Communication numérique sécurisée par synchronisation du chaos

Moez FEKI, Guillaume GELLE, Maxime COLAS, Bruno ROBERT, Georges DELAUNAY

DéCom - Université de Reims Champagne Ardenne
UFR Sciences Exactes, Moulin de la Housse - BP 1039, 51687 Reims cedex 2 France
moez.feki@univ-reims.fr, guillaume.gelle@univ-reims.fr
maxime.colas@univ-reims.fr, bruno.robert@univ-reims.fr, georges.delaunay@univ-reims.fr

Résumé – Ce travail concerne les communications numériques sécurisées basées sur un principe de modulation par des signaux chaotiques. Le système de communication présenté ici repose sur un nouveau concept, l'emploi d'une rétroaction dans la chaîne de transmission. Il permet notamment d'élargir la classe de signaux chaotiques potentiels pour ce type d'applications sans alterer la vitesse de synchronisation du système.

Abstract – This paper deals with a secure digital communication scheme using discrete chaotic signals. In our approach a message is encrypted at the transmitter using chaotic modulation and feedback. This new method helps to cover a larger class of chaotic systems that can be used for communication application. To demonstrate the efficiency of our communication scheme Hénon's map is considered as an illustrative example.

1 Introduction

De nombreux travaux ont été présentés ces dernières années exploitant les signaux chaotiques dans le contexte des télécommunications. En effet, leurs caractéristiques, sensibilités aux conditions initiales, aspects aléatoires et spectres continus large bande, sont bien adaptées aux transmissions sécurisées [1, 2, 3]. Nous présentons dans cet article un nouveau schéma de communication numérique sécurisée mettant à profit les propriétés des systèmes chaotiques discrets. Notre système est basé sur un principe de modulation par un signal chaotique combiné à l'effet d'une rétroaction. A la réception, connaissant la structure du modulateur chaotique, il suffit d'assurer la synchronisation du récepteur pour reconstruire le signal chaotique et retrouver le message par démodulation. Nous proposons dans cette communication une méthode ayant l'avantage d'être adaptée à une plus grande classe de systèmes chaotiques que les systèmes par simple modulation. De plus, la synchronisation très rapide du récepteur (seulement quelques bits suffisent à la synchronisation) constitue un des avantages permettant d'envisager des transmissions sécurisées haut débit.

Après une brève introduction, la partie deux présente le principe de synchronisation des oscillateurs chaotiques. Dans la partie trois, le schéma de transmission est présenté ainsi que le principe de reconstruction. La partie quatre montre comment adapter un système chaotique à notre schéma de transmission afin d'assurer la stabilité du système et préserver le comportement chaotique. Les performances de notre système sont illustrées dans la partie cinq pour des signaux binaires en fonction du Eb/N0 ainsi que pour la transmission d'images.

2 Synchronisation basée sur les observateurs discrets

Les systèmes chaotiques à temps discret sont généralement décrits par une équation aux différences non linéaire. Il s'avère cependant intéressant de séparer la dynamique du système en une partie linéaire et une non-linéaire. De plus, la restriction aux systèmes de type Lur'e permet d'écrire :

$$x(k+1) = Ax(k) + f\big(y(k)\big) \quad (1a)$$
$$y(k) = Cx(k) \quad (1b)$$

où k est l'indice temporel discret, $x \in \mathbb{R}^n$ et $y \in \mathbb{R}$ représentent respectivement le vecteur d'état et la sortie du système d'émission. A and C sont deux matrices constantes et $f : \mathbb{R} \to \mathbb{R}^n$ est une fonction vectorielle réelle.

Le récepteur est conçu sur la base d'un observateur discret de type Luenberger où $y(k)$ correspond à l'entrée de commande.

$$\hat{x}(k+1) = A\hat{x}(k) + f\big(y(k)\big) \quad (2a)$$
$$+L\big(y(k) - \hat{y}(k)\big) \quad (2b)$$
$$\hat{y}(k) = C\hat{x}(k) \quad (2c)$$

avec $\hat{x}$ le vecteur d'état associé au récepteur et où $L \in \mathbb{R}^n$ est un gain d'observateur choisi afin de satisfaire aux conditions de synchronisation *i.e.,* $\lim_{k\to\infty} \big(x(k) - \hat{x}(k)\big) = 0$.

En définissant l'erreur de synchronisation telle que $e(k) = x(k) - \hat{x}(k)$, la dynamique d'erreur est donnée par :

$$e(k+1) = \big(A - LC\big)e(k) = A_c e(k) \quad (3)$$

avec les conditions initiales $e(0) = x(0) - \hat{x}(0)$, la solution de (3) est telle que :

$$e(k) = A_c^k e(0) \quad (4)$$

Si la paire (A, C) est observable alors on peut choisir L tel que le rayon spectral de A_c soit inférieur à 1. L'équation (3) est alors stable et $\lim_{k\to\infty} e(k) = 0$. De plus, si L est choisi de telle sorte que A_c soit une matrice nilpotente d'ordre p *i.e.,* $A_c^p = 0$ alors, l'erreur s'annule après p échantillons. On obtient une synchronisation en un temps fini appelé *dead-beat synchronization* [4], quelles que soient les conditions initiales.

3 Modulation numérique chaotique par multiplication et rétroaction (MCMR)

Nous introduisons dans cette partie un nouveau système de communication basé sur les principes énoncés en section 2. La séquence chaotique utilisée pour la synchronisation est modulée par un signal binaire, ce qui implique quelques modifications de l'émetteur et du récepteur afin de permettre la synchronisation. Classiquement, la sortie chaotique de l'émetteur est modulée par le message à émettre puis le signal résultant est émis dans le canal. Simultanément, la séquence chaotique est réintroduite dans l'émetteur. Ce principe constitue une nouvelle méthode pour synchroniser l'émetteur et le récepteur sans requérir les hypothèses classiques propres aux systèmes de transmission chaotiques par modulation telles que :

- l'obligation que le message binaire transmis soit codé en $(-1, +1)$.
- que A soit stable et que la non-linéarité f soit paire.

Les auteurs ont publié une comparaison détaillée de ces méthodes en [5].

Ce nouveau système de communication que nous appelons MCMR est alors décrit par les équations suivantes où $m(k)$ représente l'information à transmettre.
Emetteur (Fig. 1) :

$$\begin{cases} x(k+1) &= Ax(k) + f(s(k)) + L\big(s(k) - y(k)\big) \\ y(k) &= Cx(k) \\ s(k) &= y(k).m(k) \end{cases} \tag{5}$$

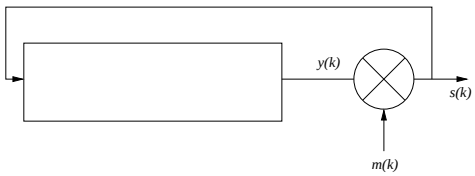

FIG. 1: Principe de l'émetteur chaotique

Récepteur (Fig. 2) :

$$\begin{cases} \hat{x}(k+1) &= A\hat{x}(k) + f\big(s(k)\big) + L\big(s(k) - \hat{y}(k)\big) \\ \hat{y}(k) &= C\hat{x}(k) \end{cases} \tag{6}$$

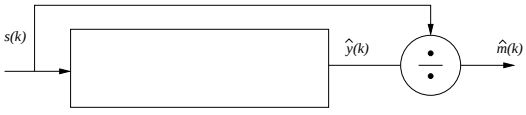

FIG. 2: Principe du récepteur chaotique

La synchronisation du système est assurée si :

$$\begin{aligned} e(k+1) &= Ae(k) + L\big(s(k) - y(k)\big) \\ &\quad -L\big(s(k) - \hat{y}(k)\big) \\ &= A_c e(k) \end{aligned}$$

Si la paire (A, C) est observable alors, L peut être choisi tel que A_c soit nilpotent, afin d'obtenir la *dead beat synchronization*.

La reconstruction est ensuite réalisée en inversant le système, soit :

$$\hat{m}(k) = \frac{s(k)}{\hat{y}(k)} = \frac{Cx(k)}{C\hat{x}(k)}.m(k) \tag{7}$$

4 Modification de la récurrence de Hénon

Un inconvénient de la procédure MCMR énoncée ci-dessus concerne l'étude des effets de la rétroaction sur le comportement chaotique du modulateur. Nous avons mené cette analyse pour la récurrence de Hénon [6] :

$$x_1(k+1) = 1 - 1.4x_1(k)^2 + x_2(k) \tag{8a}$$
$$x_2(k+1) = 0.3x_1(k) \tag{8b}$$

en choisissant $y(k) = x_1(k)$, la récurrence de Hénon peut s'écrire sous la forme (1) avec

$$A = \begin{bmatrix} 0 & 1 \\ 0.3 & 0 \end{bmatrix} \quad \text{et} \quad f(x) = \begin{pmatrix} 1 - 1.4x^2 \\ 0 \end{pmatrix}$$

En prenant $L = (0, 0.05)^T$, A_c est stable, et de 5 on déduit :

$$x_1(k+1) = 1 - 1.4s(k)^2 + x_2(k) \tag{9a}$$
$$x_2(k+1) = 0.3x_1(k) + 0.05x_1(k)(m(k) - 1) \tag{9b}$$
$$s(k) = x_1(k).m(k) \tag{9c}$$

Compte tenu de la parité de f, (9) peut être écrit sous la forme :

$$x(k+1) = \begin{cases} A_{(-1)}x + f(x) & \text{if } m(k) = -1 \\ A_{(+1)}x + f(x) & \text{if } m(k) = +1 \end{cases} \tag{10}$$

où

$$A_{(-1)} = \begin{bmatrix} 0 & 1 \\ 0.2 & 0 \end{bmatrix} \qquad A_{(+1)} = \begin{bmatrix} 0 & 1 \\ 0.3 & 0 \end{bmatrix}$$

L'équation (10) génère deux oscillateurs de Hénon possédant chacun un attracteur différent. Ainsi, si l'on se place hors de l'intersection des deux bassins d'attraction correspondant, alors le système peut diverger et par conséquent ne plus présenter un comportement chaotique. Pour éviter cet inconvénient, notre idée est d'étendre les bassins d'attraction à l'espace $\mathbb{R}^2$.

En écrivant $f(x(k)) = Bu(k)$ avec $B = (1, 0)^T$ et $u(k) = f_1(x_1(k)) = 1 - 1.4x_1(k)^2$, la récurrence de Hénon aura une forme générale linéaire

$$x(k+1) = Ax(k) + Bu(k)$$

Soit $H(k)$ la réponse impulsionnelle de ce système, et $x_1(k)$ la sortie, on en déduit alors que

$$x_1(k) = \sum_{j=0}^{k} u(k-j)H(j) \ .$$

Du fait que A est stable, $H(k)$ est une fonction décroissante c.à.d. il existe deux constantes positives $M > 0$ et $1 > \sigma > 0$ telles que

$$|H(k)| < M|\sigma|^k.$$

D'une part, si $x_1(k) \in [-1.2746, 1.2746]$ alors $u(k) \in [-1.2746, 1.2746]$ et :

$$x_1(k) < 1.275 \sum_{j=0}^{k} |H(j)| < 1.275 \frac{M}{1 - |\sigma|} \tag{11}$$

D'autre part, si $x_1(k) \notin [-1.2746, 1.2746]$ alors $|u(k)| > |x_1(k)|$, et on peut s'attendre à ce que $x_1(k)$ diverge car chaque itération est excitée par une entrée $u(k)$ plus ample que la précédente.

Pour éviter la divergence, il suffit de rendre $u(k)$ borné pour toutes valeurs de $x_1(k)$. Pour cela on va remplacer $f_1(x_1(k))$ par

$$\hat{f}_1(x_1(k)) = 1 - 1.4\Big(x_1(k) - \text{floor}\Big(\frac{x_1(k)+P}{2P}\Big)2P\Big)^2$$

où P est une constante et $\text{floor}(a)$ est la fonction d'arrondi à l'entier inférieur. Les fonctions $f_1(x_1(k))$ et $\hat{f}_1(x_1(k))$ sont présentées dans la figure 3. Il est clair que pour $x_1(k) \in [-P, P]$, on a $\hat{f}_1(x_1(k)) = f_1(x_1(k))$. $\hat{f}_1(x_1(k))$ repliant $\mathbb{R}$ sur l'intervalle $[-P, P]$, la divergence est évitée. Le choix $P = 1.2746$ assure la condition (11) pour tout $x_1(k)$.

finalement, cette récurrence de Hénon modifiée demeure localement instable mais devient globalement bornée donc chaotique.

5 Résultats et simulations

Nous présentons dans un premier temps les résultats obtenus en simulation pour la transmission d'un message binaire en absence de bruit. La figure 4 illustre bien le fait que la reconstruction du message est possible après un temps de synchronisation de 2 échantillons. Le signal émis dans le canal $s(k)$ bien que déterministe à toutefois une "allure" aléatoire assurant ainsi la sécurisation de la transmission. Les performances d'un tel système sur un canal BABG (bruit additif blanc Gaussien) sont présentées sur la figure 5 et comparées à celles théoriques d'une transmission BPSK. Nous constatons bien évidemment que la sécurisation de la transmission conduit à une nette chute des performances du système.

Un autre exemple de transmission sécurisée par MCMR est illustré sur la figure 6. L'image originale a été transformée en séquence binaire puis émise dans un canal de transmission idéal (non bruité). L'image reconstruite sans le démodulateur MCMR est illustrée en haut à droite. L'image reconstruite dans le cas de ce canal idéal est présentée en bas à gauche. Le cas d'une transmission dans un canal BABG à 30 dB est présentée en bas à droite. Cet exemple illustre bien le fait que le décodage de l'image sans connaissance du système chaotique initial (hard decision) est impossible, ce qui permet la sécurisation de la transmission.

6 Conclusion

Dans cette communication, nous avons souhaité présenter un nouveau schéma de modulation chaotique pour la transmission de messages numériques. Nous avons mis à profit les propriétés de synchronisation des systèmes chaotiques discrets afin de construire un modulateur qui, grâce à sa boucle de rétroaction permet d'intégrer une classe élargie de systèmes chaotiques en comparaison des modulateurs chaotiques classiques par multiplication. Le récepteur est élaboré à l'aide d'un démodulateur basé sur un observateur opérant par synchronisation avec le système d'émission. Par ailleurs, nous avons montré que les risques de divergence liés à la boucle de retours pouvaient être maîtrisés en bornant la non-linéarité sans pour autant compromettre le caractère chaotique de la récurrence.

Bien que le travail présenté se limite à l'accès simple, l'extension au cas multi-utilisateurs n'introduit pas de difficulté majeure et laisse entrevoir de nouvelles perspectives induites par les caractéristiques statistiques des séquences issues des systèmes chaotiques discrets. Enfin, nous travaillons actuellement à l'amélioration des performances en termes de probabilité d'erreur de bit pour un rapport signal à bruit fixé.

References

[1] K. M. Cuomo, A. V. Oppenheim, S. H. Strogatz, Synchronization of lorenzed-based chaotic circuits with applications to communications, IEEE Transactions on Circuits and Systems-II 40 (10) (1993) 626–633.

[2] H. Dedieu, M. P. Kennedy, M. Hasler, Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuit, IEEE Transactions on Circuits and Systems-II 40 (10) (1993) 634–642.

[3] M. Itoh, H. Murakami, New communication systems via chaotic synchronizations and modulation, IEICE Trans. Fundamentals E78-A (3) (1995) 285–290.

[4] A. Angeli, R. Gebesio, A. Tesi, Dead-beat chaos synchronization in discrete-time systems, IEEE Transactions on Circuits and Systems-I 42 (1) (1995) 54–56.

[5] M. Feki, B. Robert, G. Gelle, M. Colas, Secure digital communication using discrete-time chaos synchronization, Chaos, Solitons & Fractals 18 (4) (2003) 881–890.

[6] H. Peitgen, H. Jürgens, D. Saupe, Chaos and fractals: New frontiers of science, Springer-Verlag, New York, 1992.

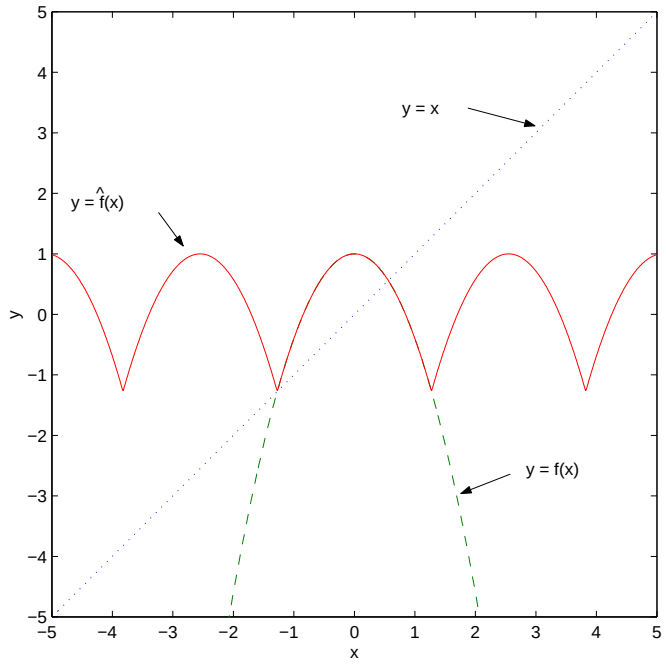

FIG. 3: Fonction proposée pour la modification de la recurrence de Hénon.

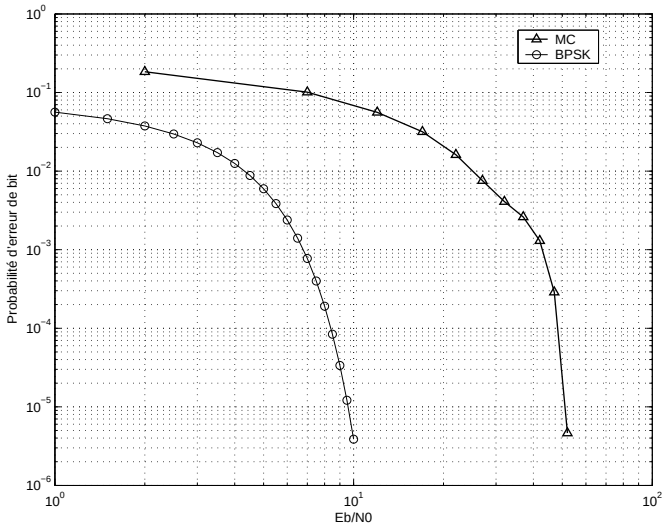

FIG. 5: Performance sur canal BABG en fonction de Eb/N0

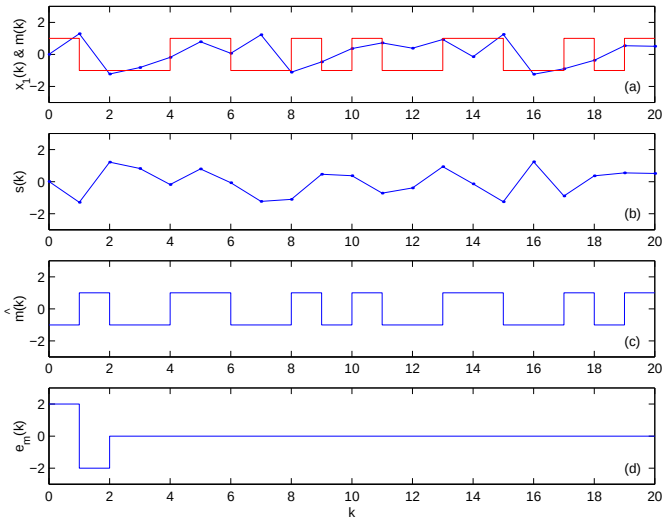

FIG. 4: Transmission d'un signal binaire en absence de bruit.

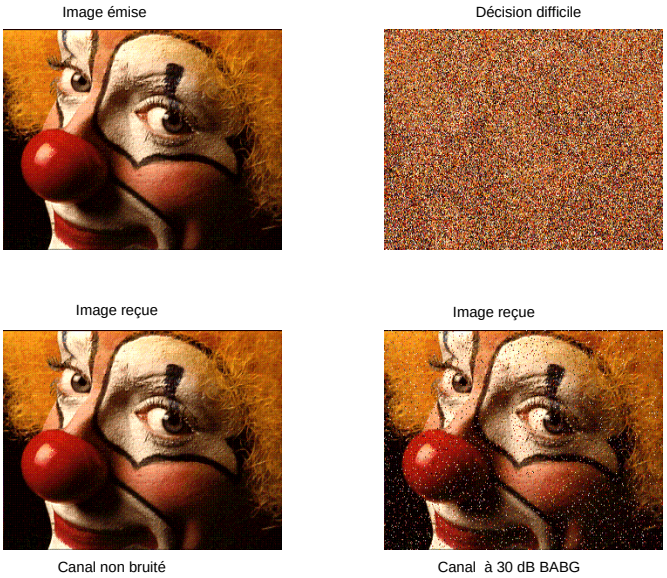

FIG. 6: Transmission d'image par MCMR en absence de bruit et sur canal BABG (AWGN).