

09

Хаотическая схема связи с умножением

© А.М. Бобрешов, А.А. Караваев

Воронежский государственный университет
E-mail: akv80@mail.ru

Поступило в Редакцию 21 сентября 2006 г.

Предложена схема передачи информации с нелинейным подмешиванием, в которой в качестве двух взаимно обратных операций применяются операции умножения и деления, обеспечивающие мультипликативную смесь информационного и хаотического сигналов и потенциально более высокую степень конфиденциальности. Особенностью данной схемы является отсутствие связанных с делением на ноль ограничений на виды используемых информационных сигналов.

PACS: 05.45.-a

Одним из перспективных направлений исследования динамического хаоса является использование хаотических сигналов для конфиденциальной передачи и приема информации [1]. Особое место среди таких систем связи занимают хаотические системы с нелинейным подмешиванием [2], важной особенностью которых является возможность выделения информационной составляющей из широкополосного хаотического сигнала на основе синхронного хаотического отклика. Эта возможность обусловлена применением в системе связи двух взаимно-обратных операций. Последнее время широко исследуется схема [3], где в качестве взаимно обратных операций используются операции сложения и вычитания. Такая схема обеспечивает на выходе передатчика аддитивную смесь информационного и хаотического сигналов и тем самым маскировку информационного сигнала хаотическим. Применение других взаимно обратных операций сталкивается с рядом трудностей. Например, возможность использования операций умножения и деления, обеспечивающих мультипликативную смесь информационного и хаотического сигналов на выходе передатчика, ограничивается видами применяемых сигналов из-за невозможности деления на ноль.

В данном сообщении предлагается схема передачи информации, основанная на принципе синхронного хаотического отклика, в которой

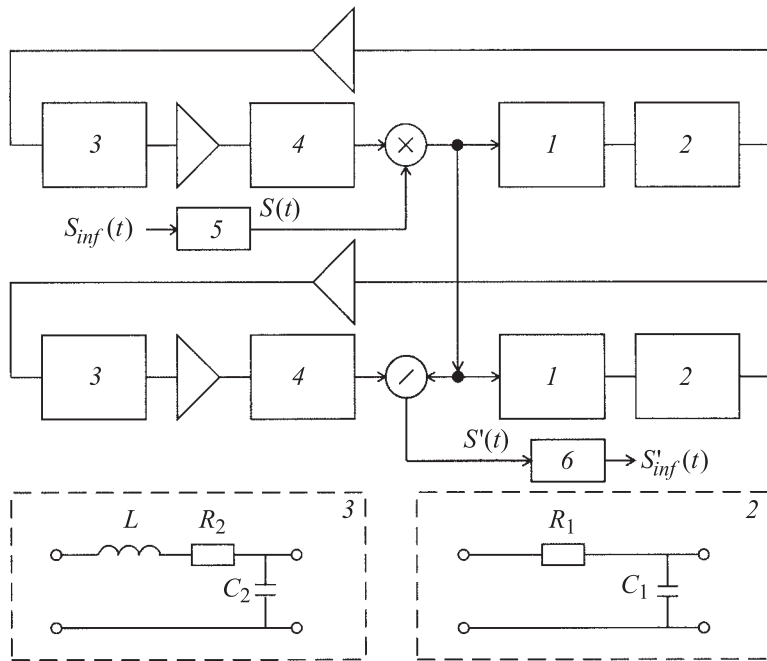


Рис. 1. Функциональная схема.

в качестве двух взаимно обратных операций применяются операции умножения и деления, обеспечивающие потенциально более высокую степень конфиденциальности схемы связи. Особенностью предлагаемой схемы является отсутствие ограничений, связанных с делением на ноль, на виды используемых информационных сигналов.

Рассмотрим принцип работы коммуникационной схемы, представленной на рис. 1. При этом будем считать, что параметры передатчика и приемника идентичны и в канале связи отсутствуют какие-либо помехи. Передатчик и приемник включают в себя нелинейный элемент I (см. рис. 1), инерционное звено 2 , линейный фильтр 3 , дополнительный нелинейный преобразователь 4 , два операционных усилителя, используемых в качестве буферных элементов. Характеристика нелинейного элемента $f(x) = Mx \exp\{-x^2\}$, где M — постоянный

коэффициент, x — сигнал на входе нелинейного элемента. В качестве характеристики нелинейного преобразователя 4 возьмем функцию $v(x)$, которая будет определена далее. В передатчике для введения информационного сигнала используется умножитель и прямой преобразователь сигнала 5, который формирует сигнал $S(t) = S_{inf}(t) + 1$ и тем самым обеспечивает генерацию хаотического сигнала при $S_{inf}(t) \ll 1$. На умножителе образуется мультипликативная смесь преобразованного информационного и хаотического сигналов. Далее эта смесь поступает в канал связи. В приемнике на делителе формируется сигнал $S'(t)$, который поступает на вход обратного преобразователя 6, реализующего операцию $S'_{int}(t) = S'(t) - 1$.

Модель данной схемы связи с умножением описывается следующими системами уравнений для передатчика (1) и приемника (2):

$$\begin{cases} \dot{X}_1(t) = f(S(t)v[Y_1(t)])/T - X_1(t)/T, \\ \dot{Y}_1(t) = \omega^2 Z_1(t) - qY_1(t), \\ \dot{Z}_1(t) = X_1(t) - Y_1(t); \end{cases} \quad (1)$$

$$\begin{cases} \dot{X}_2(t) = f(U(t))/T - X_2(t)/T, \\ \dot{Y}_2(t) = \omega^2 Z_2(t) - qY_2(t), \\ \dot{Z}_2(t) = X_2(t) - Y_2(t), \\ \dot{S}(t) = U(t)/v(Y_2(t)). \end{cases} \quad (2)$$

Параметры в системах уравнений (1) и (2) определяются следующим образом: $T = R_1 C_1$, $\omega^2 = 1/LC_2$, $q = R_2/L$. Здесь R_1 , R_2 , C_1 , C_2 , L — параметры элементов приемника и соответственно передатчика (рис. 1); $X_1(t)$ и $X_2(t)$ — сигналы на выходе инерционного звена; $Y_1(t)$ и $Y_2(t)$ — сигналы на выходе линейного фильтра; $U(t)$ — сигнал, поступающий на вход приемника, в нашем случае $U(t) = S(t)v[Y_1(t)]$. Первое уравнение в (1) описывает инерционное звено, на вход которого поступает сигнал $f(S(t)v[Y_1(t)])$. Второе и третье уравнения описывают линейный фильтр. Как видно из системы уравнений (2), сигнал на выходе делителя в приемнике определяется следующим образом:

$$S'(t) = U(t)/v[Y_2(t)] = S(t)(v[Y_1(t)]/v[Y_2(t)]). \quad (3)$$

В (3), как и для схем с операциями сложение–вычитание, сигналы $v[Y_1(t)]$ и $v[Y_2(t)]$ идентичны, так как образуются из сигнала $S(t)v[Y_1(t)]$,

прошедшего через цепочки с идентичными параметрами — нелинейный элемент, инерционное звено, линейный фильтр, дополнительный нелинейный преобразователь — в передатчике и приемнике соответственно. Очевидно, что если дополнительный нелинейный преобразователь отсутствует, то $S'(t) = S(t)(Y_1(t)/Y_2(t))$. Тогда для моментов времени t^* , таких что $Y_2(t^*) = 0$, возникает ошибка деления на ноль. Очевидно, что характеристика применяемого дополнительного нелинейного преобразователя $v(x)$ не должна обращаться в ноль для всех возможных значений x входного сигнала, поэтому для определенности возьмем $v(x) = \sin^2(x) + a$, где $a > 0$.

При численном моделировании значения параметров схемы выбирались таким образом, чтобы обеспечивалась генерация хаотического сигнала в передатчике: $R_1 = 50 \Omega$, $C_1 = 1 \mu\text{F}$, $R_2 = 100 \Omega$, $C_2 = 100 \text{ nF}$, $L = 20 \text{ mH}$, $M = 21$, $a = 1$. Для проверки работоспособности схемы в качестве информационного сигнала был взят монохроматический сигнал $S_{inf}(t) = A \sin(2\pi f t)$, $A = 20 \cdot 10^{-3} \text{ V}$, $f = 5 \cdot 10^3 \text{ Hz}$. Спектр сигнала $U(t)$ на выходе передатчика, полученный в результате численного моделирования, представлен на рис. 2, из которого очевидно, что информационный сигнал скрыт в хаотическом спектре. Далее в эксперименте из хаотической смеси $U(t)$ на выходе приемника восстанавливался сигнал $S'_{inf}(t)$, который полностью повторял сигнал $S_{inf}(t)$.

Однако необходимо заметить, что при физической реализации как данной схемы, так и других схем с нелинейным подмешиванием возникает ряд проблем. Во-первых, это сложность реализации нелинейных функций с заданными параметрами на аналоговой элементной базе. Во-вторых, это проблема точного согласования параметров элементов приемной и передающей схем. Эти проблемы могут быть эффективно решены с использованием цифровых методов для генерации и обработки хаотических сигналов [4]. В-третьих, и воздействие внешних помех, и особенности распространения сигналов в физической среде канала связи, и сопряжение цифровых сигналов передатчика и приемника с каналом связи (модуляция и демодуляция) могут вносить существенные искажения в принимаемый сигнал. В этом случае сигнал, поступающий на вход нелинейного элемента приемника, упрощенно можно представить в виде (4):

$$U(t) = S(t)v[Y_1(t)] + N(t), \quad (4)$$

где $N(t)$ — дополнительная составляющая, которая возникает вследствие неидеальности канала связи или воздействия помех. Например,

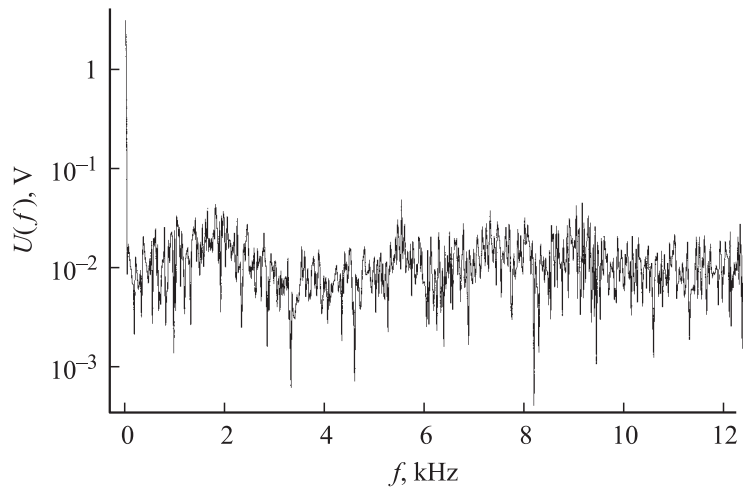


Рис. 2. Спектр сигнала на выходе передатчика.

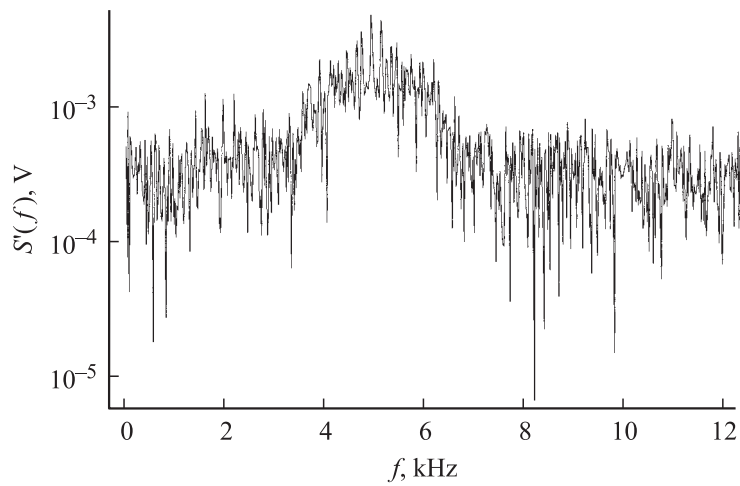


Рис. 3. Спектр сигнала на выходе приемника.

для $N(t)$, представляющего собой равномерный шум с максимальной амплитудой $h = 15$ mV измеренное при численном моделировании отношение мощности сигнала $S'_{inf}(t)$ (рис. 3) к мощности шума на выходе приемника для информационного сигнала вида $S_{inf}(t) = A \sin(2\pi f(1 + 0.01 \sin(2\pi \cdot 100t))t)$ с $A = 20 \cdot 10^{-3}$ V и $f = 5 \cdot 10^3$ Hz составило $K_{SNR} = +14$ dB, причем с уменьшением h наблюдалось увеличение соотношения K_{SNR} . Такая высокая чувствительность к внешним воздействиям характерна для идеальных секретных систем [5], что и обуславливает применение в таких системах как блоков модуляции и демодуляции с высокой помехоустойчивостью, так и дополнительного помехозащитного кодирования. Однако и после выделения из хаотической смеси приемником сигнала $S'_{inf}(t)$ возможна дальнейшая его обработка, например статистическими методами, нацеленная на улучшение качества принятого сигнала.

Таким образом, информационный сигнал, вводимый в передатчике хаотической схемы связи с умножением, может быть скрыт в канале связи и с достаточной степенью точности восстановлен приемником из принимаемой хаотической смеси $U(t)$. Представленная схема расширяет класс хаотических систем связи с нелинейным подмешиванием.

Список литературы

- [1] Гуляев Ю.В., Беляев Р.В., Воронцов Г.М. и др. // РЭ. 2003. Т. 48. В. 10. С. 1157–1185.
- [2] Волковский А.Р., Рульков Н.В. // Письма в ЖТФ. 1993. Т. 19. В. 3. С. 71–75.
- [3] Бобрешов А.М., Караваев А.А. // Вестник ВГУ. Сер. физика, математика. 2003. В. 2. С. 20–24.
- [4] Емец С.В., Старков С.О. // РЭ. 2000. Т. 45. В. 4. С. 462–470.
- [5] Shannon C.E. // Bell System Tech. Journal. 1949. V. 28. P. 656–715.