

Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов

© А.А. Короновский, О.И. Москаленко, А.Е. Храмов

Саратовский государственный университет им. Н.Г. Чернышевского,
410012 Саратов, Россия
e-mail: moskalenko@nonlin.sgu.ru

(Поступило в Редакцию 20 мая 2009 г.)

Предложен способ передачи информации на основе обобщенной хаотической синхронизации, характеризующийся достаточно высокой степенью надежности, достигаемой за счет изменения характеристик сигнала, содержащего полезную информацию, генератором шума с заданными характеристиками. Показано, что в рассматриваемом методе на основе обобщенной синхронизации шум оказывает конструктивную роль в повышении конфиденциальности передачи данных. Основные идеи метода проиллюстрированы на примере однонаправленно связанных систем Ресслера, используемых в качестве генераторов передающего и принимающего устройств.

Введение

Одним из наиболее важных практических приложений явления хаотической синхронизации является ее использование для скрытой передачи информации [1–3]. На протяжении последнего десятилетия это направление научных исследований является востребованным широким кругом теоретиков и экспериментаторов [14–19]. Однако техническая реализация большинства известных схем и устройств представляется достаточно сложной задачей. Требование идентичности генераторов на различных сторонах каналов связи, низкая устойчивость к шумам, проблемы конфиденциальности — вот перечень основных проблем, выявляемых лишь путем теоретического анализа известных систем связи на основе хаотической синхронизации [16,20,21]. Преодоление этих проблем — весьма сложная задача. Повышение степени конфиденциальности передачи информации в ряде случаев влечет за собой чрезмерное усугубление других недостатков. Например, схема, предложенная в работе [22], требует наличия двух и трех идентичных друг другу генераторов и остается работоспособной лишь при передаче информации по идеальным (бесшумовым) каналам связи (см. также [23]). Идентичность генераторов на различных сторонах канала связи и достаточно низкая устойчивость к шумам характерны почти для всех известных систем связи на основе хаотической синхронизации [4,7,16,20,24].

Исключением является предложенный нами ранее способ скрытой передачи информации, основанный на явлении обобщенной хаотической синхронизации [21]. Ввиду использования именно этого типа синхронного поведения он позволяет преодолеть сразу два недостатка, присущих известным схемам и устройствам аналогичного назначения. Во-первых, он не требует идентичности генераторов, располагаемых на различных сторонах канала связи. Вместо этого два идентичных между собой генератора используются на принимающей

стороне (где они могут быть легко отъюстированы). Во-вторых, схема, предложенная в [21], характеризуется достаточно высокой устойчивостью по отношению к шумам, появляющимся, в первую очередь, в каналах связи. Кроме того, обнаружена возможность диагностирования режима обобщенной синхронизации в микроволновом диапазоне [25], который обычно и используется в современных телекоммуникационных системах.

Недостатком этой схемы является тот факт, что сигнал, передаваемый по каналу связи, несет на себе следы модуляции управляющего параметра полезным сигналом, что теоретически может позволить третьей стороне в некоторых случаях декодировать информационное сообщение. Поэтому этот способ не обеспечивает достаточной надежности при конфиденциальной передаче информации, оставаясь при этом сверхустойчивым к шумам.

В настоящей работе предлагается новый способ скрытой передачи информации, представляющий собой модификацию предложенного нами ранее метода, обеспечивающий скрытие следов модуляции управляющих параметров и гарантирующий высокую степень надежности при ее передаче. В основу метода положен режим обобщенной хаотической синхронизации, но в присутствии дополнительного источника шума, наличие которого, как будет показано ниже, играет в данном случае конструктивную роль.

1. Режим обобщенной синхронизации хаотических осцилляторов и передача информации

Обобщенная синхронизация вводится в рассмотрение для системы двух однонаправленно связанных хаотических осцилляторов — ведущего $x(t)$ и ведомого $u(t)$ — и означает, что после завершения переходного процесса устанавливается функциональная зависимость между их

состояниями, т.е. $\mathbf{u}(t) = \mathbf{F}[\mathbf{x}(t)]$ [26], вид которой $\mathbf{F}[\cdot]$ может быть достаточно сложным, а процедура ее нахождения весьма нетривиальной [27].

В литературе предложены несколько методов для диагностирования режима обобщенной синхронизации, такие как метод ближайших соседей [26,28], метод расчета условных ляпуновских экспонент [29,30], а также часто используемый и относительно легко осуществимый на практике метод вспомогательной системы [31]. Для нас здесь важны два последних метода.

Суть метода вспомогательной системы сводится к следующему: наряду с ведомой системой $\mathbf{u}(t)$ рассматривается идентичная ей вспомогательная система $\mathbf{v}(t)$. Начальные условия для вспомогательной системы $\mathbf{v}(t_0)$ выбираются отличными от начального состояния ведомой системы $\mathbf{u}(t_0)$, однако лежащими в бассейне притяжения того же аттрактора (в эксперименте это означает небольшую расстройку начальных условий, которая реализуется автоматически из-за наличия флуктуаций). В режиме обобщенной синхронизации в силу выполнения соотношений $\mathbf{u}(t) = \mathbf{F}[\mathbf{x}(t)]$ и соответственно $\mathbf{v}(t) = \mathbf{F}[\mathbf{x}(t)]$ после завершения переходного процесса состояния ведомой и вспомогательной систем должны стать идентичными $\mathbf{u}(t) \equiv \mathbf{v}(t)$, что является критерием наличия обобщенной синхронизации между ведущим и ведомым осцилляторами.

Анализ режима обобщенной синхронизации может быть проведен также с помощью вычисления условных ляпуновских экспонент [29,30]. Если размерности фазовых пространств ведущей и ведомой систем соответственно равны N_d и N_r , то поведение однонаправленно связанных хаотических осцилляторов может быть охарактеризовано с помощью спектра ляпуновских показателей $\lambda_1 \geq \lambda_2 \dots \geq \lambda_{N_d+N_r}$. Вследствие независимости поведения ведущей системы от состояния ведомого осциллятора спектр ляпуновских показателей может быть разделен на две части: ляпуновские показатели ведущей системы $\lambda_1^d \geq \dots \geq \lambda_{N_d}^d$ и условные ляпуновские показатели $\lambda_1^r \geq \dots \geq \lambda_{N_r}^r$. Критерием существования обобщенной синхронизации в однонаправленно связанных системах [27,29] является отрицательность старшего условного ляпуновского показателя λ_1^r .

Использование режима обобщенной синхронизации для скрытой передачи информации открывает ряд новых возможностей, не характерных для других типов синхронного поведения, например, для полной [32] и фазовой [33] синхронизации.

Во-первых, в отличие от полной синхронизации обобщенная синхронизация может наблюдаться в совершенно различных взаимодействующих динамических системах [27], что говорит о возможности упрощения технической реализации способов скрытой передачи данных, основанных на этом типе синхронного поведения.

Во-вторых, вид функциональной зависимости $\mathbf{F}[\cdot]$, устанавливаемой между состояниями взаимодействующих систем, может быть очень сложным, в том числе и фрактальным [34], что значительно усложняет

возможность получения информации о характеристиках генератора на принимающей стороне канала связи (например, путем реконструкции параметров сигнала по наблюдаемой [35,36]) третьей стороной по временной реализации передаваемого сигнала, т.е. повышает конфиденциальность.

В-третьих, поведение границы обобщенной синхронизации при изменении расстройки генераторов существенно отличается от поведения границ других известных типов синхронного поведения, демонстрируя аномальное поведение. В частности, для ряда систем при небольшом изменении частоты наблюдается быстрое изменение порога возникновения режима обобщенной синхронизации в области малых расстройок частоты [37,38]. Эта особенность позволяет обеспечить возникновение/разрушение синхронного режима при очень слабой модуляции управляющего параметра, что гарантирует эффективную модуляцию управляющего параметра для передачи информации по каналам связи.

В-четвертых, как будет показано ниже, шум практически не влияет на порог возникновения режима обобщенной синхронизации, т.е. синхронный режим возникает в однонаправленно связанных динамических системах в отсутствие и при наличии шума при близких значениях силы связи между системами. Поэтому можно ожидать высокую устойчивость схем на основе режима обобщенной синхронизации к шумам в каналах связи [39,40]. Более того, дополнительный шум может быть использован для создания дополнительной маскировки передаваемого по каналу связи сигнала.

Первые три достоинства режима обобщенной синхронизации были полностью учтены при разработке способа скрытой передачи информации на основе обобщенной синхронизации [21], о котором упоминалось во Введении. В то же время четвертая особенность в нем в полной мере не использовалась. Действительно, способ обладает высокой устойчивостью к шумам, но шум не применяется в нем в конструктивных целях. На решение этой задачи и направлена настоящая работа. Перед тем как перейти к обсуждению способа скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума, коротко остановимся о причинах устойчивости режима обобщенной синхронизации к шумам.

2. Устойчивость режима обобщенной синхронизации к шумам

Известно, что режим обобщенной синхронизации может наблюдаться в системах с диссипативным и недиссипативным типами связи [27,41]. Для систем с диссипативной связью (которые будут рассматриваться далее) уравнения, описывающие динамику взаимодействующих систем в присутствии шума, могут быть записаны в

виде [41]

$$\begin{aligned}\dot{\mathbf{x}}(t) &= \mathbf{G}(\mathbf{x}(t), \mathbf{g}_d), \\ \dot{\mathbf{u}}(t) &= \mathbf{H}(\mathbf{u}(t), \mathbf{g}_r) + \varepsilon \mathbf{A}(\mathbf{x}(t) - \mathbf{u}(t) + D\xi(t)),\end{aligned}\quad (1)$$

где $\mathbf{x}(t)$ и $\mathbf{u}(t)$ — векторы состояния ведущей и ведомой систем соответственно, $\xi(t)$ — шумовой сигнал, \mathbf{G} и \mathbf{H} определяют векторные поля взаимодействующих систем, \mathbf{g}_d и \mathbf{g}_r — векторы управляющих параметров, $\mathbf{A} = \{\delta_{ij}\}$ — матрица связи, $\delta_{ii} = 0$ или $\delta_{ii} = 1$, $\delta_{ij} = 0$ ($i \neq j$), ε — параметр связи, D — интенсивность шума.

Механизмы возникновения режима обобщенной синхронизации могут быть выявлены при помощи метода модифицированной системы, предложенного в наших работах [41,42]. Согласно этому подходу, ведомая система $\mathbf{u}(t)$ может быть рассмотрена как модифицированная система

$$\dot{\mathbf{u}}_m(t) = \mathbf{H}'(\mathbf{u}_m(t), \mathbf{g}_r, \varepsilon) \quad (2)$$

под внешним воздействием $\varepsilon(\mathbf{A}\mathbf{x}(t) + D\xi(t))$

$$\dot{\mathbf{u}}_m(t) = \mathbf{H}'(\mathbf{u}_m(t), \mathbf{g}_r, \varepsilon) + \varepsilon(\mathbf{A}\mathbf{x}(t) + D\xi(t)), \quad (3)$$

где $\mathbf{H}'(\mathbf{u}(t)) = \mathbf{H}(\mathbf{u}(t)) - \varepsilon \mathbf{A}\mathbf{u}(t)$. Слагаемое $\varepsilon \mathbf{A}\mathbf{u}(t)$ вносит дополнительную диссипацию в модифицированную систему (2).

Режим обобщенной синхронизации, возникающий в системе (1), может быть рассмотрен как следствие двух взаимосвязанных процессов, протекающих одновременно: увеличения диссипации в модифицированной системе (2) и возрастания амплитуды внешнего (хаотического и шумового) сигнала [41,42]. Увеличение диссипации в модифицированной системе (2) приводит к упрощению ее поведения и переходу от хаотических колебаний к периодическим (или к стационарному состоянию). Внешнее воздействие, наоборот, стремится усложнить поведение модифицированной системы и навязать ей свою динамику. Как было показано в [41,42], возникновение режима обобщенной синхронизации возможно только, когда собственная хаотическая динамика в ведомой системе оказывается подавленной за счет диссипации.

Таким образом, устойчивость режима обобщенной синхронизации определяется, прежде всего, свойствами модифицированной системы. Если аддитивный шум не изменяет существенно характеристик модифицированной системы (2), то он и не должен сильно влиять на порог возникновения режима обобщенной синхронизации (1).

Действительно, как упоминалось в разд. 1, анализ режима обобщенной синхронизации возможен путем расчета условных ляпуновских экспонент. Понятно, что ведомая и вспомогательная системы могут быть рассмотрены как две идентичные системы, стартующие с близких начальных условий. Вычисление производной от разности их состояний $\Delta(t) = \mathbf{v}(t) - \mathbf{u}(t)$ при наличии ($D > 0$) и отсутствии шума ($D = 0$) ввиду идентичности

детерминированных и стохастических сигналов, воздействующих на каждую из систем, приводит к одному и тому же уравнению:

$$\dot{\Delta}(t) = (\mathbf{J}\mathbf{H}(\mathbf{u}(t)) - \varepsilon \mathbf{A})\Delta(t) = \mathbf{J}\mathbf{H}'(\mathbf{u}(t))\Delta(t), \quad (4)$$

(где \mathbf{J} — матрица Якоби). Поскольку уравнение (4) может быть рассмотрено как уравнение в вариациях при вычислении условных ляпуновских экспонент, можно заключить, что старшие условные ляпуновские показатели λ_1^t (определяющие порог возникновения режима обобщенной синхронизации) будут вести себя схожим образом как в отсутствие, так и при наличии шума, пересекая порог $\lambda_1^t = 0$ при одних и тех же значениях ε , соответствующих установлению режима обобщенной синхронизации. Поэтому порог возникновения обобщенной синхронизации, как следует из (4), не должен зависеть от интенсивности шума, а сам тип синхронного поведения должен обладать значительной устойчивостью к шумам. Тем не менее следует обратить внимание на то, что вектор состояния ведомой системы $\mathbf{u}(t)$ в (4) все-таки зависит от случайного сигнала ξ , и соответственно шум большой интенсивности D может изменять свойства модифицированной системы, что, в конечном итоге, может привести к изменению границы возникновения режима обобщенной синхронизации.

Справедливость теоретических рассуждений подтверждается результатами численного моделирования и физического эксперимента. Как показывают проведенные исследования, режим обобщенной синхронизации обладает структурной устойчивостью к шумам как в системах с малым числом степеней свободы [40], так и пространственно распределенных средах [39].

3. Способ скрытой передачи информации

Перейдем к описанию предлагаемого способа скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума. Принципиальная схема для его реализации приведена на рис. 1.

Способ скрытой передачи информации предназначен для передачи цифровых сигналов и заключается в следу-

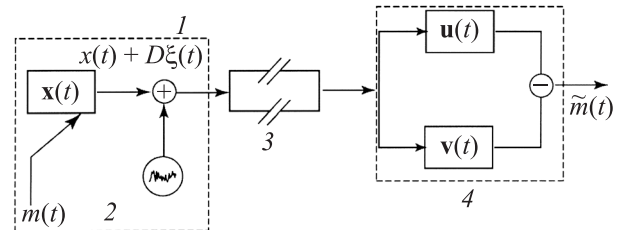


Рис. 1. Схема для реализации способа скрытой передачи информации на основе режима обобщенной хаотической синхронизации в присутствии шума (1 — передающее устройство, 2 — генератор шума, 3 — канал связи, 4 — принимающее устройство).

ющем. Информационный сигнал $m(t)$ кодируется в виде бинарного кода, который используется для модуляции одного или нескольких управляющих параметров передающего генератора хаоса $\mathbf{x}(t)$. Модуляция параметров должна осуществляться таким образом, чтобы характеристики передаваемого сигнала изменялись незначительно, но при этом оставалась возможность возникновения/разрушения режима обобщенной синхронизации между генераторами передающего и принимающего устройств в зависимости от передаваемого бинарного бита. Для этого расположение границы обобщенной синхронизации на плоскости „параметр модуляции–интенсивность связи“, как обсуждалось в разд. 1, должно обладать принципиальной особенностью: при малом изменении соответствующего параметра порог возникновения синхронного режима должен изменяться достаточно резко.

Для обеспечения дополнительной маскировки информационного сигнала и изменения характеристик передаваемого сигнала используется генератор шума. Сигнал, генерируемый передающей системой, примешивается в сумматоре к шумовому сигналу и далее передается по каналу связи. Здесь он также подвергается влиянию шумов и искажений, неизбежно присутствующих в реальных устройствах. Принимающее устройство находится на другой стороне канала связи. Оно представляет собой два идентичных между собой хаотических генератора $\mathbf{u}(t)$ и $\mathbf{v}(t)$, способных находиться в режиме обобщенной синхронизации с передающим. Принцип работы принимающего устройства основан на диагностике режима обобщенной синхронизации при помощи метода вспомогательной системы. Сигнал с канала связи поступает на идентичные генераторы принимающего устройства. Полученные на выходе сигналы проходят через вычитающее устройство, затем детектируется восстановленный полезный сигнал $\tilde{m}(t)$.

Как видно из проведенного рассмотрения, способ скрытой передачи информации является высококонфиденциальным: шум скрывает следы модуляции управляющего параметра передающего генератора информационным сигналом, а следовательно, ликвидирует возможность дешифровки исходного информационного сообщения третьей стороной. Кроме того, этот метод обладает двумя другими достоинствами по сравнению с известными аналогами: простотой технической реализации (в связи с отсутствием идентичных генераторов на различных сторонах канала связи) и высокой устойчивостью к шумам.

4. Эффективность способа скрытой передачи информации

Чтобы проверить эффективность способа скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума, проведем численное моделирование схемы (рис. 1). В качестве генераторов

передающего и принимающего устройств, следуя [21], выберем однонаправленно связанные системы Ресслера. В этом случае передающий генератор описывается следующей системой дифференциальных уравнений:

$$\begin{aligned}\dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c),\end{aligned}\quad (5)$$

где $\mathbf{x}(t) = (x_1, x_2, x_3)^T$ — вектор состояния передающего генератора, $a = 0.15$, $p = 0.2$ и $c = 10$ — управляющие 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 $\omega_x = 0.91$ на протяжении всего интервала. При передаче бинарного бита 0 параметр ω_x принимает случайное значение из диапазона $\omega_x \in [0.9, 0.91)$, т.е. расстройка параметров оказывается чрезвычайно малой — порядка 1.1%. Выбор значений параметра ω_x обусловлен характером расположения границы обобщенной синхронизации, изученным в [38]. Отметим, что параметр ω_x может принимать достаточно произвольные значения: необходимым условием является лишь чередование областей с асинхронной динамикой и режимом обобщенной синхронизации.

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

$$\begin{aligned}\dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \\ \dot{u}_2 &= \omega_u u_1 + a u_2, \\ \dot{u}_3 &= p + u_3(u_1 - c).\end{aligned}\quad (6)$$

Здесь $\mathbf{u}(t) = (u_1, u_2, u_3)^T$ — вектор состояния первого принимающего генератора. Пусть $\mathbf{v}(t) = (v_1, v_2, v_3)^T$, также удовлетворяющий (6), будет вектором состояния второго принимающего генератора (см. рис. 1). Управляющие параметры a , p и c выберем идентичными последним для передающего генератора. Управляющий параметр $\omega_u = 0.95$, характеризующий собственную частоту принимающих генераторов, выберем неизменным на протяжении всего времени передачи сигнала.

Сигнал, генерируемый передающим устройством, суммируется со стохастическим, производимым генератором шума, и далее передается по каналу связи. В исследуемой модели (5)–(6) это реализуется путем связи принимающего генератора с передающими, т.е. добавлением компоненты $\varepsilon s(t)$ в первое уравнение системы (6), где $s(t) = x_1(t) + D\xi(t)$ — сигнал в канале связи. Слагаемое $D\xi(t)$ моделирует шумы, как производимые генератором шума, так и появляющиеся в канале связи, ξ представляется как δ -коррелированный гауссов шум ($\langle \xi(t)\xi(t') \rangle = \delta(t - t')$) с нулевым средним. Параметр D определяет суммарную интенсивность шума.

Интенсивность связи между передающим и принимающим генераторами характеризуется параметром $\varepsilon = 0.14$, при котором, как известно [38], в отсутствие шумов ($D = 0$) режим обобщенной синхронизации в системе (5)–(6) имеет место при $\omega_x < 0.91$ и $\omega_x > 0.97$, в то время как для $\omega_x \in [0.91; 0.97]$ обобщенной синхронизации не наблюдается. Ввиду устойчивости режима обобщенной синхронизации к шумам граница возникновения режима обобщенной синхронизации ведет себя подобным образом и при наличии шума [40,43].

Вычитающее устройство выполняет операцию $(u_1 - v_1)^2$. Тогда после прохождения через него, согласно методу вспомогательной системы, должны наблюдаться отсутствие колебаний для $\omega_x \in [0.9; 0.91]$ и наличие хаотических колебаний для $\omega_x = 0.91$. Восстановленный сигнал будет представлять собой последовательность областей с различными типами поведения.

В качестве примера рассмотрим передачу информационного сигнала, представленного простой последовательностью бинарных битов 0/1, по каналу связи вышеописанным способом. Исходная цифровая последовательность приведена на рис. 2, *a*. Для интегрирования

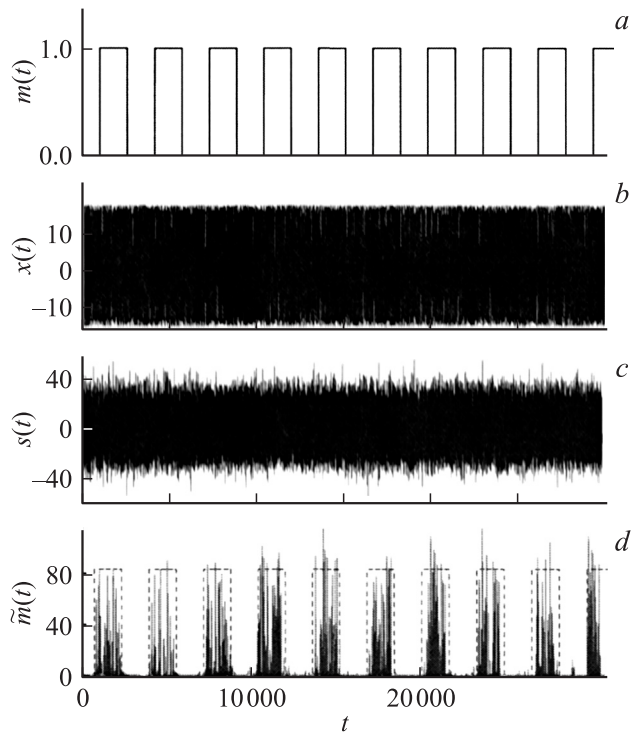


Рис. 2. Иллюстрация численной реализации способа скрытой передачи информации на основе обобщенной хаотической синхронизации в присутствии шума ($D = 10$): информационный сигнал $m(t)$, представленный простой последовательностью бинарных битов 0/1 (*a*), сигнал $x(t)$, генерируемый передающей хаотической системой (*b*), сигнал $s(t)$, передаваемый по каналу связи (*c*), восстановленный сигнал $\hat{m}(t)$ (*d*), сплошная линия. На рисунке представлен также детерминированный информационный сигнал (пунктир) после пропускания через фильтр нижних частот.

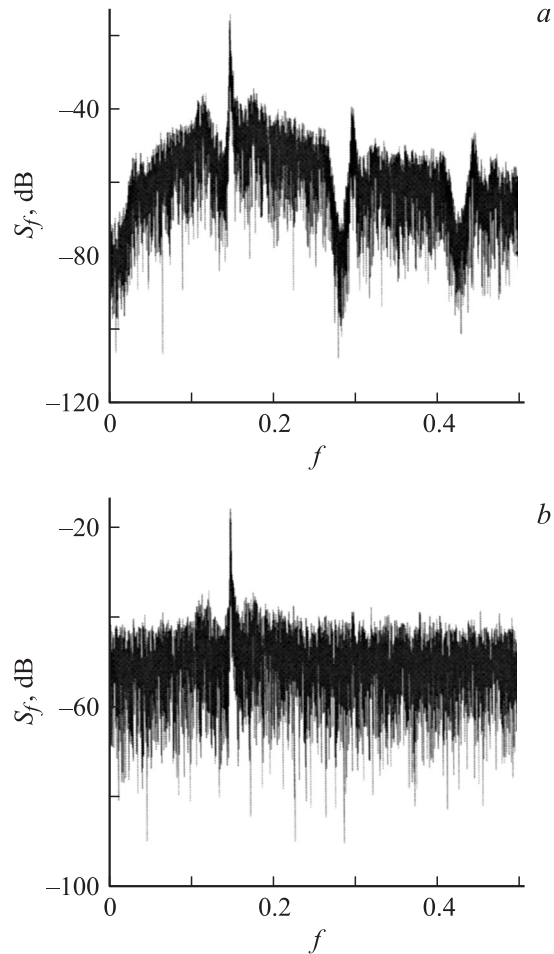


Рис. 3. Спектры мощности сигнала $x(t)$, генерируемого передающей хаотической системой (*a*), и сигнала $s(t)$, передаваемого по каналу связи (*b*).

стохастического уравнения (6) воспользуемся методом Рунге–Кутты 4-го порядка, адаптированным для решения стохастических дифференциальных уравнений [44], с шагом дискретизации по времени $h = 0.001$.

Работоспособность предложенного способа скрытой передачи информации при наличии шума иллюстрирует рис. 2. Выберем интенсивность шума $D = 10$ (в этом случае мощность шума превышает мощность передаваемого сигнала примерно в два раза). Как видно из рис. 2, *b*, модуляция управляющего параметра ω_x практически не изменяет характеристики сигнала, производимого передающим генератором хаоса. Более того, шум достаточно большой интенсивности еще больше искажает передаваемый сигнал (см. рис. 2, *c*). Спектр мощности такого сигнала, как при наличии, так и при отсутствии шума, содержит только одну четко выраженную спектральную компоненту (рис. 3). В этом случае третья сторона не имеет возможности декодировать исходное информационное сообщение без полной информации о характеристиках принимающего генератора хаоса. В то

же время качество информации, восстановленной в принимающем устройстве, является достаточно высоким.

Нетрудно заметить, что сигналы, приведенные на рис. 2, *a* (исходный информационный сигнал) и *d*, пунктир (декодированный информационный сигнал), в точности совпадают, что и свидетельствует о высоком качестве передачи информации. Аналогичная ситуация имеет место при дальнейшем увеличении интенсивности шума D (способ становится неработоспособным при отношении энергии на бит к спектральной плотности мощности шума [45,46] $E_b / N_0 = -10.01$ dB). Таким образом, в данном случае шум играет конструктивную роль для увеличения конфиденциальности передачи информации без потери качества.

5. Влияние характеристик шума на эффективность способа скрытой передачи информации и пути его возможного совершенствования

Теперь обсудим вопрос о том, какими характеристиками должен обладать стохастический сигнал, производимый генератором шума на передающей стороне канала связи, чтобы предложенный способ скрытой передачи информации был работоспособным и эффективным. В разд. 4 было показано, что способ скрытой передачи информации работает в том случае, если генератор шума характеризуется нормальным законом распределения плотности вероятности. Согласно теоретическим рассуждениям, изложенным в разд. 2, устойчивость режима обобщенной синхронизации, а следовательно и способа скрытой передачи информации, основанного на этом режиме, не должна сильно зависеть от характеристик шумового сигнала, воздействующего на ведомую систему (принимающий генератор хаоса).

Чтобы подтвердить корректность вышеприведенных рассуждений, проанализируем эффективность способа скрытой передачи информации в том случае, если генератор шума производит сигнал, характеризующийся равномерным распределением плотности вероятности. В качестве информационного сигнала выберем более сложную последовательность бинарных битов, нежели цифровой сигнал, рассмотренный в разд. 4. Результаты анализа представлены на рис. 4. Интенсивность стохастического сигнала, производимого генератором шума, как и выше, $D = 10$. Как видно из приведенного рисунка, исследуемый метод работает и в этом случае, и по восстановленному сигналу $m(t)$ исходная последовательность бинарных битов может быть легко определена.

Увеличение амплитуды стохастического сигнала и в этом случае практически не оказывает влияния на эффективность способа скрытой передачи информации. Более того, как показали проведенные расчеты, изменение характера распределения случайной величины, амплитуды, среднего и дисперсии слабо влияет на работоспособность способа. Эта особенность позволяет

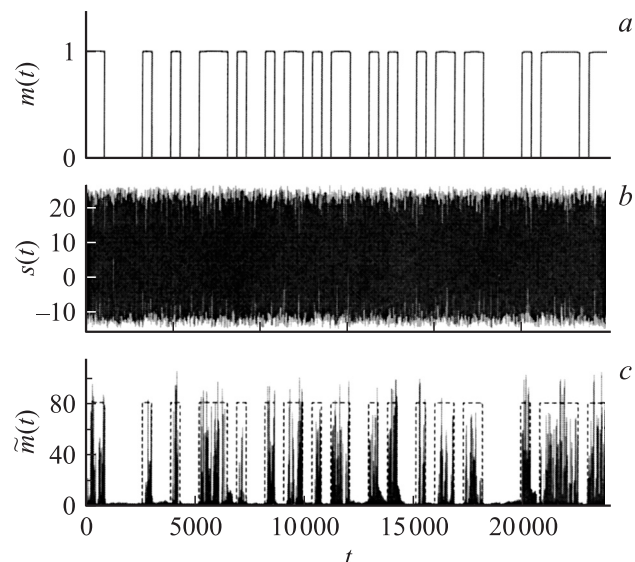


Рис. 4. Иллюстрация работоспособности метода скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума в случае, если генератор шума производит стохастический сигнал, характеризующийся равномерным распределением плотности вероятности, интенсивность стохастического сигнала $D = 10$: информационный сигнал $m(t)$, представленный последовательностью бинарных битов 0/1 (*a*), сигнал $s(t)$, передаваемый по каналу связи (*b*), восстановленный сигнал $\tilde{m}(t)$ (*c*), сплошная линия. На рисунке представлен также детектированный информационный сигнал (пунктир).

изменять характеристики сигнала, производимого генератором шума, случайным образом в течение всего времени передачи сигнала, тем самым обеспечивая в некоторых случаях создание „ложной“ модуляции и, следовательно, наталкивая третью сторону на дешифрование ложного сообщения. Передача ложного сообщения может интерпретироваться также как нескрытая передача информационного сообщения по каналу связи. В этом случае предложенный способ „расширяет“ пропускную способность канала связи, т.е. позволяет передавать сразу два информационных сообщения, содержащих полезную и ложную информацию соответственно (рис. 5). Характеристики генератора шума модулируются здесь простой последовательностью бинарных битов, являющейся в данном случае ложным сообщением с неверной информацией: если передается бинарный бит 0 — генератор шума производит сигнал с равномерным распределением плотности вероятности, в случае передачи бинарного бита 1 — коррелированный гаусов шум с нулевым средним. Интенсивность стохастических сигналов в обоих случаях $D = 10$. Возможно также модулирование характеристик шумового сигнала более сложным информационным сообщением.

Как видно из рис. 5, *b* вследствие наличия амплитудной модуляции в сигнале $s(t)$, третья сторона дешифрует простую последовательность бинарных битов,

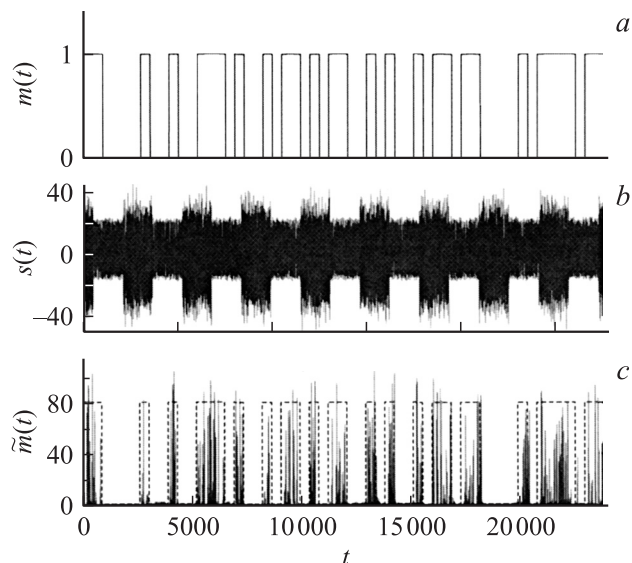


Рис. 5. Иллюстрация работоспособности метода скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума в случае, если характеристики генератора шума модулируются последовательностью бинарных битов: информационный сигнал $m(t)$, представленный последовательностью бинарных битов 0/1 (a), сигнал $s(t)$, передаваемый по каналу связи (b), восстановленный сигнал $\hat{m}(t)$ (c), сплошная линия. На рисунке представлен также детектированный информационный сигнал (пунктир).

в то время как исходное информационное сообщение по-прежнему останется для нее недоступным. В то же время на принимающей стороне канала связи изменение характера шума останется по-прежнему незаметным, а качество передачи информации будет таким же высоким, как и при изменении характеристик сигнала генератором шума с постоянными характеристиками или при отсутствии такового вообще.

Таким образом, возможно совершенствование способа скрытой передачи информации на основе обобщенной синхронизации в присутствии шума путем изменения характеристик генератора шума заведомо ложным информационным сообщением, что повышает конфиденциальность передачи информации предложенным способом.

Заключение

В работе предложен способ скрытой передачи информации на основе режима обобщенной синхронизации в присутствии шума, позволяющий преодолеть сразу три недостатка, свойственных известным схемам и устройствам аналогичного назначения. Этот способ позволяет скрыть следы модуляции управляющих параметров информационным сигналом, обладает высокой устойчивостью к шумам и позволяет избавиться от требования идентичности генераторов на разных сторонах канала связи. Эффективность метода проиллюстрирована на примере использования систем Ресслера в качестве

генераторов передающего и принимающего устройств, но в то же время способ остается работоспособным и в случае использования других генераторов в передающем и принимающем устройствах (например, генераторов Рулькова и Чуа „TORUS“, генераторов с запаздыванием, а также систем СВЧ-диапазона, способных демонстрировать режим обобщенной синхронизации).

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты № 08-02-00102, 09-02-92421), Президентской программы поддержки ведущих научных школ РФ (проект НШ-355.2008.2), НОЦ „Нелинейная динамика и биофизика“ при СГУ (CRDF REC-006), аналитической ведомственной целевой программы „Развитие научного потенциала высшей школы“, ФЦП „Научные и научно-педагогические кадры инновационной России“ на 2009–2013 гг., а также ФНП „Династия“ и Международного центра фундаментальной физики (Москва).

Список литературы

- [1] Roy R. // Nature. 2005. Vol. 438. P. 298–299.
- [2] Jaeger H, Haas H. // Science. 2008. Vol. 304. P. 78–80.
- [3] Parlitz U, Chua L.O., Kocarev L., Halle K.S., Shang A. // Int. J. Bifurcation and Chaos. 1992. Vol. 2(4). P. 973–977.
- [4] Cuomo M.K., Oppenheim A.V., Strogatz S.H. // IEEE Trans. Circuits and Syst. 1993. Vol. 40(10). P. 626.
- [5] Murali K., Lakshmanan M. // Phys. Rev. E. 1993. Vol. 48(3). P. R1624–R1626.
- [6] Fischer L., Liu Y., Davis P. // Phys. Rev. A. 2000. Vol. 62. P. 011 801(R).
- [7] Terry J., Van Wiggeren G. // Chaos, Solitons and Fractals. 2001. Vol. 12. P. 145–152.
- [8] Rulkov N.F., Vorontsov M.A., Illing L. // Phys. Rev. Lett. 2002. Vol. 89(27). P. 277 905.
- [9] Lucamarini M., Mancini S. // Phys. Rev. Lett. 2005. Vol. 94. P. 140 501.
- [10] Yuan Z.L., Shields A.J. // Phys. Rev. Lett. 2005. Vol. 94. P. 048 901.
- [11] Li Q.S., Liu Y. // Phys. Rev. E. 2006. Vol. 73. P. 016 218.
- [12] Rohde G.K., Nichols J.M., Bucholtz F. // Chaos. 2008. Vol. 18. P. 013 114.
- [13] Materassi D., Basso M. // Int. J. of Bifurcation and Chaos. 2008. Vol. 18(2). P. 567–575.
- [14] Boccaletti S., Farini A., Arecchi F.T. // Phys. Rev. E. 1997. Vol. 55(5). P. 4979–4981.
- [15] Eguia M.C., Rabinovich M.I., Abarbanel H.D.I. // Phys. Rev. E. 2000. Vol. 62(5). P. 7111–7122.
- [16] Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. М.: Физматлит, 2002.
- [17] Xiang-Jun W. // Chaos. 2006. Vol. 16. P. 043 118.
- [18] Cruz-Hernandez C., Romero-Haros N. // Communications in Nonlinear Science and Numerical Simulation. 2008. Vol. 13. P. 645–659.
- [19] Annovazzi-Lodi V., Benedetti M., Merlo S., Norgia M., Provinzano B. // IEEE Photonics Technology Letters. 2005. Vol. 17(9). P. 1995–1997.

- [20] Yang T. // Int. J. of Computational Cognition. 2004. Vol. 2(2). P. 81–130.
- [21] Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. // Изв. РАН Сер. Физ. 2008. Т. 72(1). С. 143–147.
- [22] Murali K., Lakshmanan M. // Phys. Lett. A. 1998. Vol. 241. P. 303–310.
- [23] Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. // Первая Милля. 2008. Т. 4(1). С. 14–16.
- [24] Dedieu H., Kennedy M.P., Hasler M. // IEEE Trans. on Circ. Sys. 1993. Vol. I. N 40. P. 653–642.
- [25] Dmitriev B.S., Hramov A.E., Koronovskii A.A., Starodubov A.V., Trubetskov D.I., Zharkov Y.D. // Phys. Rev. Lett. 2009. Vol. 102(7). P. 074 101.
- [26] Rulkov N.F., Sushchik M.M., Tsimring L.S., Abarbanel H.D.I. // Phys. Rev. E. 1995. Vol. 51(2). P. 980–994.
- [27] Pyragas K. // Phys. Rev. E. 1996. Vol. 54(5). P. R4508–R4511.
- [28] Pecora L.M., Carroll T.L., Heagy J.F. // Phys. Rev. E. 1995. Vol. 52(4). P. 3420–3439.
- [29] Pecora L.M., Carroll T.L. // Phys. Rev. A. 1991. Vol. 44(4). P. 2374–2383.
- [30] Pyragas K. // Phys. Rev. E. 1997. Vol. 56(5). P. 5183–5188.
- [31] Abarbanel H.D.I., Rulkov N.F., Sushchik M.M. // Phys. Rev. E. 1996. Vol. 53(5). P. 4528–4535.
- [32] Pecora L.M., Carroll T.L. // Phys. Rev. Lett. 1990. Vol. 64(8). P. 821–824.
- [33] Rosenblum M.G., Pikovsky A.S., Kurths J. // Phys. Rev. Lett. 1996. Vol. 76(11). P. 1804–1807.
- [34] Rulko N.F. // Chaos. 1996. Vol. 6. P. 262–279.
- [35] Ponomarenko V.I., Prokhorov M.D. // Phys. Rev. E. 2002. Vol. 66(2). P. 026 215.
- [36] Prokhorov M.D., Ponomarenko V.I. // Phys. Rev. E. 2005. Vol. 72. P. 016 210.
- [37] Zheng Z., Hu G. // Phys. Rev. E. 2000. Vol. 62(6). P. 7882–7885.
- [38] Hramov A.E., Koronovskii A.A., Moskalenko O.I. // Europhys. Lett. 2005. Vol. 72(6). P. 901–907.
- [39] Короновский А.А., Попов П.В., Храмов А.Е. // ЖЭТФ. 2006. Т. 130. № 4. С. 748–764.
- [40] Moskalenko O.I., Hramov A.E., Koronovskii A.A., Ovchinnikov A. // Phys. Rev. E. (submitted.)
- [41] Короновский А.А., Москаленко О.И., Храмов А.Е. // ЖТФ. 2006. Т. 76. Вып. 2. С. 1–9.
- [42] Hramov A.E., Koronovskii A.A. // Phys. Rev. E. 2005. Vol. 71(6). P. 067 201.
- [43] Москаленко О.И. Хаотическая синхронизация (различные механизмы и применение для скрытой передачи информации). Автореф. дис. ... докт. физ.-мат. наук, 2008.
- [44] Никитин Н.Н., Первачев С.В., Разевиг В.Д. // Автоматика и телемеханика. 1975. Т. 4. С. 133–137.
- [45] Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М., 2003.
- [46] Побережский Е.С. Цифровые радиоприемные устройства. М., 1987.