09

Система скрытой передачи информации на основе системы с запаздыванием с переключаемым временем задержки

© *В.И. Пономаренко, А.С. Караваев, Е.Е. Глуховская, М.Д. Прохоров*

Саратовский филиал Института радиотехники и электроники им. В.А. Котельникова РАН
E-mail: mdprokhorov@yandex.ru

Поступило в Редакцию 3 августа 2011 г.

Предложена система скрытой передачи информации, основанная на генераторе с запаздывающей обратной связью с переключаемым временем задержки. Эффективность системы связи продемонстрирована в численном эксперименте на модельных кольцевых системах с запаздыванием. Показана ее высокая устойчивость к шумам в канале связи.

Открытие явления синхронизации хаотических колебаний взаимодействующих систем [1] положило начало разработки новых систем скрытой передачи информации, основанных на использовании различных видов хаотической синхронизации (полной, с запаздыванием, фазовой, обобщенной) [2–9]. Были предложены различные способы передачи информационного сигнала на основе синхронизации хаотических динамических систем: хаотическая маскировка [2], переключение хаотических режимов [3], нелинейное подмешивание информационного сигнала к хаотическому [4], модуляция параметров передатчика в сочетании с адаптивными методами приема [6] и др. Однако оказалось, что многие системы связи, использующие хаотические сигналы, характеризуются в действительности ограниченной конфиденциальностью [10,11]. Для того чтобы повысить уровень защиты передаваемой информации, в [12–15] было предложено осуществлять скрытую передачу данных на основе систем с запаздыванием, демонстрирующих хаотическую динамику очень высокой размерности.

В данной работе предложена схема передачи информации на базе генератора с запаздывающей обратной связью, основанная на переклю-

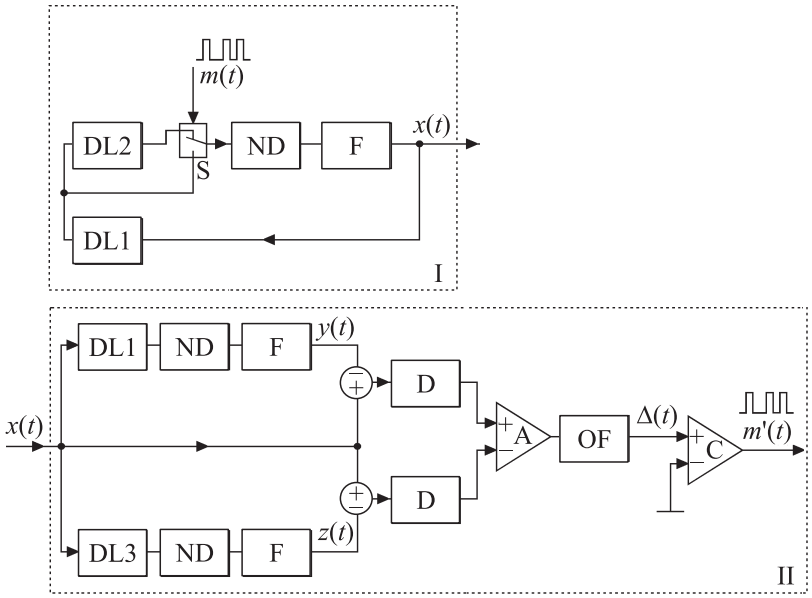

Рис. 1. Блок-схема системы передачи информации с переключением времени задержки: I — передатчик, II — приемник, DL1, DL2, и DL3 — линии задержки, ND — нелинейный элемент, F — фильтр, S — коммутирующее устройство, D — детектор, A — дифференциальный усилитель, OF — выходной фильтр, C — компаратор.

чении времени задержки в передатчике и выделении информационного сигнала с использованием в приемнике двух различных систем с запаздыванием. Блок-схема системы передачи информации представлена на рис. 1.

Передатчик представляет собой кольцевую систему из двух линий задержки с временами запаздывания τ_1 и τ_2, нелинейного элемента и линейного фильтра низких частот, генерирующую хаотический сигнал. В качестве информационного сигнала выбран бинарный сигнал $m(t)$, состоящий из последовательности бинарных 0 и 1. Информационный сигнал $m(t)$ управляет коммутирующим устройством, которое переключает время запаздывания в системе таким образом, что когда передается бинарный 0, время запаздывания в системе равно τ_1, а когда

передается бинарная 1, время запаздывания в системе равно $\tau_1 + \tau_2$. Такой передатчик описывается дифференциальным уравнением первого порядка с запаздыванием:

$$\varepsilon \dot{x}(t) = -x(t) + f\big(x(t - (\tau_1 + m(t)\tau_2))\big), \tag{1}$$

где $x(t)$ — состояние системы в момент времени t, f — нелинейная функция, ε — параметр, характеризующий инерционность системы. Таким образом, информационный сигнал изменяет параметры передающей системы и определяет свойства хаотического сигнала, передаваемого в канал связи. Отметим, что в интересах конфиденциальности передачи данных сигналы передатчика должны иметь сходные спектральные и статистические свойства при τ_1 и $\tau_1 + \tau_2$.

Приемник состоит из двух ведомых систем с запаздыванием, одна из которых имеет линию задержки с временем запаздывания τ_1, а вторая — с временем запаздывания $\tau_3 = \tau_1 + \tau_2$ (рис. 1). Параметры фильтров и нелинейных элементов этих систем идентичны соответствующим параметрам передатчика. Расположенный после фильтра вычитатель разрывает цепь обратной связи в каждой из ведомой систем приемника. Входным сигналом для обеих систем с запаздыванием приемника является хаотическая несущая $x(t)$ передатчика. Их уравнения имеют следующий вид:

$$\varepsilon \dot{y}(t) = -y(t) + f\big(x(t - \tau_1)\big), \tag{2}$$

$$\varepsilon \dot{z}(t) = -z(t) + f\big(x(t - \tau_3)\big). \tag{3}$$

Параметры передатчика и приемника должны быть выбраны таким образом, чтобы синхронизация с сигналом $x(t)$ в каждый момент времени могла наблюдаться только в одной из ведомых систем. В случае если передается бинарный 0 (время запаздывания в передатчике равно τ_1), с сигналом $x(t)$ синхронизуется выходной сигнал $y(t)$ первой системы с запаздыванием в приемнике. При отсутствии шума в канале связи в результате синхронизации имеем $x(t) = y(t)$, сигнал на выходе вычитателя первой ведомой системы с запаздыванием равен 0. При этом отсутствует синхронизация $x(t)$ и выходного сигнала $z(t)$ второй системы с запаздыванием в приемнике. Поскольку $x(t) \neq z(t)$, сигнал на выходе вычитателя второй системы с запаздыванием отличен от 0. Если передается бинарная 1 (время запаздывания в передатчике равно τ_3), то $x(t) \neq y(t)$ и $x(t) = z(t)$. В результате на выходе вычитателя первой

ведомой системы сигнал отличен от 0, а на выходе вычитателя второй — равен 0.

На описанном выше принципе основана работа большинства известных схем связи с переключением хаотических режимов [5,7]. Наличие синхронизации хаотической несущей $x(t)$ с сигналом первой (или единственной) ведомой системы приемника говорит о передаче бинарного 0, а отсутствие синхронизации — о передаче бинарной 1. Однако наличие шумов мешает установлению режима поной синхронизации приемника и передатчика. В результате на выходе вычитателей ведомых систем приемника сигнал всегда отличен от 0, что затрудняет восстановление передаваемого бинарного сигнала.

Для увеличения помехоустойчивости схемы мы добавили в нее новые элементы — два амплитудных детектора, дифференциальный усилитель, фильтр и компаратор (рис. 1). На выходе каждого детектора получаем модуль огибающей поступающего на его вход разностного сигнала. Затем сигналы с выходов детекторов вычитаются и сглаживаются фильтром низких частот, на входе которого имеем сигнал $\Delta(t)$. Выходной компаратор формирует из сигнала $\Delta(t)$ восстановленный информационный сигнал $m'(t)$. Если $\Delta(t) \leqslant 0$, то на выходе компаратора имеем бинарный 0, в противном случае — бинарную 1.

После такой модификации системы передачи информации ее устойчивость по отношению к шуму в канале связи оказывается существенно выше, чем у ранее известных схем с переключением хаотических режимов. Рассмотрим качественно, что происходит при добавлении аддитивного шума к хаотическому сигналу в канале связи. Предположив, что информационный, маскирующий хаотический и шумовой сигналы можно рассматривать как независимые случайные процессы, получим, что дисперсия сигналов на выходе каждого из детекторов увеличится относительно случая отсутствия шума на величину, равную дисперсии аддитивного шума. Следовательно, усредненная разность сигналов на выходе детекторов будет иметь тот же знак, что и в отсутствие шума. А значит, информационный сигнал восстановится точно. Приведенные рассуждения являются качественными. В реальности между хаотическим сигналом и аддитивным шумом после прохождения элементов приемника может появится корреляция, зависящая от значений параметров системы, кроме того, нелинейность системы в приемнике нарушает принцип суперпозиции. Однако строгое определение пределов

работоспособности преложенной схемы в присутствии шума является отдельной задачей и выходит за рамки данной работы.

Проиллюстрируем работу предложенной системы передачи информации в численном эксперименте. В качестве передатчика возьмем генератор с запаздывающей обратной связью, имеющий квадратичную нелинейность $f(x) = \lambda - x^2$, где λ — параметр нелинейности, и фильтр низких частот в виде фильтра Баттерворта первого порядка с частотой среза f_c. Параметры передатчика выберем следующими: $\tau_1 = 1000$, $\tau_2 = 10$, $\lambda = 1.8$, $f_c = 0.005$ ($\varepsilon = 200$). При них передатчик генерирует хаотический сигнал. В приемнике первая ведомая система с запаздыванием имеет линию задержки с $\tau_1 = 1000$, а вторая — с временем запаздывания $\tau_3 = 1010$. В обеих ведомых системах приемника $\lambda = 1.8$, $f_c = 0.005$. Выходной фильтр приемника является фильтром низких частот Баттерворта восьмого порядка с частотой среза $f_r = 0.0002$. Информационный сигнал $m(t)$ состоит из последовательности бинарных 0 и 1.

Временная реализация передаваемого информационного сигнала приведена на рис. 2, *a*. На рис. 2, *b* представлен фрагмент хаотического сигнала $x(t)$, передаваемого в канал связи. Поскольку значения τ_1 и τ_3 близки друг другу, соответствующие им участки временной реализации $x(t)$ визуально неразличимы, то есть, определить, какой из бинарных символов (0 или 1) передается в канал связи, затруднительно. Временная реализация сигнала $\Delta(t)$, снимаемого после выходного фильтра приемника, приведена на рис. 2, *c* тонкой линией. Восстановленный информационный сигнал $m'(t)$ на выходе приемника показан на рис. 2, *c* толстой линией. Из сравнения рис. 2, *a* и рис. 2, *c* видно, что информационный сигнал восстанавливается точно, но с некоторой задержкой. Ее величина зависит от времен запаздывания системы и параметров выходного фильтра.

Для численного исследования устойчивости предложенной схемы к шумам в канале связи мы добавляли гауссовский шум с нулевым средним значением к хаотическому сигналу $x(t)$, передаваемому в канал связи. На рис. 2, *d* приведены результаты выделения скрытого сообщения для случая, когда дисперсия аддитивного шума была равна дисперсии хаотической несущей, то есть уровень шума составлял 100%. Временная реализация сигнала $\Delta(t)$ показана тонкой линией, а сиганл $m'(t)$ — толстой линией. Несмотря на очень высокий уровень шума, качество восстановления информационного сигнала хорошее.

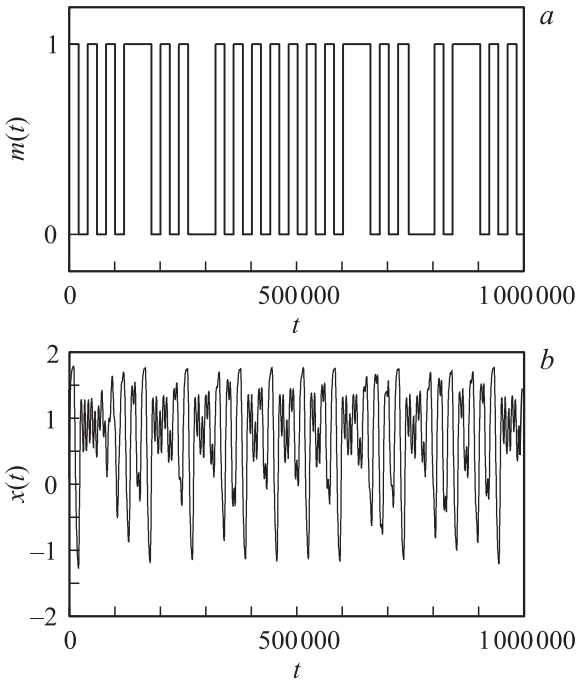

Рис. 2. *a* — временная реализация информационного сигнала $m(t)$; *b* — фрагмент временной реализации хаотического сигнала $x(t)$ в канале связи, *c* — временные реализации сигналов $\Delta(t)$ (тонкая линия) и $m'(t)$ (толстая линия) в отсутствии шума, *d* — временные реализации сигналов $\Delta(t)$ (тонкая линия) и $m'(t)$ (толстая линия) в присутствии 100% шума.

Следует отметить, что рассмотренная схема связи, как и все схемы с переключением хаотических режимов, имеет ограничение на скорость передачи информации. Это связано с возникновением переходных процессов после каждого переключения хаотических режимов. После переключения времени задержки в передатчике требуется некоторое время на установление синхронизации между передатчиком и одной из ведомых систем с запаздыванием в приемнике. Скорость передачи информации можно увеличить, уменьшив характерные временные масштабы системы. С другой стороны, в отличие от других систем

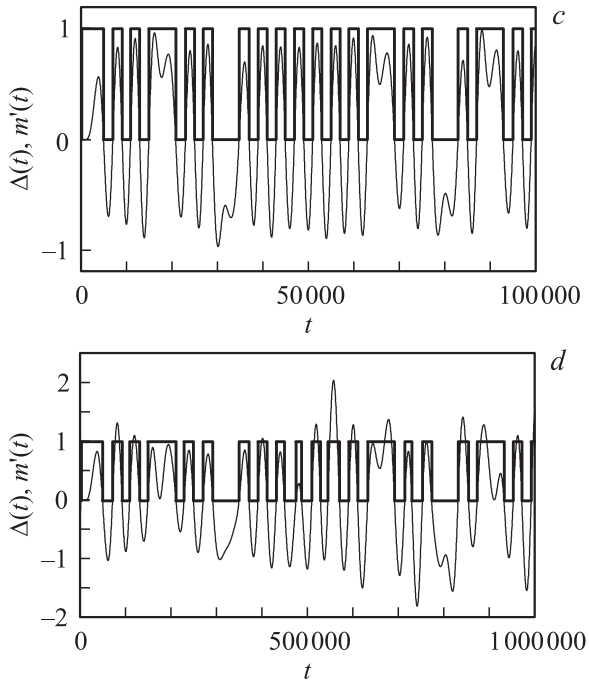

Рис. 2 (*продолжение*).

связи с переключением хаотических режимов, ипользующих в качестве передатчиков конечномерные системы, предлагаемая схема обладает большей конфиденциальностью, поскольку построена на базе систем с запаздыванием, обладающих бесконечно большим числом степеней свободы.

Несомненным достоинством предложенной системы передачи информации является также ее высокая устойчивость к шумам в канале связи. Показано, что качество восстановления скрытого сигнала сообщения остается высоким даже при уровнях шума, сопоставимых с уровнем хаотической несущей.

Работа выполнена при поддержке РФФИ, грант № 10-02-00980 и целевой программы „Развитие научного потенциала высшей школы“, проект № 2.1.1/1738.

Список литературы

[1] *Pecora L.M., Carroll T.L.* // Phys. Rev. Lett. 1990. V. 64. N 8. P. 821–824.
[2] *Kocarev L., Halle K.S., Eckert K.* et al. // Int. J. of Bifurcation and Chaos. 1992. V. 2. N 3. P. 709–713.
[3] *Parlitz U., Chua L.O., Kocarev L.* et al. // Int. J. of Bifurcation and Chaos. 1992. V. 2. N 4. P. 973–977.
[4] *Волковский А.Р., Рульков Н.Ф.* // Письма в ЖТФ. 1993. Т. 19. В. 3. С. 71–75.
[5] *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. Москва. Физматлит. 2002. 252 с.
[6] *Sun Y.H., Cao J., Feng G.* // Phys. Lett. A. 2008. V. 372. N 33. P. 5442–5447.
[7] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // УФН. 2009. Т. 179. В. 12. С. 1281—1310.
[8] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // ЖТФ. 2010. Т. 80. В. 4. С. 1–8.
[9] *Lavrov R., Jacquot M., Larger L.* // IEEE J. of Quantum Electronics. 2010. V. 46. N 10. P. 1430–1435.
[10] *Pérez G., Gerdeira H.A.* // Phys. Rev. Lett. 1995. V. 74. N 11. P. 1970–1973.
[11] *Short K.M.* // Int.J. of Bifurcation and Chaos. 19097. V. 7. N 7. P. 1579–1597.
[12] *Mensour B., Longtin A.* // Phys. Lett. A. 1998. V. 244. N 1–3. P. 59–70.
[13] *Ponomarenko V.I., Prokhorov M.D.* // Phys. Rev. E. 2002. V. 66. N 2. 026215.
[14] *Кальянов Э.В.* // Письма в ЖТФ. 2009. Т. 35. В. 6. С. 56–62.
[15] *Караваев А.С., Пономаренко В.И., Селезнев Е.П., Глуховская Е.Е., Прохоров М.Д.* // Письма в ЖТФ. 2011. Т. 37. В. 14. С. 24–31.