2D-06

ファジィ推論に基づく状態推定を用いたカオス同期のセキュリティ向上

清水　能理†
八戸工業大学†

１まえがき

一般に，カオス系の内部状態は全て得られるわけではないが，制御においては正確な数学モデルでなくても，同じ入出力を実現できる等価システムが得られれば操作量を設計できる．一方，カオス同期系を用いたカオス通信が提案されている．送信側・受信側の二つのサブ系において，暗号鍵の生成を担う二つのカオス同期部間で送受信される同期化信号は，情報セキュリティ上から可能な限り次元数が小さい方が良い．低次元の同期化信号から元の高次元系を再構築できれば，通信系の秘匿性を向上できる．例えば，状態観測器を用いて受信側の状態を完全に再構築できるなら，送信側の同期化制御の操作量設計に必要な受信側の状態を全て知ることができる[1,2]．

２状態オブザーバを用いたカオス制御

対象とする非線形離散時間システムを式(1)(2)とする．

$$x(k+1) = f(x(k), u(k)) \quad (1)$$

$$y(k) = g(x(k)) \quad (2)$$

$$x_f = f(x_f, 0)$$

$$y_f = g(x_f)$$

系の不安定平衡点x_f近傍の線形化システムは，式(3)(4)となる．

$$\bar{x}(k) = x(k) - x_f$$

$$\bar{x}(k+1) = A\,\bar{x}(k) + B\,u(k) \quad (3)$$

$$\bar{y}(k) = \mathrm{y}(k) - y_f = C\,\bar{x}(k) \quad (4)$$

$$u(k) = K\bar{x}(k) = K(\,x(k) - x_f) \quad (5)$$

$$\bar{x}(k+1) = (A + BK)\,\bar{x}(k) \quad (6)$$

式(5)の$u(k)$は制御入力で，入力ゲインKは式(6)より$(A,\ B)$によって設計する．x_f近傍における線形オブザーバは式(7)(8)となる．

$$\hat{x}(k+1) = A\,\hat{x}(k) + B\,u(k) + H(\hat{y}(k) - \mathrm{y}(k) + y_f) \quad (7)$$

$$\hat{y}(k) = C\,\hat{x}(k) \quad (8)$$

Security Improvement of Chaos Synchronization Using the State Estimation Based on Fuzzy Inference
†Yoshimasa Shimizu
†Hachinohe Institute of Technology

$$e(k) = \bar{x}(k) - \hat{x}(k)$$

$$e(k+1) = A\left(\bar{x}(k) - \hat{x}(k)\right) + HC\left(\bar{x}(k) - \hat{x}(k)\right) = (A + HC)e(k) \quad (9)$$

式(9)より，オブザーバゲインHは$(A,\ C)$によって設計する．

３オブザーバを用いたカオス同期化制御

カオス同期を用いた通信系では，送信側・受信側の二つのサブ系において，暗号鍵生成を担うカオス同期部が式(10)(11)となる．

$$x1(k+1) = f(x1(k), u(k)) \quad (10)$$

$$x2(k+1) = f(x2(k)) \quad (11)$$

$$y2(k) = g(x2(k)) \quad (12)$$

$$x_f = f(x_f, 0)$$

$$y_f = g(x_f)$$

x_f近傍における線形化系は式(13)(14)となる．

$$\bar{x}2(k) = x2(k) - x_f$$

$$\bar{x}2(k+1) = A\,\bar{x}2(k) \quad (13)$$

$$\bar{y}2(k) = \mathrm{y}2(k) - y_f = C\,\bar{x}2(k) \quad (14)$$

式(13)(14)より式(11)の線形状態オブザーバを設計する．x_f近傍におけるオブザーバゲイン指定による同一次元オブザーバは式(15)となる．

$$\hat{x}2(k+1) = A\,\hat{x}(k) + H(\hat{y}2(k) - \mathrm{y}2(k) + y_f) \quad (15)$$

$$\hat{y}2(k) = C\hat{x}2(k)$$

$$e2(k) = \bar{x}2(k) - \hat{x}2(k)$$

$$e2(k+1) = (A + HC)e2(k) \quad (16)$$

式(16)より，オブザーバゲインHは，$(A,\ C)$によって設計できる．よって，x_f近傍における非線形オブザーバは，式(17)となる．

$$\hat{x}2(k+1) = f\left(\hat{x}2(k)\right) + H(\hat{y}2(k) - \mathrm{y}2(k)) \quad (17)$$

$$\hat{y}2(k) = g\left(\hat{x}2(k)\right)$$

式(17)に基づき式(11)の状態を推定する．非線形状態フィードバックを用いた式(10)の同期化制御則$u(k)$は式(18)となる．x_f近傍にあるときのみ状態推定を行う．

$$u(k) = K(\,x1(k) - \hat{x}2(k)) \quad (18)$$

$$\hat{x}2(k+1) = \begin{cases} f\left(\hat{x}2(k)\right) + H\left(g\left(\hat{x}2(k)\right) - \mathrm{y}2(k)\right), \\ \qquad ||x1(k) - x_f|| < \varepsilon \; and \; ||\mathrm{y}2(k) - y_f|| < \varepsilon \\ x1(k+1), \qquad\qquad Otherwise \end{cases}$$

1次元信号から3次元信号を推定するオブザーバを用いた同期系を考える．システム2の同期信号をシステム1のオブザーバへ入れると，システム2の状態を再構成できる（図1）．

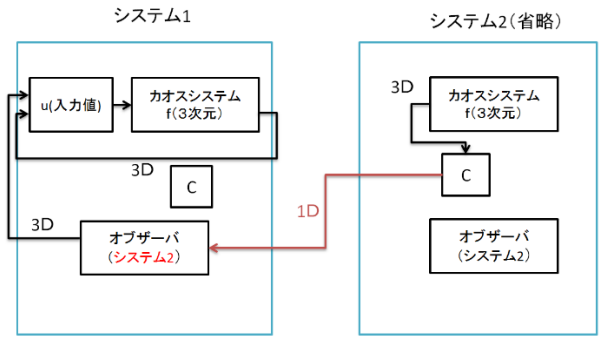

Fig.1 Chaos synchronization system design using state observer.

4 ファジィモデルに基づく同期化制御

モデルが得られないシステムをファジィモデルとして構築する．式(19)は，高木・菅野タイプとなる．

$$x(k+1) = A\big(x(k)\big)x(k) + B\big(x(k)\big)u(k) + a\big(x(k)\big) \quad (19)$$
$$y(k) = C(x(k))\, x(k)$$

時系列から不安定周期領域を算出する．その各重心の不安定周期点c_f近傍における式(19)のファジィモデルは式(20)となる．

$$c_f \sim x_f = f\big(x_f\big)$$
$$x(k+1) = A\big(c_f\big)x(k) + B\big(c_f\big)u(k) + a\big(c_f\big) \quad (20)$$
$$y(k) = C(c_f)\, x(k)$$

式(19)から同一次元非線形オブザーバは式(21)となる．

$$\hat{x}2(k+1) = A\left(\hat{x}2(k)\right)\hat{x}2(k) + B\left(\hat{x}2(k)\right)u(k) + a\left(\hat{x}2(k)\right) + h(k)\left(C\left(\hat{x}2(k)\right)\hat{x}2(k) - \mathrm{y}2(k)\right) \quad (21)$$
$$\hat{y}2(k) = C\left(\hat{x}2(k)\right)\hat{x}2(k)$$

式(21)のオブザーバゲイン$h(k)$は，時変パラメータとなる．平衡点c_f近傍における非線形オブザーバは式(22)となる．

$$d_f = C(c_f)c_f \sim y_f = g\big(x_f\big)$$

$$\hat{x}2(k+1) = \begin{cases} A(c_f)\,\hat{x}2(k) + B(c_f)u(k) + a(c_f) + H(c_f)\left(C(c_f)\hat{x}2(k) - \mathrm{y}2(k)\right), \\ \qquad ||x1(k) - c_f|| < \varepsilon \; and \; ||\mathrm{y}2(k) - d_f|| < \varepsilon \\ x1(k+1), \qquad\qquad Otherwise \end{cases} \quad (22)$$

$$u(k) = K(c_f)\left(x1(k+1) - \hat{x}2(k+1)\right)$$
$$= (k1(c_f), \ldots, kn(c_f))\left(f(x1(k)) - f\left(\hat{x}2(k)\right)\right) \quad (23)$$

5 シミュレーション

エノン写像を未知システムと仮定して用いてMATLAB/Simulinkによって設計した式(20)のファジィモデルを用いた．式(21)の非線形状態オブザーバを構築し，式(11)のカオス系と式(21)の非線形オブザーバは，初期値の違いで異なった振舞をしている．式(21)のオブザーバの推定状態を式(11)のカオス状態に追従させる。式(11)の状態と式(21)の推定値からなる誤差システムの値は，漸近的に収束している（図2）．

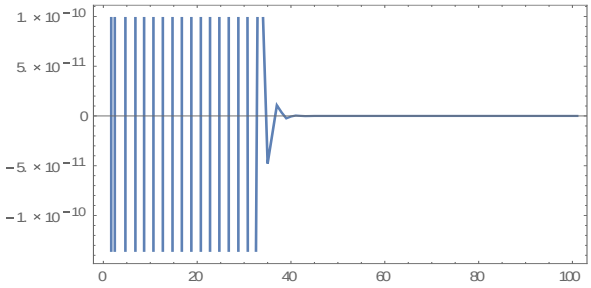

Fig.2 The behavior of the error system.

6 まとめ

状態オブザーバに基づくカオス制御系を設計し，状態オブザーバに基づくカオス同期化制御系に応用した．ファジィモデルに基づく状態オブザーバを設計し，カオス同期部の状態推定を行った．さらにファジィモデルに基づく制御則を設計し，非線形状態フィードバックによる同期化制御を行った．

参考文献

1) Y. Shimizu, M. Miyazaki, H.-H. Lee, and F. Qian, A Method of the Secrecy Communication Using Fuzzy and Chaos, Special Issue of Int. J. of Innovative Computing, Information and Control on Recent Advances in Stochastic Systems Theory and Its Applications, Vol.5, No.1, pp.97-108 (2009)

2) T. Ushio: Control and Its Application to Chaos Synchronization Secure Communication, J. of Information Processing Society of Japan, Vol.36, No.3, pp. 525-530 (1995)