УДК 681.5

Д.А. Деменков

СИНЕРГЕТИЧЕСКИЙ МЕТОД ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ РЕКОНСТРУКЦИИ СИСТЕМЫ ТИПА РЕССЛЕРА

В последние годы возник интерес к новому научному направлению, основанному на изучении процессов самоорганизации в нелинейных системах с динамическим хаосом. Подобные системы характеризуются так называемыми «странными» аттракторами, которые могут применяться в качестве гибких информационных процессоров, эффективно обрабатывающих информацию.

К генераторам информации – аттракторам – предъявляются следующие основные требования: во-первых, большая емкость памяти и, во-вторых, способность к значительному сжатию информации. Известно, что регулярные аттракторы типа Ван дер Поля, Релея, Пуанкаре и др., имеющие размерность 1, малоэффективны как модули для хранения информации, но практически идеальны как устройства для сжатия информации [1]. Однако в нелинейной динамике были обнаружены хаотические («странные») аттракторы, обладающие с информационной точки зрения универсальными свойствами: с одной стороны, они имеют значительную информационную размерность, а с другой – являются «компрессорами» информации. Хаотические аттракторы, например аттрактор Ресслера, осуществляют процессы обработки информации путем уменьшения числа степеней свободы в фазовом пространстве – процесс сжатия фазового пространства.

В статье предложен метод обработки и защиты информации, основанный на глобальной реконструкции динамической хаотической системы типа Ресслера 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 Ресслера [2, 4]:

$$\dot{x}(t) = -y - z; \qquad \dot{y}(t) = x + ay; \qquad \dot{z}(t) = bx + xz - cz, \tag{7}$$

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

Сначала преобразуем модель (7) к виду (5), для чего используем замену переменных [3]:

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

В результате получим новую систему:

$$\dot{X}(t) = Y; \qquad \dot{Y}(t) = Z; \qquad \dot{Z}(t) = f\left(X, Y, Z, m^0\right), \tag{8}$$

где

$$f\left(X, Y, Z, m^0\right) = bX + X\left(\frac{X - Z}{a} - Y\right) - c\left(\frac{X - Z}{a} - Y\right). \tag{9}$$

Итак, рассмотрим новый управляющий параметр генератора Ресслера:

$$c^*(t) = c + \mu(t) \ . \tag{10}$$

Для этого будем полагать, что в канал связи передается сигнал $Z(t)$, сгенерированный системой (8-10). Примем следующие допущения: модулирующий сигнал $\mu(t)$ является кусочно-постоянным, т.е. осуществляется передача цифровой информации; параметры *a, b* известны, а параметр $c(t) > 0$ является модулируемым параметром.

Покажем процедуру построения наблюдателя за параметром c на принимающей стороне для системы (8). 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:

$$\dot{X}(t) = Y; \quad \dot{Y}(t) = Z; \quad \dot{Z}(t) = G_1 - c(\frac{X - Z}{a} - Y); \quad \dot{w}(t) = 0, \tag{11}$$

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

Как видно, в системе (11), в отличие от (8), параметр c заменен переменной состояния модели w. В системе (11) 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

$$\psi = w - \hat{w} \tag{12}$$

и запишем уравнение редукции

$$\hat{w} = Q(X, Y, Z) + v_1, \tag{13}$$

где $Q(X, Y, Z)$ – неизвестная функция от наблюдаемых переменных состояния системы (11), v_1 – переменная состояния динамического наблюдателя. Тогда производная по времени уравнения редукции принимает вид

$$\frac{d\hat{w}}{dt} = \frac{\partial Q(X, Y, Z)}{\partial X}\frac{dX}{dt} + \frac{\partial Q(X, Y, Z)}{\partial Y}\frac{dY}{dt} + \frac{\partial Q(X, Y, Z)}{\partial Z}\frac{dZ}{dt} + \frac{dv_1}{dt}. \tag{14}$$

Согласно [6-8], макропеременная (12) должна удовлетворять функциональному уравнению

$$\dot{\psi}(t) + L(X, Y, Z)\psi = 0, \tag{15}$$

где $L(X, Y, Z)$ – неизвестная функция, обеспечивающая устойчивость уравнения (15).

Производная по времени макропеременной (12) имеет вид

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

Тогда, подставив в это уравнение соответствующие выражения (11)-(14), получим

$$\begin{aligned} &-\frac{\partial Q(X, Y, Z)}{\partial X}Y - \frac{\partial Q(X, Y, Z)}{\partial Y}Z - \frac{\partial Q(X, Y, Z)}{\partial Z}\left(G_1 - w(\frac{X - Z}{a} - Y)\right) - \\ &-\frac{dv_1}{dt} + L(X, Y, Z)(w - \hat{w}) = 0. \end{aligned} \tag{16}$$

Поскольку уравнение наблюдателя не должно содержать в себе ненаблюдаемые переменные состояния, то необходимо выписать из уравнения (16) 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

$$\frac{\partial Q(X,Y,Z)}{\partial Z}\left(\frac{X-Z}{a}-Y\right)+L(X,Y,Z)=0 , \qquad (17)$$

так как $w \neq 0$. Тогда из (17) 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

$$Q(X,Y,Z)=\frac{L(X,Y,Z)}{\left(\frac{X-Z}{a}-Y\right)}Z . \qquad (18)$$

С учетом полученного соотношения, примем

$$L(X,Y,Z)=\alpha X^2 , \qquad (19)$$

здесь $\alpha > 0$ – постоянный коэффициент, задающий динамику (скорость) оценивания неизвестного параметра c . Тогда из (18) и (19) имеем

$$Q(X,Y,Z)=\frac{\alpha}{\left(\frac{X-Z}{a}-Y\right)}X^2 Z . \qquad (20)$$

Теперь, зная $Q(X,Y,Z)$ (20) и $L(X,Y,Z)$ (19), мы можем из (16) выписать уравнение динамической составляющей наблюдателя возмущения:

$$\frac{dv_1}{dt}=-\frac{\partial Q(X,Y,Z)}{\partial X}Y-\frac{\partial Q(X,Y,Z)}{\partial Z}G_1-L(X,Y,Z)\hat{w}=$$

$$=-\left(\frac{\alpha}{\left(\frac{X-Z}{a}-Y\right)}Z\right)Y-\left(\frac{\alpha}{\left(\frac{X-Z}{a}-Y\right)}X\right)G_1-\alpha X^2\left(\frac{\alpha}{\left(\frac{X-Z}{a}-Y\right)}X^2 Z+v_1\right), \qquad (21)$$

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

Кроме того, имеем выражение для оценки параметра c :

$$\hat{w}=\hat{c}=\frac{\alpha}{\left(\frac{X-Z}{a}-Y\right)}X^2 Z+v_1 . \qquad (22)$$

Таким образом, синтезированный синергетический наблюдатель параметра η состоит из двух составляющих: во-первых, динамической, заданной дифференциальным уравнением (16), и, во-вторых, статической, заданной выражением (18). Теперь из соотношения (10) найдем реконструированный на принимающей стороне информационный сигнал:

$$\mu_{реконстр.}(t)=\hat{c}-c , \qquad (23)$$

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.

УДК 621.306

А.А. Строцев, С.В. Синицын, А.А. Жадько

МЕТОДИКА ТЕОРЕТИКО-ИГРОВОЙ ОПТИМИЗАЦИИ АЛГОРИТМА КОНТРОЛЯ СЛОЖНОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ СМЕШАННОГО РАСШИРЕНИЯ МАТРИЧНОЙ ИГРЫ С ОГРАНИЧЕНИЯМИ

Эффективность функционирования сложной системы (СС) зависит от качества алгоритмов ее контроля. Методы оптимизации алгоритмов контроля можно классифицировать относительно информационных условий выработки решения, принятых в теории принятия решений: определённости, риска и неопределённости.

Периоды приработки и старения СС характеризуются повышенными значениями интенсивности отказов $\Lambda(t)$, которые носят неопределенный характер. В [1] рассмотрена теоретико-игровая оптимизация алгоритмов контроля на основе моделей матричных игр, позволяющая учесть неопределенность возникновения неисправностей СС. Однако в предложенных моделях отсутствуют ограничения на процесс контроля технического состояния, которые могут быть обусловлены как спецификой самого объекта контроля, так и применением средств и методов контроля. Такие ограничения, например, могут быть связаны известными вероятностями возникновения ряда неисправных состояний, а также с требованиями эксплуатационной документации на применение отдельных алгоритмов контроля. Таким образом, рассмотрение вопросов построения теоретико-игровых моделей с ограничениями для оптимизации алгоритмов контроля в условиях сочетания случайных и неопределённых факторов является актуальной задачей.

Рассмотрим процесс контроля функционирования СС с условной остановкой алгоритма контроля. Будем полагать заданными:

– множество всех состояний системы $E=\{e_j\}$, $j=\overline{1,m}$, где $\{e_1\}=E^1$ – исправное состояние СС и соответствующее ему множество; $\{e_2,e_3,...,e_m\}=E^н$ –