Декабрь 2009 г. *Том 179, № 12*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

ОБЗОРЫ АКТУАЛЬНЫХ ПРОБЛЕМ

О применении хаотической синхронизации для скрытой передачи информации

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

Представлен обзор результатов по применению хаотической синхронизации для скрытой передачи информации. Рассмотрен ряд способов и устройств для скрытой передачи данных, основанных на различных типах синхронного поведения. С целью сопоставления известных методов друг с другом введены в рассмотрение и оценены различные количественные характеристики работоспособности схем. Обнаружен сверхустойчивый к шумам способ скрытой передачи информации, основанный на явлении обобщённой хаотической синхронизации. Впервые эффективность всех рассмотренных методов систематически проверена с помощью численного моделирования однонаправленно связанных хаотических систем Рёсслера, выбранных в качестве генераторов передающего и принимающего устройств. Рассмотрены принципиальные достоинства и недостатки схем передачи информации на основе синхронизации хаотических колебаний. Приведён обзор экспериментальных результатов в этой области.

PACS numbers: **05.45.–a**, 05.45.Pq, 05.45.Tp, 05.45.Vx, 05.45.Xt DOI: 10.3367/UFNr.0179.200912c.1281

Содержание

А.А. Короновский, О.И. Москаленко, А.Е. Храмов. Саратовский государственный университет им. Н.Г. Чернышевского, факультет нелинейных процессов
ул. Астраханская 83, 410012 Саратов, Российская Федерация
Тел. (8452) 51-21-11, (8452) 51-42-94
Факс (8452) 52-38-64, (8452) 52-38-64
E-mail: moskalenko@nonlin.sgu.ru, aeh@nonlin.sgu.ru, hramov@gmail.com

Статья поступила 27 февраля 2009 г., после доработки 10 августа 2009 г.

1. Введение

Синхронизация автоколебательных процессов представляет собой одно из фундаментальных нелинейных явлений, которое в течение уже нескольких столетий со времён Гюйгенса (впервые описавшего это явление на примере связанных механических систем (маятниковых часов) [1]) привлекает пристальное внимание исследователей [2–16]. В последние десятилетия центр исследований в этой области смещается к исследованию синхронизации хаотических автоколебаний, что обусловлено большим интересом в нелинейной физике к проблеме детерминированного хаоса и различным приложениям теории хаоса [12, 13, 17–23]. Поэтому изучение хаотической синхронизации стало естественным развитием теории динамического хаоса, что обусловлено как большим фундаментальным значением исследования хаотической синхронизации [11, 13, 14], так и её широкими практическими приложениями, например, при скрытой передаче информации [24–35], в биологических [36–43], физиоло-

гических [44 – 54] и химических задачах [55 – 59], при управлении хаосом [60 – 66], в том числе, в системах сверхвысокочастотной (СВЧ) электроники [67 – 70] и т.д.

В последнее время внимание исследователей всё более привлекают не только радиофизические модели и системы, для которых были получены основные результаты в этой области (см. обзоры [11, 71]), но и системы живой природы [46, 72, 73] (в частности, воздействие внешнего стимула на электроэнцефалограммы мозга [74, 75], взаимодействие ритмов респираторной и сердечно-сосудистой системы [45, 47, 53], синхронизация динамики нейронных ансамблей различных участков головного мозга человека больного эпилепсией [76, 77] и др.). Данные приложения весьма важны и находят всё большее применение в физиологии и медицине, обработке экспериментальных данных. Однако возможности использования хаотической синхронизации не ограничиваются физиологическими и медицинскими приложениями. Одним из интересных, важных и бурно развивающихся направлений является применение хаотической синхронизации в телекоммуникационных задачах, в первую очередь, при создании систем скрытой передачи информации. В то же время обзорных работ по применению хаотической синхронизации в информационно-телекоммуникационных системах очень мало. В качестве исключения можно отметить работы [23, 78], однако сведения, содержащиеся в них, ввиду быстрого развития этого направления, оказываются далеко не полными. Так, только за последние десять лет по данным *ISI Web of Knowledge* количество публикаций по данной тематике возросло более чем в 50 раз (в частности, появились работы [79 – 92]). При этом индекс цитирования работ в указанной области возрастает практически экспоненциально (рис. 1). Наконец, важно отметить, что в последние годы произошёл переход от теоретического рассмотрения проблемы к созданию практических образцов, позволивших осуществить передачу информации на основе хаотической синхронизации на несколько десятков километров с использованием ранее созданных систем телекоммуникации [93]. Всё вышесказанное свидетельствует о важности и актуальности рассматриваемого направления и необходимости обзора по данной тематике, который бы суммировал, обобщал и, что не менее важно, позволял сравнить результаты, полученные в этом направлении.

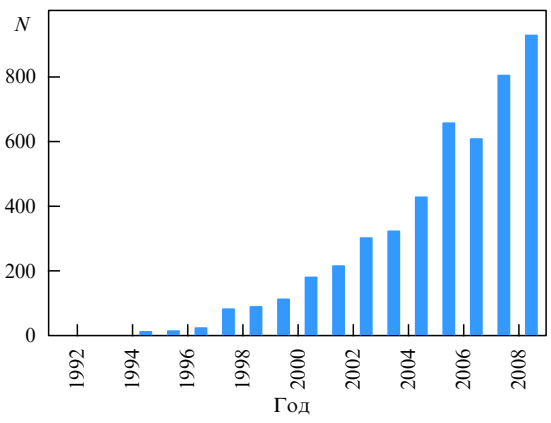

Рис. 1. Количество цитирований в центральных реферируемых научных журналах публикаций, посвящённых использованию хаотической синхронизации в информационно-телекоммуникационных системах, по годам (по данным *ISI Web of Knowledge* на декабрь 2008 г.).

Большинство способов скрытой передачи информации с использованием синхронизации хаоса основано, в первую очередь, на режиме полной хаотической синхронизации [94, 95], что влечёт за собой требование к высокой степени идентичности генераторов, располагающихся на различных сторонах канала связи. В связи с открытием и интенсивным изучением других типов синхронного поведения связанных хаотических систем, таких как фазовая синхронизация [96], обобщённая синхронизация [97], синхронизация с запаздыванием [98], синхронизация, индуцированная шумом [99 – 104], совершенствование методов скрытой передачи данных на их основе стало одной из важных задач исследований в области создания информационно-телекоммуникационных систем на основе динамического хаоса.

Структура обзора следующая. Раздел 2 посвящён краткому описанию различных типов синхронного поведения связанных хаотических систем, на основе которых могут быть созданы схемы скрытой передачи информации. Прежде всего — это режимы полной, фазовой и обобщённой хаотической синхронизации. В разделе 3 проведено рассмотрение методов скрытой передачи данных на основе полной синхронизации, в разделе 4 обсуждается применение других вышеназванных типов синхронного поведения для скрытой передачи данных, а также рассматриваются методы передачи информации, использующие несколько типов синхронного поведения одновременно. В разделе 5 описан сверхустойчивый к шумам способ скрытой передачи данных, лишённый ряда недостатков, присущих всем ранее известным схемам и устройствам аналогичного назначения. В разделе 6 проводится сравнительный анализ работоспособности способов скрытой передачи данных, рассмотренных в разделах 3 – 5: на основе оценки количественных характеристик работоспособности этих схем выявляются принципиальные достоинства сверхустойчивой схемы в сравнении с другими схемами. Раздел 7 посвящён описанию результатов экспериментальной реализации способов скрытой передачи информации на основе хаотической синхронизации в радиодиапазоне, микроволновом и оптическом диапазонах. В разделе 8 представлены итоговое обсуждение и выводы.

Следует отметить, что часть способов скрытой передачи информации, рассмотренных в настоящем обзоре, пригодна для передачи как аналоговых, так и цифровых сигналов. Однако часть методов может быть применена только для передачи цифровых сигналов. С целью достижения общности и возможности сопоставления всех рассмотренных способов нами использовались в качестве информационных только цифровые сигналы [1]. Отметим также, что строго в соответствии с названием обзора мы рассматриваем только способы передачи информации с использованием явления хаотической синхронизации. Эти способы относятся к стеганографическим методам защиты информации, которые, в отличие от криптографических, скрывают не саму информацию, а факт её передачи.

[1] Отметим, что аналоговые сигналы могут быть преобразованы в цифровые, что делает подобное рассмотрение обоснованным и не приводит к потере его общности.

Принципиальным достоинством методов на основе хаотической синхронизации по сравнению с традиционными методами (методом LSB (Least Significant Bit), эхометодами, методами расширенного спектра и др.) являются значительное повышение устойчивости к шумам и искажениям в канале связи, а также увеличение скорости передачи информации [105]. Кроме того, использование именно хаотической синхронизации чрезвычайно важно для повышения конфиденциальности передачи данных. Известны и другие подходы к созданию способов скрытой передачи информации с использованием динамического хаоса, рассмотрению которых во многом посвящена монография А.С. Дмитриева и А.И. Панаса [23], ставшая сейчас уже классической и активно цитируемой. Это прежде всего прямохаотические системы связи, принцип работы которых заключается в непосредственной генерации несущих информацию хаотических колебаний, в том числе в СВЧ-диапазоне, и модуляции этих колебаний информационным сигналом. Такие методы являются сравнительно легко реализуемыми и позволяют достичь скорости передачи данных до 200 Мб $с^{-1}$. Однако конфиденциальность схем на основе хаотической синхронизации является значительно более высокой.

Несмотря на многообразие работ, посвящённых использованию хаотической синхронизации в информационно-телекоммуникационных системах (см., например, [106–110]), можно с достаточно высокой степенью уверенности утверждать, что в основе большинства способов передачи информации лежат самые первые, достаточно хорошо известные способы скрытой передачи данных, использующие явление полной хаотической синхронизации. Впервые один из таких методов был предложен в работе [95]. Эти методы легли в основу последующих, более совершенных методов, которые, тем не менее, сохраняют ряд недостатков, свойственных их предшественникам. Поэтому в данном обзоре наряду с самыми ранними методами будут рассмотрены те методы, которые в наибольшей степени отличаются от них.

Одной из важных проблем, с точки зрения передачи информации, является влияние шумов и искажений сигналов на работоспособность схем передачи информации. Известно, что шумы практически всегда оказывают воздействие на динамику систем, причём это воздействие может приводить к существенным изменениям в поведении систем [111–122], что применительно к схемам передачи информации, основанным на явлении хаотической синхронизации, может отрицательно сказываться на их работоспособности. Нелинейные искажения также могут приводить к снижению работоспособности таких схем [23]. Между тем рассмотрение схем передачи информации, основанных на использовании режимов явления хаотической синхронизации, в подавляющем большинстве случаев проводится в предположении отсутствия шумов и искажений, что оставляет ряд важнейших вопросов о возможности практического применения этих схем и их эффективности открытыми. В настоящем обзоре эти вопросы рассмотрены достаточно подробно (см. раздел 6).

2. Основные типы хаотической синхронизации связанных динамических систем

Как упоминалось во введении, основными типами хаотической синхронизации, лежащими в основе современных систем связи, являются режимы полной, фазовой и обобщённой синхронизации. Для создания целостной картины кратко остановимся на описании этих типов синхронного поведения.

Режим *полной синхронизации* [94, 95] означает точное совпадение векторов состояния взаимодействующих (однонаправленно или взаимно связанных) систем $\mathbf{x}(t) \equiv \mathbf{u}(t)$, и, следовательно, этот режим возможен лишь в случае их идентичности по управляющим параметрам. Если управляющие параметры слегка различаются, возможно возникновение режима *синхронизации с запаздыванием* [98, 123], в котором взаимодействующие системы демонстрируют близкие к идентичным, но сдвинутые на некоторый временной интервал τ колебания, т.е. $\mathbf{x}(t) \approx \mathbf{u}(t+\tau)$. С увеличением силы связи между слегка расстроенными осцилляторами, временной сдвиг τ стремится к нулю, а режим синхронизации с запаздыванием — к режиму полной хаотической синхронизации. Для диагностики режима полной синхронизации достаточно часто проводят непосредственное сравнение векторов состояний взаимодействующих систем $\mathbf{x}(t)$ и $\mathbf{u}(\mathbf{t})$, рассчитывая ошибку синхронизации [124]:

$$\langle e \rangle = \int_0^\infty \|\mathbf{x}(t) - \mathbf{u}(t)\| \, \mathrm{d}t \,. \qquad (1)$$

Следует отметить, что в литературе достаточно часто, наряду с полной хаотической синхронизацией, рассматривают синхронизацию хаотических систем, полученных в результате декомпозиции [94] автоколебательной системы, или "хаотический синхронный отклик" [125]. В результате декомпозиции автоколебательная система приобретает вид кольцевой структуры, в которой подсистемы образуют единое кольцо обратной связи. На следующем шаге используются две идентичные системы, полученные в результате одинаковой декомпозиции, одну из которых оставляют в первоначальном виде (ведущая автоколебательная, или активная, система), а в другой кольцо обратной связи разрывают (ведомая, или пассивная, система). Если сигнал с выхода одной из подсистем ведущей системы подать на вход другой подсистемы ведомой системы, то при определённых условиях разность между входным и выходным сигналами ведомой системы будет стремиться к нулю, т.е. возникнет полная синхронизация между состояниями ведущей и ведомой систем [23].

Обобщённая синхронизация, которая вводится в рассмотрение для системы двух однонаправленно связанных хаотических осцилляторов — ведущего $\mathbf{x}(t)$ и ведомого $\mathbf{u}(t)$, означает, что после завершения переходного процесса устанавливается функциональная зависимость между их состояниями, т.е. $\mathbf{u}(t) = F[\mathbf{x}(t)]$ [97]. При этом вид зависимости $F[\cdot]$ может быть достаточно сложным, а процедура её нахождения весьма нетривиальной [126].

Предложено несколько методов для диагностирования режима обобщённой синхронизации между хаотическими осцилляторами, такие как метод ближайших соседей [97, 127], метод расчёта условных ляпуновских экспонент [95, 128] и часто используемый и относительно легко осуществимый на практике метод вспомогательной системы [129].

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 начальных условий ведомой системы $\mathbf{u}(t_0)$, однако лежащими в бассейне притяжения того же аттрактора (на практике это обозначает небольшую расстройку начальных условий, которая реализуется автоматически из-за наличия флуктуаций). При отсутствии режима обобщённой синхронизации между взаимодействующими системами векторы состояния ведомой $\mathbf{u}(t)$ и вспомогательной $\mathbf{v}(t)$ систем принадлежат одному и тому же хаотическому аттрактору, но являются различными. В том случае, когда имеет место режим обобщённой синхронизации, после завершения переходного процесса состояния ведомой и вспомогательной систем должны стать идентичными, $\mathbf{u}(t) \equiv \mathbf{v}(t)$, в силу выполнения соотношений $\mathbf{u}(t) = F[\mathbf{x}(t)]$ и соответственно $\mathbf{v}(t) = F[\mathbf{x}(t)]$. Таким образом, эквивалентность состояний ведомой и вспомогательной систем после переходного процесса является критерием наличия обобщённой синхронизации между ведущим и ведомым осцилляторами.

Анализ режима обобщённой синхронизации может быть проведён также с помощью вычисления условных ляпуновских экспонент [95, 128]. Если размерности фазовых пространств ведущей (drive system) и ведомой (response system) систем соответственно равны N_d и N_r, то поведение однонаправленно связанных хаотических осцилляторов может быть охарактеризовано с помощью спектра ляпуновских показателей $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{N_\mathrm{d}+N_\mathrm{r}}$. Ввиду независимости поведения ведущей системы от состояния ведомого осциллятора спектр ляпуновских показателей может быть разделен на две части: ляпуновские показатели ведущей системы $\lambda_1^\mathrm{d} \geqslant \ldots \geqslant \lambda_{N_\mathrm{d}}^\mathrm{d}$ и условные ляпуновские показатели $\lambda_1^\mathrm{r} \geqslant \ldots \geqslant \lambda_{N_\mathrm{r}}^\mathrm{r}$. Критерием существования обобщённой синхронизации в однонаправленно связанных динамических системах [95, 126] является отрицательность старшего условного ляпуновского показателя λ_1^r. Отметим, что для однонаправленно связанных хаотических осцилляторов режимы полной синхронизации и синхронизации с запаздыванием являются частными случаями режима обобщённой синхронизации [126].

Фазовая синхронизация [96, 130] означает, что происходит захват фаз хаотических сигналов, в то время как амплитуды этих сигналов остаются несвязанными между собой и выглядят хаотическими. В основе концепции хаотической фазовой синхронизации лежит понятие мгновенной фазы $\phi(t)$ хаотического сигнала [96, 130–132]. Следует отметить, что не существует универсального способа введения фазы хаотического сигнала, который бы давал корректные результаты для любых динамических систем. Так, существует несколько способов введения фазы, подходящих для систем с достаточно простой топологией хаотического аттрактора, которые в литературе называют "системами с хорошо определённой фазой" или "системами с фазово-когерентным аттрактором" [13, 133]. Хаотический аттрактор таких систем должен быть таким, чтобы проекция фазовой траектории на некоторую плоскость состояний (x, y) всё время вращалась вокруг некоторого центра, не пересекая и не огибая его. Тогда мгновенная фаза $\phi(t)$ хаотического сигнала может быть введена в рассмотрение одним из следующих способов: как угол в полярной системе координат [98, 134], с помощью преобразования Гильберта временно́й реализации сигнала [96, 131] или с использованием поверхности сечения Пуанкаре [96, 131]. Однако для систем с плохо определённой фазой (см., например, [133, 135]) эти методы не работают [136]. Тем не менее в ряде случаев фазовая синхронизация подобных систем может быть выявлена с помощью косвенных наблюдений [134, 137] и измерений [138, 139].

Фазовая синхронизация возникает в том случае, когда разность мгновенных фаз хаотических сигналов $\mathbf{x}_{1,2}(t)$, введённая одним из вышеперечисленных способов, является ограниченной во времени:

$$\left|\phi_1(t) - \phi_2(t)\right| < \mathrm{const}\,. \qquad (2)$$

Отметим, что понятие "фазовая синхронизация" может быть обобщено введением в рассмотрение множества временны́х масштабов s и ассоциированных с ними фаз $\phi_s(t)$ хаотического сигнала с помощью непрерывного вейвлетного преобразования с комплексным базисом [140, 141]. Если существует диапазон (или набор диапазонов) временны́х масштабов $s_\mathrm{m} < s < s_\mathrm{b}$, для каждого из которых выполняется условие захвата фаз, аналогичное (2), и доля энергии вейвлетного спектра, приходящейся на этот диапазон, отлична от нуля, то временны́е масштабы s оказываются синхронизованными, а хаотические осцилляторы находятся в режиме синхронизации временны́х масштабов. Если хотя бы один временной масштаб оказывается синхронизованным, то в некоторых случаях (см., например, [142]) можно говорить о наличии фазовой синхронизации. Однако в случае систем с фазово-некогерентным аттрактором, в которых фазовую синхронизацию диагностировать традиционными методами не представляется возможным, говорят о возникновении *синхронизации временных масштабов* [69, 77, 140, 143].

Следует также отметить, что синхронизация временны́х масштабов позволяет рассматривать с единых позиций все вышеописанные типы хаотической синхронизации. Характер синхронного режима при этом определяется лишь диапазоном синхронизованных временны́х масштабов [140, 141, 144].

3. Способы скрытой передачи информации, основанные на явлении полной хаотической синхронизации

Перейдём к рассмотрению способов скрытой передачи информации на основе хаотической синхронизации. Начнём с рассмотрения режима полной синхронизации, поскольку большинство известных способов и устройств основанно именно на этом типе синхронного поведения.

Использование полной хаотической синхронизации для скрытой передачи информации подразумевает наличие, как минимум, двух однонаправленно связанных идентичных хаотических генераторов. Предложено достаточно много таких способов скрытой передачи данных. Это, в первую очередь, хаотическая маскировка [25], переключение хаотических режимов [145], нелинейное подмешивание информационного сигнала к хаотическому [146], модулирование управляющих параметров передающего генератора полезным цифровым сигналом [147] и др. На основе этих методов было предложено множество способов скрытой передачи данных. Поэтому рассмотрение основных принципов работы таких схем является очень важным. Остановимся на них более подробно.

3.1. Хаотическая маскировка

Хаотическая маскировка — один из первых и наиболее простых способов скрытой передачи данных [25]. Принципиальная схема реализации этого способа приведена на рис. 2. На передающей стороне информационный сигнал $m(t)$ подмешивается в сумматоре к несущему сигналу, генерируемому передающей хаотической системой $\mathbf{x}(t)$, и далее передаётся по каналу связи. В приёмнике осуществляется полная хаотическая синхронизация находящегося в нём хаотического генератора $\mathbf{u}(t)$ с помощью принимаемого сигнала, в результате чего динамика принимающего генератора становится идентичной динамике передающего. Детектированный сигнал $\tilde{m}(t)$ получается после прохождения через вычитающее устройство как разность между принимаемым сигналом и синхронным откликом генератора хаоса в приёмнике (см., например, [23, 25]).

Такая схема скрытой передачи данных работает достаточно эффективно (т.е. позволяет качественно передавать информацию и детектировать её на выходе) в отсутствие шумов в канале связи в том случае, когда мощность сигнала, генерируемого передающей системой, превышает мощность информационного сигнала на 35–65 дБ [148]. Добавление шума в канал связи приводит к резкому ухудшению качества передаваемой информации, а следовательно, к высоким отношениям сигнал/шум, при которых схема остаётся работоспособной. Кроме того, введение расстройки управляющих параметров между идентичными хаотическими генераторами (находящимися на различных сторонах канала связи) также приводит к появлению на выходе дополнительных шумов десинхронизации и делает передачу информации труднореализуемой [23]. Более того, существует проблема конфиденциальности передачи информации [2]. Несмотря на низкий уровень информационного сигнала по сравнению с уровнем несущего, существуют методы и подходы, позволяющие восстановить исходный хаотический сигнал по сигналу, передаваемому по каналу связи, а следовательно, выделить полезную информацию [149–151].

Все вышеуказанные недостатки делают схемы скрытой передачи информации на основе хаотической маскировки малоприменимыми на практике.

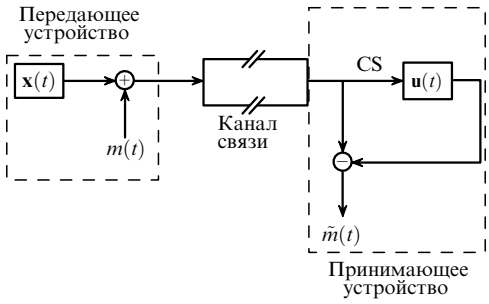

Рис. 2. Схема скрытой передачи информации с помощью хаотической маскировки (CS — полная хаотическая синхронизация).

3.2. Переключение хаотических режимов

В начале 90-х годов XX в. было предложено, помимо хаотической маскировки ещё несколько способов скрытой передачи данных, объединённых общим названием "переключение хаотических режимов" [145]. Одна из схем переключения хаотических режимов приведена на рис. 3. Передающее устройство содержит два хаотических генератора, $\mathbf{x}_1(t)$ и $\mathbf{x}_2(t)$, которые могут быть разными или одинаковыми, но с различающимися параметрами, однако в интересах конфиденциальности передачи данных предпочтительнее использовать последние; более того, сигналы, генерируемые этими системами должны иметь сходные спектральные и статистические свойства. Полезный цифровой сигнал $m(t)$, представленный последовательностью бинарных битов 0/1, используется для переключения передаваемого сигнала, т.е. сигнал, производимый первым хаотическим генератором, кодирует, например, бинарный бит 0, а сигнал от второго генератора хаоса соответственно — бинарный бит 1. Полученный таким образом сигнал передаётся по каналу связи на принимающее устройство. В зависимости от числа генераторов, находящихся на принимающей стороне канала связи, различают несколько схем скрытой передачи данных на основе переключения хаотических режимов. В схеме, представленной на рис. 3, принимающее устройство содержит один хаотический генератор $\mathbf{x}(t)$, идентичный любому из передающих, например первому. Параметры генераторов должны быть выбраны таким образом, чтобы генерируемые ими сигналы приводили к возникновению режима полной хаотической синхронизации лишь в том случае, если передаётся только бинарный бит 0 (или только бинарный бит 1). Так же как и при хаотической маскировке, восстановленный сигнал $\tilde{m}(t)$ получается после прохождения через вычитающее устройство сигнала, передаваемого по каналу связи, и синхронного отклика хаотического генератора принимающего устройства.

Другие схемы скрытой передачи информации с использованием переключения хаотических режимов, которые основаны на той же идее, отличаются от описанной выше схемы только строением и работой принимающего устройства. Например, в схеме, описанной в работе [23], принимающее устройство содержит два хаотических генератора, идентичных передающим генераторам, и, следовательно, два вычитающих устройства для детектирования полезного сигнала. В этом случае полезный сигнал диагностируется по наличию или от-

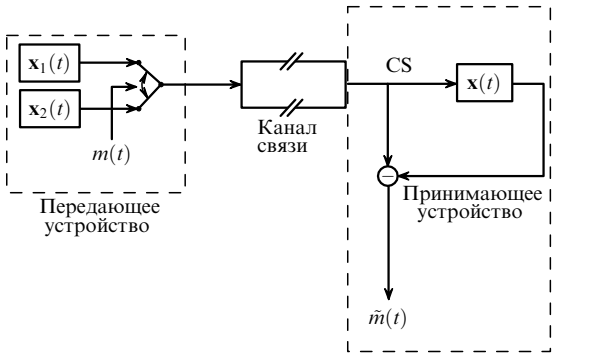

Рис. 3. Схема скрытой передачи информации на основе переключения хаотических режимов.

[2] Здесь и далее под конфиденциальностью мы понимаем отсутствие возможности детектирования третьей стороной информационного сообщения по сигналу, передаваемому по каналу связи.

сутствию хаотических колебаний в сигналах на выходе принимающего устройства.

Такие схемы передачи данных оказываются более устойчивыми к шумам в канале связи, чем схемы с хаотической маскировкой, но их устойчивость к шумам, тем не менее, остаётся весьма ограниченной. Принципиальным недостатком таких схем является возникновение переходных процессов при переключении (длительность которых может быть весьма продолжительной [152, 153]), что проявляется во временно́й задержке включения в синхронный режим принимающего генератора. Поэтому такие схемы являются достаточно медленными [23]. Кроме того, степень секретности (конфиденциальности) таких схем является довольно низкой [154].

3.3. Нелинейное подмешивание информационного сигнала к хаотическому

Усовершенствования метода хаотической маскировки были направлены на повышение секретности и конфиденциальности передачи информации. В результате было предложено несколько способов, которые можно объединить общим названием "нелинейное подмешивание информационного сигнала к хаотическому". Особенностью работы таких схем является непосредственный ввод информационного сигнала в передающую систему и его участие в формировании выходного сигнала [23, 146].

Среди схем, в которых применяются различные операции ("сложение – вычитание", "деление – умножение", "сложение по модулю с основанием 2", "преобразование напряжение – ток" и др.), наибольшее распространение сейчас получили схемы, использующие "сложение – вычитание" [125, 146]. В таких схемах информационный сигнал подмешивается к хаотическому и участвует тем самым в формировании сложного поведения системы. Наиболее простым и технически реализуемым способом обеспечения "нелинейного подмешивания" является установка на передающей стороне канала связи дополнительного хаотического генератора, идентичного первому передающему и взаимно связанного с ним. Принципиальная схема реализации такого способа скрытой передачи данных приведена на рис. 4.

Итак, передающая сторона содержит два идентичных по управляющим параметрам хаотических генератора, $\mathbf{x}_1(t)$ и $\mathbf{x}_2(t)$. Информационный сигнал $m(t)$ подмешивается к сигналу, производимому одним из генераторов передающего устройства (или к обоим сигналам одновременно). В результате прохождения по кольцу обратной связи (обеспечиваемого взаимной связью генераторов передающего устройства) сигнал претерпевает нелинейные изменения. Таким образом, по каналу связи будет передаваться сигнал, полученный в результате нелинейного подмешивания информационного сигнала к хаотическому. Принимающее устройство, как и в рассмотренных выше схемах, содержит хаотический генератор $\mathbf{x}(t)$, идентичный по управляющим параметрам передающим генераторам. Сигнал, поступающий по каналу связи на принимающее устройство, синхронизует принимающий генератор в случае передачи бинарного бита 0 (и не синхронизует при передаче бинарного бита 1). После прохождения через вычитающее устройство сигналов от передающего и принимающего генераторов детектируется восстановленный сигнал $\tilde{m}(t)$.

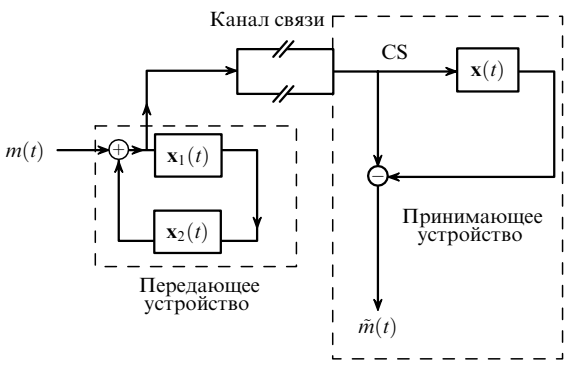

Рис. 4. Схема скрытой передачи информации посредством нелинейного подмешивания информационного сигнала к хаотическому.

Важным преимуществом таких схем перед схемами, основанными на хаотической маскировке, является возможность варьирования уровня вводимого информационного сообщения, что позволяет управлять качеством передачи информации (т.е. варьировать точность дешифрации исходного информационного сообщения принимающей стороной). Однако увеличение качества передачи информации влечёт за собой потерю её конфиденциальности, что является существенным недостатком [23]. Кроме того, такие схемы характеризуются достаточно низкой устойчивостью к шумам в канале связи и расстройке управляющих параметров изначально идентичных хаотических генераторов. Необходимость обеспечения идентичности трёх генераторов хаоса, два из которых находятся на разных сторонах канала связи, представляет собой труднорешаемую техническую задачу, а следовательно, является ещё одним недостатком такой схемы.

Кроме того, зависимость передаваемого сигнала от информационного, поскольку передающий генератор по сути является неавтономной системой, что не гарантирует формирования им именно хаотического сигнала при изменении тех или иных параметров схемы, может приводить к потере конфиденциальности.

3.4. Модулирование управляющих параметров передающего генератора информационным сигналом

Схемы на основе модулирования управляющих параметров, или адаптивные методы, — естественный этап при переходе от дискретной модуляции управляющего параметра передающего генератора в схеме с переключением хаотических режимов (см. раздел 3.2) к модуляции непрерывным сигналом [147]. При этом роль модулирующего сигнала играет информационный сигнал. Необходимым условием реализации таких схем является предварительное определение допустимого диапазона изменения параметра и нормирование модулирующего информационного сигнала. Частным случаем является использование бинарного цифрового сигнала в качестве информационного и модулирование им управляющего параметра передающего генератора. Схема скрытой передачи информации таким способом приведена на рис. 5. Принцип её работы аналогичен принципу работы схемы на основе переключения хаотических режимов, описанной в разделе 3.2. Полезный цифровой сигнал $m(t)$ модулирует один из параметров передающего генератора $\mathbf{x}(t)$ таким образом, чтобы в зависимости от передаваемого бинарного бита 0 (1) между передающим $\mathbf{x}(t)$ и принимающим $\mathbf{u}(t)$ генераторами существовал

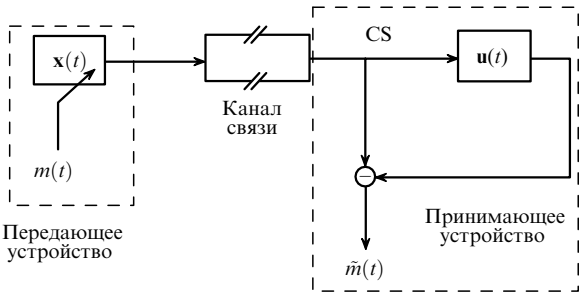

Рис. 5. Схема скрытой передачи информации путём модулирования управляющего параметра передающего генератора информационным сигналом.

(отсутствовал) режим полной хаотической синхронизации. Тогда после прохождения через вычитающее устройство сигналов передающего и принимающего устройств детектируется восстановленный сигнал $\tilde{m}(t)$. Для возможности реализации режима полной синхронизации управляющие параметры принимающего генератора должны быть выбраны идентичными управляющим параметрам передающего (точнее, одному из наборов параметров передающего генератора, отвечающему, например, бинарному биту 0).

Особенности работы, достоинства и недостатки схем, основанных на модулировании управляющих параметров, являются теми же, что и в случае схем с переключениями. Однако для рассматриваемой схемы техническая реализация несколько упрощается благодаря наличию на передающей стороне канала связи только одного генератора.

4. Использование других типов хаотической синхронизации для скрытой передачи информации

В разделе 3 мы рассмотрели основные типы схем скрытой передачи информации на основе полной хаотической синхронизации. Существуют и другие схемы, но они являются разновидностями уже известных схем и не представляют принципиального интереса, отражая скорее те или иные особенности технической реализации. Схемы, рассмотренные в разделе 3, являются простейшими системами, представляющими собой основу для использования хаотической синхронизации для скрытой передачи данных. Понятно, что ни одна из них не лишена недостатков, о которых мы упоминали в разделе 3. Дальнейшие исследования идут в направлении создания новых схем, в которых делаются попытки устранить указанные недостатки, повышая в некоторых случаях конфиденциальность схем, в некоторых — устойчивость к шумам, в некоторых — избавляясь от необходимости идентичности генераторов и обеспечивая тем самым возможность более простой технической реализации схем. Естественным путём в этом случае является переход от полной хаотической синхронизации к другим типам синхронного поведения. Следует отметить, что описание таких попыток, хотя и не часто, встречается в литературе. Например, в работе [155] предложено использовать фазовую синхронизацию для скрытой передачи данных.

Принципиальная схема реализации такого способа приведена на рис. 6. На передающей стороне канала

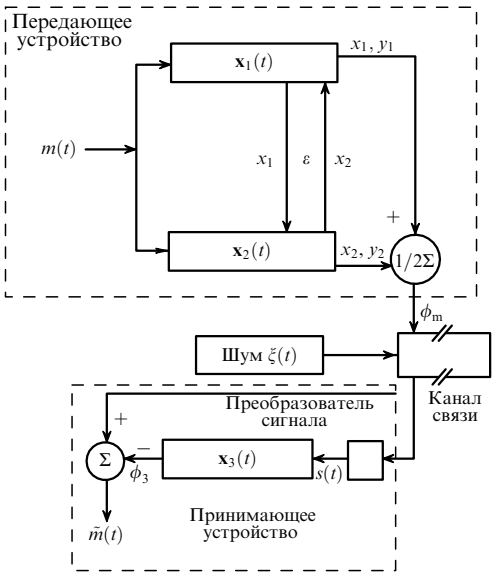

Рис. 6. Схема скрытой передачи информации на основе фазовой хаотической синхронизации.

связи находятся два идентичных взаимосвязанных хаотических генератора с 1,5 степенями свободы, характеризующихся векторами состояний $\mathbf{x}_{1,2}(t) = (x_{1,2}, y_{1,2}, z_{1,2})$. Связь между генераторами является диссипативной, что позволяет обеспечить фазовую синхронизацию при достаточно малом параметре связи ε. Один из управляющих параметров этих генераторов (один и тот же в обеих системах) модулируется полезным цифровым сигналом $m(t)$. В качестве передаваемого сигнала используется мгновенная фаза $\phi_{\mathrm{m}}(t)$ сигнала $\mathbf{x}_{\mathrm{m}}(t) = (x_{\mathrm{m}}, y_{\mathrm{m}}, z_{\mathrm{m}})$, представляющего собой среднее значение сигналов $\mathbf{x}_{1,2}(t)$, генерируемых этими системами (фаза вводится в рассмотрение на плоскости $(x_{\mathrm{m}}, y_{\mathrm{m}})$, где $x_{\mathrm{m}} = (x_1 + x_2)/2$, $y_{\mathrm{m}} = (y_1 + y_2)/2$). Полученный таким образом сигнал $\phi_{\mathrm{m}}(t)$, содержащий полезную информацию, передаётся по каналу связи (в котором он подвергается влиянию шумов) на принимающее устройство, содержащее хаотический генератор $\mathbf{x}_3(t) = (x_3, y_3, z_3)$, идентичный генераторам передающего устройства, что обеспечивает возникновение режима фазовой синхронизации между ними. В качестве сигнала, непосредственно воздействующего на принимающий генератор хаоса, используется сигнал $s(t) = \eta(r_3 \cos\phi_{\mathrm{m}} - x_3)$, где $r_3 = = (x_3 + y_3)^{1/2}$, η — амплитуда сигнала. Восстановленный сигнал $\tilde{m}(t)$ получают в результате анализа поведения разности фаз $\Delta\phi = \phi_{\mathrm{m}} - \phi_3$ соответствующих сигналов.

Как видно из приведённого описания схемы скрытой передачи информации на основе фазовой синхронизации, принцип её работы существенно отличается от принципа работы схем, рассмотренных в разделе 3. Тем не менее бóльшая часть недостатков, свойственных схемам на основе полной хаотической синхронизации, здесь остаётся. Кроме того, этот способ обладает существенными дополнительными сложностями с точки зрения технической реализации (например, экспериментальное определение фазы хаотических сигналов, создание сигнала $s(t)$, наличие дополнительных идентичных генераторов на различных сторонах канала связи). Поэтому на этой схеме мы более подробно останавливаться не будем.

Имеются также попытки использовать для скрытой передачи данных, наряду с фазовой синхронизацией, обобщённую синхронизацию [98]. Использование этого типа синхронного поведения открывает ряд новых возможностей, нехарактерных, например, для полной и фазовой синхронизации. Во-первых, обобщённая синхронизация, в отличие от полной хаотической синхронизации, может наблюдаться в совершенно разных взаимодействующих динамических системах [126], что говорит о возможности упрощения технической реализации способов скрытой передачи данных, основанных на этом типе синхронного поведения. Во-вторых, вид функциональной зависимости, устанавливаемой между состояниями взаимодействующих систем при реализации обобщённой синхронизации, может быть очень сложным, в том числе фрактальным [156], что значительно уменьшает возможность получения третьей стороной информации о характеристиках генератора на принимающей стороне канала связи по временно́й реализации передаваемого сигнала, т.е. повышает конфиденциальность. В-третьих, поведение границы обобщённой синхронизации, располагающейся на плоскости параметров "частота расстройки — интенсивность связи", является аномальным, существенно отличающимся от поведения границ всех известных типов синхронного поведения. В частности, для ряда систем порог возникновения режима обобщённой синхронизации в области относительно слабых значений расстройки частот превосходит аналогичное значение по параметру связи в области больших значений частотной расстройки примерно в два раза [157, 158]. Эта особенность позволяет обеспечить возникновение или разрушение синхронного режима при очень слабой модуляции управляющего параметра, что гарантирует эффективную модуляцию управляющего параметра для передачи информации по каналам связи. Наконец, как будет показано в разделе 5, шум практически не влияет на порог возникновения режима обобщённой синхронизации, т.е. синхронный режим возникает в однонаправленно связанных динамических системах в отсутствие и при наличии шума при близких значениях силы связи между системами (см. также [159, 160]). Поэтому можно ожидать высокой устойчивости схем на основе режима обобщённой синхронизации к шумам в каналах связи. Более того, дополнительный шум может быть использован для создания дополнительной маскировки передаваемого по каналу связи сигнала.

Тем не менее необходимо отметить, что большинство известных способов скрытой передачи информации на основе режима обобщённой синхронизации не используют в полной мере всех достоинств этого режима. Остановимся на некоторых наиболее интересных и важных из них в разделах 4.1, 4.2.

4.1. Способ скрытой передачи информации на основе обобщённой синхронизации

Одной из немногих работ, в которых используется режим обобщённой синхронизации для скрытой передачи информации, является работа [109]. Принципиальная схема реализации такого способа скрытой передачи данных приведена на рис. 7. Передающая сторона содержит два хаотических генератора, ведущий $\mathbf{x}(t)$ и ведомый $\mathbf{u}(t)$, которые могут быть неидентичными. Сигнал с ведущего генератора передаётся на ведомый, причём его интенсивность модулируется полезным

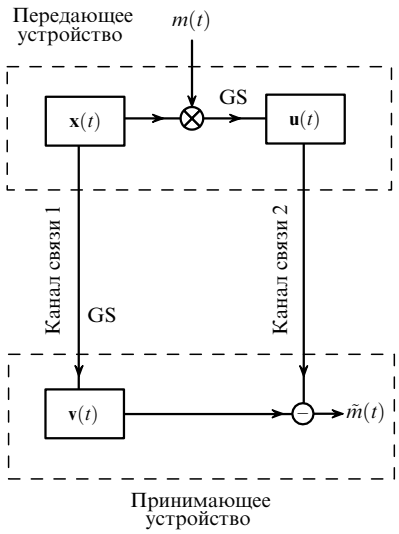

Рис. 7. Схема скрытой передачи информации с помощью обобщённой хаотической синхронизации, предложенная в работе [109] (GS — обобщённая хаотическая синхронизация).

цифровым сигналом $m(t)$ таким образом: если передаётся бинарный бит 0, то между ведущим и ведомым генераторами устанавливается режим обобщённой синхронизации, а если передаётся бинарный бит 1, то режим обобщённой синхронизации между ними разрушается. На принимающей стороне канала связи находится так называемый вспомогательный хаотический генератор $\mathbf{v}(t)$, идентичный ведомому по управляющим параметрам. Сигнал с ведущего генератора по каналу связи передаётся на вспомогательный, что обеспечивает возникновение режима обобщённой синхронизации между ними, причём интенсивность передаваемого по каналу связи сигнала должна совпадать с интенсивностью сигнала, поступающего к ведомой системе при передаче бинарного бита 0. Сигнал с ведомого генератора уже по другому каналу связи передаётся принимающей стороне. Так же как и в способах скрытой передачи данных, основанных на режиме полной хаотической синхронизации, принимающая сторона имеет в своём распоряжении как хаотический сигнал, содержащий полезную информацию, так и сигнал без неё. Поэтому можно легко выделить полезный цифровой сигнал $\tilde{m}(t)$ простым вычитанием одного сигнала из другого.

Нетрудно видеть, что в такой схеме скрытой передачи информации активно используется метод вспомогательной системы (см. раздел 2), что требует наличия двух идентичных по управляющим параметрам хаотических генераторов. Так же как и в схемах, основанных на режиме полной хаотической синхронизации, эти генераторы располагаются на разных сторонах канала связи, что представляет собой существенную проблему с точки зрения технической реализации данного метода. Небольшая расстройка значений управляющих параметров в этих системах приводит к появлению шумов десинхронизации [3], делая такую схему неработоспособ-

[3] Под шумом десинхронизации понимается сигнал $\Delta\mathbf{x} = \mathbf{x}_2 - \mathbf{x}_1$, где $\mathbf{x}_{1,2}(t)$ — сигналы, поступающие на вычитающее устройство, в данном случае сигналы с ведомого и вспомогательного генераторов хаоса плюс шумы канала связи. При наличии синхронного режима $\Delta\mathbf{x} = 0$.

ной. Кроме того, реализация двух каналов связи является существенным недостатком не только из-за дополнительных затрат при реализации, но и вследствие того, что наличие двух каналов способствует появлению дополнительных шумов в канале связи (возможно, даже совершенно другой природы), искажающих передаваемый сигнал. Поэтому такая схема скрытой передачи данных характеризуется достаточно низкой устойчивостью к шумам в канале связи и является труднореализуемой на практике.

Возникают также проблемы с конфиденциальностью передачи информации. Понятно, что использование другого типа синхронного поведения, а также наличие дополнительного канала связи, с этой точки зрения, играют положительную роль. Однако, так же как и в схемах на основе нелинейного подмешивания информационного сигнала к хаотическому (см. раздел 3.3), повышение качества передаваемой информации влечёт за собой потерю конфиденциальности. Но эта проблема здесь является менее существенной по сравнению с аналогичной проблемой для схем, основанных на режиме полной хаотической синхронизации (см. раздел 3).

4.2. Использование нескольких типов синхронного поведения для скрытой передачи информации

Повысить конфиденциальность передачи информации можно с помощью использования нескольких типов синхронного поведения одновременно. Например, в работах [109, 161] предложены способы скрытой передачи данных, использующие одновременно режимы обобщённой и полной хаотической синхронизации.

Схема, предложенная в работе [109] (рис. 8), является модификацией схемы, рассмотренной в разделе 4.1. Принцип работы передающего устройства аналогичен принципу работы передающего устройства схемы, описанной в разделе 4.1. Модификация заключается в том, что на принимающей стороне каналов связи находится дополнительный хаотический генератор $\mathbf{x}_2(t)$, идентичный ведущему $\mathbf{x}_1(t)$ по управляющим параметрам (далее — второй ведущий генератор). Сигнал, генерируемый ведущей системой, передается по первому каналу связи, переводя второй ведущий генератор в режим полной синхронизации. Конфиденциальность можно повысить за счёт того, что сигналы, поступающие на ведомый и второй ведущий генераторы, могут быть различными (например, ведомой системе передаётся сигнал, представляющий собой x-координату ведущей системы, а второй ведущей — сигнал, представляющий собой y-координату)[4]. На принимающей стороне канала связи сигнал от второго ведущего генератора, воздействуя на вспомогательный, обеспечивает возникновение режима обобщённой синхронизации между ними. Сигнал с ведомого генератора поступает по второму каналу связи на принимающую сторону. Вследствие идентичности сигналов, воздействующих на ведомый и вспомогательный генераторы, как и в предыдущем случае, принимающая сторона имеет в своём распоряжении как сигнал, содержащий полезную информацию, так и сигнал без неё. После прохождения через вычитающее устройство полезный сигнал может быть легко детектирован.

Понятно, что такая схема является более эффективной с точки зрения конфиденциальности, т.е. снижается вероятность детектирования информационного сообщения третьей стороной. Однако ряд других проблем до сих пор остаётся нерешённым. Наличие идентичных генераторов в передающем и принимающем устройствах (теперь это уже две пары идентичных генераторов), реализация двух каналов связи, низкая устойчивость к шумам в канале связи, которая становится ещё ниже вследствие разрушения полной хаотической синхронизации, — все эти недостатки делают подобные схемы скрытой передачи данных малоприменимыми на практике.

В работе [161] был предложен другой способ скрытой передачи информации, в котором также используются два типа синхронного поведения — обобщённая и полная хаотическая синхронизация, но схема [161] является модификацией одной из схем для скрытой передачи данных, основанных на нелинейном подмешивании информационного сигнала к хаотическому (см. раздел 3.3).

Принципиальная схема реализации такого способа скрытой передачи данных приведена на рис. 9. Передаю-

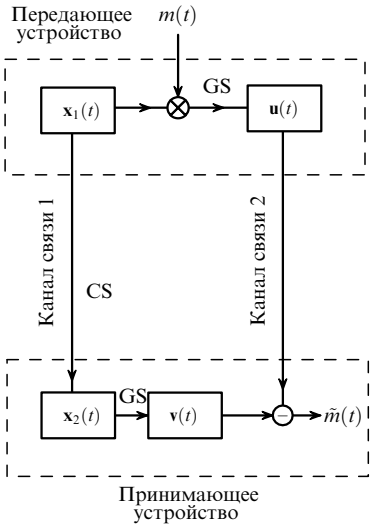

Рис. 8. Схема скрытой передачи информации с помощью обобщённой и полной хаотической синхронизации, предложенная в работе [109].

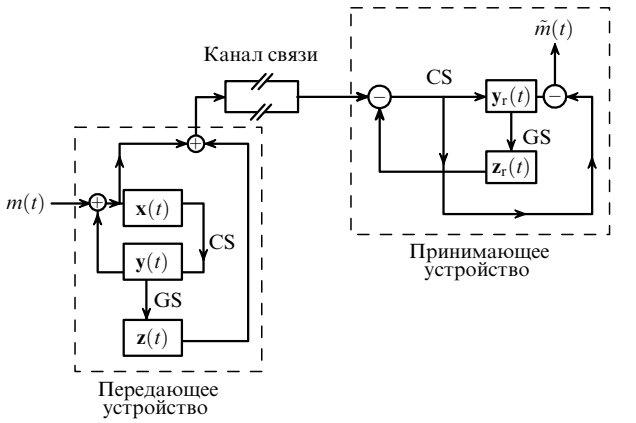

Рис. 9. Схема скрытой передачи информации с использованием комбинированного хаотического сигнала.

[4] Это может соответствовать сигналам напряжения, снятым в различных точках радиотехнической схемы генератора.

щее устройство, так же как и в схеме на основе нелинейного подмешивания информационного сигнала к хаотическому (см. раздел 3.3), содержит два взаимосвязанных идентичных хаотических генератора $\mathbf{x}(t)$ и $\mathbf{y}(t)$ (далее — первый и второй). Информационный сигнал $m(t)$ подмешивается к сигналам, производимым этими генераторами, и тем самым претерпевает нелинейные изменения. Кроме того, на передающей стороне канала связи находится ещё один генератор $\mathbf{z}(t)$ (будем называть его третьим), неидентичный первому и второму по управляющим параметрам и однонаправленно связанный со вторым. Значения управляющих параметров генераторов передающего устройства должны быть выбраны таким образом, чтобы второй и третий генераторы находились в режиме обобщённой хаотической синхронизации, в то время как первый и второй являлись бы полностью синхронизованными, т.е. находились в режиме полной синхронизации. Третий генератор используется для повышения конфиденциальности: он формирует сигнал, который в простейшем случае просто добавляется к сигналу, содержащему полезную информацию, что формирует уже комбинированный сигнал, создавая тем самым дополнительную маскировку.

Такой способ передачи информации в оригинальной работе [161] был назван "скрытая передача информации с использованием комбинированного сигнала хаотических систем в режиме обобщённой синхронизации" (secure communication using a compound signal from generalized synchronizable chaotic systems). Комбинированный сигнал по каналу связи передаётся на принимающее устройство, содержащее два генератора: четвёртый — $\mathbf{y}_{\text{г}}(t)$, идентичный первому и второму по управляющим параметрам, и пятый — $\mathbf{z}_{\text{г}}(t)$, идентичный в том же самом смысле третьему. Четвёртый и пятый генераторы должны находиться в режиме обобщённой синхронизации. Тогда согласно методу вспомогательной системы, вследствие идентичности четвёртой и второй систем, третий и пятый генераторы будут совершать идентичные колебания. Сигналы из канала связи и пятого генератора поступают на вычитающее устройство. На четвёртый генератор и второе вычитающее устройство будут уже поступать сигналы, свободные от дополнительных составляющих. В случае воздействия на четвёртый генератор этот сигнал синхронизует его при передаче бинарного бита 0 и не синхронизует при передаче бинарного бита 1. На выходе будет получен восстановленный сигнал $\tilde{m}(t)$, представляющий собой последовательность участков с синхронным (бинарный бит 0) и несинхронным (бинарный бит 1) поведением.

Из приведённого выше рассмотрения следует, что такая схема является достаточно конфиденциальной: по комбинированному сигналу, передаваемому по каналу связи, в большинстве случаев даже в отсутствие шумов, диагностировать информационное сообщение третьей стороной не представляется возможным. Однако, как и в схемах на основе нелинейного подмешивания, качество передачи информации (а следовательно, и возможность восстановления качественной информации) сильно зависит от конфиденциальности, а именно: чем выше конфиденциальность, тем ниже качество. В то же время понятно, что за счёт создания комбинированного сигнала эта зависимость будет не столь резкой, что является некоторого рода преимуществом этой схемы перед другими. Однако одно достоинство не закрывает ряд недостатков. Создание пяти генераторов, три и два из которых должны быть идентичны между собой, является практически нерешаемой технической задачей, особенно если генераторы располагаются на различных сторонах канала связи. Введение достаточно малой расстройки управляющих параметров этих генераторов сразу же делает схему неработоспособной. Кроме того, шумы в канале связи, несомненно, приведут к искажению передаваемого сигнала, а следовательно, к разрушению режимов полной синхронизации между вторым и четвёртым генераторами и обобщённой синхронизации между четвёртым и пятым. Сигналы на разных сторонах канала связи станут неидентичными, и детектирование информационного сообщения на принимающей стороне канала связи окажется невозможным.

Таким образом, частичная ликвидация одних недостаков в большем числе случаев приводит к усугублению других. Ввиду низкой устойчивости к шумам и расстройке управляющих параметров техническая реализация таких схем, обладающих достаточно высокой конфиденциальностью, является очень сложной. Поэтому "экстенсивный" путь совершенствования способов скрытой передачи данных — использование нескольких типов синхронного поведения для передачи информации — по всей видимости, является неоптимальным.

5. Сверхустойчивый к шумам способ скрытой передачи информации

Анализ схем, рассмотренных в разделах 3 и 4, показывает, что, несмотря на использование различных типов синхронного поведения для скрытой передачи информации, специфические особенности этих способов, их характерные различия, достоинства и недостатки в той или иной степени присущи всем известным сейчас схемам. Это в первую очередь:

- требование высокой степени идентичности к хаотическим генераторам, располагающимся на разных сторонах канала связи;
- низкая устойчивость к шумам в канале связи;
- низкая конфиденциальность, т.е. возможность в ряде случаев реконструкции параметров передающего генератора по сигналу, передаваемому по каналу связи (особенно для схем на основе полной хаотической синхронизации), с последующим восстановлением информационного сигнала.

В этом разделе мы рассмотрим способ скрытой передачи информации [162, 163], который во многом лишён всех вышеупомянутых недостатков. Более того, этот способ обладает значительной устойчивостью к шумам и, как следствие, характеризуется достаточно высокой степенью конфиденциальности. Способ основан на обобщённой синхронизации, однако в отличие от способа, рассмотренного в разделе 4.1, он учитывает все особенности режима обобщённой синхронизации, упомянутые в разделе 4, и поэтому обладает принципиальными достоинствами по сравнению с известными аналогами.

Прежде, чем перейти к описанию самого способа скрытой передачи данных, кратко остановимся на причинах структурной устойчивости режима обобщённой синхронизации к шумам.

5.1. Устойчивость режима обобщённой синхронизации к шумам

Известно, что режим обобщённой синхронизации может наблюдаться в системах с диссипативным и недиссипативным типами связи [126, 164]. Для систем с диссипативной связью уравнения, описывающие динамику взаимодействующих систем в присутствии шума, могут быть представлены в виде

$$\dot{\mathbf{x}}(t) = \mathbf{G}\big(\mathbf{x}(t),\, \mathbf{g}_{\mathrm{d}}\big)\,,$$

$$\dot{\mathbf{u}}(t) = \mathbf{H}\big(\mathbf{u}(t),\, \mathbf{g}_{\mathrm{r}}\big) + \varepsilon A\big(\mathbf{x}(t) - \mathbf{u}(t) + D\boldsymbol{\xi}(t)\big)\,, \qquad (3)$$

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

Механизмы возникновения режима обобщённой синхронизации могут быть выявлены с помощью метода модифицированной системы, впервые предложенного в наших работах [164, 165]. Согласно этому методу, ведомая система $\mathbf{u}(t)$ может быть рассмотрена как некоторая модифицированная система:

$$\dot{\mathbf{u}}_{\mathrm{m}}(t) = \mathbf{H}'\big(\mathbf{u}_{\mathrm{m}}(t),\, \mathbf{g}_{\mathrm{r}}, \varepsilon\big)\,, \qquad (4)$$

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

$$\dot{\mathbf{u}}_{\mathrm{m}}(t) = \mathbf{H}'\big(\mathbf{u}_{\mathrm{m}}(t),\, \mathbf{g}_{\mathrm{r}}, \varepsilon\big) + \varepsilon\big(A\mathbf{x}(t) + D\boldsymbol{\xi}(t)\big)\,, \qquad (5)$$

где $\mathbf{H}'\big(\mathbf{u}(t)\big) = \mathbf{H}\big(\mathbf{u}(t)\big) - \varepsilon A\mathbf{u}(t)$. Слагаемое $-\varepsilon A\mathbf{u}(t)$ вносит дополнительную диссипацию в модифицированную систему (4).

Режим обобщённой синхронизации, возникающий в системе (3), может быть рассмотрен как следствие двух взаимосвязанных процессов, протекающих одновременно: увеличения диссипации в модифицированной системе (4) и возрастания амплитуды внешнего (хаотического и шумового) сигнала. Оба процесса связаны между собой посредством параметра ε и не могут быть реализованы в ведомой системе (3) по отдельности. Однако увеличение диссипации в модифицированной системе (4) приводит к упрощению её 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. Очевидно, что возникновение режима обобщённой синхронизации возможно только тогда, когда собственная хаотическая динамика в ведомой системе оказывается подавленной вследствие диссипации.

Таким образом, устойчивость режима обобщённой синхронизации определяется прежде всего свойствами самой модифицированной системы. Поэтому порог возникновения режима обобщённой синхронизации не должен сильно зависеть от интенсивности шума $D\boldsymbol{\xi}(t)$, воздействующего на однонаправленно связанные хаотические системы. Если шум не изменяет характеристики модифицированной системы (4), то он не должен и влиять на порог возникновения режима обобщённой синхронизации.

Действительно, как упоминалось в разделе 2, диагностирование режима обобщённой синхронизации возможно как с помощью метода вспомогательной системы, так и путём расчёта условных ляпуновских экспонент. Понятно, что ведомая и вспомогательная системы могут быть рассмотрены как две идентичные системы с близкими начальными условиями. Вычисление производной от разности их состояний $\boldsymbol{\Delta}(t) = \mathbf{v}(t) - \mathbf{u}(t)$ при наличии $(D > 0)$ и отсутствии шума $(D = 0)$, вследствие идентичности детерминированных и стохастических сигналов, воздействующих на эти системы, приводит к одному и тому же уравнению:

$$\dot{\boldsymbol{\Delta}}(t) = \big(\mathbf{JH}(\mathbf{u}(t)) - \varepsilon A\big)\,\boldsymbol{\Delta}(t) = \mathbf{JH}'\big(\mathbf{u}(t)\big)\,\boldsymbol{\Delta}(t)\,, \qquad (6)$$

где $\mathbf{J}$ — матрица Якоби. Так как уравнение (6) может быть рассмотрено как уравнение в вариациях при вычислении условных ляпуновских экспонент, можно заключить, что старшие условные ляпуновские показатели (определяющие порог возникновения режима обобщённой синхронизации) будут вести себя схожим образом как в отсутствие, так и при наличии шума. Поэтому порог возникновения режима обобщённой синхронизации не должен зависеть от интенсивности шума, а сам тип синхронного поведения должен обладать значительной устойчивостью к шумам.

Справедливость теоретических рассуждений подтверждается результатами численного моделирования [160, 166] и физического эксперимента [159]. Как показывают результаты исследований, режим обобщённой синхронизации обладает структурной устойчивостью к шумам как в системах с малым числом степеней свободы [160], так и в пространственно распределённых средах [159]. Экспериментальное подтверждение данного факта было получено в рамках радиотехнического эксперимента с низкочастотными генераторами хаоса в работе [160].

5.2. Описание способа

Перейдём к описанию сверхустойчивого к шумам способа скрытой передачи информации. Принципиальная схема реализации такого способа приведена на рис. 10.

Способ скрытой передачи информации заключается в следующем [162]. Информационный сигнал $m(t)$ кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего генератора $\mathbf{x}(t)$ модулируются бинарным сигналом таким образом, чтобы характеристики передаваемого сигнала изменялись незначительно. Полученный таким образом сигнал передаётся по каналу связи. Здесь он подвергается искажению под влиянием шумов. Приёмник, который находится на другой стороне канала связи, представляет собой два идентичных генератора $\mathbf{u}(t)$ и $\mathbf{v}(t)$, способных находиться в режиме обобщённой синхронизации с

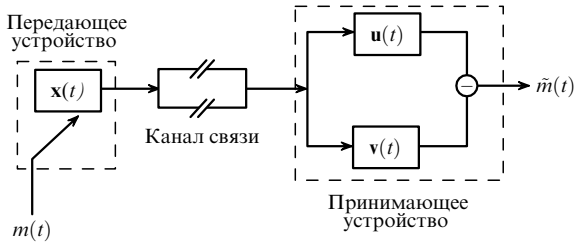

Рис. 10. Схема реализации сверхустойчивого к шумам способа скрытой передачи информации на основе обобщённой хаотической синхронизации.

передающим генератором. Принцип работы приёмника основан на диагностике режима обобщённой синхронизации с помощью метода вспомогательной системы (см. раздел 2). Сигнал с канала связи поступает на генераторы приёмника. Полученные на выходе сигналы проходят через вычитающее устройство, и затем детектируется восстановленный полезный сигнал [5] $\tilde{m}(t)$.

Модуляция управляющих параметров передающего генератора должна быть осуществлена таким образом, чтобы в зависимости от передаваемого бинарного бита 0(1) между передающим и принимающим генераторами существовал (отсутствовал) режим обобщённой синхронизации. Например, если режим обобщённой синхронизации наблюдается в том случае, если передаётся бинарный бит 0, тогда оба принимающих генератора 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 обобщённая синхронизация не наблюдается, а колебания принимающих генераторов являются неидентичными. Тогда после прохождения через вычитающее устройство будет наблюдаться ненулевая амплитуда хаотических колебаний, т.е. бинарный бит 1.

Принципиальным достоинством рассматриваемого способа скрытой передачи данных является отсутствие требования идентичности генераторов на разных сторонах канала связи. Два идентичных генератора располагаются на принимающей стороне. Следует отметить, что наличие идентичных генераторов на одной стороне канала связи позволяет легко осуществить их юстировку, что снижает требование к степени идентичности генераторов, а следовательно, упрощает техническую реализацию схемы.

Кроме того, сигналы, поступающие на генераторы принимающего устройства, всегда будут одинаковыми, даже при наличии шума в канале связи. Следовательно, как обсуждалось в разделе 5.1, при диссипативной связи между генераторами передающего и принимающего устройств шум не должен оказывать сильного влияния на порог возникновения режима обобщённой синхронизации. Эта особенность позволяет говорить о возможности создания устойчивых к шумам способов скрытой передачи данных на основе режима обобщённой синхронизации.

6. Сравнение известных способов скрытой передачи информации

Проведём сравнительный анализ работоспособности способов скрытой передачи информации с помощью хаотической синхронизации, рассмотренных в настоящем обзоре. Для проверки эффективности этих методов при наличии шума используем численное моделирование и оценим некоторые количественные характеристики работоспособности схем. В качестве генераторов передающего и принимающего устройств во всех случаях выберем однонаправленно связанные системы Рёсслера с близкими значениями управляющих параметров [6], а в качестве информационных сигналов — простые последовательности бинарных битов. Выбор именно этих моделей радиотехнических генераторов связан с тем, что: 1) система Рёсслера достаточно хорошо исследована, в том числе, и с точки зрения хаотической синхронизации (см., например, [97, 129, 140, 157, 165, 167, 168]); 2) в однонаправленно связанных системах Рёсслера возможно установление всех типов синхронного поведения, на основе которых построены рассматриваемые схемы скрытой передачи данных [98, 131, 138, 140, 157, 164, 167–169]; 3) расположение границы обобщённой синхронизации на плоскости параметров "частота расстройки — интенсивность связи" удовлетворяет требованиям, указанным в разделе 4 (см. также [158]); 4) возможно построение радиотехнического генератора, динамика которого будет описываться уравнениями системы Рёсслера [170]. Такой выбор позволит нам корректно сопоставить рассмотренные схемы друг с другом и, более того, при необходимости проверить эффективность их работы на реальных устройствах [170].

6.1. Численная реализация сверхустойчивого к шумам способа скрытой передачи информации

Начнем с рассмотрения численной реализации наиболее эффективного метода скрытой передачи информации, обладающего сверхустойчивостью к шумам и не требующего наличия идентичных генераторов на разных сторонах канала связи (см. раздел 5.2, рис. 10). В этом случае передающий генератор описывается следующей системой дифференциальных уравнений:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3\,, \\ \dot{x}_2 &= \omega_x x_1 + a x_2\,, \\ \dot{x}_3 &= p + x_3(x_1 - c)\,, \end{aligned} \tag{7}$$

где $\mathbf{x}(t) = (x_1, x_2, x_3)$ — вектор состояния передающего генератора, управляющие параметры $a = 0{,}15$, $p = 0{,}2$ и $c = 10$, ω_x — управляющий параметр, характеризующий собственную частоту колебаний системы.

Величина параметра ω_x модулируется полезным цифровым сигналом следующим образом. Если в заданный интервал времени передаётся бинарный бит 1, то $\omega_x = 0{,}95$ на протяжении всего этого интервала. При передаче бинарного бита 0 $\omega_x = 1$. Следует отметить, что такой выбор значений параметра ω_x продиктован исключительно демонстрационными целями и обусловлен характером расположения границы обобщённой синхронизации, подробно изученным в [158]. На самом деле параметр ω_x может принимать достаточно произвольные значения (например, результаты, аналогичные описанным ниже, были получены для $\omega_x = 0{,}91$ при передаче бинарного бита 1 и $\omega_x \in [0{,}9,\ 0{,}91]$ при передаче бинарного бита 0). Необходимым условием является лишь чередование областей с асинхронной динамикой и режимом обобщённой синхронизации.

Принимающее устройство содержит два идентичных хаотических генератора, каждый из которых описы-

[5] Следует отметить некоторую аналогию рассматриваемого способа скрытой передачи информации и способа на основе модулирования управляющих параметров, описанного в разделе 3.4. В основе обоих способов лежит модулирование управляющих параметров передающего генератора бинарным сигналом, но в рассматриваемом способе используется режим обобщённой синхронизации вместо полной, что позволяет преодолеть ряд недостатков, указанных в разделе 3.4.

[6] Подробное описание этих систем и значения управляющих параметров приведены в разделах 6.1, 6.2.

вается следующей системой уравнений:

$$\dot{u}_1 = -\omega_u u_2 - u_3 + \varepsilon\big(s(t) - u_1\big)\,,$$
$$\dot{u}_2 = \omega_u u_1 + a u_2\,, \qquad (8)$$
$$\dot{u}_3 = p + u_3(u_1 - c)\,.$$

Здесь $\mathbf{u}(t) = (u_1, u_2, u_3)$ — вектор состояния первого принимающего генератора. Пусть $\mathbf{v}(t) = (v_1, v_2, v_3)$, также удовлетворяющий (8), является вектором состояния второго принимающего генератора (см. рис. 10). Управляющие параметры a, p и c выберем идентичными соответствующим параметрам передающего 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 исследуемой модели (7), (8) это реализуется посредством связи принимающего генератора с передающими, т.е. добавлением компоненты $\varepsilon(s(t) - u_1)$ в первое уравнение системы (8). Здесь $s(t) = x_1 + D\xi$ — это сигнал в канале связи. Слагаемое $D\xi$ моделирует шумы в канале связи, ξ— стохастический гауссов процесс, характеризующийся следующим распределением вероятности:

$$p(\xi) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left[-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right], \qquad (9)$$

где $\xi_0 = 0$ и $\sigma = 1$ — среднее и дисперсия [7]. Параметр D определяет интенсивность добавляемого шума.

Интенсивность 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 обобщённой синхронизации в системе (7), (8) имеет место при $\omega_x = 1$, в то время как при $\omega_x = 0{,}95$ обобщённая синхронизация не наблюдается (см. подробнее [158]).

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 будет представлять собой последовательность областей с различными типами поведения.

Простая последовательность бинарных битов 0/1, выбранная в качестве исходного информационного сообщения, приведена на рис. 11а. Для интегрирования стохастического уравнения (8) воспользуемся методом Эйлера с шагом дискретизации по времени $h = 0{,}0001$ [171].

Начнём рассмотрение с идеализированной ситуации, при которой шумы в канале связи отсутствуют (т.е. амплитуда шума $D = 0$). Понятно, что такой случай фактически нереализуем на практике, так как шумы всегда присутствуют в реальных устройствах. В то же время именно на основе рассмотрения схем с идеальными ("бесшумовыми") каналами связи были предложены и протестированы практически все способы скрытой передачи данных, а влияние шума на работоспособность таких схем, как правило, не анализировалось. Поэтому рассмотрение идеализированной ситуации важно как для проверки работоспособности схемы, так и для её сопоставления с известными ранее схемами скрытой передачи данных.

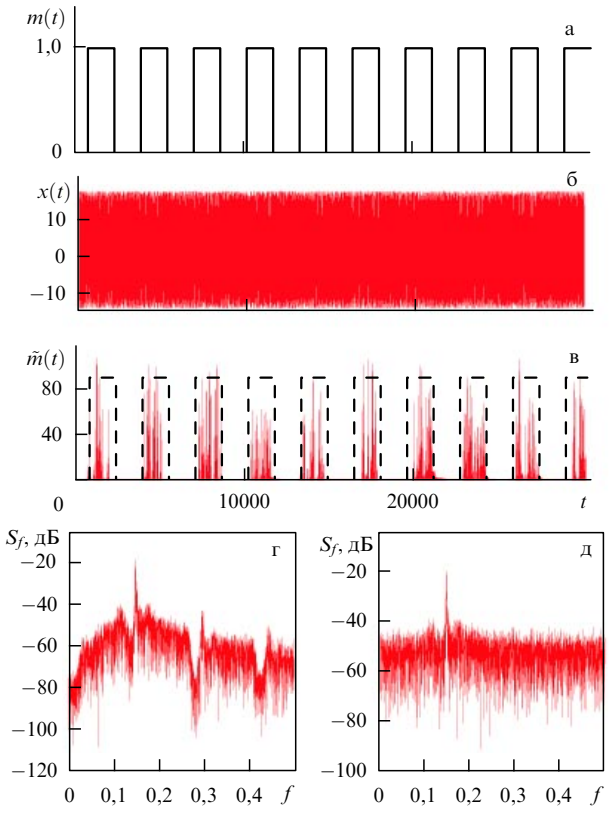

Рис. 11. Иллюстрация численной реализации способа скрытой передачи информации на основе обобщённой хаотической синхронизации в отсутствие шумов и флуктуаций в канале связи ($D = 0$): (а) информационный сигнал $m(t)$, представленный простой последовательностью бинарных битов 0/1, (б) сигнал $x(t)$, производимый передающим генератором для последующей передачи по каналу связи, (в) восстановленный сигнал $\tilde{m}(t)$ и детектированный информационный сигнал (штриховая линия). Спектры мощности сигнала в канале связи (г) в отсутствие шума и (д) при шуме интенсивностью $D = 10$.

Работоспособность схемы в отсутствие шумов иллюстрирует рис. 11б, в. Сигнал $x(t)$, генерируемый передающей системой для передачи по каналу связи, приведён на рис. 11б. Характеристики этого сигнала практически не изменяются в зависимости от передаваемого бинарного бита 0/1 (изменения параметра ω_x), что отчётливо видно по отсутствию следов амплитудной и частотной модуляции в сигнале $x(t)$. В спектре мощности такого сигнала благодаря относительно малой частотной расстройке содержится только одна чётко выраженная спектральная компонента (рис. 11г), что делает невозможной дешифрацию информационного сообщения третьей стороной. На рисунке 11в показан восстановленный в принимающем устройстве сигнал $\tilde{m}(t)$, после пропускания которого через фильтр нижних частот и правильного выбора пороговых значений

[7] Важно отметить, что характер распределения случайной величины ξ не имеет особого значения и подобные результаты были получены для других типов плотности распределения вероятностей $p(\xi)$ (например, для равномерного).

может быть легко детектирован исходный информационный сигнал[8].

Рассмотрим теперь, какое влияние оказывает шум, неизбежно присутствующий в каналах связи реальных устройств, на эффективность рассматриваемого способа скрытой передачи информации на основе обобщённой синхронизации. Понятно, что шум резко искажает передаваемый сигнал, что может серьёзно отразиться на качестве передачи информации или, более того, сделать её вовсе невозможной (как будет показано в разделе 6.2, такая ситуация присуща всем другим схемам, описанным в обзоре). Однако, как отмечалось в разделе 5.1, шум практически не влияет на порог возникновения режима обобщённой синхронизации в диссипативно связанных хаотических системах, т.е. синхронный режим и при наличии, и при отсутствии шума возникает в таких системах при приблизительно одинаковых значениях параметра связи ε. В то же время анализ устойчивости рассматриваемой схемы к шумам показывает, что при достаточно больших амплитудах шума возможна ситуация, когда шум не только не разрушает режим обобщённой синхронизации, но и, наоборот, приводит к его возникновению при меньших значениях интенсивности связи, при которых в отсутствие шума режим обобщённой синхронизации не наблюдается. Это может отрицательно сказаться на качестве передачи информации, т.е. привести к возможности детектирования только бинарного бита[9] 0. Однако лишь шум с очень большой амплитудой способен "усилить" обобщённую синхронизацию. Как следует из результатов проведённых исследований, для системы (7), (8) с указанными значениями управляющих параметров такая ситуация возникает при амплитудах шума $D > 400$.

Работоспособность анализируемого способа скрытой передачи данных при наличии достаточно сильных шумов в канале связи ($D = 10$) показывает рис. 12. Так же как и на рис. 11, представлены информационный сигнал $m(t)$ (рис. 12а), сигнал $s(t)$ (рис. 12б), передаваемый по каналу связи (т.е. сигнал, генерируемый передающей системой (рис. 11б) плюс шумы канала связи) и восстановленный сигнал $\tilde{m}(t)$ до (сплошная линия) и после (штриховая линия) пропускания через фильтр нижних частот и выбора пороговых значений. За счёт добавления шума с достаточно большой амплитудой сигнал, передаваемый по каналу связи, становится практически не отличающимся от стохастического, что отчётливо видно как по характеру временно́й реализации сигнала, так и по характеру распределения его амплитуд (которое является близким к гауссову (ср. рис. 12г и д, на которых приведены подобные распределения в отсутствие и при наличии шума). В спектре мощности такого сигнала (рис. 11д), так же как и при отсутствии шума в канале связи, содержится одна чётко выраженная спектральная компонента, а добавление шума приводит лишь к увеличению интенсивности шумого пьедестала, присутствующего в нём. В этом случае детектирование информационного сообщения третьей стороной является практически невозможным. В то же время качество информации, восстановленной в принимающем устройстве, остаётся таким же высоким, как и в отсутствие шумов в канале связи (ср. рис. 11в и рис. 12в). Аналогичная ситуация имеет место при любых значениях интенсивности шума D в диапазоне $0-400$, что ещё раз подтверждает значительную устойчивость способа скрытой передачи информации на основе обобщённой синхронизации к шуму в канале связи и свидетельствует о конструктивной роли шума в увеличении конфиденциальности передачи информации этим способом без потери качества.

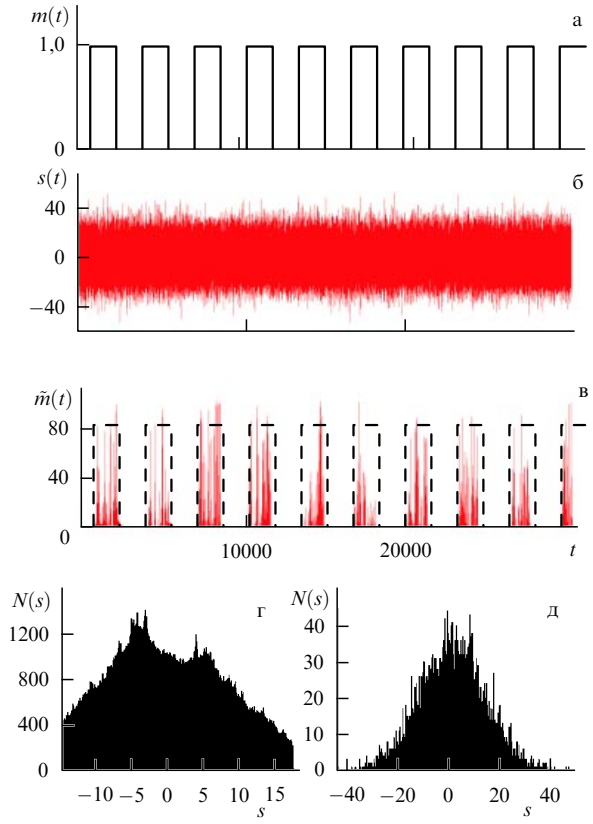

Рис. 12. Иллюстрация численной реализации способа скрытой передачи информации на основе обобщённой хаотической синхронизации при наличии сильных шумов в канале связи ($D = 10$): информационный сигнал $m(t)$, представленный простой последовательностью бинарных битов 0/1 (а), сигнал $s(t)$, передаваемый по каналу связи (б), восстановленный сигнал $\tilde{m}(t)$ (в); детектированный информационный сигнал показан штриховой линией. Распределение амплитуд сигнала в канале связи в отсутствие (г) и при наличии шума интенсивностью $D = 10$ в канале связи (д).

6.2. Численная реализация других рассмотренных способов скрытой передачи информации на основе хаотической синхронизации

Теперь перейдём к численному моделированию других способов скрытой передачи информации на основе хаотической синхронизации, рассмотренных в обзоре. Прежде всего следует отметить, что численная реализация схем на основе хаотической маскировки (см. раздел 3.1), переключения хаотических режимов (см. раздел 3.2), модулирования управляющих параметров (см. раздел 3.4), а также двух предложенных в работе [109] схем, рассмотренных в разделах 4.1 и 4.2, не приводит к существенным изменениям уравнений для

[8] Видно, что исходный информационный сигнал, приведённый на рис. 11а, и детектированный информационный сигнал на рис. 11в (штриховая линия) в точности совпадают, что свидетельствует о высоком качестве передачи информации.

[9] Когда другие схемы становятся неработоспособными, всегда детектируется только бинарный бит 1.

передающих и принимающих генераторов. Поэтому, если не оговаривается особо, будем считать, что все они описываются системами дифференциальных уравнений (7), (8) соответственно с управляющими параметрами $a = 0{,}15$, $p = 0{,}2$, $c = 10$, $\omega_u = 0{,}95$. Значения остальных управляющих параметров сильно зависят от типа синхронного поведения, который используется в данном способе, и специфики его реализации, поэтому они будут выбираться для каждой схемы разными. Кроме того, от схемы к схеме меняется также характер сигнала в канале связи. Однако во всех случаях мы будем также использовать цифровой сигнал, представленный простой последовательностью бинарных битов 0/1, в качестве информационного и предполагать, что шумы в канале связи подчиняются распределению (9).

Для реализации способа скрытой передачи информации на основе хаотической маскировки (см. раздел 3.1, рис. 2) необходимо наличие двух идентичных генераторов, передающего и принимающего, на разных сторонах канала связи. Поэтому выберем $\omega_x = 0{,}95$ на протяжении всего времени передачи сигнала. Хаотическая маскировка осуществляется непосредственным примешиванием информационного сигнала к хаотическому, т.е. сигнал в канале связи будет иметь вид $s(t) = x_1 + m(t) + D\xi$. Кроме того, для возможности реализации режима полной хаотической синхронизации необходимо увеличить интенсивность связи между системами, поэтому выберем $\varepsilon = 0{,}25$.

В схеме на основе переключения хаотических режимов (см. раздел 3.2, рис. 3) передающее устройство содержит два генератора, один из которых находится в режиме полной хаотической синхронизации с принимающим генератором, т.е. является его точной копией ($\omega_x = 0{,}95$) и кодирует бинарный бит 0. Второй передающий генератор, который не идентичен принимающему и не синхронизован с ним (выберем $\omega_x = 1$ в этом случае), кодирует бинарный бит 1. Сигнал в канале связи тогда будет иметь вид $s(t) = x_1 + D\xi$, а интенсивность связи между системами, по аналогии со схемой на основе хаотической маскировки, выберем равной $\varepsilon = 0{,}25$.

Для схемы на основе модулирования управляющих параметров (см. раздел 3.4, рис. 5) целесообразно выбрать те же значения управляющих параметров, что и для схемы на основе переключения хаотических режимов, так как численная реализация этих двух способов скрытой передачи данных (при выборе в качестве передающих генераторов двух идентичных систем со слегка различающимися параметрами в схеме на основе переключения хаотических режимов) является одинаковой. Поэтому выберем $s(t) = x_1 + D\xi$, $\varepsilon = 0{,}25$,

$$\omega_x = \begin{cases} 0{,}95, & m(t) = 0, \\ 1{,}00, & m(t) = 1. \end{cases}$$

Схема на основе режима обобщённой хаотической синхронизации [109] (см. также раздел 4.1, рис. 7) требует наличия дополнительного хаотического генератора, идентичного принимающему, на передающей стороне канала связи. Как и в работе [109], будем называть генераторы передающего устройства ведущим и ведомым, а идентичный ведомому генератор на принимающей стороне канала связи — вспомогательным. В этом случае ведущий генератор описывается системой уравнений (7) с вышеуказанными значениями управляющих параметров и $\omega_x = 1$ (с целью обеспечения неидентичности с другими генераторами), а ведомый и вспомогательный генераторы — системой (8), но воздействующие на них сигналы $s(t)$ будут различными: $s(t) = n(t)x_1$, где

$$n(t) = \begin{cases} 0{,}9, & m(t) = 1, \\ 1{,}0, & m(t) = 0, \end{cases}$$

в случае воздействия на генератор передающего устройства и $s(t) = x_1 + D\xi$ при передаче сигнала по каналу связи на принимающий генератор. С целью обеспечения возможности возникновения режима обобщённой синхронизации между неидентичными генераторами выберем параметр связи $\varepsilon = 0{,}14$ (как и в способе, предложенном в разделе 6.1).

В схеме на основе обобщённой и полной хаотической синхронизации, описанной в [109] (см. также раздел 4.2, рис. 8), на принимающей стороне канала связи появляется дополнительный генератор, идентичный первому передающему по управляющим параметрам и однонаправленно связанный с ним (далее — второй ведущий генератор). Этот генератор описывается системой уравнений (7) с добавлением дополнительного слагаемого, т.е.

$$\begin{aligned} \dot{y}_1 &= -\omega_x y_2 - y_3 + \varepsilon_2\big(g(t) - y_1\big), \\ \dot{y}_2 &= \omega_x y_1 + a y_2, \\ \dot{y}_3 &= p + y_3(y_1 - c), \end{aligned} \tag{10}$$

где $\mathbf{y}(t) = (y_1, y_2, y_3)$ — вектор состояния этого генератора, $\varepsilon_2 = 0{,}2$ — параметр, характеризующий силу связи между "ведущими" генераторами, $g(t) = x_1 + D\xi$ — сигнал, передаваемый по первому каналу связи. Сигнал $s(t)$ в этом случае также претерпевает некоторые изменения: теперь на вспомогательный генератор будет воздействовать сигнал $s(t) = y_1$.

При моделировании обеих схем, предложенных в работе [109], необходимо принимать во внимание наличие второго канала связи, т.е. при передаче сигнала от ведомого генератора на принимающее устройство к нему также примешиваются шумы. Поэтому на вычитающее устройство будут поступать не только детерминированные сигналы, производимые ведомым и вспомогательным генераторами, но и стохастический сигнал со второго канала связи. Восстановленный сигнал тогда будет иметь вид $\tilde{m}(t) = (u_1 + D\xi - v_1)^2$, если не принимать во внимание, что шумы в двух каналах связи являются различными (учёт этого значительно ухудшает возможность детектирования полезного сигнала).

При численной реализации схем на основе нелинейного подмешивания информационного сигнала к хаотическому (см. раздел 3.3, рис. 4) передающее устройство описывается следующими системами дифференциальных уравнений:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3 + \varepsilon\big(y_1 + m(t) - x_1\big), \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \\ \dot{y}_1 &= -\omega_x y_2 - y_3 + \varepsilon\big(x_1 + m(t) - y_1\big), \\ \dot{y}_2 &= \omega_x y_1 + a y_2, \\ \dot{y}_3 &= p + y_3(y_1 - c), \end{aligned} \tag{11}$$

т.е. представляет собой два идентичных взаимно связанных хаотических генератора. Здесь $\mathbf{x}(t) = (x_1, x_2, x_3)$ и $\mathbf{y}(t) = (y_1, y_2, y_3)$ — векторы состояний первого и второго передающих генераторов соответственно, $m(t)$ — информационный сигнал, $\omega_x = 1{,}00$, $\varepsilon = 0{,}25$. Принимающий генератор описывается системой уравнений (8), $\omega_u = 1$. Сигнал в канале связи в этом случае представляет собой просто сумму сигнала, генерируемого одной из передающих хаотических систем, и шумов канала связи, т.е. $s(t) = x_1 + D\xi$.

Реализация способа скрытой передачи информации, предложенного в работе [161] (см. также раздел 4.2, рис. 9), является некоторого рода усложнением схемы на основе нелинейного подмешивания информационного сигнала к хаотическому, заключающимся в появлении ещё двух идентичных генераторов на различных сторонах канала связи. Поэтому уравнения и параметры трёх генераторов, присутствующих в обеих схемах, оставим теми же самыми. Дополнительный генератор на передающей стороне канала связи описывается следующей системой уравнений:

$$\begin{aligned} \dot{z}_1 &= -\omega_z z_2 - z_3 + \varepsilon(y_1 - z_1)\,, \\ \dot{z}_2 &= \omega_z z_1 + a z_2\,, \\ \dot{z}_3 &= p + z_3(z_1 - c)\,, \end{aligned} \tag{12}$$

где $\mathbf{z}(t) = (z_1, z_2, z_3)$ — вектор состояния этого генератора, $\omega_z = 0{,}95$. Аналогичный генератор на принимающей стороне канала связи, характеризуемый вектором состояния $\mathbf{v}(t) = (v_1, v_2, v_3)$, также удовлетворяет системе уравнений (12) с точностью до замены $\mathbf{z}(t) \to \mathbf{v}(t)$, $\mathbf{y}(t) \to \mathbf{u}(t)$, где $\mathbf{u}(t) = (u_1, u_2, u_3)$ — вектор состояния принимающего генератора, удовлетворяющий системе уравнений (8), но в этом случае $s(t) = y_1 + z_1 - v_1 + D\xi$. Сигнал $-v_1$ не передаётся по каналу связи, а добавляется после прохождения через него, но до поступления на принимающий генератор.

Численная реализация способа скрытой передачи информации на основе фазовой хаотической синхронизации (см. раздел 4, рис. 6) на примере систем Рёсслера с близкими значениями управляющих параметров была осуществлена в работе [155]. В этом случае генераторы передающего и принимающего устройств описываются следующими системами уравнений:

$$\begin{aligned} \dot{x}_{1,2} &= -(\omega_x + \Delta\omega)\, y_{1,2} - z_{1,2} + \varepsilon(x_{2,1} - x_{1,2})\,, \\ \dot{y}_{1,2} &= (\omega_x + \Delta\omega)\, x_{1,2} + a y_{1,2}\,, \\ \dot{z}_{1,2} &= p + z_{1,2}(x_{1,2} - c)\,, \\ \dot{x}_3 &= -\omega_u y_3 - z_3 + \eta(r_3 \cos\phi_{\mathrm{m}} - x_3)\,, \\ \dot{y}_3 &= \omega_u x_3 + a y_3\,, \\ \dot{z}_3 &= p + z_3(x_3 - c)\,, \end{aligned} \tag{13}$$

где $\mathbf{x}_{1,2} = (x_{1,2}, y_{1,2}, z_{1,2})$, $\mathbf{x}_3 = (x_3, y_3, z_3)$ — векторы состояний генераторов передающего и принимающего устройств соответственно, $\omega_x = \omega_u = 1$, $\varepsilon = 5 \times 10^{-3}$ и $\eta = 5{,}3$ — параметры связи, $\Delta\omega = \pm 0{,}01$ — расстройка параметра ω_x, модулируемая полезным цифровым сигналом (знак плюс соответствует передаче бинарного бита 1, минус — бинарному биту 0), $r_3 = (x_3^2 + y_3^2)^{1/2}$ — амплитуда сигнала, генерируемого принимающей системой. Следует отметить, что бóльшая часть результатов, необходимых для сравнения этой схемы с рядом аналогов, описанных в настоящем обзоре, содержится в работе [155]. Поэтому результаты, касающиеся работоспособности этой схемы, представленные ниже, во многом основаны на этих материалах.

Численная реализация всех остальных рассмотренных способов скрытой передачи информации с вышеуказанными значениями управляющих параметров ещё раз подтверждает, что все они обладают весьма ограниченной устойчивостью к шумам[10]. Более того, несмотря на использование в них различных типов синхронного поведения и совершенно разные принципы их работы, качественно шум влияет на них совершенно одинаково.

Наиболее наглядно влияние шума на работоспособность способа скрытой передачи информации с помощью обобщённой хаотической синхронизации, предложенного в работе [109], иллюстрирует рис. 13, на котором наряду с информационным сигналом $m(t)$,

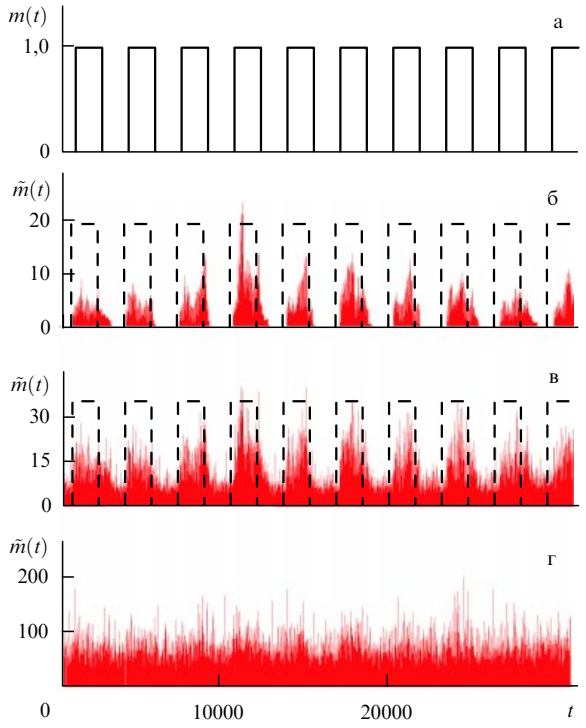

Рис. 13. Влияние шума в канале связи на эффективность способа скрытой передачи информации с помощью обобщённой хаотической синхронизации, предложенного в работе [109]. Информационный сигнал $m(t)$, представленный простой последовательностью бинарных битов 0/1 (а) и восстановленный сигнал $\tilde{m}(t)$ при различных значениях амплитуды шума: $D = 0$ — отсутствие шумов и флуктуаций в канале связи (б), $D = 1{,}5$ — шумы с достаточно слабой интенсивностью (в), $D = 3$ — шумы с более сильной интенсивностью (г). Видно, что в случаях (б) и (в) информационный сигнал может быть детектирован (штриховая линия), в то время как в случае (г) диагностировать информационный сигнал не представляется возможным.

[10] Для интегрирования стохастических дифференциальных уравнений, моделирующих генераторы передающего и принимающего устройств, во всех случаях, как и в разделе 6.1, использовался метод Эйлера с шагом дискретизации по времени $h = 0{,}0001$.

представленным простой последовательностью бинарных битов (рис. 13а), приведены восстановленные сигналы $\tilde{m}(t)$ (сплошные линии) при различных значениях амплитуды шума (рис. 13б–г). В отсутствие шумов в канале связи (рис. 13б) такой способ работает достаточно эффективно. Информационный сигнал тогда может быть легко детектирован по отсутствию/наличию хаотических колебаний в сигнале $\tilde{m}(t)$. Восстановленный таким образом сигнал показан штриховой линией. Нетрудно заметить, что качество передачи информации является достаточно высоким, хотя в некоторых случаях из-за наличия переходных процессов ошибочное диагностирование бинарного бита 1 остаётся возможным.

Появление шумов в канале связи приводит к возникновению шумов десинхронизации. Если интенсивность шума достаточно мала, то ещё остаётся возможность декодировать информационное сообщение $m(t)$ по восстановленному сигналу $\tilde{m}(t)$. Как видно из рис. 13в, соответствующего случаю $D = 1{,}5$, несмотря на наличие шумов десинхронизации во всём сигнале $\tilde{m}(t)$, участки, соответствующие бинарному биту 0, характеризуются более низкой амплитудой. Поэтому при правильном выборе порогового значения информационный сигнал можно будет детектировать; восстановленный сигнал показан штриховой линией.

Дальнейшее увеличение амплитуды шума приводит к "выравниванию" интенсивности амплитуд колебаний на участках, соответствующих бинарным битам 0 и 1 (см., например, рис. 13г, на котором показан сигнал $\tilde{m}(t)$ при $D = 3$). Нетрудно заметить, что в данном случае не имеется никакой возможности декодировать информационное сообщение.

Качественно аналогичная ситуация наблюдается для всех способов скрытой передачи информации, рассмотренных в разделах 3 и 4. Таким образом, проведённые исследования позволяют заключить, что на подавляющее большинство известных способов скрытой передачи информации шум влияет деструктивно. Однако, для того чтобы количественно сопоставить схемы друг с другом, необходимо оценить некоторые другие характеристики работоспособности этих схем.

6.3. Количественные характеристики работоспособности схем

Основными количественными характеристиками работоспособности схем скрытой передачи информации являются:

1. Критическое значение $\mathrm{SNR_c}$ отношения энергии на бит к спектральной плотности мощности шума (SNR) [172, 173], при котором схема передачи данных становится неработоспособной, т.е. оказывается невозможным восстановление исходного полезного цифрового сигнала $m(t)$ по получаемому на выходе сигналу $\tilde{m}(t)$. Отношение энергии на бит к спектральной плотности шума, которое вводится в рассмотрение для цифровых систем связи, является аналогом отношения сигнал/шум в аналоговой связи:

$$\mathrm{SNR} = 10 \lg \frac{E_\mathrm{b}}{N_0} \ [\text{дБ}], \tag{14}$$

где E_b — энергия сигнала, приходящаяся на один бит передаваемой информации, N_0 — спектральная плотность мощности шума. При этом энергия, приходящаяся на один бит, описывается как

$$E_\mathrm{b} = P_\mathrm{sign} T, \tag{15}$$

где $\mathrm{P_{sign}}$ — мощность передаваемого сигнала в отсутствие шума, T — время передачи одного бита, а спектральная мощность шума определяется как

$$N_0 = \frac{P_\mathrm{noise}}{\Delta f}, \tag{16}$$

где P_noise — мощность шума в канале связи, Δf — ширина полосы пропускания канала. Так как шумы неизбежно присутствуют в каналах связи реальных устройств, оценка работоспособности схем передачи информации при наличии шумов является очень важной и актуальной задачей.

Расчёт мощности как детермированного, так и стохастического сигналов осуществлялся по их временно́й реализации. При проведении численных расчётов предполагалось, что ширина полосы пропускания $\Delta f = f_2 - f_1 = 0{,}2$, где $f_1 = 0{,}05$, $f_2 = 0{,}25$ — границы полосы пропускания канала в случае использования генераторов Рёсслера.

Для характеристики степени устойчивости схем скрытой передачи информации по отношению к внешним шумам в цифровых системах связи достаточно часто используют, наряду с характеристикой, описанной выше, зависимость вероятности ошибки на бит (BER — Bit Error Rate) от отношения энергии на бит к спектральной плотности мощности шума [174]. Вероятность ошибки на бит характеризует качество передачи информации и представляет собой количество ошибок, отнесённое к числу переданных битов. Предположим, что схема корректно передаёт бинарный бит 0 с вероятностью P_{00} и бинарный бит 1 с вероятностью P_{11}. Тогда ошибочное диагностирование бинарного бита 1 при передаче бинарного бита 0 характеризуется вероятностью $P_{01} = 1 - P_{00}$, а вероятность $P_{10} = 1 - P_{11}$ характеризует ошибочное диагностирование бинарного бита 0 при передаче бинарного бита 1. Если символы появляются в передаваемой последовательности с вероятностями P_0 и P_1 соответственно, то вероятность ошибки на бит вычисляется следующим образом:

$$\mathrm{BER} = 2(P_{01} P_0 + P_{10} P_1), \tag{17}$$

причём вероятности P_{01} и P_{10} зависят от типа и параметров системы связи.

2. Максимальное значение $\mathrm{PM_c}$ расстройки управляющих параметров (PM, %) генераторов, которые изначально должны быть идентичными. Как уже обсуждалось в разделах 3 и 4, в большинстве случаев такие генераторы должны располагаться на различных сторонах канала связи. Ввиду сложности технической реализации таких устройств влияние расстройки их управляющих параметров на эффективность работы способов передачи информации является весьма актуальной проблемой.

3. Максимальный уровень $\mathrm{ND_c}$ нелинейных искажений в канале связи, при котором схема работает:

$$\mathrm{ND} = 10 \lg \frac{P_x}{P_y} \ [\text{дБ}]. \tag{18}$$

Здесь P_x — мощность сигнала $x(t)$ на выходе передающего генератора, P_y — мощность сигнала $y(t)$ на входе принимающего устройства. Традиционно в численных расчётах используются нелинейные искажения в виде кубической нелинейности $y = x(1 - \alpha x^2)$, где α — малый параметр [23], поэтому далее будем считать, что при прохождении через каналы связи всех схем и устройств сигнал претерпевает искажения такого рода.

Для того чтобы количественно сравнить способы скрытой передачи информации, описанные в настоящем обзоре, оценим вышеупомянутые характеристики для всех рассмотренных схем. Следует отметить, что в работе [23] была введена другая характеристика работоспособности схемы передачи данных, основанная на оценке степени близости сигналов, которая определяется как

$$\eta = \frac{\Delta P}{P}\,, \tag{19}$$

где ΔP — мощность шума десинхронизации, P — мощность шума на входе генератора. Однако данная характеристика имеет смысл только для схем, основанных на полной хаотической синхронизации, поэтому в целях достижения общности и возможности сравнения различных методов мы её здесь не рассматриваем.

Результаты расчёта количественных характеристик работоспособности схем представлены в таблице.

Как видно из таблицы, схема 9, описанная в разделе 5.2, становится неработоспособной при отношении энергии на бит к спектральной плотности шума $\mathrm{SNR_c} = -10{,}01$ дБ, в то время как для других рассмотренных нами схем $\mathrm{SNR_c}$ оказывается положительным. То есть при наличии в канале связи шумов определённого уровня (даже если мощность шумов меньше мощности передаваемого сигнала) большинство схем становится неработоспособным. Понятно, что значения таких характеристик будут меняться от схемы к схеме. Из схем 1–8 лучшими в этом отношении являются схемы на основе переключения хаотических режимов и модулирования управляющих параметров (схемы 2 и 4, $\mathrm{SNR_c} = 30{,}76$ дБ). Но положительное значение отношения энергии на бит к спектральной плотности шума свидетельствует об ограниченной устойчивости к шумам и деструктивной роли шума при передаче информации.

Схема 9, описанная в разделе 5.2, обладает значительной устойчивостью к шумам в канале связи. При этом, ещё более искажая передаваемый сигнал, шум препятствует третьей стороне декодировать информационное сообщение. В этом случае можно говорить о конструктивной роли шума в повышении конфиденциальности передачи информации, тогда как в остальных случаях роль шума является деструктивной.

Справедливость вышеприведённых рассуждений подтверждается также зависимостью вероятности ошибки на бит от спектральной плотности мощности шума для различных схем скрытой передачи информации. Указанные зависимости представлены на рис. 14. При расчёте вероятности ошибки на бит пороговое значение, позволяющее восстановить исходную последовательность

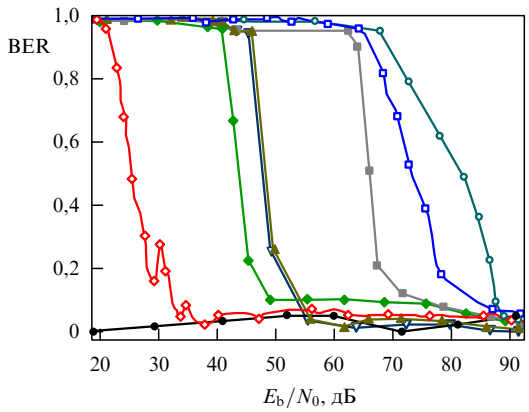

Рис. 14. Зависимости вероятности ошибки на бит (BER) от отношения энергии на бит к спектральной плотности мощности шума (E_b/N_0) для различных схем скрытой передачи информации: ○ — хаотическая маскировка, ◆ — переключение хаотических режимов (модулирование управляющих параметров), ■ — нелинейное подмешивание, ◇ — схема на основе режима фазовой синхронизации (кривая частично перенесена из работы [155], ▲ — схема на основе режима обобщённой синхронизации, △ — схема на основе обобщённой и полной синхронизации, □ — схема с комбинированным сигналом, ● — сверхустойчивая к шумам схема.

Таблица. Критические значения отношения энергии на бит к спектральной плотности шума $\mathrm{SNR_c}$, расстройки управляющих параметров $\mathrm{PM_c}$ изначально идентичных генераторов и уровня нелинейных искажений в канале связи $\mathrm{ND_c}$

№	Название схемы	$\mathrm{SNR_c}$, дБ	$\mathrm{PM_c}$, %	$\mathrm{ND_c}$, дБ	Раздел*	Литература
1	Хаотическая маскировка	56,48	0,30	1,03	3.1	[25]
2	Переключение хаотических режимов	30,76	2,00	23,3	3.2	[145]
3	Нелинейное подмешивание	64,99	0,30	0,26	3.3	[146]
4	Модулирование управляющих параметров	30,76	2,00	23,3	3.4	[147]
5	Схема на основе режима фазовой синхронизации	32,40	0,80	10,7	4	[155]
6	Схема на основе режима обобщённой синхронизации	39,52	1,00	7,75	4.1	[109]
7	Схема на основе обобщённой и полной синхронизации	39,24	0,50	4,83	4.2	[109]
8	Схема со "сложным сигналом"	61,47	0,20	2,63	4.2	[161]
9	Сверхустойчивая к шумам схема	−10,01	2,00	27,2	5.2	[162]

* Раздел настоящего обзора.

бинарных битов по сигналу $\tilde{m}(t)$, выбиралось фиксированным независимо от интенсивности шума, воздействующего на систему, тогда как при определении характеристик, представленных в таблице, оно менялось. В то же время, как видно из рис. 14, для различных способов скрытой передачи информации (схемы 1–8 таблицы) вероятность ошибки на бит достаточно быстро становится равной 1, тогда как для сверхустойчивого к шуму способа (схема 9) она оказывается близкой к 0, вне зависимости от интенсивности шума, воздействующего на систему, что достаточно хорошо согласуется с результатами, представленными выше.

Оценим теперь влияние расстройки управляющих параметров на эффективность работы рассмотренных способов скрытой передачи данных. Для этого введём расстройку в параметр ω_u одной из двух изначально идентичных систем (т.е. если имеются две пары идентичных систем, то расстроим по параметру ω каждую пару). Тогда параметр ω одной из систем заменится параметром $\omega(1 \pm \eta)$, где η — расстройка по ω (РМ). Для определённости во всех случаях будем брать знак "плюс" (аналогичные результаты получены при выборе знака "минус").

Подобные оценки позволяют заключить, что схема на основе режима обобщённой синхронизации (см. раздел 5) будет оставаться работоспособной до тех пор, пока генераторы принимающего устройства не будут расстроены более чем до 2 % по параметру ω_u. Конечно, это не столь большая величина, и в этом отношении рассматриваемая схема имеет конкурентов, которыми снова являются схемы передачи информации на основе переключения хаотических режимов и модулирования управляющих параметров (схемы 2 и 4 в таблице соответственно). Однако схема 9 и с этой точки зрения обладает принципиальным преимуществом перед схемами 2 и 4. Изначально идентичные хаотические генераторы в схемах 2 и 4 таблицы (так же как и во всех остальных, кроме схемы 9) должны располагаться на различных сторонах канала связи (для возможности реализации режима полной синхронизации между ними). В схеме 9 идентичные генераторы располагаются только на принимающей стороне канала связи, что позволяет легко осуществить при необходимости их юстировку.

Что касается устойчивости к нелинейным искажениям в канале связи, то и по этой характеристике рассмотренная в разделе 5 схема превосходит все известные аналоги. Понятно, что чем больше влияние нелинейных искажений на сигнал, тем выше должен быть максимально допустимый уровень нелинейных искажений, при котором способ скрытой передачи данных будет оставаться ещё работоспособным. Как видно из таблицы, максимальный уровень нелинейных искажений для схемы 9 $\mathrm{ND_c} = 27{,}2$ дБ. Наиболее близкими показателями опять обладают способы скрытой передачи информации на основе переключения хаотических режимов и модулирования управляющих параметров (схемы 2 и 4), однако устойчивость схемы 9 к нелинейным искажениям оказывается несколько выше. Кроме того, схемы 2 и 4 обладают ограниченной устойчивостью к шумам, в то время как устойчивость схемы 9 является практически неограниченной в реальных пределах.

Понятно, что изменение значений управляющих параметров и уравнений генераторов (например, во всех случаях в передающем и принимающем устройствах можно использовать генераторы Чуа [175, 176], кольцевые генераторы хаоса с запаздыванием [151, 177–179], генераторы хаоса на основе систем фазовой автоподстройки [180–183], генераторы хаоса с 2,5 степенями свободы [184] и т.д.), а также изменение характера распределения случайной величины ξ может привести к изменению количественных значений анализируемых характеристик. В то же время порядки этих величин и соотношения между ними всегда будут оставаться примерно одинаковыми (см., например, [78]). Более того, как будет показано в разделе 7, соответствующие результаты хорошо согласуются с результатами экспериментальных исследований передачи информации как в радиодиапазоне, так и оптическом диапазоне. В частности, следует отметить, что теоретически полученный вывод о сильной чувствительности работоспособности схем, основанных на использовании полной и обобщённой синхронизаций, к расстройке параметров генераторов, расположенных на различных сторонах канала связи, подтверждается рядом проведённых в Институте радиотехники и электроники РАН под руководством А.С. Дмитриева экспериментальных исследований, которые рассмотрены более подробно в разделе 7.1. Здесь только отметим, что в работе [23] обнаружено, что допустимая расстройка генераторов на различных сторонах канала связи обычно не превышает 0,5–1 %. Так, было показано, что для схемы, основанной на хаотическом синхронном отклике, увеличение расстройки даже одного параметра на 3–4 % приводит к полному разрушению синхронизации и потере работоспособности схемы. В качестве генераторов хаоса в данном эксперименте рассматривались схемы Чуа. Разрушение синхронного режима происходило по сценарию on-off-перемежаемости [185–187], который характеризуется срывом синхронизации в отдельные моменты времени [185, 188]. Следует отметить, что использование кольцевых генераторов хаоса обычно позволяет предотвратить возникновение перемежающегося поведения [23].

7. Экспериментальная реализация схем передачи информации на основе хаотической синхронизации

Итак, в разделах 2–6 были рассмотрены теоретические основы и различные конкретные схемы реализации передачи информации на основе явления хаотической синхронизации. Детальный теоретический и численный анализ разнообразных методов передачи информации с использованием хаотической синхронизации выявил основные преимущества и недостатки различных схем, а также позволил предложить новые методы передачи на основе обобщённой хаотической синхронизации, которые свободны от ряда выявленных недостатков. Необходимо отметить, что положенный в основу этого рассмотрения подход, опирающийся на численное моделирование и анализ различных схем, представляется весьма важным, так как, с одной стороны, он позволил провести анализ большого числа схем с единых позиций, выявить однотипным образом недостатки и достоинства каждого из рассмотренных методов, что было бы весьма сложно сделать, например, при экспериментальном исследовании. В последнем случае было бы чрезвычайно сложно реализовать сходные условия постановки экспе-

риментов и создания макетов для самых различных схем. С другой стороны, методы численного моделирования и анализа становятся всё более стандартными методами проектирования и отладки современных телекоммуникационных систем, позволяя проводить первые этапы работ с помощью компьютерных технологий. Известны различные комплексы программного обеспечения, такие как MultiSim [11], Micro-Cap [12], Microwave Office [13], позволяющие проводить моделирование подобных систем на уровне инженерных расчётов, что даёт возможность уже на основе численных расчётов создавать вполне работоспособные макеты устройств. Всё это делает численное моделирование весьма мощным средством анализа и исследования приложений теории хаоса в области передачи информации. Удачные примеры использования подобных технологий в научных исследованиях приведены, в частности, в монографии А.С. Дмитриева, А.И. Панаса [23]. Тем не менее необходимость экспериментальных исследований при таком подходе не только не снижается, но и значительно повышается. В этом случае исследования экспериментальных макетов позволяют, во-первых, подтвердить основные теоретические выводы, а во-вторых, уточнить математические модели и те предположения, которые были положены в их основу. Поэтому только детальное сопоставление данных и тесное взаимосвязанное проведение теоретических и экспериментальных работ могут дать ответ на вопрос о реальности применения тех или иных идей на практике.

Поэтому ниже в этом разделе мы остановимся подробнее на некоторых основных результатах экспериментального исследования схем передачи информации с использованием хаотической синхронизации. Следует отметить, что работ, посвящённых экспериментальным исследованиям этой проблемы, существенно меньше, чем работ, содержащих результаты численного рассмотрения, что обусловлено прежде всего сложностями, связанными с практической реализацией таких схем. Одной из основных проблем здесь является создание эффективных генераторов хаотических сигналов для подобных систем. Основные требования к таким генераторам являются достаточно очевидными и могут быть сформулированы на основе предыдущего рассмотрения: возможность хаотической синхронизации, возможность построения идентичных легко тиражируемых генераторов, лёгкая управляемость, что необходимо для введения информационного сигнала в хаотический сигнал и т.д. Наибольшие успехи здесь достигнуты в радиочастотном и оптическом диапазонах длин волн и значительно меньшие — в микроволновом (СВЧ) диапазоне, поэтому представляется наиболее целесообразным рассмотреть примеры экспериментальных реализаций схем передачи информации и возможности получения синхронизации хаотических колебаний отдельно для радиотехнических и оптических систем.

7.1. Экспериментальная реализация схем передачи информации в радио- и микроволновом диапазонах

Большинство экспериментальных работ по реализации различных методов передачи информации с использованием явления хаотической синхронизации выполнено на базе радиотехнических систем. При этом были предприняты попытки реализации некоторых вышеописанных схем на основе полной хаотической синхронизации. Наиболее планомерные исследования по реализации и технической оптимизации систем передачи информации с применением хаотических сигналов в качестве носителя информации были проведены на основе схем хаотической маскировки (и модификации этих схем, использующих понятие синхронного отклика [94]), переключения хаотических режимов и нелинейного подмешивания информационного сигнала к хаотическому. Исторически одной из первых предложенных схем скрытой передачи информации с использованием синхронизации хаоса стала хаотическая маскировка, поэтому большое количество экспериментальных работ было выполнено именно для этой схемы.

В работе [189] продемонстрирована возможность передачи информационных сообщений при использовании переключения хаотических режимов и хаотической маскировки на основе низкочастотного (НЧ) радиотехнического генератора, реализующего систему Лоренца. Схема работала в диапазоне частот 0–10 кГц. На рисунке 15 показаны характеристики работы схемы: тестовый информационный сигнал $m(t)$, представляющий собой последовательность битов, который модулировал параметры передающего генератора, и квадрат восстановленного сигнала $\tilde{m}^2(t)$. Состояние сигнала $m = 0$ соответствовало полной синхронизации принимающего устройства, состояние $m = 1$ — асинхронной динамике. Хорошо видно, что система демонстрирует возможность передачи цифрового сигнала. В работе [189] на основе тех же радиотехнических генераторов также была реализована схема с хаотической маскировкой, которая использовалась уже для передачи аналоговых сигналов (речевых сообщений). На рисунке 16а, б показан пример передаваемого и восстановленного звукового сообщения "He has the bluest eyes". Данная схема оказалась работоспособной только при достаточно большом отношении информационный сигнал/маскирующий хаотический сигнал — порядка 20–30 дБ, что делает

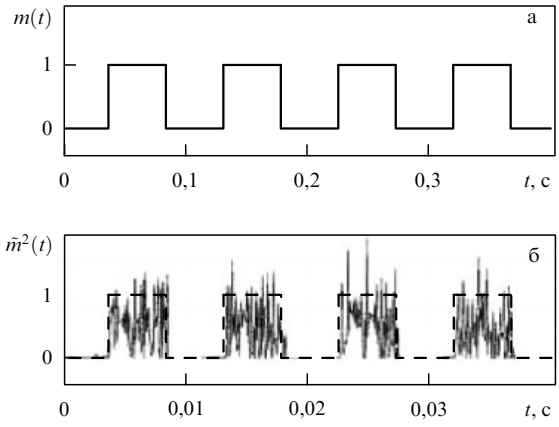

Рис. 15. Иллюстрация экспериментальной реализации схемы передачи информации на основе переключения хаотических режимов: (а) информационный сигнал $m(t)$, представленный простой последовательностью бинарных битов 0/1, (б) восстановленный в принимающем устройстве сигнал $\tilde{m}^2(t)$ (сплошная линия). Штриховой линией представлен детектированный информационный сигнал. (Из работы [189].)

[11] www.ni.com/multisim
[12] www.spectrum-soft.com/index.shtm
[13] web.awrcorp.com/Russian

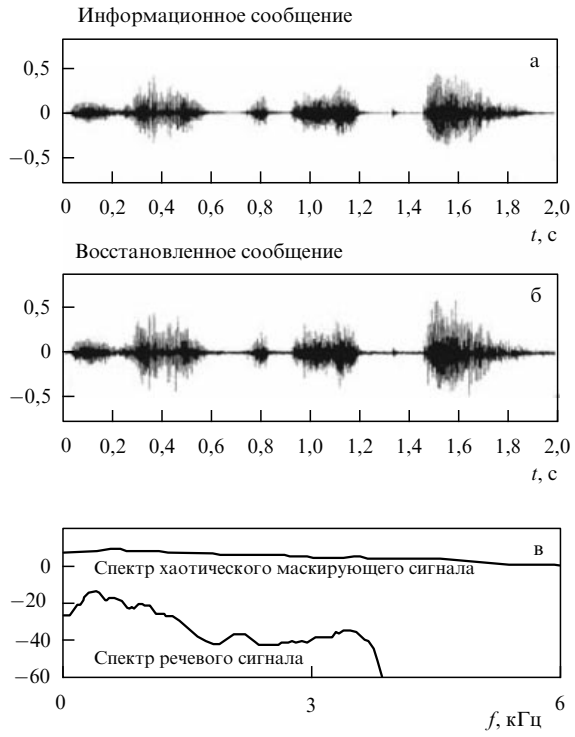

Рис. 16. Результаты экспериментов по передаче аналоговой информации с помощью метода хаотической маскировки: передаваемое (а) и детектированное (б) на выходе приёмного устройства речевое сообщение, соотношение спектров мощности информационного и маскирующего хаотического сигнала (в). (Из работы [189].)

передаваемый информационный сигнал соизмеримым с уровнем шумов канала связи (рис. 16в). В работе [189] не были проведены эксперименты по анализу устойчивости данных схем к неидентичности генераторов и уровню шумов в канале связи. Впервые проведённые в работе [148] специальные эксперименты по выявлению условий работоспособности схем передачи информации с использованием полной хаотической синхронизации показали, что существуют очень жёсткие требования к отношению сигнал/шум, идентичности систем на обоих концах канала связи и т.д. для схем переключения хаотических режимов, хаотической маскировки и нелинейного подмешивания, что полностью согласуется с нашим теоретическим рассмотрением.

Детальные исследования вопросов передачи информационных сообщений с использованием хаотической синхронизации были проведены в работах группы А.С. Дмитриева (ИРЭ РАН), обобщённых в монографии [23]. В этих работах, во-первых, были проведены эксперименты по передаче информации с использованием хаоса в радиодиапазоне на основе схемы с нелинейным подмешиванием информации с использованием стандартных систем связи с амплитудной модуляцией [146, 190]. Основной проблемой данной схемы стали искажения сигналов, связанные с переносом хаотических НЧ-сигналов в радиодиапазон и обратно. В качестве рабочей несущей частоты в эксперименте была выбрана частота 27 МГц. Во время этой процедуры над сигналами осуществлялись дополнительные манипуляции (которые не проводились в рассмотренных выше НЧ-экспериментах): усиление, модуляция, фильтрация, демодуляция и т.д., каждая из которых приводит к дополнительным искажениям и тем самым затрудняет получение в принимающем устройстве точной копии переданного хаотического сигнала для обеспечения полной хаотической синхронизации. Поэтому достижение необходимой точности прямых и обратных преобразований сигнала, а также учёт шумов и фильтрации в канале связи при постановке подобных экспериментов выходят на первый план. Было показано, что для качественной передачи информации суммарные искажения вдоль цепочки преобразований сигнала в передающем и принимающем устройствах не должны превышать 1 – 2 %, что представляется очень жёстким условием с точки зрения реализации в эксперименте. Вместе с тем эксперименты [23] показали принципиальную возможность проводной и беспроводной передачи информации в радиодиапазоне с использованием схемы с нелинейным подмешиванием. Однако одновременно были выявлены также определённые сложности и ограничения этой системы передачи информации.

Так, было показано, что точность соответствия параметров одинаковых по функциональному назначению элементов в передающем и принимающем устройствах должна быть не менее 0,5 %. Однако даже при таком условии не наблюдалось хорошего качества полной хаотической синхронизации. Это было связано с неудачным выбором генератора хаотического сигнала на базе схемы Чуа [176, 191, 192] для приёмного и передающего устройств. Для данной схемы не наблюдается устойчивого отклика, возникают эффекты on-off-перемежаемости, что резко ухудшает качество приёма информационного сообщения. Очень серьёзным ограничением работоспособности схемы оказались и искажения сигнала в канале связи, которые проявлялись как в виде неравномерности амплитудно-частотной характеристики канала связи (фактически в фильтрации передаваемого сигнала), так и в виде нелинейных искажений. Специально проведённые эксперименты показали, что эффективность схемы определяется соотношением частоты среза ω_c фильтра высоких частот, которым моделировались искажения в канале связи, и верхней граничной частоты Ω спектра мощности сигнала на выходе передающего устройства. При $\omega_c \gg \Omega$ фильтрация не сказывалась на качестве передачи информации, однако сопоставимость этих величин, $\omega_c \sim \Omega$, приводила к ухудшению качества детектирования информационного сигнала [193].

Возрастание нелинейных искажений также приводило к быстрой потере работоспособности схемы. В частности, при коэффициенте нелинейных искажений 1 % от амплитуды сигнала отношение сигнал/шум на выходе принимающего устройства составляло 35 – 40 дБ, а при коэффициенте нелинейных искажений 10 % уменьшалось до 10 дБ. Аналогичную динамику показывала экспериментальная схема и при увеличении влияния аддитивного нормально распределённого шума в канале связи при беспроводной передаче информации: с возрастанием мощности шума отношение сигнал/шум на выходе приёмного устройства увеличивается значительно быстрее, чем отношение сигнал/шум в канале связи (на входе в принимающее устройство), что объясняется потерями качества при выделении подмешанного информационного сигнала из хаотического путём установления режима полной хаотической синхронизации в приёмнике. Здесь опять большую роль играла необходимость выбора более эффективного источника хаотического сигнала в передающем и принимающем устройствах.

В связи с этим в работах А.С. Дмитриева с соавторами был исследован важный вопрос об оптимальных радиотехнических генераторах хаотического сигнала для коммуникационных применений. Как отмечалось в разделе 6.3, был сделан вывод о наибольшей перспективности кольцевых схем построения подобных систем, что связано с их большей стабильностью и отсутствием срывов полной синхронизации при расстройке параметров ведущего и ведомого генераторов (on-off-перемежаемости) [178]. Исследования показали, что устойчивость кольцевых схем к расстройке параметров и внешним шумам примерно в 2–3 раза выше, чем классических радиотехнических источников хаоса на основе цепи Чуа [23, 178, 194, 195]. Также важным достоинством кольцевых генераторов хаоса является их прецизионность, под которой авторы [23, 196] понимают воспроизводимость сходных хаотических режимов в различных образцах и при замене одних элементов схемотехнического решения другими в одном генераторе, низкая чувствительность к изменениям внешних условий (например, температуры), а также то, что при реализации синхронных режимов синхронизируемый прецизионный генератор хаоса демонстрирует устойчивый отклик без срывов синхронизации в те или иные моменты времени. Альтернативным решением проблемы выбора генераторов хаоса для коммуникационных систем стало применение цифровых сигнальных процессоров для реализации схемы передачи информации с нелинейным подмешиванием [197].

Итогом этих исследований стало создание экспериментальных макетов коммуникационных систем низкочастотного диапазона и радиодиапазона, на которых была показана принципиальная возможность реализации передачи информации на основе схемы с нелинейным подмешиванием информационного сигнала к хаотическому [23]. Следует отметить, что противоречивыми требованиями здесь стали требования высокого качества и конфиденциальности передачи информации: улучшение качества передачи информации снижало скрытность передачи и наоборот.

Следует отметить, что роль вышеописанных коммуникационных хаотических систем, функционирующих в низкочастотном диапазоне и радиодиапазоне, в основном ограничивается апробированием тех или иных технических решений, выбором оптимальных генераторов хаотического сигнала и схем передачи информации. Очевидно, что для использования на практике методов скрытой передачи информации с использованием синхронизации хаотических колебаний необходим переход в микроволновый диапазон, который активно эксплуатируется в современных телекоммуникационных системах. Однако подобных работ, в которых бы исследовалась хаотическая синхронизация и методы передачи информации на её основе в микроволновом диапазоне, практически нет, что, по-видимому, обусловлено сложностью проведения соответствующих экспериментов. Одновременно возникает проблема диагностики режимов хаотической синхронизации генераторов хаоса СВЧ-диапазона, которые требуют использования дорогостоящей цифровой измерительной аппаратуры и разработки специальных методов анализа. Единственными известными авторам исследованиями в данном направлении являются работы [198, 199].

В докладе [198] было сообщено о первой (и, видимо, пока единственной) попытке создать экспериментальный прототип системы передачи информации с генераторами хаоса на основе мощного СВЧ-усилителя (широкополосной лампы бегущей волны (ЛБВ)), которая может применяться для передачи информации на большие расстояния, в том числе, в спутниковых системах. В качестве источника хаотического сигнала выступал генератор, построенный по кольцевой схеме с запаздывающей обратной связью на базе мощной ЛБВ диапазона 2–4 ГГц, созданный в Университете штата Висконсин [200]. Генераторы хаоса СВЧ-диапазона на основе ЛБВ с запаздывающей обратной связью, которые являются одними из первых исследованных источников хаотического сигнала, впервые были предложены в работах Кислова В.Я. и др. (ИРЭ РАН) [201–203] и позднее подробно исследовались в различных хаотических режимах в работах [200, 204–206]. До сих пор подобные системы являются одними из наиболее надёжных, простых и мощных источников хаотического сигнала в СВЧ-диапазоне, поэтому выбор именно такого генератора для прототипа телекоммуникационных систем был наиболее оправдан. В качестве метода для передачи информации в работе [198] использовался простейший метод хаотической маскировки (см. раздел 3.1), который позволил продемонстрировать принципиальную возможность работы схемы с мощными вакуумными СВЧ-приборами для передачи информации с использованием режима хаотической синхронизации. Схема эксперимента практически полностью совпадала с приведённой в разделе 3.1 (см. рис. 2). Теоретически подобная схема с генератором на основе ЛБВ-усилителя ранее была рассмотрена в работе [207]. Внешний вид экспериментальной СВЧ-установки представлен на рис. 17 [198]. Информационный сигнал смешивался с хаотическим в цепи запаздывающей обратной связи, которой был охвачен ЛБВ-усилитель. Хаотический СВЧ-сигнал с примешанным к нему информационным аналоговым сообщением излучался с помощью рупорной антенны (см. рис. 17) и затем поступал в приёмник, который содержал почти идентичную копию передающего генератора. Предварительные исследования показали возможность скрытой передачи информации в такой, основанной на явлении полной хаотической синхронизации, схеме, однако результаты дальнейших исследований в работе [198] не представлены.

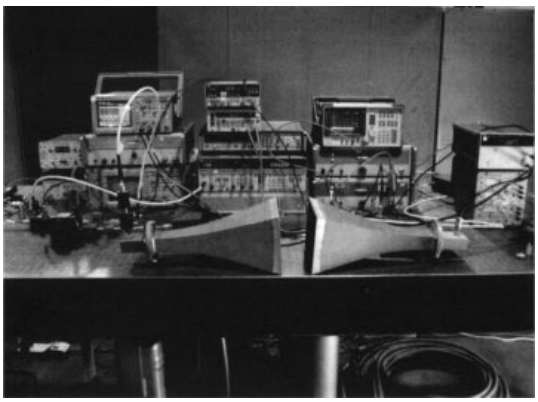

Рис. 17. Экспериментальная установка для скрытой передачи информации с помощью метода хаотической маскировки в СВЧ-диапазоне (2–4 ГГц) на основе ЛБВ с запаздывающей обратной связью. (Из работы [198].)

Вместе с тем вопрос о применении других типов хаотической синхронизации для передачи информации в СВЧ-диапазоне по-прежнему остаётся открытым. Наиболее важным здесь с точки зрения создания систем передачи информации является реализация режимов обобщённой хаотической синхронизации в микроволновом диапазоне в системах, которые можно было бы использовать в качестве задающих и принимающих генераторов хаоса в телекоммуникационных системах. Следует отметить, что из всех типов хаотической синхронизации обобщённая синхронизация хуже всего изучена экспериментально и все основные результаты для неё получены в низкочастотном диапазоне [97, 156], который, как отмечалось выше, не представляет существенного интереса для телекоммуникационных систем, и роль данных работ заключается в экспериментальном подтверждении возможности реализации обобщённой хаотической синхронизации, а также различных методов её диагностики.

Пока единственной работой, в которой были проведены соответствующие исследования, является экспериментальная работа [199]. В этой работе была показана возможность возникновения режима обобщённой хаотической синхронизации в связанных клистронных генераторах хаоса сантиметрового диапазона длин волн. Клистронные генераторы хаоса, созданные на основе многорезонаторных клистронных усилителей по кольцевой схеме, демонстрируют стабильную генерацию хаотических сигналов в широком диапазоне управляющих параметров [208–210]. Схема эксперимента, который реализует однонаправленную связь между двумя микроволновыми хаотическими генераторами, показана на рис. 18а. С увеличением связи в системе наблюдалось установление режима обобщённой хаотической синхронизации. Для её диагностики был предложен эффективный метод для микроволнового диапазона, основанный на анализе спектров генерируемых сигналов, который в перспективе может найти применение в системах передачи информации, основанных на обобщённой хаотической синхронизации [199].

Для анализа синхронизации также использовалась модификация метода вспомогательной системы, который подробно описан в разделе 2. Результаты представлены на рис. 18б, в, где показаны экспериментальные временны́е ряды сигналов ведущего $x(t)$ и ведомого $y(t)$ генераторов, полученные с помощью высокочастотного цифрового осциллографа. В ходе экспериментов был выбран временной интервал T длительностью 130 нс, который примерно соответствовал времени запаздывания в цепи обратной связи генератора. Затем выбирались два временны́х интервала: $\Delta_1 = (t_1, t_1 + T)$ и $\Delta_2 = (t_2, t_2 + T)$, в которых отрезки сигнала ведущего

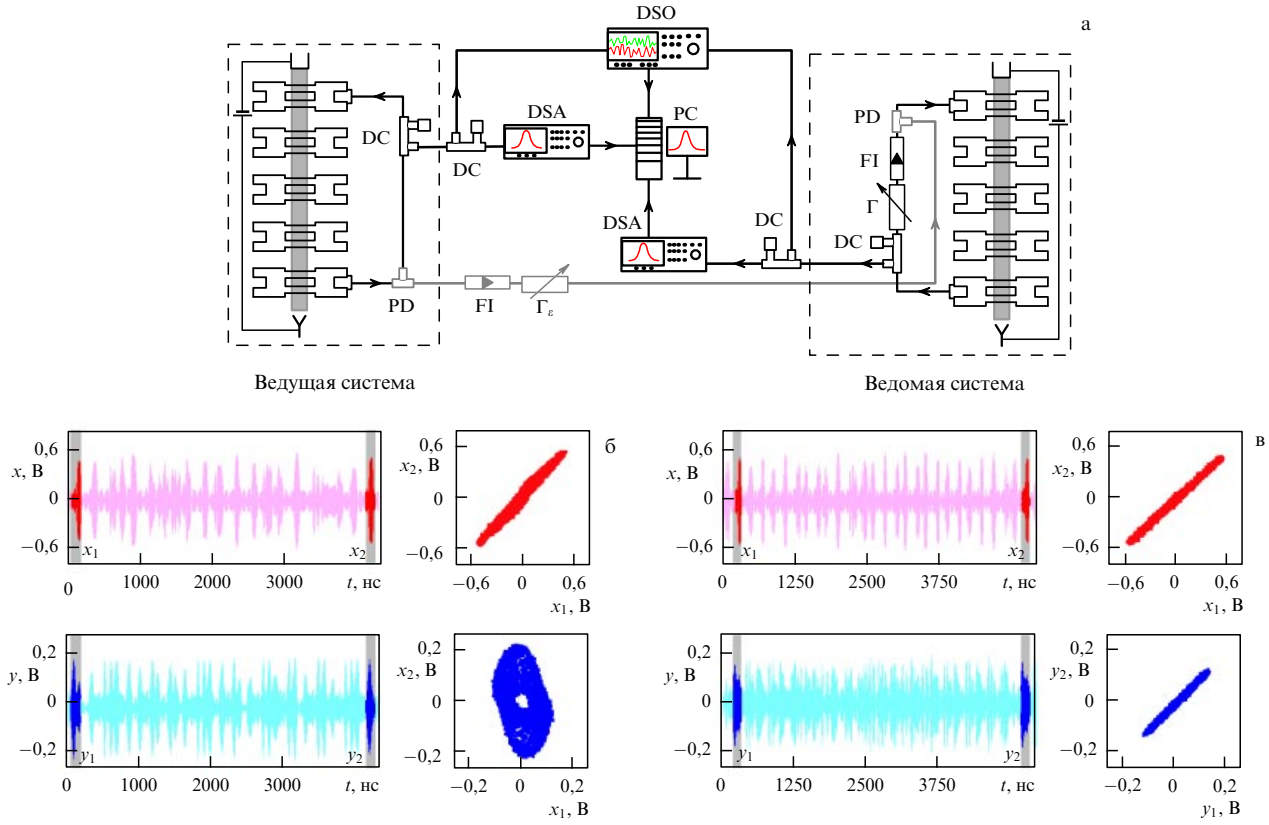

Рис. 18. (а) Схема эксперимента по наблюдению обобщённой синхронизации в микроволновом диапазоне на базе клистронных генераторов хаоса с линией обратной связи. Штиховыми рамками обозначены клистронные генераторы хаоса на основе пятирезонаторных пролётных клистронов КУ-12 с запаздывающей обратной связью. FI — ферритовый вентиль, PD — делитель мощности, Г — волноводный аттенюатор, DSO — цифровой ВЧ-осциллограф (Agilent Technologies DSO81004B), DSA — спектроанализаторы, PC — персональный компьютер. (б, в) Выделенные фрагменты временны́х рядов выходных сигналов ведущего, $x(t)$, и ведомого, $y(t)$, генераторов, а также соответствующие корреляционные диаграммы (x_1, x_2) и (y_1, y_2) для малой и большой связи ε между генераторами: (б) $\varepsilon = 0{,}1$ (отсутствие режима обобщённой синхронизации); (в) $\varepsilon = 0{,}89$ (режим обобщённой хаотической синхронизации). Связь между ведущим и ведомым генераторами регулировалась волноводным аттенюатором Γ_ε, включённым в цепь.

генератора $x_1(t)$ и $x_2(t)$ были близки между собой, $(x_1(t) \approx x_2(t))$. Одновременно рассматривались отрезки $y_1(t)$ и $y_2(t)$ сигнала ведомой системы в тех же временны́х интервалах. Согласно методу вспомогательной системы режим обобщённой синхронизации соответствует ситуации, при которой состояния ведомой системы в интервалы времени Δ_1 и Δ_2 близки друг другу: $y_1(t) \approx y_2(t)$. Это иллюстрируют диаграммы (x_1, x_2) и (y_1, y_2), представленные на рис. 18б, в для различных коэффициентов связи между генераторами. Диаграммы (x_1, x_2) иллюстрируют близость двух выбранных состояний ведущей системы, диаграммы (y_1, y_2) представляют метод диагностики обобщённой синхронизации. Хорошо видно, что в случае малой связи состояния $y_1(t)$ и $y_2(t)$ ведомого генератора в те моменты времени, в которые ведущий клистронный генератор демонстрирует идентичную динамику, различны, т.е. функциональной связи между состояниями не наблюдается. С увеличением связи между однонаправленно связанными генераторами ситуация меняется: состояния $y_1(t)$ и $y_2(t)$ становятся идентичными, о чём свидетельствует наличие диагонали на плоскости (y_1, y_2). Данные результаты являются первым экспериментальным подтверждением возможности наблюдения обобщённой синхронизации в микроволновом диапазоне и дают основания предположить возможность эффективной диагностики и, как следствие, использования режимов обобщённой синхронизации в современных системах передачи и обработки информации.

7.2. Эксперименты по передаче информации с помощью хаотической синхронизации в оптическом диапазоне

В разделе 7.1 мы рассмотрели некоторые важные экспериментальные исследования по передаче информационных сигналов с использованием хаотической синхронизации в радио- и микроволновом диапазонах. В то же время сейчас представляются весьма перспективными и поэтому активно исследуются и совершенствуются генераторы хаотических колебаний в оптическом диапазоне на основе различных кольцевых схем, использующих в качестве активного элемента лазеры [211, v. 2, ch. 4, p. 353 – 427]. Ряд экспериментов показал, что подобные системы могут рассматриваться как эффективные легко управляемые генераторы хаотических автоколебаний для систем передачи информации (см., например, [93, 212 – 216]). Позднее в оптическом диапазоне были обнаружены различные типы хаотической синхронизации, включая полную, обобщённую и фазовую [121, 122, 215, 216 – 221], что открыло возможности использования оптических систем в качестве базовых элементов для создания схем передачи информации на основе эффекта хаотической синхронизации [222 – 225].

Уже первые лабораторные эксперименты по передаче сигналов с помощью хаотической несущей показали работоспособность подобных схем с использованием полной хаотической синхронизации [226 – 229]. Основным достоинством реализации подобных схем в оптическом диапазоне следует, видимо, считать высокую скорость передачи информации (до 1 Гб $с^{-1}$), которая недостижима в таких системах при других диапазонах частот. Наиболее часто в подобных экспериментах по передаче информации использовалась полная хаотическая синхронизация, что накладывало весьма жёсткие требования на интенсивность шумов в канале связи и расстройку параметров оптических генераторов хаоса на обоих концах канала связи [230]. Однако в оптическом диапазоне существует возможность применения в качестве каналов связи волоконно-оптических линий, которые характеризуются весьма низким уровнем шумов и помех, вносимых в передаваемый сигнал, что значительно облегчает создание работоспособных схем скрытой передачи информации [231]. Более того, в данном случае существует возможность использования ранее созданных коммерческих линий волоконно-оптической связи.

Наиболее хорошо проработанным и достигшим практических результатов проектом, направленным на изучение возможностей хаотической синхронизации для скрытой передачи на большие расстояния на основе уже существующих коммерческих волоконно-оптических каналов связи, стали исследования, проведённые международной группой исследователей из Греции, Испании, Германии и Бельгии, по высокоскоростной передаче данных на расстояние 120 км по волоконно-оптической линии связи метрополитена города Афины (Греция) с использованием хаотических генераторов на основе лазерных диодов [232]. Остановимся на описании этого эксперимента более подробно, так как данную работу следует признать одной из наиболее интересных на сегодня экспериментальных реализаций идей передачи информации на основе полной хаотической синхронизации в оптическом диапазоне.

В качестве источников хаотических сигналов с большой размерностью аттрактора и высокой информационной энтропией использовались генераторы на основе полупроводниковых диодов с запаздывающей обратной связью, которая реализовывалась двумя различными способами, а именно, рассматривались электронно-оптическая [233] и полностью оптическая [234] обратные связи. Использование двух типов обратной связи в генераторе хаоса оптического диапазона позволило авторам работы [232] реализовать два способа передачи информации, описанных выше: нелинейное подмешивание информационного сигнала к хаотическому (см. раздел 3.3) и модулирование параметров хаотического сигнала информационным сигналом (см. раздел 3.4). В первом случае (схема соответствующего эксперимента приведена на рис. 19а) излучение лазерного диода LD проходит через интегрированный электро-оптический интерферометр Маха – Зендера MZI, который управляется электро-оптической запаздывающей обратной связью (включающей в себя линию задержки DL, фотодиод PD и электронный усилитель A) и работает как нелинейный модулятор лазерного излучения. Информационный сигнал в этом случае подмешивается к сигналу обратной связи через волоконно-оптический смеситель OFC. Выходной хаотический сигнал генератора, содержащий информационное сообщение, дополнительно усиливается перед подачей в канал связи для достижения необходимого уровня мощности. Во втором случае (рис. 19б) источником лазерного излучения снова является лазерный диод LD, а оптическая обратная связь реализуется с помощью зеркала R, коэффициент отражения которого нелинейно зависит от интенсивности падающего излучения. Длина внешнего резонатора системы составляла 6 м. В резонатор помещался поляризатор P для обеспечения необходимой поляризации света, отражённого от зеркала R с переменным коэффи-

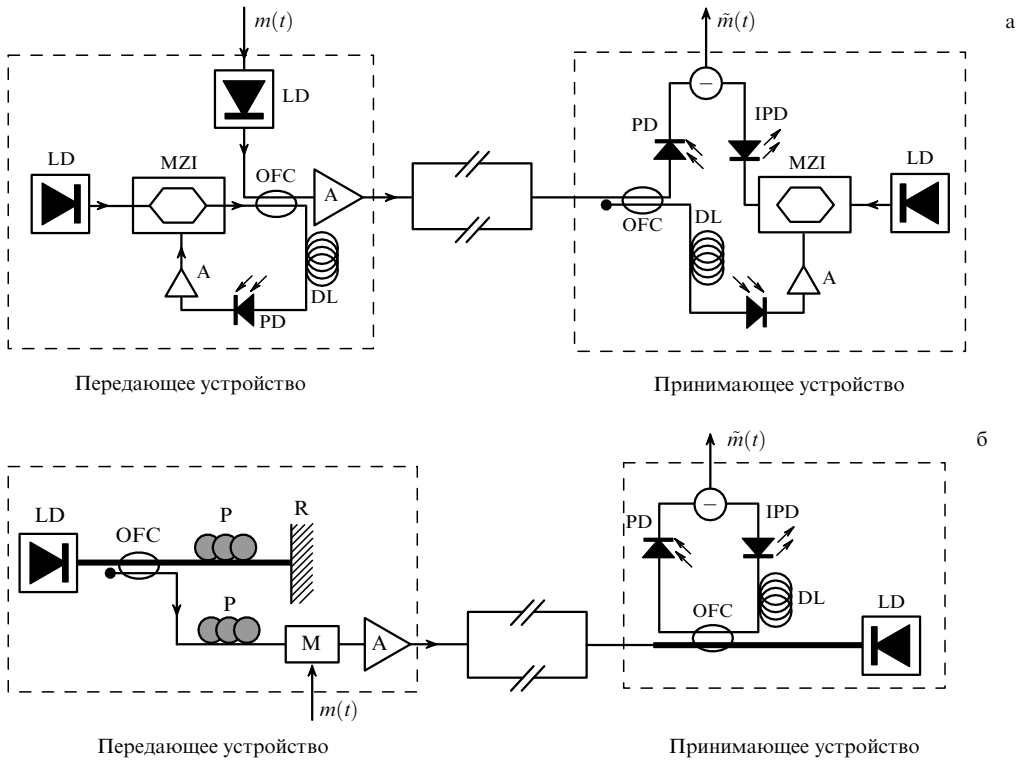

Рис. 19. Экспериментальные схемы скрытой передачи информации в оптическом диапазоне на основе (а) нелинейного подмешивания информационного сигнала к хаотическому и (б) модулирования параметров передающего генератора информационным сигналом: LD — лазерный диод, MZI — электрооптический интерферометр Маха–Зендера, OFC — волоконно-оптический смеситель, R — зеркало с переменным коэффициентом отражения, A — усилитель, PD и IPD — фотодиоды, DL — линии задержки, P — поляризатор, M — модулятор.

циентом отражения. Информационный сигнал вводился посредством модуляции параметров хаотического сигнала с помощью модулятора M. Затем передаваемый по оптическому каналу сигнал усиливался, как и в первой схеме. В схемах также имелись не показанные на рис. 19 фильтры для подавления влияния шумов, связанных со спонтанной эмиссией [231, 235].

В обеих схемах полезный информационный сигнал декодировался в принимающем устройстве путём достижения режима полной хаотической синхронизации между генераторами на различных сторонах канала связи, как это подробно обсуждалось в разделе 3. Основной проблемой эксперимента стало создание близких к идентичным генераторов на обоих концах канала связи. В обеих схемах наибольшие сложности при достижении идентичности генераторов вызывали активные элементы генераторных схем, а именно полупроводниковые лазеры. В экспериментах использовались лазеры с длинами волн 1552,0 и 1552,9 нм в приёмном и передающем устройствах соответственно. Для обеспечения одинаковых длин волн и стабильной работы лазерных диодов для каждого из лазеров подбирался свой температурный режим, который поддерживался в течение всего эксперимента. Подбор с высокой степенью идентичных пассивных элементов не вызывал принципиальных сложностей. При достаточно точной настройке параметров оптических генераторов хаоса в однонаправленно связанной системе наблюдалось устойчивое возникновение режимов полной хаотической синхронизации при достаточной мощности сигнала, подаваемого на принимающее устройство [232]. Было показано, что расстройка генераторов на различных сторонах канала связи для устойчивости работы схемы передачи информации (для достижения полной хаотической синхронизации) не может превышать 3 %. При передаче сигнала на большие расстояния возникала проблема разрушения режима синхронизации из-за влияния дисперсии в волоконно-оптическом канале связи (она составляла в рассматриваемом эксперименте порядка -850 пс нм$^{-1}$). В связи с этим на выходе канала используемой коммерческой волоконно-оптической сети перед подачей сигнала на приёмное устройство вводились отрезки волоконно-оптических линий с дисперсией другого знака, компенсирующие дисперсионное искажение сигнала, а также дополнительные усилители для обеспечения необходимого уровня мощности (данные элементы не показаны на рис. 19).

На рисунке 20 приведены результаты передачи информационного сообщения с помощью схемы с электронно-оптической обратной связью, в которой применялось нелинейное подмешивание информационного сигнала к хаотическому. Информационное сообщение, представляющее собой псевдослучайную последовательность 2^7-1 битов, модулировало хаотический сигнал, как описывалось выше (рис. 19а). Рисунок 20а представляет глазковую диаграмму (осциллограмму суперпозиции большого числа передаваемых/принимаемых битов) информационного сигнала $m(t)$ (в верхней части рисунка), передаваемого хаотического сигнала с информационным сообщением на выходе передатчика и декодированное сообщение $\tilde{m}(t)$ в принимающем устройстве. Вероятность ошибки на бит (BER) для данной экспериментальной схемы составляет 10^{-7} при скорости передачи информации 3 Гб с$^{-1}$. Аналогичные результаты

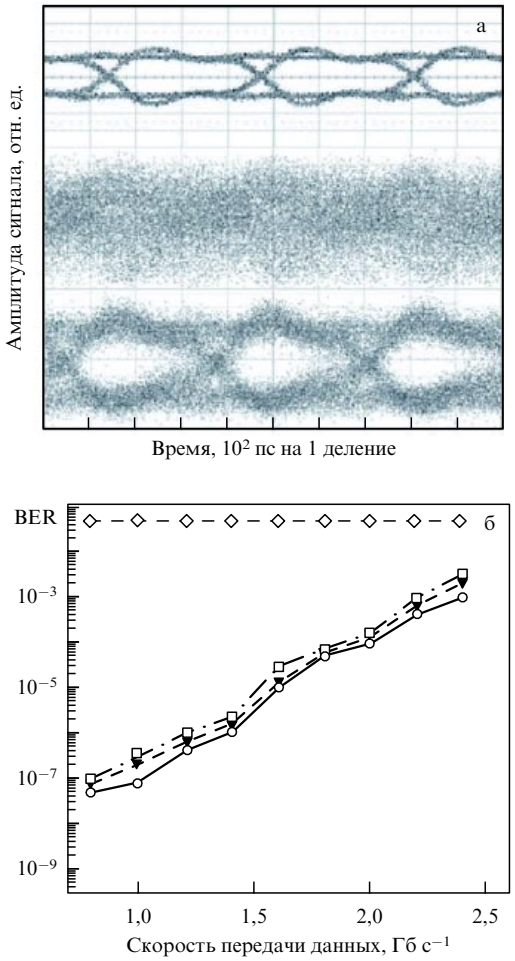

Рис. 20. (а) Глазковые диаграммы передаваемого цифрового информационного сигнала $m(t)$ (в верхней части рисунка), хаотического сигнала на выходе передающего устройства (в середине) и декодированного инфомационного сигнала $\tilde{m}(t)$ на выходе принимающего устройства (в нижней части рисунка) при использовании схемы нелинейного подмешивания информационного сигнала к хаотическому. (б) Зависимость вероятности ошибки на бит (BER) от скорости передачи информационного сообщения при использовании схемы с модуляцией параметров передающего генератора. Символами ◇ показаны результаты анализа закодированного сообщения на выходе из передающего устройства, ○ — результаты лабораторного эксперимента по передаче информации на малое расстояние, ▼ — результаты эксперимента по передаче информационного сообщения с малой длиной ($2^7 - 1$) на большое расстояние (порядка 120 км) по коммерческой волоконно-оптической линии связи, □ — результаты эксперимента по передаче информационного сообщения длиной $2^{23} - 1$ на большое расстояние. (Из работы [232].)

получены и при использовании схемы с модулированием параметров, однако при той же величине $\mathrm{BER} = 10^{-7}$ скорость передачи оказалась почти в три раза меньше (~ 1 Гб $с^{-1}$).

Учитывая важность вопроса устойчивости схем передачи информации на основе хаотической синхронизации к различным факторам, остановимся подробнее на вопросе качества передачи информации, которое удобно оценивать в данном эксперименте такой характеристикой, как вероятность ошибки на бит, при различной скорости передачи информации. Уменьшение скорости передачи информации удлиняет интервал времени, в течение которого передаётся один бит, а следовательно, существенно облегчает диагностику состояния принимающей системы для надёжного приёма сообщения. Авторами работы [232] были проведены исследования при различных скоростях передачи информации — от 0,1 Гб $с^{-1}$ до 2,4 Гб $с^{-1}$ — для двух длительностей передаваемых псевдослучайных последовательностей битов: $2^7 - 1$ и $2^{23} - 1$. На рисунке 20б приведены зависимости величины BER от скорости передачи информации при использовании схемы на основе модулирования параметров (рис. 19б). Хорошо видно, что с возрастанием скорости передачи информации качество передачи быстро уменьшается. Кодирование хаотического сигнала происходит практически без ошибок (см. кривую с ромбами), однако далее неидентичность генераторов и шумы в генераторах и канале связи начинают оказывать деструктивную роль, ограничивая скорость передачи данных. Причём дальность передачи данных практически не влияла на величину ошибки, а значит, основные ограничения метода, обусловленные требованием качества и, как следствие, требованием высокой скорости передачи данных, в рассматриваемом случае связаны с неидентичностью генераторов на различных сторонах канала связи и флуктуациями, возникающими в самих генераторах.

Полученные в работе [232] результаты представляются весьма важными и открывают серьёзные перспективы применения схем передачи информации с использованием хаотической синхронизации в оптическом диапазоне в современных информационно-телекоммуникационных системах. Все исследования были выполнены на основе уже существующих телекоммуникационных сетей, т.е. внедрение соответствующих технологий не требует принципиальной замены уже созданного оборудования, что чрезвычайно важно для практического использования. К недостаткам рассматриваемой схемы следует отнести сравнительно низкую скорость передачи данных, что, как обсуждалось выше, связано с общими недостатками подобных схем скрытой передачи информации, а именно с необходимостью достижения режимов полной хаотической синхронизации, которые весьма чувствительны к расстройке хаотических генераторов на различных сторонах телекоммуникационного канала и шумам, всегда присутствующим в реальных экспериментах.

8. Заключение

В настоящем обзоре проведено рассмотрение способов скрытой передачи информации с использованием хаотических сигналов, в основе которых лежат различные типы синхронного поведения хаотических систем: полная хаотическая синхронизация, фазовая синхронизация, обобщённая хаотическая синхронизация и несколько типов синхронного поведения одновременно (например, обобщённая и полная синхронизации). Каждая из схем характеризуется своими особенностями и принципами работы и обладает свойственными только ей достоинствами и недостатками. В то же время большинство недостатков и трудностей технической реализации характерно для ряда схем и устройств подобного назначения. Это, в первую очередь: 1) требование высокой степени идентичности генераторов на различных сторонах канала связи; 2) низкая устойчивость к шумам в канале связи; 3) довольно низкая конфиденциальность.

Рассмотрен способ скрытой передачи информации с помощью обобщённой хаотической синхронизации, лишённый вышеупомянутых недостатков. Посредством численного моделирования однонаправленно связанных систем Рёсслера, выбранных в качестве генераторов передающего и принимающего устройств, проведено сравнение между собой всех способов, рассмотренных в обзоре.

Расчёт количественных характеристик работоспособности способов скрытой передачи данных показал, что рассмотренный метод на основе режима обобщённой хаотической синхронизации обладает значительной, практически неограниченной в реальных пределах устойчивостью к шумам в канале связи, в то время как устойчивость других рассмотренных схем является ограниченной. Кроме того, этот метод достаточно устойчив к расстройке управляющих параметров изначально идентичных хаотических генераторов (которые располагаются на одной стороне канала связи, что также является принципиальным достоинством) и к нелинейным искажениям в канале связи.

Такой способ скрытой передачи информации открывает ряд новых возможностей для экспериментальной реализации скрытой передачи информации на основе хаотической синхронизации. Отсутствие ряда недостатков, свойственных большинству схем скрытой передачи информации, делает эту задачу актуальной и перспективной.

Проведён обзор результатов по экспериментальной реализации различных способов скрытой передачи информации. Обобщены основные экспериментальные результаты и приведены конкретные примеры реализации схем на основе хаотической маскировки, нелинейного подмешивания и модулирования управляющих параметров в радиодиапазоне, микроволновом и оптическом диапазонах. Описаны первые результаты экспериментального наблюдения режима обобщённой синхронизации в СВЧ-диапазоне.

Авторы выражают благодарность А.С. Дмитриеву и Д.И. Трубецкову за полезные обсуждения и критические замечания. Авторы благодарят рецензента за полезные замечания, позволившие улучшить качество статьи. Работа выполнена при поддержке РФФИ (проект 08-02-00102), Президентских программ 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 годы.

Список литературы

1. Huygens C *Horologium Oscillatorium, Sive de Motu Pendulorum ad Horologia Aptato Demonstrationes Geometrical* (Paris: A.F. Muguet, 1673) [Translated into English: *The Pendulum Clock or, Geometrical Demonstrations Conceptning the Motion of Pendula as Applied to Clocks* (Ames: Iowa State Univ. Press, 1986)]
2. Van der Pol B *Proc. IRE* **22** 1051 (1934) [Ван-дер-Поль Б *Нелинейная теория электрических колебаний* (М.: Связьтехиздат, 1935)]
3. Гапонов В И *ЖТФ* **6** 801 (1936)
4. Теодорчик К Ф *ДАН СССР* **40** (2) 63 (1943)
5. Adler R *Proc. IRE* **34** (6) 351 (1946); reprinted: *Proc IEEE* **61** 1380 (1973)
6. Хохлов Р В *ДАН СССР* **9** (6) 411 (1954)
7. Андронов А А, Витт А А, в кн. Андронов А А *Собрание трудов* (М.: Изд-во АН СССР, 1956)
8. Минакова И И, Теодорчик К Ф *ДАН СССР* **106** 658 (1956)
9. Андронов А А, Витт А А, Хайкин С Э *Теория колебаний* (М.: Наука, 1981) [Andronov A A, Vitt A A, Khaikin S E *Theory of Oscillators* (New York: Dover, 1987)]
10. Блехман И И *Синхронизация динамических систем* (М.: Наука, 1971)
11. Блехман И И *Синхронизация в природе и технике* (М.: Наука, 1981) [Blekhman I I *Synchronization in Science and Technology* (New York: ASME Press, 1988)]
12. Анищенко В С, Вадивасова Т Е, Астахов В В *Нелинейная динамика хаотических и стохастических систем. Фундаментальные основы и избранные проблемы* (Саратов: Изд-во Сарат. ун-та, 1999)
13. Анищенко В С и др. *Нелинейные эффекты в хаотических и стохастических системах* (Под ред. В С Анищенко) (М.–Ижевск: Инст. компьют. исслед., 2003)
14. Пиковский А С, Розенблюм М Г, Куртс Ю *Синхронизация. Фундаментальное нелинейное явление* (М.: Техносфера, 2003)
15. Трубецков Д И *Синхронизация: ученый и время* (Саратов: Изд-во ГосУНЦ "Колледж", 2005) с. 70
16. Анищенко В С и др. *Синхронизация регулярных, хаотических и стохастических колебаний* (М.–Ижевск: РХД, 2008)
17. Анищенко В С, Астахов В В, Летчфорд Т Е *Радиотехника и электроника* **27** 1972 (1980)
18. Кузнецов Ю И и др. *ДАН СССР* **275** 1388 (1984) [Kuznetsov Yu I et al. *Sov. Phys. Dokl.* **29** 318 (1984)]
19. Дмитриев А С, Кислов В Я, Старков С О *ЖТФ* **55** 2417 (1985) [Dmitriev A S, Kislov V Ya, Starkov S O *Sov. Phys. Tech. Phys.* **29** 318 (1985)]
20. Афраймович В С, Веричев Н Н, Рабинович М И *Изв. вузов. Радиофизика* **29** 1050 (1986) [Afraimovich V S, Verichev N N, Rabinovich M I *Radiophys. Quantum Electron.* **29** 795 (1986)]
21. Неймарк Ю И, Ланда П С *Стохастические и хаотические колебания* (М.: Наука, 1987) [Neimark Yu I, Landa P S *Stochastic and Chaotic Oscillations* (Dordrecht: Kluwer Acad. Publ., 1992)]
22. Анищенко В С *Сложные колебания в простых системах* (М.: Наука, 1990)
23. Дмитриев А С, Панас А И *Динамический хаос: новые носители информации для систем связи* (М.: Физматлит, 2002)
24. Parlitz U et al. *Int. J. Bifurcat. Chaos* **2** 973 (1992)
25. Cuomo K M, Oppenheim A V, Strogatz S H *IEEE Trans. Circuits Syst. II Analog Digital Signal Process.* **40** 626 (1993)
26. Kocarev L, Parlitz U *Phys. Rev. Lett.* **74** 5028 (1995)
27. Peng J H, Ding E J, Ding M, Yang W *Phys. Rev. Lett.* **76** 904 (1996)
28. Anishchenko V S, Pavlov A N *Phys. Rev. E* **57** 2455 (1998)
29. Анищенко В С, Павлов А Н, Янсон Н Б *ЖТФ* **68** (12) 1 (1998) [Anishchenko V S, Pavlov A N, Yanson N B *Tech. Phys.* **43** 1401 (1998)]
30. Eguia M C, Rabinovich M I, Abarbanel H D I *Phys. Rev. E* **62** 7111 (2000)
31. Fischer I, Liu Y, Davis P *Phys. Rev. A* **62** 011801 (2000)
32. Rulkov N F, Vorontsov M A, Illing L *Phys. Rev. Lett.* **89** 277905 (2002)
33. Yuan Z L, Shields A J *Phys. Rev. Lett.* **94** 048901 (2005)
34. Li Q S, Liu Y *Phys. Rev. E* **73** 016218 (2006)
35. Fradkov A L, Andrievsky B, Evans R J *Phys. Rev. E* **73** 066209 (2006)
36. Strogatz S H *Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering* (Reading, Mass.: Addison-Wesley, 1994)
37. Elson R C et al. *Phys. Rev. Lett.* **81** 5692 (1998)
38. Landa P S, Rabinovitch A *Phys. Rev. E* **61** 1829 (2000)
39. Porcher R, Thomas G *Phys. Rev. E* **64** 010902 (2001)
40. Glass L *Nature* **410** 277 (2001)
41. Pavlov A N et al. *Physica A* **316** 233 (2002)
42. Sosnovtseva O V et al. *Phys. Rev. E* **66** 061909 (2002)

43. Rosenblum M G, Pikovsky A S, Kurths J *Fluctuat. Noise Lett.* **4** L53 (2004)
44. Постнов Д Э, Хан С К *Письма в ЖТФ* **25** (4) 11 (1999) [Postnov D É, Han S K *Tech. Phys. Lett.* **25** 128 (1999)]
45. Anishchenko V S et al. *Int. J. Bifurcat. Chaos* **10** 2339 (2000)
46. Mosekilde E, Maistrenko Y, Postnov D *Chaotic Synchronization: Applications to Living Systems* (River Edge, NJ: World Scientific, 2002)
47. Prokhorov M D et al. *Phys. Rev. E* **68** 041913 (2003)
48. Rulkov N F *Phys. Rev. E* **65** 041922 (2002)
49. Sosnovtseva O V и др. *Изв. вузов. Прикладная нелинейная динамика* **11** (3) 133 (2003)
50. Sosnovtseva O V et al. *Phys. Rev. E* **70** 031915 (2004)
51. Sosnovtseva O V et al. *Physiol. Meas.* **26** 351 (2005)
52. Sosnovtseva O V et al. *Phys. Rev. Lett.* **94** 218103 (2005)
53. Hramov A E et al. *Phys. Rev. E* **73** 026208 (2006)
54. Sosnovtseva O V et al. *Am. J. Physiol. Renal Physiol.* **293** F1545 (2007)
55. Parmananda P *Phys. Rev. E* **56** 1595 (1997)
56. Kiss I Z, Hudson J L *Phys. Rev. E* **64** 046215 (2001)
57. Rosenblum M, Pikovsky A *Contemp. Phys.* **44** 401 (2003)
58. Kiss I Z et al. *Phys. Rev. E* **70** 026210 (2004)
59. Yoshioka M *Phys. Rev. E* **71** 061914 (2005)
60. Ditto W L, Rauseo S N, Spano M L *Phys. Rev. Lett.* **65** 3211 (1990)
61. Meucci R et al. *Phys. Rev. E* **49** R2528 (1994)
62. Kittel A, Parisi J, Pyragas K *Phys. Lett. A* **198** 433 (1995)
63. Шалфеев В Д и др. *Зарубежная радиоэлектроника. Успехи современной радиоэлектроники* (10) 27 (1997)
64. Boccaletti S et al. *Phys. Rep.* **329** 103 (2000)
65. Ticos C M et al. *Phys. Rev. Lett.* **85** 2929 (2000)
66. Rosa E (Jr.) et al. *Int. J. Bifurcat. Chaos* **10** 2551 (2000)
67. Трубецков Д И, Храмов А Е *Радиотехника и электроника* **48** 116 (2003) [Trubetskov D I, Khramov A E *J. Commun. Technol. Electron.* **48** 105 (2003)]
68. Трубецков Д И, Короновский А А, Храмов А Е *Изв. вузов. Радиофизика* **47** 343 (2004) [Trubetskov D I, Koronovsky A A, Khramov A E *Radiophys. Quantum Electron.* **47** 305 (2004)]
69. Hramov A E et al. *Chaos* **15** 013705 (2005)
70. Белоглазкина М В, Короновский А А, Храмов А Е *ЖТФ* **79** (6) 13 (2009) [Beloglazkina M V, Koronovskii A A, Hramov A E *Tech. Phys.* **54** 775 (2009)]
71. Фрадков А Л *УФН* **175** 113 (2005) [Fradkov A L *Phys. Usp.* **48** 103 (2005)]
72. Абарбанель Г Д И и др. *УФН* **166** 363 (1996) [Abarbanel H D I et al. *Phys. Usp.* **39** 337 (1996)]
73. Безручко Б П и др. *УФН* **178** 323 (2008) [Bezruchko B P et al. *Phys.Usp.* **51** 304 (2008)]
74. Tass P et al. *Phys. Rev. Lett.* **81** 3291 (1998)
75. Tass P A et al. *Phys. Rev. Lett.* **90** 088101 (2003)
76. Meinecke F C et al. *Phys. Rev. Lett.* **94** 084102 (2005)
77. Chavez M et al. *Chaos* **15** 023904 (2005)
78. Yang T *Int. J. Computat. Cognition* **2** (2) 81 (2004)
79. Tang Y, Fang J, Chen L *Int. J. Mod. Phys. B* **22** 4175 (2008)
80. Zheng G, Boutat D, Floquet T, Barbot J-P *Int. J. Bifurcat. Chaos* **18** 2063 (2008)
81. Bowong S, Yamapi R *Int. J. Bifurcat. Chaos* **18** 2425 (2008)
82. Hoang T M, Nakagawa M *Chaos Solitons Fractals* **38** 1423 (2008)
83. Liang X, Zhang J, Xia X *IEEE Trans. Circuits Syst. II Express Briefs* **55** 680 (2008)
84. Wang X et al. *Mod. Phys. Lett. B* **22** 2077 (2008)
85. Tronciu V Z et al. *Opt. Commun.* **281** 4747 (2008)
86. Gámez-Guzmán L et al. *Rev. Mex. Fís.* **54** (4) 299 (2008)
87. Sun Y, Cao J, Feng G *Phys. Lett. A* **372** 5442 (2008)
88. Wang Yun-Cai, Zhao Qing-Chun, Wang An-Bang *Chinese Phys. B* **17** 2373 (2008)
89. Yu W, Cao J, Yuan K *Phys. Lett. A* **372** 4438 (2008)
90. Materassi D, Basso M *Int. J. Bifurcat. Chaos* **18** 567 (2008)
91. Xia W, Cao J *Chaos* **18** (2008)
92. Lu S, Chen L *Kybernetika* **44** (1) 43 (2008)
93. Annovazzi-Lodi V et al. *IEEE Photonics Technol. Lett.* **17** 1995 (2005)
94. Pecora L M, Carroll T L *Phys. Rev. Lett.* **64** 821 (1990)
95. Pecora L M, Carroll T L *Phys. Rev. A* **44** 2374 (1991)
96. Rosenblum M G, Pikovsky A S, Kurths J *Phys. Rev. Lett.* **76** 1804 (1996)
97. Rulkov N F et al. *Phys. Rev. E* **51** 980 (1995)
98. Rosenblum M G, Pikovsky A S, Kurths J *Phys. Rev. Lett.* **78** 4193 (1997)
99. Fahy S, Hamann D R *Phys. Rev. Lett.* **69** 761 (1992)
100. Martian A, Banavar J R *Phys. Rev. Lett.* **72** 1451 (1994)
101. Kaulakys B, Vektaris G *Phys. Rev. E* **52** 2091 (1995)
102. Chen Y-Y *Phys. Rev. Lett.* **77** 4318 (1996)
103. Kaulakys B, Ivanauskas F, Meškauskas T *Int. J. Bifurcat. Chaos* **9** 533 (1999)
104. Toral R et al. *Chaos* **11** 665 (2001)
105. Грибунин В Г, Оков И Н, Туринцев И В *Цифровая стеганография* (М.: СОЛОН-Пресс, 2002)
106. Murali K, Lakshmanan M *Phys. Rev. E* **48** R1624 (1993)
107. Boccaletti S, Farini A, Arecchi F T *Phys. Rev. E* **55** 4979 (1997)
108. Carroll T L, Johnson G A *Phys. Rev. E* **57** 1555 (1998)
109. Terry J R, VanWiggeren G D *Chaos Solitons Fractals* **12** 145 (2001)
110. Lucamarini M, Mancini S *Phys. Rev. Lett.* **94** 140501 (2005)
111. Eckmann J-P, Thomas L, Wittwer P *J. Phys. A* **14** 3153 (1981)
112. Kye W-H, Kim C-M *Phys. Rev. E* **62** 6304 (2000)
113. Kye W-H et al. *Phys. Rev. E* **68** 036203 (2003)
114. Hramov A E et al. *Phys. Rev. E* **76** 026206 (2007)
115. Koronovskii A A, Hramov A E *Eur. Phys. J. B* **62** 447 (2008)
116. Pikovsky A S, Kurths J *Phys. Rev. Lett.* **78** 775 (1997)
117. Mangioni S et al. *Phys. Rev. Lett.* **79** 2389 (1997)
118. Zaikin A A, Kurths J, Schimansky-Geier L *Phys. Rev. Lett.* **85** 227 (2000)
119. Neiman A B, Russell D F *Phys. Rev. Lett.* **88** 138103 (2002)
120. Zhou C et al. *Phys. Rev. Lett.* **89** (1) 014101 (2002)
121. Zhou C S et al. *Phys. Rev. E* **67** 015205 (2003)
122. Boccaletti S et al. *Phys. Rev. Lett.* **89** 194101 (2002)
123. Taherion S, Lai Y-C *Phys. Rev. E* **59** R6247 (1999)
124. Boccaletti S et al. *Phys. Rep.* **366** 1 (2002)
125. Волковский А Р, Рульков Н Ф *Письма в ЖТФ* **19** (3) 71 (1993) [Volkovskii A R, Rul'kov N F *Tech. Phys. Lett.* **19** 97 (1993)]
126. Pyragas K *Phys. Rev. E* **54** R4508 (1996)
127. Pecora L M, Carroll T L, Heagy J F *Phys. Rev. E* **52** 3420 (1995)
128. Pyragas K *Phys. Rev. E* **56** 5183 (1997)
129. Abarbanel H D I, Rulkov N F, Sushchik M M *Phys. Rev. E* **53** 4528 (1996)
130. Osipov G V et al. *Phys. Rev. E* **55** 2353 (1997)
131. Pikovsky A, Rosenblum M, Kurths J *Int. J. Bifurcat. Chaos* **10** 2291 (2000)
132. Rosenblum M G et al., in *Nonlinear Analysis of Physiological Data* (Eds H Kantz, J Kurths, G Mayer-Kress) (Berlin: Springer, 1998) p. 91
133. Вадивасова Т Е, Анищенко В С *Радиотехника и электроника* **49** 77 (2004) [Vadivasova T E, Anishchenko V S *J. Commun. Technol. Electron.* **49** 69 (2004)]
134. Pikovsky A S et al. *Physica D* **104** 219 (1997)
135. Pikovsky A, Rosenblum M, Kurths J *Synchronization: a Universal Concept in Nonlinear Sciences* (Cambridge: Cambridge Univ. Press, 2001)
136. Anishchenko V S, Vadivasova T E, Strelkova G I *Fluctuat. Noise Lett.* **4** L219 (2004)
137. Pikovsky A S, Rosenblum M G, Kurths J *Europhys. Lett.* **34** 165 (1996)
138. Короновский А А, Храмов А Е, Храмова А Е *Письма в ЖЭТФ* **82** 176 (2005) [Koronovskii A A, Hramov A E, Khramova A E *JETP Lett.* **82** 160 (2005)]
139. Rosenblum M G et al. *Phys. Rev. Lett.* **89** 264102 (2002)
140. Hramov A E, Koronovskii A A *Chaos* **14** 603 (2004)
141. Hramov A E, Koronovskii A A, Levin Yu I *ЖЭТФ* **127** 886 (2005) [*JETP* **100** 784 (2005)]

142. Короновский А А, Куровская М К, Храмов А Е *Письма в ЖТФ* **31** (19) 76 (2005) [Koronosvkii A A, Kurovskaya M K, Hramov A E *JETP Lett*. **31** 847 (2005)]
143. Короновский А А, Храмов А Е *Радиотехника и электроника* **50** 969 (2005) [Koronovskii A A, Khramov A E *J. Commun. Technol. Electron*. **50** 894 (2005)]
144. Hramov A E, Koronovskii A A *Physica D* **206** 252 (2005)
145. Dedieu H, Kennedy M P, Hasler M *IEEE Trans. Circuits Syst. I Regular Papers* **40** 634 (1993)
146. Dmitriev A S, Panas A I, Starkov S O *Int. J. Bifurcat. Chaos* **5** 1249 (1995)
147. Yang T, Chua L O *IEEE Trans. Circuits Syst. I Regular Papers* **43** 817 (1996)
148. Downes P T *SPIE* **2038** 227 (1993)
149. Pérez G, Cerdeira H A *Phys. Rev. Lett*. **74** 1970 (1995)
150. Short K M *Int. J. Bifurcat. Chaos* **6** 367 (1996)
151. Ponomarenko V I, Prokhorov M D *Phys. Rev. E* **66** 026215 (2002)
152. Короновский А А и др. *Докл. РАН* **383** 322 (2002) [Koronovskii A A et al. *Dokl. Phys*. **47** 181 (2002)]
153. Короновский А А и др. *Изв. вузов. Радиофизика* **45** 880 (2002) [Koronovsky A A et al. *Radiophys. Quantum Electron*. **45** 806 (2002)]
154. Yang T *Int. J. Circuit Theory Appl*. **23** 611 (1995)
155. Chen J Y et al. *Chaos* **13** 508 (2003)
156. Rulkov N F *Chaos* **6** 262 (1996)
157. Zheng Z, Hu G *Phys. Rev. E* **62** 7882 (2000)
158. Hramov A E, Koronovskii A A, Moskalenko O I *Europhys. Lett*. **72** 901 (2005)
159. Короновский А А, Попов П В, Храмов А Е *ЖЭТФ* **130** 748 (2006) [Koronovskii A A, Popov P V, Hramov A E *JETP* **103** 654 (2006)]
160. Moskalenko O I et al. *Phys. Rev. E* (2009), submitted
161. Murali K, Lakshmanan M *Phys. Lett. A* **241** 303 (1998)
162. Короновский А А и др. *Изв. РАН. Сер. физ*. **72** (1) 143 (2008) [Koronovskii A A et al. *Bull. Russ. Acad. Sci. Phys*. **72** 131 (2008)]
163. Короновский А и др. *Первая Миля* (1) 14 (2008)
164. Короновский А А, Москаленко О И, Храмов А Е *ЖТФ* **76** (2) 1 (2006) [Koronovskii A A, Moskalenko O I, Hramov A E *Tech. Phys*. **51** 143 (2006)]
165. Hramov A E, Koronovskii A A *Phys. Rev. E* **71** 067201 (2005)
166. Короновский А А и др. *Изв. РАН Сер. физ*. **73** 1723 (2009)
167. Короновский А А, Храмов А Е *Письма в ЖЭТФ* **79** 391 (2004) [Koronovskii A A, Hramov A E *JETP Lett*. **79** 316 (2004)]
168. Короновский А А, Москаленко О И, Храмов А Е *Письма в ЖЭТФ* **80** 25 (2004) [Koronovskii A A, Moskalenko O I, Hramov A E *JETP Lett*. **80** 20 (2004)]
169. Короновский А А, Москаленко О И, Храмов А Е *Радиотехника и электроника* **52** 949 (2007) [Koronovskii A A, Moskalenko O I, Hramov A E *J. Commun. Technol. Electron*. **52** 881 (2007)]
170. Rico-Martínez R et al. *Physica D* **176** 1 (2003)
171. Никитин Н Н, Первачев С В, Разевиг В Д *Автоматика и телемеханика* (4) 133 (1975)
172. Sklar B *Digital Communications*: *Fundamentals and Applications* (Upper Saddle River, NJ: Prentice-Hall PTR, 2001) [Скляр Б *Цифровая связь. Теоретические основы и практическое применение* (М.: Вильямс, 2003)]
173. Побережский Е С *Цифровые радиоприемные устройства* (М.: Радио и связь, 1987)
174. Abel A, Schwarz W *Proc. IEEE* **90** 691 (2002)
175. Chua L O *Arch. Elektron. Übertragungstech*. **46** 250 (1992)
176. Chua L O, Komuro M, Matsumoto T *IEEE Trans. Circuits Syst*. **CAS-33** 1073 (1986)
177. Кузнецов С П *Изв. вузов. Радиофизика* **25** 1410 (1982) [Kuznetsov S P *Radiophys. Quantum Electron*. **25** 996 (1982)]
178. Dmitriev A S, Panas A I, Starkov S O *Int. J. Bifurcat. Chaos* **6** 851 (1996)
179. Hramov A E et al. *Phys. Rev. E* **75** 056207 (2007)
180. Пономаренко В П, Матросов В В *Радиотехника и электроника* **29** 1125 (1984)
181. Капранов М В, Чернобаев В Г *Радиотехнические тетради* (15) 86 (1998)
182. Шалфеев В Д, Матросов В В, Корзинова М В *Зарубежная радиоэлектроника. Успехи современной радиоэлектроники* (11) 44 (1998)
183. Матросов В В, Шалфеев В Д, Касаткин Д В *Изв. вузов. Радиофизика* **49** 448 (2006) [Matrosov V V, Shalfeev V D, Kasatkin D V *Radiophys. Quantum Electron*. **49** 406 (2006)]
184. Бельский Ю Л и др. *Радиотехника и электроника* **37** 660 (1992)
185. Ott E, Sommerer J C *Phys. Lett. A* **188** 39 (1994)
186. Boccaletti S, Valladares D L *Phys. Rev. E* **62** 7497 (2000)
187. Hramov A E, Koronovskii A A *Europhys. Lett*. **70** 169 (2005)
188. Lai Y-C *Phys. Rev. E* **53** R4267 (1996)
189. Cuomo K M, Oppenheim A V *Phys. Rev. Lett*. **71** 65 (1993)
190. Дмитриев А С и др. *Радиотехника и электроника* **43** 1115 (1998) [Dmitriev A S et al. *J. Commun. Technol. Electron*. **43** 1038 (1998)]
191. Matsumoto T *IEEE Trans. Circuits Systems* **31** 1055 (1984)
192. Zhong G-Q, Ayrom F *Int. J. Circuit Theory Appl*. **13** 93 (1985)
193. Dmitriev A S, Panas A I, Kuzmin L V *Nonlinear Phenom. Complex Syst*. **2** (3) 91 (1999)
194. Panas A I, Yang T, Chua L O *Int. J. of Bifurcat. Chaos* **8** 639 (1998)
195. Panas A I, in *Proc. of the 6th Intern. Workshop NDES'98, Budapest, Hungary, 1998*, p. 257
196. Кузьмин Л В, Максимов Н А, Панас А *Изв. вузов. Прикладная нелинейная динамика* **7** (2–3) 81 (1999)
197. Емец С В, Старков С О *Изв. вузов. Прикладная нелинейная динамика* **7** (2–3) 95 (1999)
198. Larsen P B, Earley L M, Wheat R M, Booske J H, in *Proc. of Vacuum Electronics Conf., 2006, Jointly with 2006 IEEE International Vacuum Electron Sources., IEEE Intern*. (2006) p. 521
199. Dmitriev B S et al. *Phys. Rev. Lett*. **102** 074101 (2009)
200. Marchewka C et al. *Phys. Plasmas* **13** 013104 (2006)
201. Кислов В Я, Мясин В Е, Богданов Е В, "Генератор СВЧ широкополосных колебаний", Заявка № 984513/19-09 от 31.07.68
202. Кислов В Я, Залогин Н Н, Мясин Е А *Радиотехника и электроника* **24** 1118 (1979)
203. Кислов В Я, Мясин Е А, Залогин Н Н *Радиотехника и электроника* **25** (10) 2160 (1980)
204. Кац В А, Трубецков Д И *Письма в ЖЭТФ* **39** (3) 116 (1984) [Kats V A, Trubetskov D I *JETP Lett*. **39** 137 (1984)]
205. Трубецков Д И, Храмов А Е *Лекции по сверхвысокочастотной электронике для физиков* Т. 2 (М.: Физматлит, 2004)
206. Ryskin N M et al. *Phys. Plasmas* **11** 1194 (2004)
207. Dronov V et al. *Chaos* **14** 30 (2004)
208. Короновский А А и др. *Обобщенная хаотическая синхронизация в диапазоне сверхвысоких частот* Т. 2 (М.: Физматлит, 2008) Гл. 9
209. Shigaev A M et al. *IEEE Trans. Electron Dev*. **52** 790 (2005)
210. Трубецков Д И, Храмов А Е *Лекции по сверхвысокочастотной электронике для физиков* Т. 1 (М.: Физматлит, 2003)
211. Evans M W (Ed.) *Modern Nonlinear Optics* (Adv. in Chem. Phys., Vol. 119, Pt. 3, Eds I Prigogine, S A Rice) Vols 1–3, 2nd ed. (New York: Wiley, 2001)
212. Udaltsov V S et al. *IEEE Trans. Circuits Syst. I Fundament. Theory Appl*. **49** 1006 (2002)
213. Uchida A et al., in *Papers of Technical Meeting on Optical and Quantum Devices, IEE Japan OQD-01* (37–46) 1 (2001)
214. Matsuura T, Uchida A, Yoshimori S *Opt. Lett*. **29** 2731 (2004)
215. Yamamoto T et al. *Opt. Express* **15** 3974 (2007)
216. Uchida A, Ogawa T, Kannari F *Jpn. J. Appl. Phys*. **37** L730 (1998)
217. McAllister R et al. *Physica D* **195** 244 (2004)
218. Uchida A et al. *Opt. Lett*. **24** 890 (1999)
219. Soriano M et al. *Phys. Rev. E* **78** 046218 (2008)
220. Uchida A et al. *Phys. Rev. E* **68** 016215 (2003)
221. Ruiz-Oliveras F R, Pisarchik A N *Phys. Rev. E* **79** 016202 (2009)
222. Chlouverakis K E et al. *Physica D* **237** 568 (2008)
223. Argyris A et al. *IEEE J. Select. Top. Quantum Electron*. **10** 927 (2004)

224. Argyris A, Syvridis D *J. Lightwave Technol.* **22** 1272 (2004)
225. Uchida A, Liu Y, Davis P *IEEE J. Quantum Electron.* **39** 963 (2003)
226. Tang S, Liu J *Opt. Lett.* **26** 1843 (2001)
227. Liu J M, Chen H F, Tang S *IEEE Trans. Circuits Systems I Fundament. Theory Appl.* **48** 1475 (2001)
228. Kusumoto K, Ohtsubo J *Opt. Lett.* **27** 989 (2002)
229. Abarbanel H D I et al. *IEEE J. Quantum Electron.* **37** 1301 (2001)
230. Bogris A, Argyris A, Syvridis D *IEEE J. Quantum Electron.* **43** 552 (2007)
231. Lee M W, Larger L, Goedgebuer J-P *IEEE J. Quantum Electron.* **39** 931 (2003)
232. Argyris A et al. *Nature* **438** 343 (2005)
233. Goedgebuer J-P, Larger L, Porte H *Phys. Rev. Lett.* **80** 2249 (1998)
234. VanWiggeren G D, Roy R *Science* **279** 1198 (1998)
235. Paul J, Lee M W, Shore K A *Opt. Lett.* **29** 2497 (2004)

On the use of chaotic synchronization for secure communication

A.A. Koronovskii, O.I. Moskalenko, A.E. Hramov
Faculty of Nonlinear Processes, N.G. Chernyshevsky Saratov State University, ul. Astrakhanskaya 83, 410012 Saratov, Russian Federation
Tel. (*7-8452*) *51-21 11,* (*7-8452*) *51-42 94*
Fax (+ *7-8452*) *52-38 64,* (*7-8452*) *52-38 64*
E-mail: *moskalenko@nonlin.sgu.ru, aeh@nonlin.sgu.ru, hramov@gmail.com*

Research on the secure communication applications of chaotic synchronization is reviewed. A number of secure communication methods and devices using different types of synchronous behavior are examined. For the purpose of comparison of existing methods, quantitative efficiency characteristics are introduced and estimated. An extremely noise-stable, generalized synchronization-based, secure information transmission method is proposed. All of the methods considered are systematically checked for efficiency for the first time by numerically simulating unidirectionally coupled chaotic Rössler systems for use as transmitting and receiving generators. Key advantages and disadvantages of secure information transmission schemes using synchronized chaotic oscillations are discussed.

PACS numbers: **05.45. – a**, 05.45.Pq, 05.45.Tp, 05.45.Vx, 05.45.Xt DOI: 10.3367/UFNr.0179.200912c.1281

Bibliography — 235 references *Received 27 February 2009, revized 10 August 2009*

Uspekhi Fizicheskikh Nauk **179** (12) 1281 – 1310 (2009) *Physics – Uspekhi* **52** (12) (2009)