УДК 681.76

Д.А. Деменков

СИНЕРГЕТИЧЕСКИЙ МЕТОД ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННЫЙ НА ИСПОЛЬЗОВАНИИ СТРАННОГО АТТРАКТОРА РЕССЛЕРА

В данной работе рассматривается метод защиты информации, основанный на применении в качестве несущего сигнала колебаний генератора хаоса типа Рёсслера и последующей глобальной реконструкции динамической системы для восстановления переданной информации.

Аттрактор, наблюдатель, параметр, реконструкция, Рёсслер, синергетика.

D.A. Demenkov

SYNERGETICS METHOD OF TREATMENT AND DEFENCE INFORMATION, BASIS ON THE SYSTEM OF TYPE RESSLER

In this article is examined method of information protection, based on the use fluctuations generator of chaos Ressler type as a carrier signal and global reconstruction dynamic system for recovery of transmitted information.

Attractor, observer, parameter, reconstruction, Ressler synergetics.

В настоящее время существует значительный интерес к новому способу защиты информации, основанному на применении в качестве несущего сигнала колебаний генератора хаоса. Генератор хаоса, в свою очередь, представляет собой одну из базовых систем нелинейной динамики – систем, характеризующихся так называемыми «странными» аттракторами. Аттрактор Рёсслера на некотором множестве в его фазовом пространстве имеет фрактальную (нецелую) размерность и, следовательно, на этом множестве могут возникнуть хаотические режимы движения с чрезвычайной чувствительностью к начальным условиям. Хаотичность этой модели вызывается только ее внутренним поведением и динамическими свойствами.

В статье предложен метод обработки и защиты информации, основанный на глобальной реконструкции динамической хаотической системы типа Рёсслера, с использованием синергетического наблюдателя.

В последнее время в литературе был предложен ряд способов скрытой передачи информации, основанных на применении в качестве несущего сигнала широкополосных колебаний генератора хаоса [2, 3]. Исходя из идеологии глобальной реконструкции [2-4], в данной статье предлагается динамический метод обработки информации, основанный на текущем вычислении параметров $\mu_i^*(t)$ с помощью синергетического наблюдателя [5,6].

Методику и синтез динамического наблюдателя проиллюстрируем на конкретном примере ХГ, представленного моделью Рёсслера [2, 4]:

$$\dot{x}(t) = -y - z; \qquad \dot{y}(t) = x + ay; \qquad \dot{z}(t) = bx + xz - cz, \tag{1}$$

здесь $x = (x, y, z)$ – вектор переменных состояния, $\mathrm{m}^0 = (a, b, c)$ – вектор постоянных (номинальных) параметров.

Сначала преобразуем модель (1), для чего используем замену переменных [3]:

$$X = x;\ Y = -y - z;\ Z = x + ay\,.$$

В результате получим новую систему

$$\dot{X}(t) = Y; \qquad \dot{Y}(t) = Z; \qquad \dot{Z}(t) = f\left(X, Y, Z, m^0\right), \tag{2}$$

где

$$f\left(X, Y, Z, m^0\right) = bX + X\left(\frac{X - Z}{a} - Y\right) - c\left(\frac{X - Z}{a} - Y\right). \tag{3}$$

Итак, рассмотрим новый управляющий параметр генератора Ресслера:

$$c^*(t) = c + \mu(t)\ . \tag{4}$$

Для этого будем полагать, что в канал связи передается сигнал $Z(t)$, сгенерированный системой (2–4). Примем следующие допущения: модулирующий сигнал $\mu(t)$ является кусочно-постоянным, т.е. осуществляется передача цифровой информации; параметры a, b – заданы, а параметр $c(t) > 0$ является модулируемым параметром.

Покажем процедуру построения наблюдателя за параметром c на принимающей стороне для системы (2). Для этого, согласно [5-7], неизвестный параметр необходимо заменить его динамической моделью, отражающей эволюцию этого параметра. В нашем случае это может быть модель вида $\dot{w}(t) = 0$, поскольку решением этого дифференциального уравнения является $w(t) = const$, что и отражает скачкообразное изменение во времени параметра $c(t)$. На этом основании сформируем следующую расширенную систему:

$$\dot{X}(t) = Y; \quad \dot{Y}(t) = Z; \quad \dot{Z}(t) = G_1 - c\left(\frac{X - Z}{a} - Y\right); \quad \dot{w}(t) = 0, \tag{5}$$

где $G_1 = bX + X\left(\frac{X - Z}{a} - Y\right)$, w – переменная состояния динамической модели параметра c.

Как видно, в системе (5), в отличие от (2), параметр c заменен переменной состояния модели w. В системе (5) наблюдаемыми (известными) являются переменные X, Y, Z, а ненаблюдаемой (неизвестной) переменной – w. Пусть $\hat{w}$ – искомая оценка параметра c, т.е. $\hat{w} = \hat{c}$. Для построения оценки этого параметра введем макропеременную

$$\psi = w - \hat{w} \tag{6}$$

и запишем уравнение редукции

$$\hat{w} = Q\left(X, Y, Z\right) + v_1\,, \tag{7}$$

где $Q\left(X, Y, Z\right)$ – неизвестная функция от наблюдаемых переменных состояния системы (5), v_1 – переменная состояния динамического наблюдателя. Тогда производная по времени уравнения редукции принимает вид

$$\frac{d\hat{w}}{dt} = \frac{\partial Q\left(X, Y, Z\right)}{\partial X}\frac{dX}{dt} + \frac{\partial Q\left(X, Y, Z\right)}{\partial Y}\frac{dY}{dt} + \frac{\partial Q\left(X, Y, Z\right)}{\partial Z}\frac{dZ}{dt} + \frac{dv_1}{dt}\,. \tag{8}$$

Согласно [6-8], макропеременная (6) должна удовлетворять функциональному уравнению:

$$\dot{\psi}(t) + L\left(X, Y, Z\right)\psi = 0\,, \tag{9}$$

где $L\left(X, Y, Z\right)$ – неизвестная функция, обеспечивающая устойчивость уравнения (9).

Производная по времени макропеременной (6) имеет вид

$$\frac{d\psi}{dt} = \frac{dw}{dt} - \frac{d\hat{G}}{dt}.$$

Тогда, подставив в это уравнение соответствующие выражения (5)-(8), получим

$$-\frac{\partial Q(X,Y,Z)}{\partial X}Y - \frac{\partial Q(X,Y,Z)}{\partial Y}Z - \frac{\partial Q(X,Y,Z)}{\partial Z}\left(G_1 - w\left(\frac{X-Z}{a} - Y\right)\right) - \\ -\frac{dv_1}{dt} + L(X,Y,Z)(w - \hat{w}) = 0. \quad (10)$$

Поскольку уравнение наблюдателя не должно содержать в себе ненаблюдаемые переменные состояния, то необходимо выписать из уравнения (10) все слагаемые, содержащие ненаблюдаемую переменную w:

$$w\left(\frac{\partial Q(X,Y,Z)}{\partial Z}\left(\frac{X-Z}{a} - Y\right) + L(X,Y,Z)\right) = 0.$$

Это равенство выполняется при условии

$$\frac{\partial Q(X,Y,Z)}{\partial Z}\left(\frac{X-Z}{a} - Y\right) + L(X,Y,Z) = 0, \quad (11)$$

так как $w \neq 0$. Тогда из (11) следует соотношение

$$\frac{\partial Q(X,Y,Z)}{\partial Z} = -\frac{L(X,Y,Z)}{\left(\frac{X-Z}{a} - Y\right)},$$

проинтегрировав которое, получим

$$Q(X,Y,Z) = \frac{L(X,Y,Z)}{\left(\frac{X-Z}{a} - Y\right)}Z. \quad (12)$$

С учетом полученного соотношения примем

$$L(X,Y,Z) = \alpha X^2, \quad (13)$$

здесь $\alpha > 0$ – постоянный коэффициент, задающий динамику (скорость) оценивания неизвестного параметра c. Тогда из (12) и (13) имеем

$$Q(X,Y,Z) = \frac{\alpha}{\left(\frac{X-Z}{a} - Y\right)}X^2 Z. \quad (14)$$

Теперь, зная $Q(X,Y,Z)$ (14) и $L(X,Y,Z)$ (13), мы можем из (10) выписать уравнение динамической составляющей наблюдателя возмущения:

$$\frac{dv_1}{dt} = -\frac{\partial Q(X,Y,Z)}{\partial X}Y - \frac{\partial Q(X,Y,Z)}{\partial Z}G_1 - L(X,Y,Z)\hat{w} = \\ = -\left(\frac{\alpha}{\left(\frac{X-Z}{a} - Y\right)}Z\right)Y - \left(\frac{\alpha}{\left(\frac{X-Z}{a} - Y\right)}X\right)G_1 - \alpha X^2\left(\frac{\alpha}{\left(\frac{X-Z}{a} - Y\right)}X^2 Z + v_1\right), \quad (15)$$

т.к. $\frac{\partial Q(X,Y,Z)}{\partial Y} = 0$.

Кроме того, имеем выражение для оценки параметра c:

$$\hat{r}_1 = \hat{c} = \frac{\alpha}{\left(\frac{X-Z}{a} - Y\right)} X^2 Z + v_1 . \qquad (16)$$

Таким образом, синтезированный синергетический наблюдатель параметра r_1 состоит из двух составляющих: во-первых, динамической, заданной дифференциальным уравнением (10), и, во-вторых, статической, заданной выражением (12). Теперь из соотношения (4) найдем реконструированный на принимающей стороне информационный сигнал:

$$\mu_{реконстр.}(t) = \hat{c} - c , \qquad (17)$$

который равен разности оцененного параметра и его номинального значения.

Таким образом, в статье предложен новый метод динамической обработки и защиты конфиденциальной информации, базирующийся на применении в качестве несущего сигнала широкополосных колебаний генератора хаоса и методе глобальной реконструкции динамки системы с использованием синергетического наблюдателя. Синтезированное уравнение синергетического наблюдателя обеспечивает достаточно точную реконструкцию информационного сигнала.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Николис Дж.* Динамика иерархических систем / Дж. Николис. – М.: Мир, 1989.
2. *Анищенко В.С., Астахов В.В., Вадивасова Т.Е., Нейман А.Б.* Нелинейные эффекты в хаотических и стохастических системах. – Москва-Ижевск: Институт компьютерных исследований, 2003.
3. *Анищенко В.С., Вадивасова Т.Е., Астахов В.В.* Нелинейная динамика хаотических и стахостических систем . – Саратов: Изд-во Саратовского университета, 1999.
4. *Anishchenko V.S., Pavlov A.N., Yanson N.B.* Reconstruction of dynamic systems as applied to secure communications // Technical Physics, 1998. –Vol. 43(12). – Pp. 1401-1407.
5. *Колесников А.А.* Синергетические методы управления сложными системами: теория системного синтеза. – М.: УРСС/Комкнига, 2006.
6. *Колесников А.А. и др.* Современная прикладная теория управления. Ч. II: Синергетический подход в теории управления. – Москва-Таганрог: Изд-во ТРТУ, 2000.

Деменков Дмитрий Александрович
Технологический институт федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г.Таганроге
E-mail: offic@ccsd.tsure.ru
347928, Таганрог, пер. Некрасовский, 44
Тел.: +7(8634)318090

Demenkov Dmitriy Aleksandrovich
Taganrog Institute of Technological – Federal State-Owned Educational Establishment of Higher Vocational Education «Southern Federal University»
E-mail: offic@ccsd.tsure.ru
44, Nekrasovskiy, Taganrog, 347928, Russia
Phone: +7(8634) 318090