計測自動制御学会東北支部第 302 回研究集会(2016. 6. 24)
資料番号 302-1

状態オブザーバを用いたカオス通信系の構築

Construction of Chaos Communication System Using the State Observer

○佐々木 健太郎, 佐藤 宏樹, 清水 能理
Kentaro Sasaki,Hiroki Satou,Yoshimasa Shimizu

八戸工業大学
Hachinohe Institute of Technology

キーワード: カオスシステム(Chaotic system), 可観測性(Observability), 状態オブザーバ(State observer), 状態推定(State estimation) , 同期系(Synchronization System)

連絡先: 〒031-8501 八戸市大字妙字大開 88-1 八戸工業大学工学部システム情報工学科
清水能理 Tel.: (0178)25- 8135, Fax.: (0178)25-1691, E-mail: shimizu@hi-tech.ac.jp

１．まえがき

現在、秘匿通信システムの中にはカオス同期を用いたカオス通信システムがある。この秘匿通信システムの情報信号はセキュリティ上から可能な限り次元数が小さいほうがよいのだが、実際は全ての内部状態を短時間ではあるが送信している。カオス通信システムの情報信号を出来る限り小さくしたい。その為にはカオス通信システム内に埋め込まれているカオス同期系の同期部の同期化信号の次元数を最小にする必要が有る。よって、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と考える[1, 2].

２．問題の記述

同一次元のカオス同期(図１)では、高次元の同期化信号をそのまま送信してしまうのでセキュリティ的に問題である。よって、低次元の同期化信号でやり取り可能なカオス同期系を、オブザーバを用いて構築する.

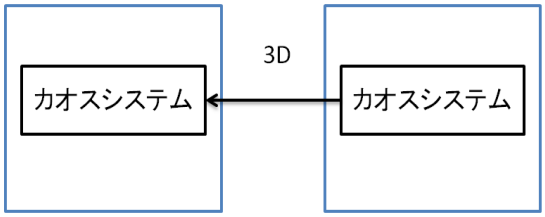

図 1　同一次元のカオス同期系

３．カオス

建築構造物や機械など、外力が周期的でも必ずしも規則正しい振動を示すとは限らず、不規則で複雑な振動を示す場合がある。人工系・自然系を問わず普遍的に存在する初期値に鋭敏な複雑で予測不能な挙動をカオスという.

４．オブザーバを用いたカオス制御

カオス制御とはアトラクタに含まれる不安定な周期軌道を安定化させることを言う.

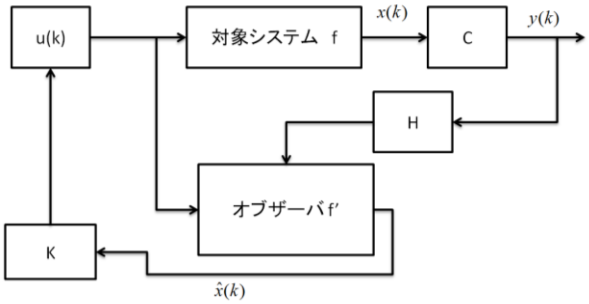

図 2　オブザーバを用いたカオス制御

推定誤差を e(k) とすると なので

$$\begin{aligned} e(k+1) &= [Ax(k)+Bu(k)]-[A\hat{x}(k)+Bu(k)+H(\hat{y}(k)-y(k))] \\ &= A(x(k)-\hat{x}(k))-H(C\hat{x}(k)-Cx(k)) \\ &= (A+HC)\,e(k) \end{aligned}$$

A と C は元々決まっているので、H の固有値を決定することにより誤差 e を 0 に収束することが出来る。以上より、図 4 のように系の状態推定を行うオブザーバを用いる場合、非線形システムに対して、出力に基づくカオス制御は式（1）のようになる.

$$\hat{x}(k+1)=\begin{cases} A\hat{x}(k)+Bu(k)+H(C\hat{x}(k)+y_f-y(k)) & \|y(k)-y_f\|<\varepsilon \text{ のとき} \\ 0 & \text{それ以外} \end{cases}$$

$$u(k)=K\hat{x}(k) \qquad (1)$$

5．提案手法

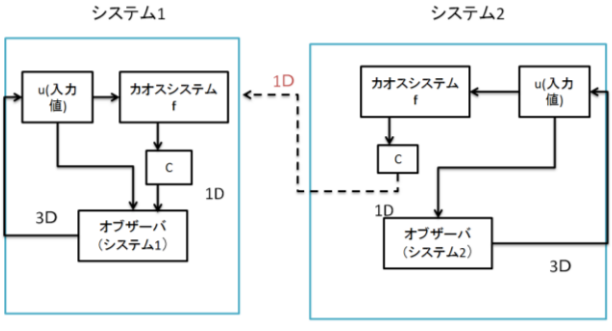

図 3　カオス同期系

１Ｄ（１次元）信号から３Ｄ（３次元）信号を推定できるオブザーバを用いたカオス制御系を考える．さらに、この制御系を２つ繋いで同期系を構築する．いまシステム 2 の同期信号をシステム 1 のオブザーバへ入れるように設計すると、システム 2 の１Ｄ同期化信号によってシステム 2 の３Ｄ状態を再構成可能なカオス同期系を構築できる.

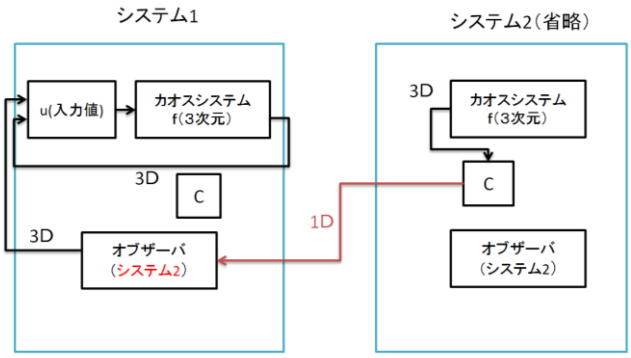

図 4 状態オブザーバを用いたカオス同期系の設計

6．オブザーバを用いたカオス同期系の状態推定

入力 $= u(k)$
システム1 $= x_1(k)$　システム 2 $= x_2(k)$
システム1のオブザーバ $= hx_1(k)$
システム2のオブザーバ $= hx_2(k)$
出力 $= y(k)$

とする. 以下の式を用いて数値実験した結果は、図 5、図 6 のようになった.

$$x_1(k+1)=1.4-x_1(k)^2+0.3x_2(k)+u(k)$$
$$x_2(k+1)=x_1(k)$$
$$hx_1(k+1)=1.4-hx_1(k)^2+0.3hx_2(k)+u(k)+2a(hx_1(k)-y_2(k))$$
$$hx_2(k+1)=hx_1(k)-(hx_1(k)-y_2(k))$$
$$\begin{bmatrix} hx_1(k+1)=x_1(k+1) \\ hx_2(k+1)=x_2(k+1) \end{bmatrix}$$
$$u(k)=x_1(k)^2-0.5x_2(k)-hx_1(k)^2+0.5hx_2(k)$$
$$y_2(k+1)=x_2(k+1)$$

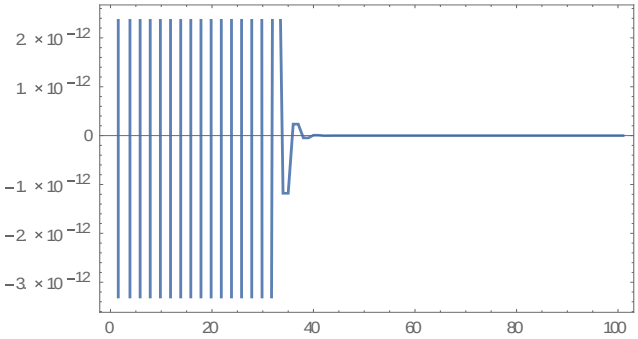

図 5 システム2の同期部の状態とシステム1のオブザーバの状態の差（システム１のオブザーバがシステム 2 の状態推定をしているか確認）

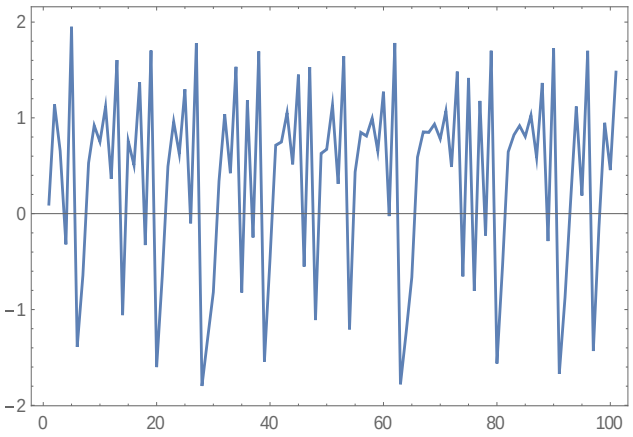

図 6 システム1の同期部の状態

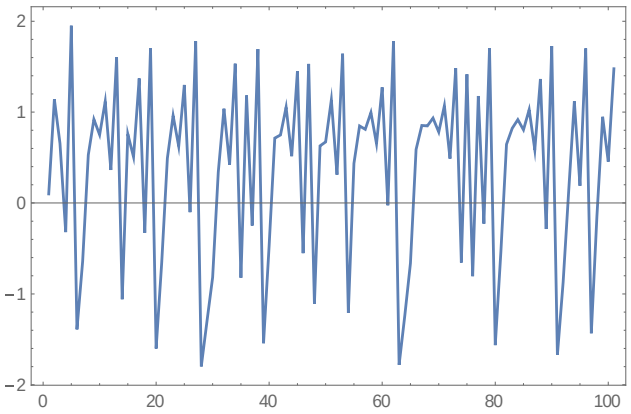

図 7 システム2の同期部の状態

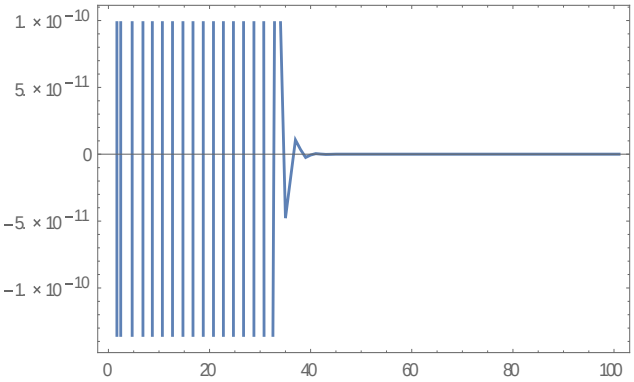

図8 システム１の状態とシステム２の状態の差（システム１，２が同期とれているかの確認）

40 超えた辺りから誤差が 0 に収束していることが分かる。これによりシステム 1 の同期化部とシステム 2 の同期部の同期がとれていることが確認できる.

7．カオス通信系への構築

実験によりカオス制御系を 2 つ並べてカオス同期系を構築できることが確認されたので、これを秘匿通信システム(図 9)の同期化部に応用することが出来る. ここでは参考文献[1]の秘匿通信システムにオブザーバを用いたカオス同期化制御を組み込み、実験を行っていく.

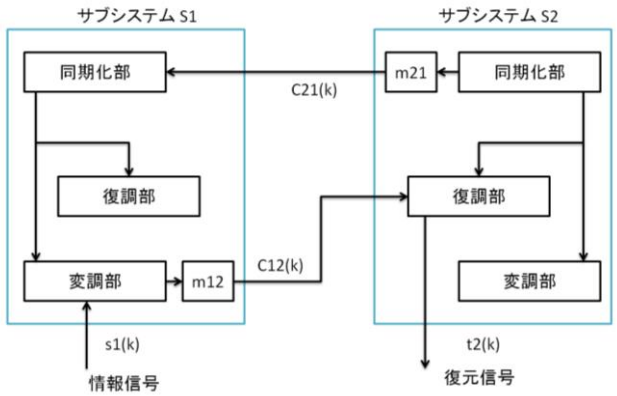

図 9　秘匿通信システム

同期化部 $x_i(k+1) = f(x_i(k)) + bu_i(k)$

変調部 $w_i(k+1) = p(x_i(k), w_i(k), s_i(k+1))$

復調部 $t_i(k+1) = p^{-1}(x_i(k-1), v_i(k-1), v_i(k))$

ここでは、以下のような通信システムを考える.

同期化部

$$x_{1,i}(k+1) = 1.4 - x_{1,i}^2(k) + 0.3x_{2,i}(k) + u_i(k)$$
$$x_{2,i}(k+1) = x_{1,i}(k)$$

変調部

$$w_i(k+1) = \left|2.7x_{2,i}(k)w_i(k)(1-w_i(k))\right| + \left(\left|4w_i(k)(1-w_i(k))\right| + 0.1\right)\left(0.03\left|x_{2,i}(k)\right| +\right.$$

復調部

$$t_i(k+1) = \frac{u_i(k) - \left|2.7x_{2,i}(k-1)v_i(k-1)(1-v_i)k-1)\right|}{\left|4v_i(k-1)(1-v_i(k-1))\right| + 0.1}$$

オブザーバ

$$hx_{12}(k+1) = 1.4 - hx_{12}^2(k) + 0.3hx_{22}(k) + 2a(hx_{12}(k) -$$
$$hx_{22}(k+1) = hx_{12}(k) - (hx_{12}(k) - y_2(k))$$

※ hx_{12} : サブシステム$S1$のオブザーバ
hx_{22} : サブシステム$S2$のオブザーバ

情報信号 s1(k)を S1 から S2 へ伝送することを考える。入力および送信信号を以下のようにセットする.

$$c_{12}(k) = w_1(k)$$
$$c_{12}(k) = x_{1,2}^2(k) - 0.5x_{2,2}(k)$$
$$u_1(k) = x_{1,1}^2(k) - 0.5x_{2,1}(k) - c_{21}(k)$$
$$w_2(k) = 0$$

実験結果は以下のとおりである.

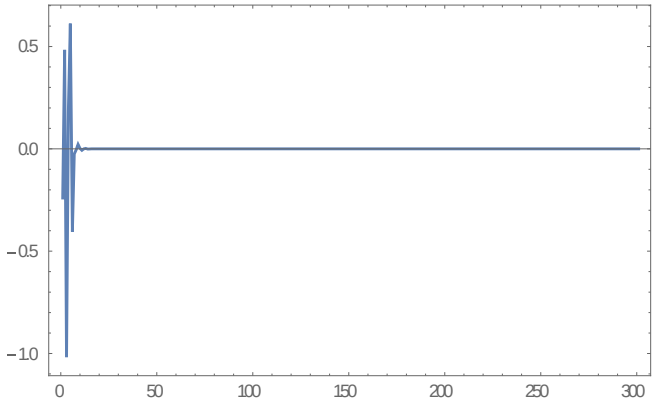

図 10　入力値の状態（ほぼ 0 に近い）

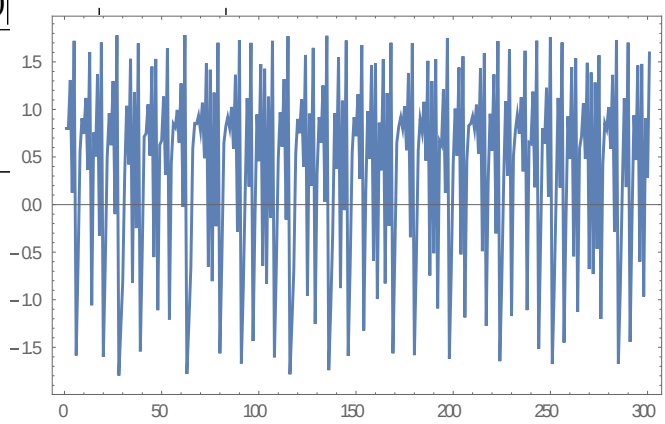

図 11　サブシステム S1 のオブザーバの状態

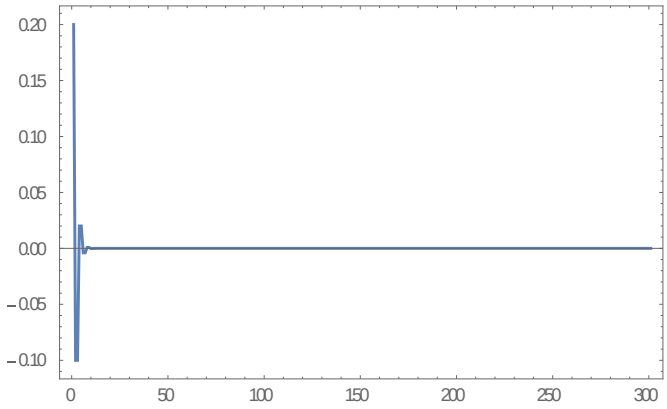

図 12　サブシステム S2 同期化部とサブシステム S1 オブザーバの差

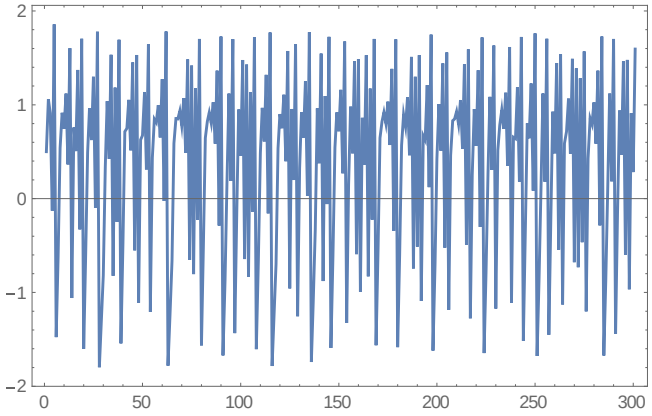

図 13　サブシステム S1 の同期化部の状態

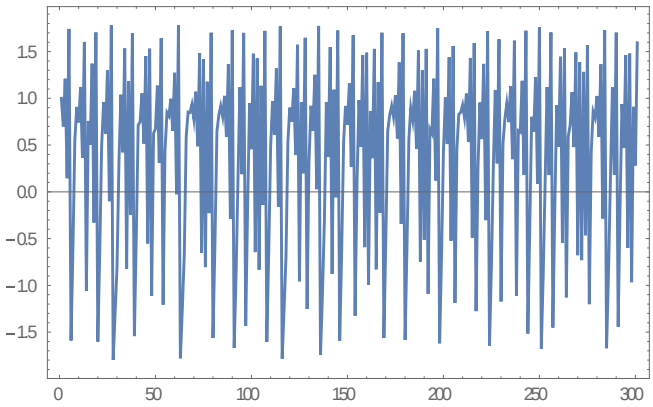

図 14　サブシステム S2 の同期化部の状態

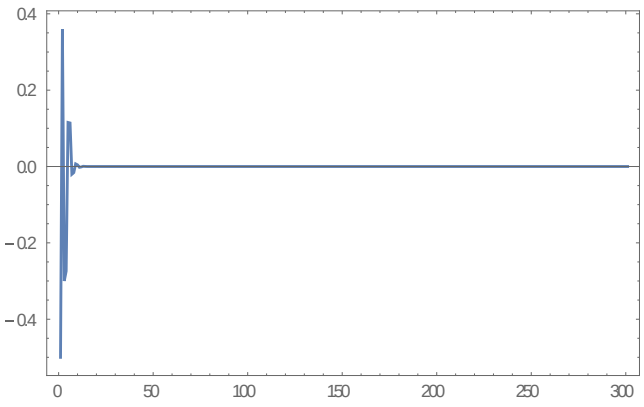

図 15 サブシステム S1, S2 のそれぞれの同期化部の差

これによりサブシステム S1 とサブシステム S2 の同期化部は同期していることが確認できる.

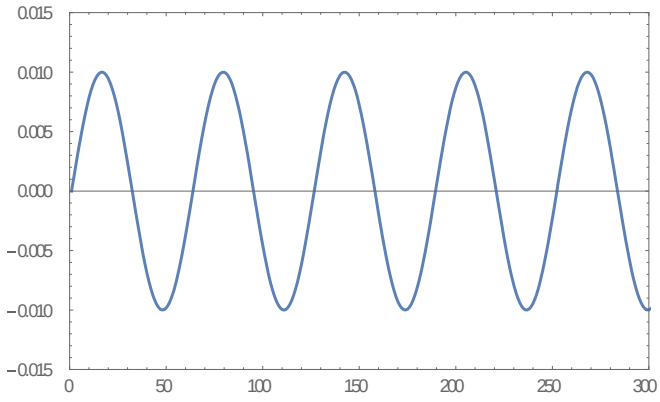

図 16 情報信号 s1(Sin(0.1k))の状態

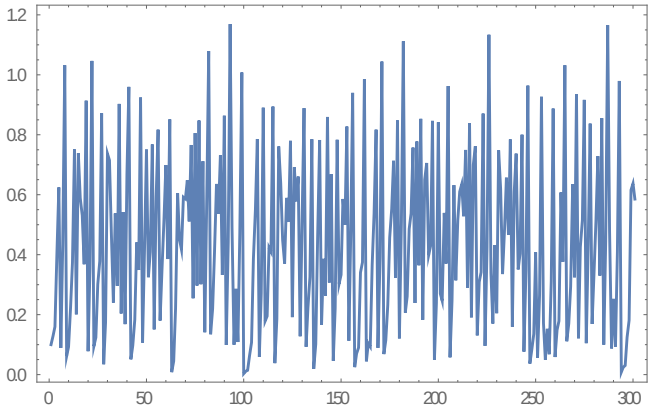

図 17　サブシステム S1 の変調部の状態

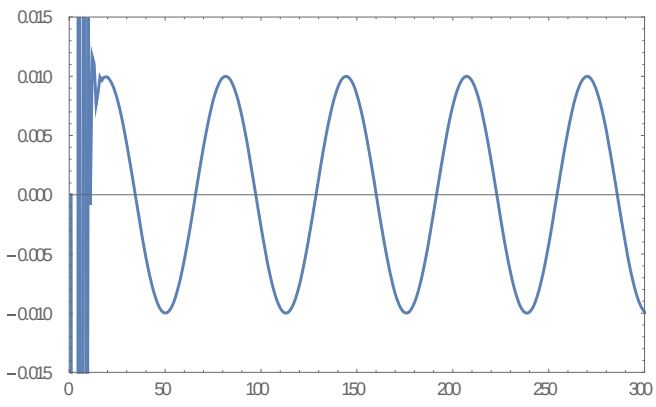

図 18　サブシステム S2 の復調部の状態

これらの実験によりオブザーバを用いたカオス同期系は今までの秘匿通信システムに応用することが可能であることが分かった.

８．おわりに

本研究では、先ず状態オブザーバを用いたカオス制御系を２つ並べたカオス同期系を設計し、次に同期化制御入力の設計を行い、オブザーバを用いたカオス同期系を構築した．数値実験により、状態推定およびカオス同期を確認できたので、この提案手法を秘匿通信システムへ応用した．参考文献[1]の秘匿通信システムを用いて数値実験を行った．まず文献の秘匿通信システムを構築し、正確に動作するか確認した．その後、提案手法を組み込み、応用実験を行った．実験結果から、従来の秘匿通信システムと変わらず、同様に暗号化および復号することを確認できた.

参考文献

[1] 潮　俊光 : カオス制御,朝倉書店,1996

[2] 鈴木　昱雄 : カオス工学への応用,科学技術出版,1998

[3] 鈴木　昱雄 : カオス入門,コロナ社,2000

[4] 梅田　玲奈・清水　能理 : 状態オブザーバを用いたカオス同期系の構築, 平成 27 年度第 2 回情報処理学会東北支部研究会,講義資料 Vol.2015-2 No.2-1, 2015.12

[5] 目黒　友紀・清水　能理 : カオス制御を応用したカオス同期化システム,平成 20 年度第 2 回情報処理学会東北支部研究会,講義資料,セッション 2,講演番号 9,2008.12