ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2008, том 72, № 1, с. 143–147

УДК 517.9

СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ, ОСНОВАННЫЙ НА ЯВЛЕНИИ ОБОБЩЕННОЙ СИНХРОНИЗАЦИИ

© 2008 г. А. А. Короновский, О. И. Москаленко, П. В. Попов, А. Е. Храмов

Саратовский государственный университет им. Н.Г. Чернышевского
E-mail: alkor@nonlin.sgu.ru

Предложен способ скрытой передачи информации, основанный на явлении обобщенной хаотической синхронизации, обладающий колоссальной устойчивостью к шумам и флуктуациям в канале связи. Основные идеи метода проиллюстрированы путем численного моделирования двух однонаправленно связанных систем Рёсслера, выбранных в качестве передатчика и приемника. Выявлены принципиальные достоинства предложенного метода по сравнению с известными ранее.

ВВЕДЕНИЕ

Использование хаотической синхронизации для скрытой передачи информации – актуальная задача нелинейной динамики [1–12]. В настоящее время известно большое число способов скрытой передачи данных. Значительная часть из них основана на явлении полной хаотической синхронизации (хаотическая маскировка [1], переключение хаотических режимов [2], нелинейное подмешивание [3] и др.), реже используют обобщенную [7] и фазовую [8] или несколько типов синхронного поведения одновременно [7, 13].

Принципиальный недостаток всех известных в настоящее время схем – достаточно низкая устойчивость к шумам и флуктуациям в канале связи. При превышении интенсивностью шума и флуктуаций некоторого порогового значения, сравнимого с естественными шумами и искажениями, известные системы передачи данных становятся неработоспособными. Кроме того, принципиальное требование почти всех таких схем – наличие в высокой степени идентичных хаотических генераторов на разных сторонах канала связи, это очень серьезная техническая проблема, особенно в течение длительного времени эксплуатации устройств. Другой недостаток таких схем (в частности, использующих полную хаотическую синхронизацию) – возможность реконструкции [14] параметров передающего генератора по сигналу, передаваемому по каналу связи. Из-за наличия точной копии передающего генератора на другой стороне канала связи третья сторона в некоторых случаях может легко дешифровать информационное сообщение.

В настоящей работе мы предлагаем новый способ скрытой передачи информации. Он основан на явлении обобщенной хаотической синхронизации, однако в отличие от известных ранее способов, использующих как этот тип синхронного поведения (например, [7, 13]), так и другие типы [1–5], позволяет избавиться от всех упомянутых выше недостатков. Эффективность предложенного способа проиллюстрирована путем численного моделирования двух однонаправленно связанных систем Рёсслера, выбранных в качестве передающего и принимающего устройств. Некоторые статистические оценки работоспособности предложенной схемы по сравнению с некоторыми известными ранее приведены также в настоящей работе.

1. ОБОБЩЕННАЯ СИНХРОНИЗАЦИЯ. СПОСОБЫ ЕЕ ДИАГНОСТИКИ

Как было упомянуто во введении, предлагаемый способ секретной передачи информации основан на явлении обобщенной синхронизации между хаотическими генераторами на передающей и принимающей сторонах канала связи. Коротко остановимся на этом типе синхронного поведения и основных способах его диагностики.

Режим обобщенной синхронизации может существовать в системе двух однонаправленно связанных хаотических осцилляторов – ведущего и ведомого, и означает, что после завершения переходного процесса между их состояниями $\vec{x}(t)$ (ведущего) и $\vec{u}(t)$ (ведомого) устанавливается некоторое функциональное соотношение $\vec{u}(t) = \vec{F}[\vec{x}(t)]$, вид которого может быть достаточно сложным, в том числе и фрактальным [15]. Как правило, найти такое соотношение далеко не всегда представляется возможным ни аналитически, ни экспериментально. Однако в настоящее время известны эффективные методы диагностики этого режима, такие как метод ближайших соседей, метод расчета условных ляпуновских экспонент и метод вспомогательной системы. Техническая реализация первых двух из них – весьма сложная, а иногда даже и невозможная задача. В то же самое время метод вспомогательной системы на практике может

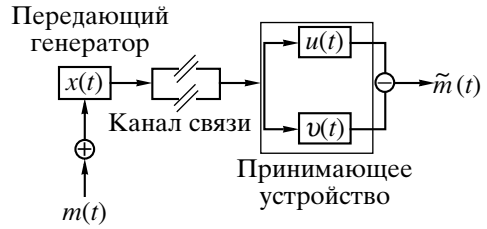

Рис. 1. Схема для секретной передачи информации при помощи обобщенной хаотической синхронизации. Здесь $m(t)$ – бинарный информационный сигнал, $\vec{x}(t)$ – вектор состояния передающего генератора, $\vec{u}(t)$ и $\vec{\upsilon}(t)$ – вектора состояний принимающего генератора, соответственно, $\tilde{m}(t)$ – восстановленный сигнал.

быть реализован достаточно просто, но при наличии точной копии ведомого генератора.

Суть метода вспомогательной системы [16] заключается в следующем: наряду с ведомой системой рассматривается идентичная ей вспомогательная система. Начальные условия для вспомогательной системы выбираются отличными от начального состояния ведомой системы, но лежащими в области притяжения одного аттрактора (как правило, на практике это означает небольшую расстройку начальных условий, которая реализуется автоматически из-за наличия флуктуаций). В случае отсутствия режима обобщенной синхронизации между взаимодействующими системами векторы состояния ведомой и вспомогательной систем принадлежат одному и тому же хаотическому аттрактору, но являются различными за счет ляпуновской неустойчивости хаотических траекторий. В том случае, когда имеет место режим обобщенной синхронизации, в силу выполнения функциональных соотношений между состояниями ведущей и ведомой систем и соответственно ведущей и вспомогательной, после завершения переходного процесса состояния ведомой и вспомогательной систем должны стать идентичными. Таким образом, эквивалентность состояний ведомой и вспомогательной систем после переходного процесса – это критерий наличия обобщенной синхронизации между ведущей и ведомой хаотическими системами.

2. СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Схема скрытой передачи информации при помощи обобщенной хаотической синхронизации приведена на рис. 1. Способ скрытой передачи информации заключается в следующем. Информационный сигнал $m(t)$ кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего генератора модулируются бинарным сигналом. Полученный таким образом сигнал передается по каналу связи. Здесь он подвергается влиянию шумов и флуктуаций, искажающих передаваемый сигнал. Приемник находится на другой стороне канала связи. Он представляет собой два идентичных генератора, способных находиться в режиме обобщенной синхронизации с передающим. Следует отметить, что наличие идентичных генераторов на одной стороне канала связи позволяет легко осуществить их юстировку. Принцип работы приемника основан на диагностике режима обобщенной синхронизации при помощи метода вспомогательной системы (см. выше). Сигнал с канала связи поступает на генераторы приемника. Полученные на выходе сигналы проходят через вычитающее устройство, и детектируется восстановленный полезный сигнал $\tilde{m}(t)$.

Параметры модуляции управляющих параметров передающего генератора должны быть выбраны таким образом, чтобы в зависимости от передаваемого бинарного бита 0/1 между передающим и принимающим генераторами существовал или отсутствовал режим обобщенной синхронизации. Например, допустим, что режим обобщенной синхронизации наблюдается в том случае, если передается бинарный бит 0. Тогда оба принимающих генератора в этом случае будут демонстрировать идентичные колебания, а после прохождения через вычитающее устройство будет наблюдаться отсутствие хаотических колебаний, т.е. бинарный бит 0. Наоборот, при передаче бинарного бита 1 обобщенная синхронизация не наблюдается, а колебания принимающих генераторов неидентичны. Тогда после прохождения через вычитающее устройство будут наблюдаться хаотические колебания ненулевой амплитуды, т.е. бинарный бит 1.

3. ЧИСЛЕННАЯ РЕАЛИЗАЦИЯ СПОСОБА СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Чтобы показать несомненные преимущества предложенного способа передачи информации по сравнению с известными ранее, проведем численное моделирование схемы (рис. 1). В качестве передающего и принимающего генераторов выберем однонаправленно связанные системы Ресслера. Выбор такой модели связан с тем, что а) система Ресслера в настоящее время достаточно хорошо изучена (в том числе и с точки зрения обобщенной синхронизации [15–20]), б) можно построить радиотехнический генератор, динамика которого будет описываться уравнениями системы Ресслера [21].

Передающий генератор описывается следующей системой дифференциальных уравнений:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \end{aligned} \qquad (1)$$

где $\vec{x}(t) = (x_1, x_2, x_3)$ – вектор состояния передающего генератора, $a = 0.15$, $p = 0.2$ и $c = 10$ – управ-

ляющие параметры, ω_x – управляющий параметр, характеризующий собственную частоту колебаний системы.

Величина параметра ω_x модулируется полезным цифровым сигналом следующим образом. Если в заданный интервал времени передается бинарный бит 1, тогда $\omega_x = 0.95$ на протяжении всего этого интервала. При передаче бинарного бита 0 $\omega_x = 1$. Следует отметить, что выбор упомянутых выше значений управляющего параметра ω_x использовался исключительно в демонстративных целях и обусловлен характером расположения границы обобщенной синхронизации, подробно изученным в [20]. На самом деле параметр ω_x может принимать достаточно произвольные значения. Необходимое условие – лишь чередование областей с асинхронной динамикой и режимом обобщенной синхронизации.

Принимающее устройство содержит два идентичных хаотических генератора, каждый из которых описывается следующей системой уравнений:

$$\begin{aligned} \dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \\ \dot{u}_2 &= \omega_u u_1 + a u_2, \\ \dot{u}_3 &= p + u_3(u_1 - c). \end{aligned} \qquad (2)$$

Здесь $\vec{u}(t) = (u_1, u_2, u_3)$ – вектор состояния первого принимающего генератора. Пусть $\vec{v}(t) = (v_1, v_2, v_3)$, также удовлетворяющий (2), будет вектором состояния второго принимающего генератора (см. рис. 1). Управляющие параметры a, p и c выберем идентичными последним для принимающего генератора. Управляющий параметр ω_u, характеризующий собственную частоту принимающих генераторов, выберем равным $\omega_u = 0.95$ на протяжении всего времени передачи сигнала.

Сигнал, генерируемый передающим устройством, передается по каналу связи. В нашей модели это реализуется путем связи принимающего генератора с передающим, т.е. добавлением компоненты $\varepsilon(s(t) - u_1)$ в первое уравнение системы (2). Здесь $s(t) = x_1 + D\xi$ – это так называемый сигнал в канале связи. Слагаемое $D\xi$ моделирует шумы и флуктуации в канале связи. ξ – стохастический гауссов процесс, характеризующийся следующим распределением вероятности:

$$p(\xi) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right), \qquad (3)$$

где $\xi_0 = 0$ и $\sigma = 1$ – среднее и дисперсия[1]. Параметр D определяет интенсивность добавляемого шума.

[1] Важно отметить, что характер распределения случайной величины ξ не имеет особого значения, и подобные результаты могут наблюдаться для других типов распределения вероятности $p(\xi)$, например, для равномерного.

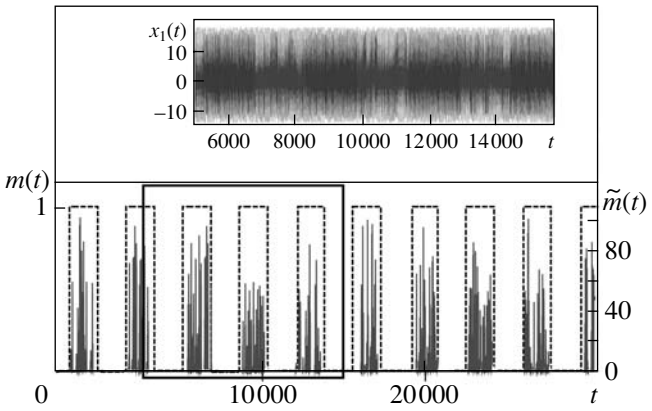

Рис. 2. Передаваемый информационный сигнал $m(t)$, представляющий собой простую последовательность бинарных битов 0/1 (пунктирная линия) и восстановленный сигнал $\tilde{m}(t)$ в отсутствие шумов и флуктуаций в канале связи ($D = 0$). На врезке показан фрагмент передаваемого по каналу связи хаотического сигнала, генерируемого передающим генератором, содержащий последовательность трех бинарных битов 0/1 (показан на рисунке прямоугольником). Видно, что третья сторона в этом случае не имеет возможности декодировать информационное сообщение.

Сила связи между передающим и принимающим генераторами характеризуется параметром ε. Он был выбран равным $\varepsilon = 0.14$. В этом случае известно, что в отсутствие шумов и флуктуаций в канале связи ($D = 0$) режим обобщенной синхронизации в системе (1)–(2) имеет место при $\omega_x = 1$, в то время как для $\omega_x = 0.95$ обобщенная синхронизация не наблюдается (более подробно см. [20]).

Вычитающее устройство выполняет операцию $(u_1 - v_1)^2$. Тогда после прохождения через него, согласно методу вспомогательной системы, должно наблюдаться отсутствие колебаний для $\omega_x = 1$ и наличие хаотических колебаний для $\omega_x = 0.95$. Восстановленный сигнал $\tilde{m}(t)$ будет представлять собой последовательность областей с различными типами поведения.

В демонстративных целях в качестве информационного сигнала $m(t)$ выберем простую последовательность бинарных битов 0/1, представленную на рис. 2 (пунктирная линия). Для интегрирования стохастического уравнения (2) будем использовать метод Эйлера с шагом дискретизации по времени $h = 0.0001$.

Рассмотрим сначала случай, когда шумы и флуктуации в канале связи отсутствуют, т.е. положим амплитуду шума $D = 0$. Понятно, что такой случай нереализуем на практике, так как шумы и флуктуации всегда присутствуют в реальных устройствах. Тем не менее рассмотрим сначала идеализированную ситуацию, чтобы проверить эффективность предлагаемого метода. Восстановленный сигнал $\tilde{m}(t)$ в этом случае приведен на рис. 2

(сплошная линия). Нетрудно видеть, что полезный сигнал в этом случае может быть легко детектирован.

Следует отметить, что изменение управляющего параметра ω_x не меняет сильно характеристики передаваемого сигнала. Фрагмент такого сигнала, содержащего последовательность шести битов 0/1 представлен на врезке к рис. 2. Понятно, что даже в отсутствие шумов и флуктуаций в канале связи третья сторона не имеет возможности декодировать информационное сообщение. Добавление шумов в канал связи еще более искажает передаваемый сигнал. Однако восстановленные сигналы $\tilde{m}(t)$ при различных значениях амплитуды шума вплоть до $D = 400$ выглядят качественно одинаково, так же как и в случае отсутствия шумов и флуктуаций (см. рис. 2, сплошная линия). В этом случае можно говорить о значительной устойчивости предлагаемой схемы к шумам и флуктуациям в канале связи.

4. СРАВНЕНИЕ ПРЕДЛАГАЕМОГО СПОСОБА СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ С ИЗВЕСТНЫМИ РАНЕЕ

Чтобы показать несомненные преимущества нашего метода по сравнению с известными ранее, проведем некоторые статистические оценки работоспособности как предлагаемой нами схемы для передачи информации, так и ряда известных ранее схем (например, [1–3, 7, 13]). Такими характеристиками являются:

а) соотношение сигнал/шум (*SNR*), при котором схема становится неработоспособной, т.е. когда нет никакой возможности восстановления исходного полезного цифрового сигнала $m(t)$ по получаемому на выходе $\tilde{m}(t)$. Так как шумы и флуктуации неизбежно присутствуют в канале связи, оценка работоспособности схем для передачи информации в присутствии шумов является очень важной и актуальной задачей.

б) максимальное значение расстройки управляющих параметров генераторов, которые изначально должны быть идентичными. Как уже обсуждалось во введении, в большинстве известных случаев такие генераторы должны располагаться на различных сторонах канала связи. Ввиду сложности технической реализации таких устройств влияние расстройки их управляющих параметров на эффективность работы способа передачи информации является актуальной проблемой.

Анализ подобных характеристик показал, что предложенная схема становится неработоспособной при соотношении сигнал/шум $SNR = -34.6$ дБ, в то время как для других рассмотренных нами схем эта величина оказывается положительной, т.е. при наличии в канале связи шумов и флуктуаций, мощность которых меньше мощности передаваемого сигнала, все известные до настоящего времени схемы становятся неработоспособными. Наша схема обладает высокой устойчивостью по отношению к шумам и флуктуациям в канале связи. Еще более искажая передаваемый сигнал, шум препятствует третьей стороне декодировать информационное сообщение. В этом случае можно говорить о конструктивной роли шума для передачи информации, в то время как в остальных случаях роль шума деструктивная.

Оценка влияния расстройки управляющих параметров на эффективность работы способа показала, что если генераторы принимающего устройства будут расстроены вплоть до 2% по параметру ω_x, наша схема будет оставаться работоспособной. Конечно, это не столь большая величина, и в этом отношении предложенная схема имеет аналоги (например, схемы передачи информации, известные как переключение хаотических режимов [2] и модулирование управляющих параметров [22]). Но не следует забывать, что в этих случаях оба генератора должны располагаться на различных сторонах канала связи (для возможности реализации режима полной синхронизации между ними). В предложенном же случае идентичные генераторы располагаются только на принимающей стороне канала связи, что позволяет легко осуществить их юстировку. Кроме того, обе упомянутые выше схемы обладают ограниченной устойчивостью к шумам и флуктуациям в канале связи, в то время как устойчивость предложенной схемы является неограниченной в реальных пределах.

ЗАКЛЮЧЕНИЕ

В настоящей работе предложен новый способ скрытой передачи информации при помощи обобщенной хаотической синхронизации. Он обладает рядом принципиальных преимуществ по сравнению с известными ранее способами секретной передачи данных. Во-первых, он не требует наличия идентичных хаотических генераторов на различных сторонах канала связи, а следовательно, легко реализуем на практике. Во-вторых, он обладает колоссальной устойчивостью по отношению к шумам и флуктуациям в канале связи. В данном случае можно говорить о конструктивной роли шума для передачи информации. В-третьих, за счет наличия шумов в канале связи передаваемый сигнал дополнительно искажается, что не дает никакой возможности третьей стороне декодировать информационное сообщение.

Работа выполнена при поддержке РФФИ (проект № 05-02-16273), Президентской программы поддержки ведущих научных школ РФ (проект НШ 4167.2006.2) и молодых докторов наук (МД-1884.2007.2), НОЦ “Нелинейная динамика и биофизика” при СГУ (грант REC-006 of U.S. CRDF), а также ФНП “Династия” и Международного центра фундаментальной физики (г. Москва).

СПИСОК ЛИТЕРАТУРЫ

1. *Cuomo M.K., Oppenheim A.V., Strogatz S.H.* // IEEE Trans. Circuits and Syst. 1993. V. 40. № 10. P. 626.
2. *Dedieu H., Kennedy M.P., Hasler M.* // IEEE Trans. on Circ. Sys. I. 1993. V. 40. P. 634.
3. *Dmitriev A.S., Panas A.I., Starkov S.O.* // Int. J. Bifurcations and Chaos. 1995. V. 5. № 4. P. 1249.
4. *Boccaletti S., Farini A., Arecchi F.T.* // Phys. Rev. E. 1997. V. 55. № 5. P. 4979.
5. *Carroll T.L., Johnson G.A.* // Phys. Rev. E. 1998. V. 57. № 2. P. 1555.
6. *Fischer I., Liu Y., Davis P.* // Phys. Rev. A. 2000. V. 62. 011801(R).
7. *Terry J.R., VanWiggeren G.D.* // Chaos, Solitons and Fractals. 2001. V. 12. P. 145.
8. *Chen J.Y., Wong K.W., Cheng L.M., Shuai J.W.* // Chaos. 2003. V. 13. № 2. P. 508.
9. *Yuan Z.L., Shields A.J.* // Phys. Rev. Lett. 2005. V. 94. 048901.
10. *Lucamarini M., Mancini S.* // Phys. Rev. Lett. 2005. V. 94. 140501.
11. *Li Q.S., Liu Y.* // Phys. Rev. E. 2006. V. 73. 016218.
12. *Fradkov A.L., Andrievsky B., Evans R.J.* // Phys. Rev. E. 2006. V. 73. 066209.
13. *Murali K., Lakshmanan M.* // Phys. Lett. A. 1998. V. 241. P. 303.
14. *Ponomarenko V.I., Prokhorov M.D.* // Phys. Rev. E. 2002. V. 66. № 2. 026215.
15. *Rulkov N.F., Sushchik M.M., Tsimring L.S., Abarbanel H.D.I.* // Phys. Rev. E. 1995. V. 51. № 2. P. 980.
16. *Abarbanel H.D.I., Rulkov N.F., Sushchik M.M.* // Phys. Rev. E. 1996. V. 53. № 5. P. 4528.
17. *Hramov A.E., Koronovskii A.A.* // Phys. Rev. E. 2005. V. 71. № 6. 067201.
18. *Zheng Z., Hu G.* // Phys. Rev. E. 2000. V. 62. № 6. P. 7882.
19. *Hramov A.E., Koronovskii A.A.* // Europhys. Lett. 2005. V. 70. № 2. P. 169.
20. *Hramov A.E., Koronovskii A.A., Moskalenko O.I.* // Europhys. Lett. 2005. V. 72. № 6. P. 901.
21. *Rico-Martinez R., Kreischer K.E., Flatgen G. et al.* // Physica D. 2003. V. 176. P. 1.
22. *Yang T., Chua L.O.* // IEEE Trans. Circuits. Syst. I. 1996. V. 43. P. 817.