УДК 537.86
doi:10.31799/1684-8853-2019-4-54-61

Научные статьи
Articles

Оценка конфиденциальности системы передачи информации на основе хаотического генератора с запаздыванием и переключаемым временем задержки

В. И. Пономаренко[а, б], *доктор физ.-мат. наук, профессор, orcid.org/0000-0002-1579-6465*
Е. В. Навроцкая[б], *канд. физ.-мат. наук, доцент, orcid.org/0000-0002-1649-440X*
Д. Д. Кульминский[а, б], *канд. физ.-мат. наук, научный сотрудник, orcid.org/0000-0002-3936-2813*
М. Д. Прохоров[а], *доктор физ.-мат. наук, профессор РАН, orcid.org/0000-0003-4069-9410, mdprokhorov@yandex.ru*
[а]*Саратовский филиал Института радиотехники и электроники им. В. А. Котельникова РАН, Зеленая ул., 38, Саратов, 410019, РФ*
[б]*Саратовский национальный исследовательский государственный университет им. Н. Г. Чернышевского, Астраханская ул., 83, Саратов, 410012, РФ*

Введение: *системы связи, основанные на использовании динамического хаоса, имеют ряд положительных свойств. Динамический хаос обладает свойствами случайных процессов, что дает возможность системам на его основе обеспечить конфиденциальность передаваемой информации. Однако количественная оценка степени скрытности таких систем связи является сложной задачей, поскольку методы оценки криптографической стойкости хорошо разработаны лишь для классических алгоритмов шифрования.* ***Цель:*** *разработка метода количественной оценки конфиденциальности передачи скрытого бинарного сигнала в системе связи, основанной на хаотическом генераторе с запаздыванием с переключаемым временем задержки.* ***Результаты:*** *предложен метод оценки конфиденциальности передачи бинарного информационного сигнала в системе связи, использующей в качестве передатчика хаотический генератор с запаздыванием с переключаемым временем задержки. Метод основан на оценке мощности ключевого пространства для исследуемой хаотической системы передачи информации. Рассмотрены случаи, при которых часть параметров передатчика известна, и наиболее общий случай, при котором все параметры передатчика являются неизвестными. Показано, что система передачи информации, основанная на динамическом хаосе, может обладать значительно более высокой конфиденциальностью, чем классический криптографический алгоритм, использующий шифр с длиной ключа 56 бит, но существенно уступает по криптографической стойкости шифру с длиной ключа 128 бит.* ***Практическая значимость:*** *предложенная методика позволяет получить количественную оценку конфиденциальности систем передачи информации, основанных на динамическом хаосе, и сравнить ее с известной стойкостью классических алгоритмов криптографии.*

Ключевые слова *— система передачи информации, динамический хаос, криптография, системы с запаздыванием.*

Для цитирования: Пономаренко В. И., Навроцкая Е. В., Кульминский Д. Д., Прохоров М. Д. Оценка конфиденциальности системы передачи информации на основе хаотического генератора с запаздыванием и переключаемым временем задержки. *Информационно-управляющие системы*, 2019, № 4, с. 54–61. doi:10.31799/1684-8853-2019-4-54-61

For citation: Ponomarenko V. I., Navrotskaya E. V., Kul'minskii D. D., Prokhorov M. D. Estimation of confidentiality of a communication system based on chaotic time-delay generator with switchable delay time. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 4, pp. 54–61 (In Russian). doi:10.31799/1684-8853-2019-4-54-61

Введение

Вторая половина прошлого века ознаменовалась широким изучением явления динамического хаоса и поиском его приложений к теории искусственного интеллекта, биологии, экономике и другим отраслям науки. Одним из направлений применения динамических систем, демонстрирующих хаотическое поведение, стало их использование для скрытой передачи информации. Было предложено множество способов скрытой передачи информации с использованием динамического хаоса [1–12]. Однако количественную оценку криптографической стойкости таких систем связи провести довольно сложно из-за существенного отличия принципов построения математических алгоритмов криптографии [13] и систем скрытой связи на динамическом хаосе [1, 2]. В то же время такая оценка важна для количественного сравнения стандартных криптографических алгоритмов и хаотических систем связи [14, 15].

В общем случае для дешифровки скрытого сообщения необходимо с высокой точностью восстановить структуру и параметры передатчика, а также алгоритм хаотической модуляции, после чего построить копию передатчика в приемнике. Таким образом, если о передающей системе почти ничего неизвестно, задача дешифровки сообщения сильно усложняется. Мы рассматриваем более простую ситуацию, предполагая, что структура передатчика и алгоритм модуляции заранее известны, а неизвестными являются только параметры передатчика.

В качестве примера системы связи, основанной на использовании динамического хаоса, рассмотрена система передачи информации на базе хаотического генератора с запаздыванием с переключаемым временем задержки. Для этой системы предложен метод количественной оценки конфиденциальности передачи скрытого бинарного сигнала. Метод основан на оценке мощности ключевого пространства для случая, когда значения всех параметров передатчика (времена запаздывания, параметры фильтра, вид нелинейной функции и ее параметры) неизвестны.

Исследуемая система передачи информации

Рассмотрим систему скрытой передачи информации на основе хаотического генератора с запаздыванием [4]. Блок-схема исследуемой системы связи показана на рис. 1.

Поясним кратко принцип ее работы. В зависимости от величины бинарного информационного сигнала $m(t)$ (0 или 1) время запаздывания в передатчике переключается с помощью ключа K между τ_1 и $\tau_1 + \tau_2$, где τ_1 и τ_2 — времена запаздывания линий задержки *ЛЗ*-1 и *ЛЗ*-2 соответственно. Передатчик описывается уравнением

$$\varepsilon_1 \dot{x}(t) = -x(t) + f\Big(x\big(t - \big(\tau_1 + m(t)\tau_2\big)\big)\Big), \qquad (1)$$

где $\varepsilon_1 = RC$ — параметр низкочастотного RC-фильтра первого порядка, определяющий инерционные свойства системы; $x(t)$ — сигнал на выходе фильтра $Ф$, передаваемый в канал связи; $f(x)$ — нелинейная функция, описывающая передаточную характеристику усилителя, играющего роль нелинейного элемента *НЭ*. Приемник состоит из двух ведомых систем с задержкой, динамика которых описывается уравнениями

$$\varepsilon_2 \dot{y}(t) = -y(t) + f\big(x(t - \tau_3)\big); \qquad (2)$$

$$\varepsilon_3 \dot{z}(t) = -z(t) + f\big(x(t - \tau_4)\big), \qquad (3)$$

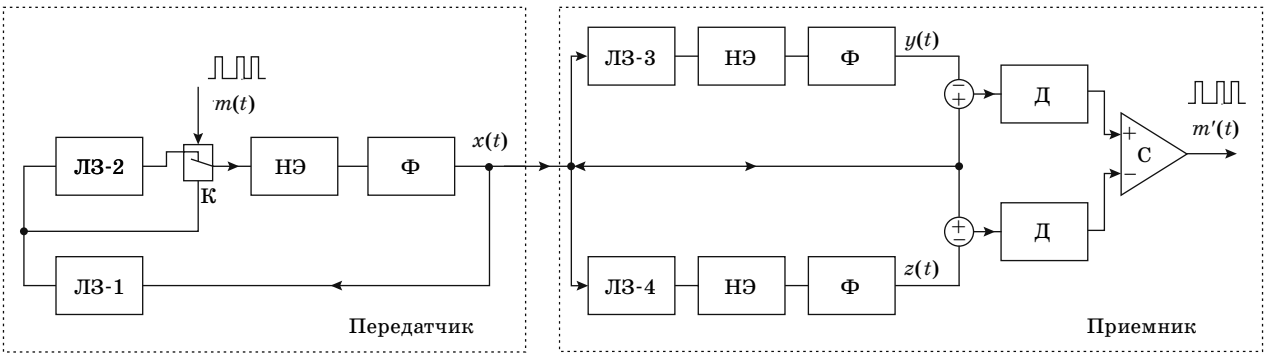
где τ_3 и τ_4 — времена запаздывания линий задержки *ЛЗ*-3 и *ЛЗ*-4 соответственно, а ε_2 и ε_3 — параметры фильтров $Ф$ в первой и во второй ведомой системе приемника соответственно.

Для расшифровки сигнала $m(t)$ параметры фильтров $Ф$ и нелинейных элементов *НЭ* приемника необходимо выбрать идентичными соответствующим параметрам передатчика, а времена запаздывания линий задержек выбрать следующим образом: $\tau_3 = \tau_1$ и $\tau_4 = \tau_1 + \tau_2$. Если $m(t) = 0$, то в результате синхронизации сигналов $x(t)$ и $y(t)$ имеем $y(t) = x(t)$ при отсутствии шума в канале связи, а $z(t) \neq x(t)$. Если $m(t) = 1$, то $z(t) = x(t)$, а $y(t) \neq x(t)$. Присутствие шумов препятствует полной синхронизации приемника с передатчиком.

Для борьбы с шумами схема содержит детекторы $Д$, которые оценивают дисперсии $\sigma_y^2(t)$ и $\sigma_z^2(t)$ разностных сигналов $x(t) - y(t)$ и $x(t) - z(t)$ соответственно на длине ряда, соответствующей длине передаваемого информационного бита. Компаратор C вычисляет разность дисперсий $r(t) = \sigma_y^2(t) - \sigma_z^2(t)$ и формирует восстановленный информационный сигнал $m'(t)$. Если $r(t) \leq 0$, то $m'(t) = 0$, а если $r(t) > 0$, то $m'(t) = 1$. Более подробное описание принципа работы схемы представлено в работах [4, 7]. Такая система передачи информации обладает высокой помехоустойчивостью, однако оценка ее конфиденциальности до настоящего времени не проводилась.

Оценка конфиденциальности системы связи

Для количественной оценки конфиденциальности системы передачи информации, представленной на рис. 1, введем ряд предположений. Будем считать, что неавторизованному пользователю известна структура передатчика и его модельное уравнение, известен алгоритм хаоти-



■ ***Рис. 1.*** Блок-схема системы передачи информации на хаотическом генераторе с запаздыванием с переключаемым временем задержки

■ ***Fig. 1.*** Block diagram of a communication system based on a chaotic time-delay generator with a switched delay time

ческой модуляции и длительность передачи одного бита информации. Параметры передатчика τ_1, τ_2, ε_1 и нелинейную функцию $f(x)$ будем считать неизвестными для стороннего наблюдателя. Неизвестные параметры передатчика являются аналогом секретного ключа, который требуется найти, имея в распоряжении лишь временной ряд хаотического сигнала $x(t)$, передаваемого в канале связи. При этом для простоты полагаем, что шумы в канале связи отсутствуют.

Для нахождения ключа будем использовать метод полного перебора. Выбор границ перебора параметров, определяющих мощность ключевого пространства, подробно обсудим в следующем разделе. В качестве критерия удовлетворительного качества дешифровки скрытого сообщения будем использовать величину BER (Bit-Error-Rate), равную нулю. Мощность ключевого пространства хаотической системы передачи информации, описываемой уравнением (1), будем сравнивать с мощностью ключевого пространства классических криптографических алгоритмов DES (Data Encryption Standard) и AES (Advanced Encryption Standard), представляющих собой шифр с длиной ключа 56 и 128 бит соответственно [16, 17].

На первом этапе будем полагать, что передаточная функция для нелинейного усилителя передатчика известна, и требуется провести подбор времен запаздывания линий задержки и время инерционности фильтра в передатчике. На втором этапе оценим, какие параметры и с каким шагом нужно перебирать для того, чтобы подобрать передаточную функцию нелинейного усилителя. Будем аппроксимировать ее степенным полиномом и перебирать коэффициенты полинома. На третьем этапе оценим, сколько вариантов набора параметров необходимо перебрать, если никакие параметры передатчика неизвестны.

Следует отметить, что исследуемая система передачи информации обладает в некоторой мере стеганографическими свойствами, т. е. она скрывает и сам факт передачи информационного сигнала. Если сторонний наблюдатель не знает, передается сообщение или нет, он сможет определить факт передачи информации только по косвенным признакам, например, по увеличению мощности принимаемого сигнала в некоторой полосе. В то же время обычная передача цифрового сигнала дает информацию не только о факте передачи, но и о скорости передачи данных.

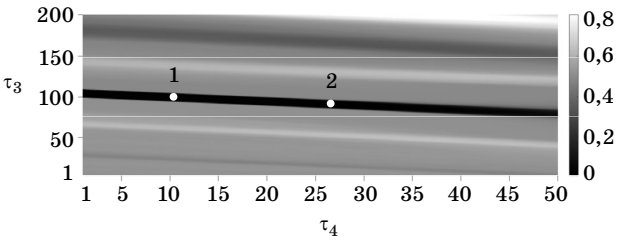
Результаты

Предположим сначала, что нам известна в явном виде нелинейная функция $f(x)$ и параметр ε_1 передатчика, а времена запаздывания τ_1 и τ_2 неизвестны. Пусть $\tau_1 = 100$, $\tau_2 = 10$, а длительность передачи одного бита информации составляет 200 единиц дискретного времени. Установим параметры фильтров и нелинейных функций приемника такими же, как в передатчике, а для определения τ_1 и τ_2 будем перебирать в приемнике значения τ_3 в диапазоне [1, 200], а τ_4 — в диапазоне [1, 50] с шагом 1. Такой выбор обусловлен длиной бита в рассматриваемой системе передачи информации. Для каждой пары значений τ_3 и τ_4 проведем численное моделирование, пытаясь извлечь передаваемый информационный сигнал и вычисляя BER для оценки качества его приема. На рис. 2 оттенками серого цвета показаны значения BER при различных значениях τ_3 и τ_4 при передаче 2000 бит информационного сигнала.

В точке *1* на рис. 2 $\tau_3 = \tau_1$, $\tau_4 = \tau_2$ и BER = 0. Из рисунка видно, что даже при существенном отличии времен запаздывания в приемнике от времен запаздывания в передатчике можно найти такую пару значений (τ_3, τ_4), при которой величина BER будет достаточно малой. Область с малыми значениями BER находится на рис. 2 внутри темной полосы. Если через середину этой полосы провести прямую линию, то лежащие на ней точки описываются эмпирическим уравнением

$$\tau_3 + 0{,}5\tau_4 = 105. \qquad (4)$$

Качество выделения информационного сигнала в приемнике падает при больших значениях τ_4, лежащих на линии (4), например, BER = 0,001 при $\tau_3 = 92$ и $\tau_4 = 26$ (точка *2*). При $\tau_4 = \text{const}$ ширина полосы на рис. 2, внутри которой BER = 0, составляет 5 единиц дискретного времени по τ_3. Это означает, что, выбрав τ_4, лежащим на линии (4), мы получим BER = 0 в интервале $[\tau_3 - 2, \tau_3 + 2]$, где $\tau_3 = 105 - 0{,}5\tau_4$ при условии, что $\tau_4 \le 25$. При $\tau_3 = \text{const}$ ширина полосы, внутри которой BER = 0, составляет 7 единиц дискретного времени по τ_4. Это означает, что, выбрав τ_3, лежащим на линии (4), мы получим BER = 0 в интервале $[\tau_4 - 3, \tau_4 + 3]$, где $\tau_4 = 2(105 - \tau_3)$ при условии, что $\tau_4 \le 25$.



■ ***Рис. 2.*** Значения BER при различных значениях τ_3 и τ_4 при передаче 2000 бит информационного сигнала при $\tau_1 = 100$, $\tau_2 = 10$

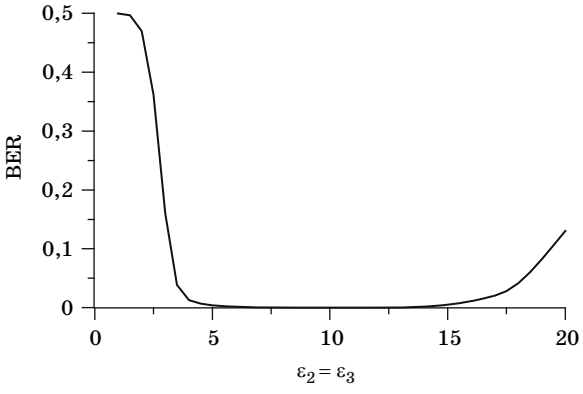
■ ***Fig. 2.*** BER values for different values of τ_3 and τ_4 at a transmission of 2000 bits of the information signal for $\tau_1 = 100$, $\tau_2 = 10$

Таким образом, для того чтобы на рис. 2 гарантированно попасть в область, внутри которой BER = 0, достаточно перебирать τ_3 с шагом 5 и τ_4 с шагом 7. Вместо полного перебора $200 \times 50 = 10\,000$ всевозможных пар значений τ_3 и τ_4 в диапазонах [1, 200] и [1, 50] соответственно для выделения скрытого информационного сигнала с качеством дешифровки BER = 0 достаточно перебрать в приемнике $40 \times 8 = 320$ пар значений τ_3 и τ_4.

Исследуем теперь зависимость качества дешифровки скрытого информационного сигнала от вариации параметров инерционности фильтров в приемнике. При фиксированных параметрах $\tau_3 = \tau_1 = 100$, $\tau_4 = \tau_2 = 10$ и $\varepsilon_1 = 10$ будем изменять в приемнике величину параметров $\varepsilon_2 = \varepsilon_3$ в диапазоне [1, 20] и вычислять BER. Полученные результаты представлены на рис. 3.

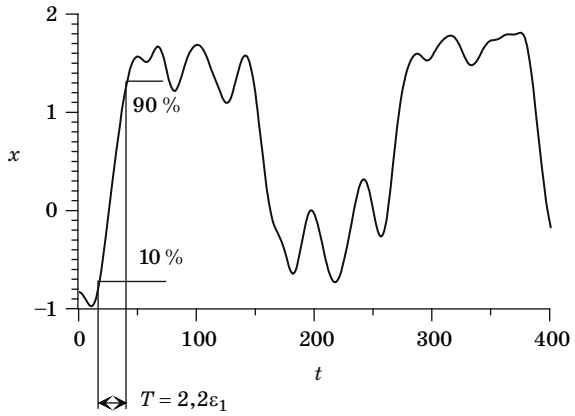
При $\varepsilon_2 = \varepsilon_3 = \varepsilon_1$ и отсутствии шумов в канале связи информационный сигнал выделяется в приемнике без ошибок и BER = 0. Однако даже при больших отличиях значений ε_2 и ε_3 от $\varepsilon_1 = 10$ величина BER увеличивается несущественно. При $8 \le \varepsilon_2 = \varepsilon_3 \le 12$ имеем BER = 0, а за пределами этой области в приемнике начинают появляться единичные ошибки при выделении информационного сигнала. Например, при $\varepsilon_2 = \varepsilon_3 = 15$ получаем BER = 0,005 (см. рис. 3). Следовательно, точность оценки параметра инерционности ε_1 не является критической для удовлетворительного качества выделения сообщения в приемнике. Оценить величину ε_1 можно по временному ряду сигнала передатчика и не подбирать ее. В дальнейших расчетах мы устанавливали $\varepsilon_2 = \varepsilon_3 = \varepsilon_1 = 10$.

Примерно оценить время инерционности фильтра в передатчике можно по временному ряду передаваемого в канал связи хаотического сигнала $x(t)$ (рис. 4), поскольку длительность T



■ ***Рис. 3.*** Зависимость BER от величины параметров $\varepsilon_2 = \varepsilon_3$ при передаче 2000 бит информационного сигнала при $\varepsilon_1 = 10$

■ ***Fig. 3.*** Dependence of BER on the parameter values $\varepsilon_2 = \varepsilon_3$ at a transmission of 2000 bits of the information signal for $\varepsilon_1 = 10$



■ ***Рис. 4.*** Оценка параметра инерционности ε_1 по временному ряду сигнала передатчика

■ ***Fig. 4.*** Estimation of the parameter of inertia ε_1 from time series of the transmitter signal

фронта сигнала по уровню от 10 до 90 % на выходе фильтра первого порядка [18] примерно равна $T = 2{,}2\varepsilon_1$. На рис. 4 представлены 10- и 90-процентные уровни между соседними минимумом и максимумом, расстояние между которыми составляет в дискретном времени $T = 23$. Откуда получаем оценку $\varepsilon_1 = 10{,}45$, которая близка к истинному значению $\varepsilon_1 = 10$.

Далее рассмотрим случай, когда времена запаздывания линий задержек и параметр инерционности фильтра в передатчике известны, а неизвестной является только нелинейная функция передатчика. Один из способов аппроксимировать нелинейную функцию — это представить ее в виде степенного полинома. При этом для аппроксимации простых нелинейных функций (квадратичной, кубической и др.) достаточно небольшого числа коэффициентов полинома. Такие нелинейные функции легко реконструировать, и их использование снижает конфиденциальность хаотических систем передачи информации.

В данной работе в качестве нелинейной функции передатчика выбрано нелинейное преобразование «сдвиг Бернулли»

$$f(x) = \{2x\}, \qquad (5)$$

где фигурные скобки обозначают дробную часть числа. Аппроксимация такого преобразования требует большего числа коэффициентов, чем аппроксимация простых функций, и, следовательно, эти коэффициенты сложнее подобрать.

Для аппроксимации функции (5) используем в приемнике степенной полином 7-го порядка

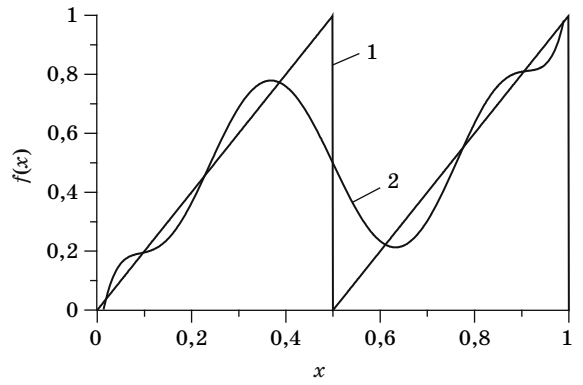
$$f(x) = p_7x^7 + p_6x^6 + p_5x^5 + p_4x^4 + p_3x^3 + p_2x^2 + p_1x + p_0. \qquad (6)$$

Выбор такого порядка полинома обусловлен тем, что при меньших порядках не удается обеспечить прием информационного сигнала без ошибок. С помощью метода наименьших квадратов мы получили при аппроксимации функции (5) следующие коэффициенты полинома (6):

$$p_7 = 948;\ p_6 = -3330;\ p_5 = 4538;\ p_4 = -3003;$$
$$p_3 = 989;\ p_2 = -152;\ p_1 = 11;\ p_0 = -0{,}12. \qquad (7)$$

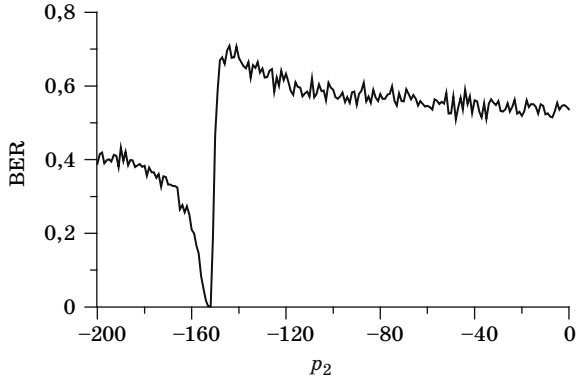
Нелинейная функция (5) в передатчике и ее аппроксимация полиномом (6) с коэффициентами (7) приведена на рис. 5. Следует отметить, что даже при такой грубой аппроксимации нелинейной функции передаваемое сообщение выделяется в приемнике без ошибок.

Исследуем зависимость BER при приеме информационного сигнала от значений коэффициентов полинома (6). На рис. 6 построена зависимость BER от коэффициента p_2 при вариации его значений в диапазоне [–200, 0] и постоянных значениях остальных коэффициентов, взятых из (7). Из рисунка видно, что BER = 0 при $p_2 = -152$, равном оптимальному значению p_2 в (7), а при отклонении от этого значения BER быстро растет. Для того чтобы попасть в минимум зависимости BER от p_2, значения коэффициента p_2 следует перебирать с шагом 1.



■ ***Рис. 5***. Нелинейная функция в виде сдвига Бернулли (линия *1*) и ее аппроксимация степенным полиномом 7-го порядка (линия *2*)

■ ***Fig. 5***. Nonlinear function in the form of Bernoulli shift (line *1*) and its approximation by a power polynomial of the 7th order (line *2*)



■ ***Рис. 6***. Зависимость BER от величины коэффициента p_2 при передаче 2000 бит информационного сигнала

■ ***Fig. 6***. Dependence of BER on the value of coefficient p_2 at a transmission of 2000 bits of the information signal

Качественно похожий вид имеет зависимость BER от коэффициентов $p_1, p_3, ..., p_7$. Величина коэффициента p_0 не влияет на величину BER, поскольку этот коэффициент отвечает за линейное вертикальное смещение графика полинома.

Для другой нелинейной функции, имеющей вид непрерывного «отображения палатки»:

$$f(x) = \begin{cases} 2x,\ 0 < x < \dfrac{1}{2} \\ 2(1-x),\ \dfrac{1}{2} \le x \le 1 \end{cases}, \qquad (8)$$

коэффициенты аппроксимирующего полинома 7-го порядка будут следующими: $p_7 = 1{,}3 \times 10^{-10}$; $p_6 = -93{,}381$; $p_5 = 280{,}14$; $p_4 = -305{,}2$; $p_3 = 143{,}49$; $p_2 = -29{,}289$; $p_1 = 4{,}2365$; $p_0 = -0{,}037984$.

Таким образом, если мы заранее не знаем нелинейную функцию, но знаем времена запаздывания и параметр инерционности, то для восстановления коэффициентов полинома, аппроксимирующего нелинейную функцию передатчика, необходимо перебрать достаточно большое количество коэффициентов в многомерном пространстве. Для того чтобы метод перебора коэффициентов позволил восстановить различные возможные нелинейные функции с количеством экстремумов не более трех, необходимо перебирать коэффициенты полинома 7-го порядка в достаточно широком диапазоне. При расчетах мы перебирали коэффициенты в следующих интервалах: $p_7 \in [-1000, 1000]$, $p_6 \in [-5000, 5000]$, $p_5 \in [-5000, 5000]$, $p_4 \in [-5000, 5000]$, $p_3 \in [-1000, 1000]$, $p_2 \in [-200, 200]$, $p_1 \in [-10, 10]$. Для нахождения оптимального набора коэффициентов (7) полинома (6) методом прямого перебора всех перечисленных коэффициентов с шагом 1 потребуется перебрать примерно $3{,}2 \times 10^{22}$ комбинаций. Для аппроксимации нелинейных функций передатчика с числом экстремумов более трех потребуются полиномы более высокого порядка, и количество перебираемых комбинаций при восстановлении их коэффициентов увеличится.

Наконец, рассмотрим случай, когда неизвестны все параметры передатчика. Для нахождения параметров, обеспечивающих выделение скрытого информационного сигнала с качеством дешифровки BER = 0, потребуется перебрать в при-

емнике $320 \times (3{,}2 \times 10^{22})$ различных комбинаций параметров. При этом параметр инерционности можно оценить по временному ряду. Общее количество вариантов примерно равно $10^{25} \approx 2^{80}$.

Таким образом, система передачи информации на основе хаотического генератора с запаздыванием с переключаемым временем задержки имеет мощность ключевого пространства примерно 2^{80} и, следовательно, обладает значительно более высокой конфиденциальностью, чем классический криптографический алгоритм DES, имеющий мощность ключевого пространства 2^{56}, но существенно уступает по криптографической стойкости алгоритму AES, имеющему мощность ключевого пространства 2^{128}.

Заключение

Итак, нами предложен метод, позволяющий получить количественную оценку конфиденциальности передачи скрытого бинарного сигнала в системе связи, основанной на хаотическом генераторе с запаздыванием с переключаемым временем задержки. Оценка криптографических свойств рассмотренной хаотической системы передачи информации получена при условии, что известна структура передающей системы, принцип модуляции ее управляющих параметров и длительность передачи одного бита информации.

Полученная оценка криптографической стойкости системы связи, основанной на использовании динамического хаоса, свидетельствует о недостаточной стойкости рассмотренной системы передачи информации согласно современным криптографическим стандартам. Криптографическая стойкость этой системы связи может быть увеличена, если увеличить число неизвестных параметров передатчика. Использование нелинейной функции более сложного вида также повысит мощность ключевого пространства.

Стойкость рассмотренной системы связи будет выше, если длительность передачи одного бита информации будет неизвестна для стороннего наблюдателя. В этом случае в дополнение к остальным параметрам необходимо также подбирать и длину бита, что увеличивает количество перебираемых вариантов. Кроме того, наличие шума в канале связи также может приводить к повышению конфиденциальности системы передачи информации, поскольку присутствие шума мешает восстановлению истинных параметров передатчика.

С другой стороны, использование априорных знаний и разумных предположений о параметрах передающей системы может существенно сократить количество перебираемых вариантов и уменьшить время восстановления параметров передатчика.

Финансовая поддержка

Работа выполнена при финансовой поддержке гранта РФФИ № 18-07-00205.

Литература

1. **Дмитриев А. С., Панас А. И.** *Динамический хаос: новые носители информации для систем связи*. М., Физматлит, 2002. 252 с.
2. **Короновский А. А., Москаленко О. И., Храмов А. Е.** О применении хаотической синхронизации для скрытой передачи информации. *Успехи физических наук*, 2009, т. 179, № 12, с. 1281–1310. doi:10.3367/UFNr.0179.200912c.1281
3. **Караваев А. С., Кульминский Д. Д., Пономаренко В. И., Прохоров М. Д.** Система цифровой передачи информации, маскируемой хаотическим сигналом системы с запаздыванием. *Информационно-управляющие системы*, 2013, № 4, с. 30–35.
4. **Кульминский Д. Д., Пономаренко В. И., Караваев А. С., Прохоров М. Д.** Система связи, основанная на синхронизации систем с задержкой с переключением хаотических режимов. *Информационно-управляющие системы*, 2015, № 3, с. 85–91. doi:10.15217/issn1684-8853.2015.3.85
5. **Ren H.-P., Bai C., Liu J., Baptista M. S., Grebogi C.** Experimental validation of wireless communication with chaos. *Chaos*, 2016, vol. 26, 083117. doi:10.1063/1.4960787
6. **Кульминский Д. Д., Пономаренко В. И., Прохоров М. Д., Безручко Б. П.** Система передачи информации, основанная на обобщенной хаотической синхронизации. *Информационно-управляющие системы*, 2016. № 2. с. 42–47. doi:10.15217/issn1684-8853.2016.2.42
7. **Кульминский Д. Д., Пономаренко В. И., Караваев А. С., Прохоров М. Д.** Устойчивая к шумам система скрытой передачи информации на хаотическом генераторе с запаздыванием с переключаемым временем задержки. *Журнал технической физики*, 2016, т. 86, вып. 5, с. 1–8.
8. **Yao J.-L., Li C., Ren H.-P., Grebogi C.** Chaos-based wireless communication resisting multipath effects. *Physical Review E*, 2017, vol. 96, 032226. doi:10.1103/PhysRevE.96.032226
9. **Carroll T. L.** Chaos for low probability of detection communications. *Chaos, Solitons & Fractals*, 2017, vol. 103. pp. 238–245. doi:10.1016/j.chaos.2017.06.011
10. **Oden J., Lavrov R., Chembo Y. K., Larger L.** Multi-Gbit/s optical phase chaos communications using a

time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity. *Chaos*, 2017, vol. 27, 114311. doi:10.1063/1.5007867
11. **Дмитриев А. С., Герасимов М. Ю., Ицков В. В., Лазарев В. А., Попов М. Г., Рыжов А. И.** Активные беспроводные сверхширокополосные сети на основе хаотических радиоимпульсов. *Радиотехника и электроника*, 2017, т. 62, № 4, с. 354–363.
12. **Дмитриев А. С., Мохсени Т. И., Сьерра-Теран К. М.** Относительная передача информации на основе хаотических радиоимпульсов. *Радиотехника и электроника*, 2018, т. 63, № 10, с. 1074–1082.
13. **Smart N.** *Cryptography: An Introduction*. McGraw-Hill, 2002. 417 p.
14. **Kocarev L., Lian S.** *Chaos-Based Cryptography. Theory, Algorithms and Applications*. Berlin Heidelberg, Springer-Verlag, 2011. 397 p.
15. **Владимиров С. Н., Измайлов И. В., Пойзнер Б. Н.** *Нелинейно-динамическая криптология. Радиофизические и оптические системы*. М., Физматлит, 2009. 2018 с.
16. **Bauer F.** *Decrypted Secrets. Methods and Maxims of Cryptology*. Berlin Heidelberg, Springer-Verlag, 2007. 555 p.
17. **Schneier B.** *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, Wiley, 1996. 662 p.
18. **Tietze U., Schenk Ch.** *Electronic Circuits. Handbook for Design and Application*. Berlin Heidelberg, Springer-Verlag, 2008. 1544 p.

UDC 537.86
doi:10.31799/1684-8853-2019-4-54-61

Estimation of confidentiality of a communication system based on chaotic time-delay generator with switchable delay time

V. I. Ponomarenko[a,b], Dr. Sc., Phys.-Math., Professor, orcid.org/0000-0002-1579-6465
E. V. Navrotskaya[b], PhD, Phys.-Math., Associate Professor, orcid.org/0000-0002-1649-440X
D. D. Kul'minskii[a,b], PhD, Phys.-Math., Research Fellow, orcid.org/0000-0002-3936-2813
M. D. Prokhorov[a], Dr. Sc., Phys.-Math., Professor of RAS, orcid.org/0000-0003-4069-9410, mdprokhorov@yandex.ru
[a]Saratov Branch of the Kotelnikov Institute of Radioengineering and Electronics of RAS, 38, Zelyonaya St., 410019, Saratov, Russian Federation
[b]Saratov State University named after N. G. Chernyshevsky, 83, Astrakhanskaya St., 410012, Saratov, Russian Federation

Introduction: Communication systems based on the use of dynamical chaos have a number of positive features. Dynamical chaos has the properties of random processes, which allows systems based on it to ensure the information transmission confidentiality. However, a quantitative security assessment of such systems is a complicated problem, since the methods for evaluating cryptographic strength are well developed only for the classical encryption algorithms. **Purpose:** Development of a method for quantitative estimation of confidentiality of a binary signal hidden transmission in a communication system based on a chaotic time-delay oscillator with switchable delay time. **Results:** A method is proposed for estimating the confidentiality of a binary information signal transmission in a communication system using a chaotic time-delay oscillator with switchable delay time as a transmitter. The method is based on estimating the power of the key space for the chaotic communication system under study. We have considered the cases when some transmitter parameters are known, and the most general case when all the transmitter parameters are unknown. A communication system based on dynamical chaos may have a much higher confidentiality than the classical cryptographic algorithm using a cipher with a key length of 56 bits, but is significantly inferior in terms of cryptographic strength to a cipher with a key length of 128 bits. **Practical relevance:** The proposed method allows us to obtain a quantitative estimation of confidentiality of communication systems based on dynamical chaos, and compare it with the known strength of classical cryptographic algorithms.

Keywords — communication system, dynamical chaos, cryptography, time-delay systems.

For citation: Ponomarenko V. I., Navrotskaya E. V., Kul'minskii D. D., Prokhorov M. D. Estimation of confidentiality of a communication system based on chaotic time-delay generator with switchable delay time. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 4, pp. 54–61 (In Russian). doi:10.31799/1684-8853-2019-4-54-61

References

1. Dmitriev A. S., Panas A. I. *Dinamicheskii khaos: novye nositeli informatsii dlya sistem svyazi* [Dynamical Chaos: New Information Carriers for Communication Systems]. Moscow, Fizmatlit Publ., 2002. 252 p. (In Russian).
2. Koronovskii A. A., Moskalenko O. I., Hramov A. E. On the use of chaotic synchronization for secure communication. *Physics — Uspekhi*, 2009, vol. 179, no. 12, pp. 1281–1310 (In Russian). doi:10.3367/UFNe.0179.200912c.1281
3. Karavaev A. S., Kul'minskii D. D., Ponomarenko V. I., Prokhorov M. D. System of digital transmission of information masked by chaotic signal of time-delay system. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 4, pp. 30–35 (In Russian).
4. Kul'minskii D. D., Ponomarenko V. I., Karavaev A. S., Prokhorov M. D. Communication system based on synchronization of time-delay systems with switching of chaotic regimes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 85–91 (In Russian). doi:10.15217/issn1684-8853.2015.3.85
5. Ren H.-P., Bai C., Liu J., Baptista M. S., Grebogi C. Experimental validation of wireless communication with chaos. *Chaos*, 2016, vol. 26, 083117. doi:10.1063/1.4960787
6. Kul'minskii D. D., Ponomarenko V. I., Prokhorov M. D., Bezruchko B. P. Communication system based on generalized chaotic synchronization. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 2,

pp. 42–47 (In Russian). doi:10.15217/issn1684-8853.2016.2.42
7. Kul'minskii D. D., Ponomarenko V. I., Karavaev A. S., Prokhorov M. D. Noise-resistant system of concealed information transfer on a chaotic delayed feedback oscillator with switchable delay time. *Technical Physics*, 2016, vol. 61, no. 5, pp. 639–647. doi:10.1134/S1063784216050121
8. Yao J.-L., Li C., Ren H.-P., Grebogi C. Chaos-based wireless communication resisting multipath effects. *Physical Review E*, 2017, vol. 96, 032226. doi:10.1103/PhysRevE.96.032226
9. Carroll T. L. Chaos for low probability of detection communications. *Chaos, Solitons & Fractals*, 2017, vol. 103, pp. 238–245. doi:10.1016/j.chaos.2017.06.011
10. Oden J., Lavrov R., Chembo Y. K., Larger L. Multi-Gbit/s optical phase chaos communications using a time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity. *Chaos*, 2017, vol. 27, 114311. doi:10.1063/1.5007867
11. Dmitriev A. S., Gerasimov M. Y., Itskov V. V., Lazarev V. A., Popov M. G., Ryzhov A. I. Active wireless ultrawideband networks based on chaotic radio pulses. *Journal of Communications Technology and Electronics*, 2017, vol. 62, no. 4, pp. 380–388. doi:10.1134/S1064226917040052
12. Dmitriev A. S., Mokhsenit T. I., Sierra-Terant C. M. Differentially coherent communication scheme based on chaotic radio pulses. *Journal of Communications Technology and Electronics*, 2018, vol. 63, no. 10, pp. 1183–1190. doi:10.1134/S1064226918100078
13. Smart N. *Cryptography: An Introduction*. McGraw-Hill, 2002, 417 p.
14. Kocarev L., Lian S. *Chaos-Based Cryptography. Theory, Algorithms and Applications*. Berlin Heidelberg, Springer-Verlag, 2011. 397 p.
15. Vladimirov S. N., Izmaylov I. V., Poyzner B. N. *Nelineyno-dinamicheskaya kriptologiya. Radiofizicheskiye i opticheskiye sistemy* [Nonlinear Dynamic Cryptology. Radiophysical and Optical Systems]. Moscow, Fizmatlit Publ., 2009. 2018 p. (In Russian).
16. Bauer F. *Decrypted Secrets. Methods and Maxims of Cryptology*. Berlin Heidelberg, Springer-Verlag, 2007. 555 p.
17. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, Wiley, 1996. 662 p.
18. Tietze U., Schenk Ch. *Electronic Circuits. Handbook for Design and Application*. Berlin Heidelberg, Springer-Verlag, 2008. 1544 p.

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org