Los Angeles, USA.
- [7] C. Boudier, S. Azou and G. Burel, "Performance analysis of a spreading sequence estimator for spread spectrum transmissions", *Journal of the Franklin Institute*, Vol. 341, Issue 7, pp. 595-614, Oct. 2004.
- [8] M. K. Tsatsanis, G. B. Proakis, " Blind estimation of direct sequence spread spectrum signals in multipath ", *IEEE Trans. Signal Processing*, Vol. 45, No. 5, pp. 1241-1252, 1997.
- [9] S. Azou, G. Burel, "Design of a demodulator in a chaos-based spread spectrum communication system using dual Unscented Kalman Filters", *IEEE-Communications 2002*, Dec. 5-7, 2002, Bucharest, Romania.

- [10] S. Azou, C. Pistre, G. Burel, "A chaotic direct sequence spread-spectrum system for underwater communication", *IEEE-Oceans'02*, Biloxi, MS, USA, Oct. 2002.
- [11] S. Azou, C. Pistre, L. Le Duff, G. Burel, "Sea trial results of a chaotic direct-sequence spread spectrum underwater communication system", *IEEE-OCEANS'03*, San Diego, CA, USA, Sept. 2003.
- [12] Y. Bar-Shalom, X.-R. Li, " Estimation and Tracking - Principles, Techniques and Software ", Artech House, 1993.
- [13] S. Julier, J. Uhlmann, H. F. Durrant-Whyte, " A new method for the nonlinear transformation of means and covariances in filters and estimators ", *IEEE Trans. Automat. Contr.*, Vol. 45, No. 3, pp. 477-482, 2000.