09

Выделение информационной компоненты хаотического сигнала системы с запаздыванием

© В.И. Пономаренко, М.Д. Прохоров

Саратовское отделение Института радиотехники и электроники РАН
E-mail: sbire@sgu.ru

Поступило в Редакцию 25 февраля 2002 г.

Предложен метод определения параметров систем с запаздыванием по временно́му ряду наблюдаемой и с его помощью продемонстрирована возможность выделения сообщения при способе передачи информации, использующем нелинейное подмешивание информационного сигнала в хаотический сигнал системы с запаздыванием.

1. Использование хаотических сигналов для скрытой передачи информации привлекает к себе в последнее время большое внимание [1–7]. Были предложены различные способы передачи информационного сигнала, использующие хаотическую динамику: хаотическая маскировка, переключение хаотических режимов, нелинейное подмешивание, частотная модуляция хаотическим сигналом и др. Однако оказалось, что некоторые способы характеризуются в действительности ограниченной конфиденциальностью. Например, при использовании хаотических систем малой размерности информационное сообщение, передаваемое различными способами, может быть выделено сторонним наблюдателем с помощью методов реконструкции динамической системы по наблюдаемой [8] и с помощью построения отображений последования [9]. При использовании высокоразмерных хаотических систем в режимах гиперхаоса передаваемая информация также может быть распознана в ряде случаев с помощью процедуры восстановления передающей системы [10], использования спектрограмм [11] и нейтронных сетей [12]. В [13] скрытую передачу данных предлагалось осуществлять на основе систем с запаздыванием, демонстрирующих хаотические движения очень высокой размерности. Однако, как было показано в [14] для случаев хаотической маскировки и модуляции хаотическим сигналом,

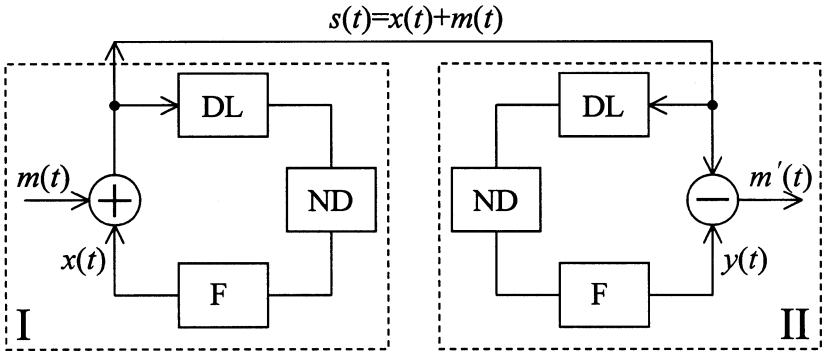

Рис. 1. Блок-схема системы связи: I — передатчик, II — приемник, DL — линия задержки, ND — нелинейный элемент, F — фильтр.

информационное сообщение и в этом случае можно выделить с помощью методов реконструкции систем с запаздыванием по временно́му ряду [15,16]. Мы предлагаем новый метод восстановления параметров хаотической передающей системы с запаздыванием по наблюдаемой и с его помощью иллюстрируем возможность выделения сообщения при способе передачи информации, использующем нелинейное подмешивание информационного сигнала.

2. Схема связи с нелинейным подмешиванием информационного сигнала в хаотический была предложена в [3] и получила дальнейшее развитие в [4]. В качестве генераторов хаотических сигналов при этом использовались соответственно кольцевой генератор с 1.5 степенями свободы и кольцевая схема на основе системы Чуа. В нашей работе в качестве хаотических несущих выбраны сигналы систем с запаздыванием, характеризуемые большим числом положительных ляпуновских показателей. Блок-схема системы связи приведена на рис. 1. В отсутствие информационного сообщения ($m(t) = 0$) передатчик может быть описан дифференциальным уравнением с запаздыванием, которое в простейшем случае имеет вид

$$\varepsilon_0 \dot{x}(t) = -x(t) + f\big(x(t-\tau_0)\big), \qquad (1)$$

где $x(t)$ — состояние системы в момент времени t, f — нелинейная функция, τ_0 — время запаздывания, ε_0 — параметр, характеризую-

щий инерционность системы. Информационный сигнал $m(t)$ с помощью сумматора добавляется к хаотическому сигналу $x(t)$, и сигнал $s(t) = x(t) + m(t)$ передается в канал связи и одновременно вводится в кольцо обратной связи передающей системы, колебания которой описываются уравнением

$$\varepsilon_0 \dot{x}(t) = -x(t) + f\big(x(t-\tau_0) + m(t-\tau_0)\big). \qquad (2)$$

Приемник состоит из тех же элементов, что и передатчик, за исключением сумматора, который заменен на вычитатель, разрывающий цепь обратной связи, и описывается уравнением

$$\varepsilon_0 \dot{y}(t) = -y(t) + f\big(x(t-\tau_0) + m(t-\tau_0)\big), \qquad (3)$$

где $y(t)$ — сигнал, поступающий на вход вычитателя. На выходе вычитателя имеем восстановленный информационный сигнал $m'(t) = x(t) + m(t) - y(t)$.

Если элементы принимающей и пердающей систем идентичны, то после переходного процесса эти системы синхронизуются между собой. Действительно, разность между колебаниями систем (2) и (3) $\Delta(t) = x(t) - y(t)$ уменьшается при любых $\varepsilon_0 > 0$, так как $\dot{\Delta}(t) = -\Delta/\varepsilon_0$. В результате синхронизации имеем $x(t) = y(t)$ и $m'(t) = m(t)$. При этом качество восстановления сигнала $m(t)$ не зависит от его амплитудных и частотных характеристик, что означает возможность передачи без искажений сложных информационных сигналов.

3. Скрытность хаотических коммуникационных систем основана на том, что параметры передающей системы известны только принимающей стороне, которая имеет точную копию передатчика. На примере рассмотренной системы передачи информации мы покажем, что информационное сообщение может быть выделено третьей стороной, имеющей лишь временну́ю реализацию передаваемого сигнала $s(t)$. Для этого нам потребуется восстановить параметры системы с запаздыванием вида (1), генерирующей маскирующий хаотический сигнал. Для восстановления по наблюдаемой времени задержки τ_0 воспользуемся методом, недавно предложенным нами в [17,18], где было показано, что во временно́й реализации систем вида (1) практически отстутствуют экстремумы, удаленные друг от друга на τ_0. Тогда для нахождения τ_0 нужно для различных значений времени τ определить число N пар экстремумов во временно́й реализации, удаленных друг от друга на τ,

и построить зависимость $N(\tau)$. Значению времени запаздывания τ_0 соответствует положение абсолютного минимума зависимости $N(\tau)$. Присутствие в передаваемом сигнале информационной компоненты небольшой амплитуды не меняет качественного вида $N(\tau)$. Как было показано в [17,18], такой метод определения τ_0 еще остается работоспособным при уровнях шума порядка 10%.

Для определения по хаотической временно́й реализации параметра инерционности ε_0 и нелинейной функции f системы (1) мы предлагаем новый метод, который проиллюстрируем сначала для случая отсутствия информационного сигнала. Как следует из уравнения (1), если построить на плоскости множество точек с координатами $\big(x(t-\tau_0), \varepsilon_0\dot{x}(t)+x(t)\big)$, то оно воспроизведет функцию f. Поскольку заранее величина ε_0 неизвестна, приходится строить зависимости $\varepsilon\dot{x}(t)+x(t)$ от $x(t-\tau_0)$ для различных значений ε, добиваясь однозначной зависимости на плоскости $\big(x(t-\tau_0), \varepsilon\dot{x}(t)+x(t)\big)$, которая возможна лишь при $\varepsilon=\varepsilon_0$. В качестве количественного критерия однозначности при таком поиске ε_0 будем использовать минимальную длину линии $L(\varepsilon)$, соединяющей точки на плоскости $\big(x(t-\tau_0), \varepsilon\dot{x}(t)+x(t)\big)$, упорядоченные по величине координаты $x(t-\tau_0)$. Минимум зависимости $L(\varepsilon)$ будет наблюдаться при $\varepsilon=\varepsilon_0$, а построенная при этом значении зависимость на плоскости $\big(x(t-\tau_0), \varepsilon_0\dot{x}(t)+x(t)\big)$ воспроизведет нелинейную функцию. В отличие от других методов [15,16], использующих для восстановления нелинейной функции только экстремальные точки или точки, выбираемые по определенному правилу, предлагаемый нами подход использует все точки временно́го ряда. Это позволяет по коротким временны́м рядам более полно восстанавливать нелинейную функцию даже в случаях слаборазвитого хаоса. Подмешивание в хаотический сигнал информационного сигнала малой амплитуды несущественно влияет на точность определения ε_0. Для оценки возможностей метода при наличии возмущений мы применили его к рядам, полученным при добавлении к временно́му ряду уравнения Маккея–Гласса

$$\dot{x}(t) = -bx(t) + \frac{ax(t-\tau_0)}{1+x^c(t-\tau_0)} \qquad (4)$$

гауссовского белого шума с нулевым средним значением. Уравнение (4) может быть приведено к виду (1) с $\varepsilon_0 = 1/b$ и $f\big(x(t-\tau_0)\big) = ax(t-\tau_0)/b\big(1+x^c(t-\tau_0)\big)$. Зависимость $L(\varepsilon)$ еще позволяет точно восстанавливать значение ε_0 при уровнях шума порядка 3%.

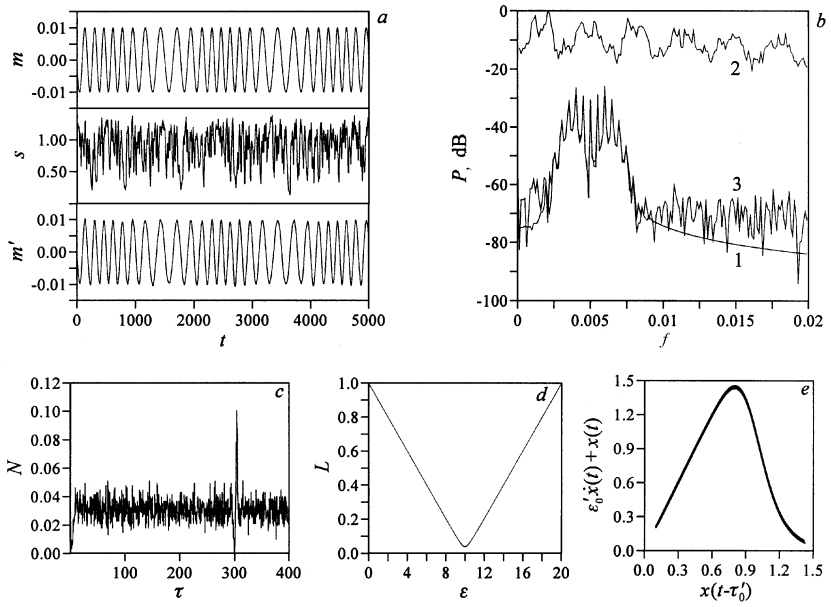

Рис. 2. *a* — фрагменты временны́х реализаций, $m(t)$ — частотно-модулированный (ЧМ) гармонический сигнал при $A = 0.01$, $B = 3$, $f_c = 5{\cdot}10^{-3}$, $f_m = 5 \cdot 10^{-4}$, $s(t)$ — сигнал в канале связи при $a = 0.2$, $b = 0.1$, $c = 10$, $\tau_0 = 300$, $m'(t)$ — выделенный ЧМ гармонический сигнал; *b* — спектры мощности сигналов $m(t)$ — 1, $s(t)$ — 2, $m'(t)$ — 3; *c* — зависимость $N(\tau)$, $N_{\min}(\tau) = N(300.0)$; *d* — зависимость $L(\varepsilon)$, $L_{\min}(\varepsilon) = L(10.0)$, $L(\varepsilon)$ нормировано таким образом, что наиболее неупорядоченному множеству точек соответствует $L = 1$; *e* — восстановленная функция.

4. Определив параметры передающей системы, можно построить принимающую систему. Для проверки работоспособности предлагаемого метода рассмотрим сначала численный пример, в котором к хаотическому сигналу, генерируемому системой Маккея–Гласса (4), нелинейно подмешивалось частотно-модулированное (ЧМ) гармоническое сообщение $m(t) = A\sin\bigl(2\pi f_c\, t - B\cos(2\pi f_m\, t)\bigr)$, где A определяет амплитуду сигнала сообщения, f_c — центральная частота спектра сигнала, B — индекс частотной модуляции, f_m — частота модуляции. На рис. 2, *a*, *b* приведены фрагменты временны́х реализаций и спектры мощности ЧМ

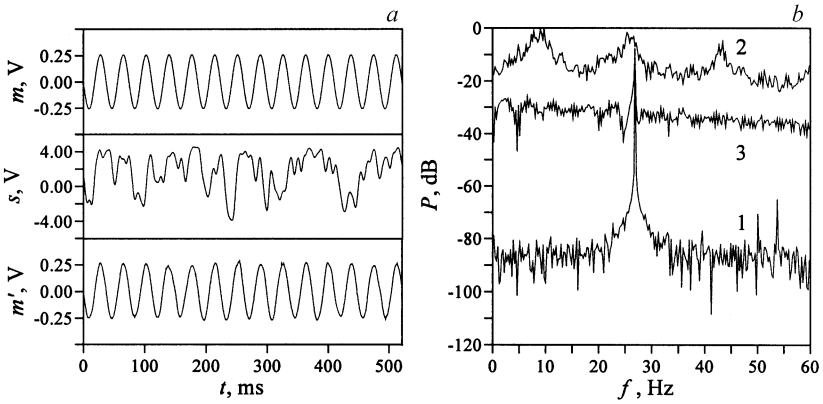

Рис. 3. *a* — фрагменты временны́х реализаций, $m(t)$ —гармонический сигнал на входе передатчика при $A = 0.25\,\mathrm{V}$, $f_c = 27\,\mathrm{Hz}$, $s(t)$ — сигнал в канале связи, $m'(t)$ — выделенный гармонический сигнал; *b* — спектры мощности сигналов $m(t)$ — 1, $s(t)$ — 2, $m'(t)$ — 3.

сигнала и передаваемого хаотического сигнала $s(t) = x(t)+m(t)$. График на рис. 2, *c* показывает число N пар экстремумов в реализации $s(t)$ на удалении τ друг от друга. Для построения зависимости $N(\tau)$ использовано 20 000 точек реализации $s(t)$, содержащей около 600 экстремумов, на общее число которых и нормировано $N(\tau)$. Для оценки производной $\dot{x}(t)$ по наблюдаемой мы использовали локальную параболическую аппроксимацию. Положение абсолютного минимума $N(\tau)$ позволяет восстановить время запаздывания $\tau_0' = 300.0$.

Для построения зависимости $L(\varepsilon)$ (рис. 2, *d*) использовано лишь 2000 точек реализации $s(t)$. Восстановленное по минимуму $L(\varepsilon)$ значение параметра инерционности $\varepsilon_0' = 10.0$ ($\varepsilon_0 = 1/b = 10$). Восстановленная при найденных τ_0' и ε_0' нелинейная функция изображена на рис. 2, *e*. Для ее аппроксимации мы использовали полиномы различной степени. Аппроксимирующая функция обеспечивала хорошее качество синхронного отклика приемника при использовании полинома не ниже 12-й степени. Фрагмент реализации выделенного информационного ЧМ гармонического сигнала и его спектр мощности показаны на рис. 2, *a*, *b*.

В качестве второго примера рассмотрим экспериментальную систему передачи информации, в которой источником хаотическо-

го сигнала выбран генератор с запаздывающей обратной связью. В случае когда фильтром (рис. 1) является низкочастотный *RC*-фильтр первого порядка, такой генератор описывается уравнением $RC\dot{V}(t) = -V(t) + f\left(V(t-\tau_0)\right)$, где $V(t)$ и $V(t-\tau_0)$ — напряжения на входе и выходе линии задержки, R и C — сопротивление и емкость элементов фильтра. Уравнение имеет вид (1) с $\varepsilon_0 = RC$. В нашем эксперименте нелинейный элемент имел квадратичную передаточную функцию. К хаотическому сигналу $V(t)$ нелинейно подмешивался гармонический сигнал $m(t) = A\sin(2\pi f_c t)$ с амплитудой A и частотой f_c. Передаваемым в канал связи являлся сигнал $s(t) = V(t) + m(t)$. Мы записывали сигналы $m(t)$ и $s(t)$ с частотой выборки $f_s = 4\,\mathrm{kHz}$. На рис. 3 приведены фрагменты временны́х реализаций и спектры мощности этих сигналов и выделенного гармонического сигнала $m'(t)$.

5. Нами предложен метод реконструкции систем с запаздыванием по наблюдаемой и показана возможность выделения сообщения в системах передачи информации, использующих для маскировки их хаотические сигналы. Таким образом, системы связи, использующие сигналы систем с запаздыванием, могут обладать недостаточной скрытностью, несмотря на высокую размерность и большое число положительных ляпуновских показателей хаотических аттракторов таких систем.

Выражаем признательность Б.П. Безручко за плодотворные обсуждения.

Работа выполнена при поддержке РФФИ, грант № 02–02–17578 и при поддержке CRDF, Award N, REC-006.

Список литературы

[1] *Kocarev L., Halle K.S., Eckert K.* et al. // Int. J. of Bifurcation and Chaos. 1992. V. 2. N 3. P. 709–713.
[2] *Cuomo K.M., Oppenheim A.V.* // Phys. Rev. Lett. 1993. V. 71. N 1. P. 65–68.
[3] *Волковский А.Р., Рульков Н.В.* // Письма в ЖТФ. 1993. Т. 19. В. 3. С. 71–75.
[4] *Dmitriev A.S., Panas A.I., Starkov S.O.* // Int. J. of Bifurcation and Chaos. 1995. V. 5. N 4. P. 1249–1254.
[5] *Дмитриев А.С., Панас А.И., Старков С.О.* // Успехи современной радиоэлектроники. 1997. № 10. С. 4–26.
[6] *Дмитриев А.С., Кузьмин Л.В.* // Письма в ЖТФ. 1999. Т. 25. В. 16. С. 71–77.
[7] *Кальянов Э.В.* // Письма в ЖТФ. 2001. Т. 27. В. 16. С. 1–9.
[8] *Short K.M.* // Int. J. of Bifurcation and Chaos. 1996. V. 6. N 2. P. 367–375.

[9] *Pérez G., Cerdeira H.A.* // Phys. Rev. Lett. 1995. V. 74. N 11. P. 1970–1973.
[10] *Short K.M., Parker A.T.* // Phys. Rev. E. 1998. V. 58. N 1. P. 1159–1162.
[11] *Yang T., Yang L.-B., Yang C.-M.* // Phys. Lett. A. 1998. V. 247. N 1, 2. P. 105–111.
[12] *Yang T., Yang L.-B., Yang C.-M.* // Physica D. 1998. V. 124. N 1–3. P. 248–257.
[13] *Mensour B., Longtin A.* // Phys. Lett. A. 1998. V. 244. N 1–3. P. 59–70.
[14] *Zhou C., Lai C.-H.* // Phys. Rev. E. 1999. V. 60. N 1. P. 320–323.
[15] *Bünner M.J., Popp M., Meyer Th.* et al. // Phys. Lett. A. 1996. V. 211. P. 345–349.
[16] *Bünner M.J., Popp M., Meyer Th.* et al. // Phys. Rev. E. 1996. V. 54. N 4. P. 3082–3085.
[17] *Караваев А.С., Пономаренко В.И., Прохоров М.Д.* // Письма в ЖТФ. 2001. Т. 27. В. 10. С. 43–51.
[18] *Bezruchko B.P., Karavaev A.S., Ponomarenko V.I., Prokhorov M.D.* // Phys. Rev. E. 2001. V. 64. N 5. 056216.