

インテリジェントシステムに基づく秘匿通信系のパラメータ評価 Parameters Assessment of Secure Communication System Based on Intelligent Systems

清水 能理

Yoshimasa Shimizu

1. はじめに

現在ネットワーク上の電子情報を保護する公開鍵暗号方式は、素因数分解や離散対数問題などを応用しているが、コンピュータ処理速度の上昇により暗号鍵長の増加が必要とされ、負担が一層増加される。暗号化関数の利便性、暗号鍵の秘匿性、モデルの秘匿性を解決するためカオス同期に基づいた秘匿通信系を構築できるが、カオス分岐を行った変調部の状態はカオス性を保持していなければならない。人工的に作り出されるカオスは限定的なものであり、分岐パラメータのとり値によっては周期性を示す窓を生じる場合がある。

2. 提案手法

非線形モデルでカオス発振システムの構築には困難が生じる。ニューラルネットワークとファジィを組み合わせることで、ファジィ理論に基づいた知識表現でモデル構成ができ、パラメータをニューラルネットワークのように学習できる。オリジナルのカオス発生モデルとして、ファジィモデルを構築する。①少ないファジィルールで非線形回路を構築できる高木・菅野ファジィモデルを用いる。②メンバシップ関数をバックプロパゲーションで学習する。③構築したモデルの時系列を比較し、カオス性の有無を検証する。

3. シミュレーション 1

ニューロファジィ推論システムツールである

ANFIS を用いる。2次元に拡張したファジィモデルを構築する。構築したファジィモデルを繰り返し使い、カオスダイナミクスの出力を得る。ファジィモデル出力データにニューラルネットワークを適用してメンバシップ関数を学習する。図 1 にモデリング結果を示す。

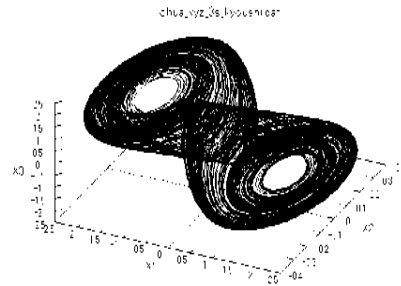


図 1：ファジィモデル・アトラクタ

アトラクタから定性的に評価できたが、定量的にカオス検定を行う必要がある。複数の共通定義を持ってカオス性を判断以外に方法が無いため、カオス判定は必要条件という性質を持つ。

4. サロゲートデータ法

カオス応答を示すための重要な要因は非線形性にある。観測された時系列信号に対する線形確率過程の存在を帰無仮説として提示し、ある非線形統計量の推定を通じて帰無仮説を検定し棄却することで、時系列信号を生み出したダイナミクスにおける非線形性の存在を示す。線形統計量としてはリアプノフ指数を用いる。サロゲートデータ Q_n の特徴量が正規分布すると仮定できる場合、

(1)式で定義する検定統計量 S を用いて評価する。 Q_H が正規分布するとき、 $S > 1.96$ であれば有意水準 $\alpha = 0.05$ で与えられた帰無仮説を棄却すること、カオス性を判定する。

$$S = \frac{|Q_0 - \mu Q_H|}{\sigma Q_H} \quad (1)$$

Q_0 : オリジナルデータの非線形統計量
 μQ_H : サロゲートデータの非線形統計量
 σQ_H : サロゲートデータの非線形統計量標本標準偏差

5. シミュレーション2

サンプリングしたデータは必ずしもカオス性を有していない。実験データの短さに問題があるが、データを長くすると負荷が大きくなり処理が難しくなる。ポアンカレ写像を用いて改善する。

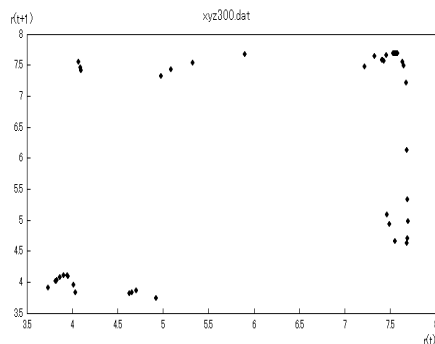


図2：ポアンカレ写像

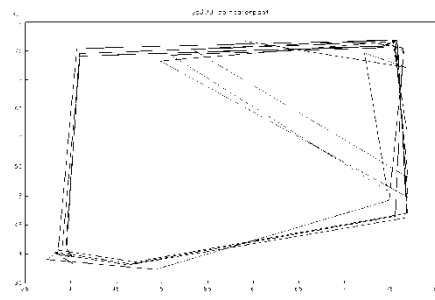


図3：ポアンカレ写像のアトラクタ

各サロゲートデータ法における検定統計量 S と検定結果を表1に示す。

表1：検定統計量 S とカオス性の有無

RS	FS	FT	AAFT	IAAFT
0.6210	3.6884	0.2123	0.3350	5.8020
×	○	×	×	○

○：カオス性を示唆 ×：カオス性の否定

6. GAを用いたカオス分岐パラメータ探索

カオス発生パラメータを決める際、分岐図を用いて範囲を推定できるが、窓が存在する。よって、最適解を求め易い遺伝的アルゴリズムを用いてパラメータ決定問題のコーディングを行うことを検討する。評価関数は、カオス写像の各分岐における時系列のリアプノフ指数を用いる。

7. ウェーブレット変換を用いたカオス特徴量の抽出とその応用

カオスは広帯域であるので、白色雑音など広帯域の雑音が混入した時、分離することが難しい。一方、カオス通信システムにおいて通信路における雑音の混入問題がある。ウェーブレット変換を広帯域であるカオス時系列と白色雑音の分離に応用することも考える。

8. まとめ

高木・菅野ファジィモデルを用いることによって、少ないファジィルールのメンバーシップ関数でモデルを構築することができた。サロゲート法を用いてカオス性の判定を行った。サンプリングの問題を解決するため、ポアンカレの手法を応用した改良を考案した。最適なポアンカレ切断面の設定手法について研究を進める。

参考文献

- [1] 潮 俊光：カオス通信への応用，電子情報通信学会論文誌 A, Vol.J82-A, pp.1801-1807, 1999
- [2] 合原 一幸，池口 徹，山田 泰司，小室 元政：カオス時系列解析の基礎と応用，産業図書，2000