

Институт радиотехники и электроники РАНук (Фрязинское отделение)
141120, Фрязино, пл. Введенского, 1, ФИРЭ РАН
Тел.: (095) 5269049, e-mail: kalyan@ms.ire.rssi.ru

Реферат. Рассмотрена схема скрытой передачи цифрового сигнала, пригодная для пакетной связи. Исследована математическая модель маскировки информации многомодовым хаосом. Показано, что возможна скрытая передача информации при использовании в передатчике и приемнике ждущих хаотических генераторов с запаздыванием, запускаемых пилот сигналом.

Маскировка информации хаотическими колебаниями, начиная с работы [1], широко исследуется и определяет одно из важных применений генераторов с хаотической динамикой. Хаотическая маскировка представляет интерес применительно к пакетной связи, которая все больше используется в последнее время. Станция пакетной связи содержит компьютер, контроллер и радиостанцию [2]. Компьютер служит для ввода-вывода буквенно-цифровой информации, а контроллер выполняет роль «посредника» между радиостанцией и компьютером. Заранее подготовленная информация передается в автоматическом режиме. При передаче конфиденциальной информации требуется тщательная ее маскировка. В этом случае наиболее эффективной представляется маскировка шумовыми или хаотическими сигналами. При этом целесообразным является применение хаотических систем с многомодовым хаосом, так как при использовании хаотических колебаний с малой фрактальной размерностью могут быть определены параметры источника хаоса.

В настоящей работе рассматривается способ хаотической маскировки применительно к пакетной радиосвязи, основанный на использовании ждущих хаотических систем с многомодовым хаосом. Этот способ иллюстрируется блок-схемой рис.1, содержащей передатчик из элементов 1-8 (рис. 1,а) и приемное устройство из элементов 9 – 16 (рис. 1,б).

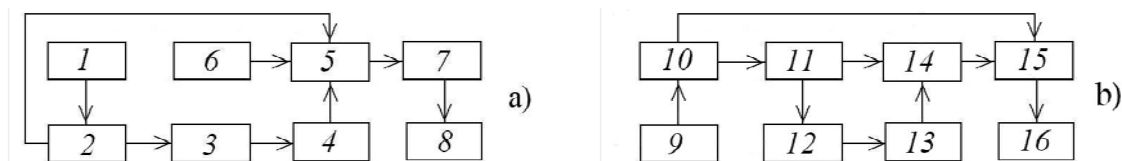


Рис. 1

Генератор 1 формирует запускающий радиоимпульс $f(t)$ ("пилот сигнал"), который можно определить следующими условиями: $f(t) = 0$ при $t < t_0$, $f(t) = A_{PS} \cos(\omega_{PS} t)$ при $t \geq t_0$ и $f(t) = 0$ при $t \geq t_p$, где A_{PS} , ω_{PS} - амплитуда и частота несущих колебаний радиоимпульса, t_0 , t_p - моменты начала и окончания импульса.

После прохождения колебаний через разветвитель 2 на одном его выходе (первом), соединенном с линией задержки 3, реализуется колебательный процесс $\gamma_P f(t)$, а на другом (втором) - процесс $(1 - \gamma_P) f(t)$ (где γ_P - коэффициент разветвления). На выходе линии задержки имеем $\varphi_1(\tau) = \gamma_P f(\tau)$, где $\tau = t - T_P$, T_P - задержка сигнала в линии 3.

Неавтономные уравнения, описывающие процессы в генераторе 4, можно представить в виде

$$d^2 x_1 / dt^2 + (\omega_1 / Q_1) dx_1 / dt + \omega_1^2 x_1 = \omega_1^2 \{ (1 / \sigma_1) [dF(y_1) / dt] + \varphi_1(\tau) \}, \quad (1a)$$

$$\delta_1 dy_1 / dt + y_1 = x_1(t - T_1), \quad (1б)$$

где $x_1 = x_1(t)$, $y_1 = y_1(t)$, ω_1 , Q_1 - собственная частота и добротность фильтра второго порядка генератора, σ_1 , δ_1 - постоянные времени дифференцирующего элемента и фильтра первого порядка, T_1 - запаздывание в цепи обратной связи, $F_1(y_1)$ - характеристика нелинейного элемента.

Жесткое возбуждение генератора обеспечивается при характеристике нелинейного элемента

$$F_1(y_1) = \sigma_1 B_1 y_1^2 / (1 + y_1^2), \quad (2)$$

где B_1 - постоянный коэффициент.

Колебания $x(t)$, модулируемые передаваемым сообщением $s(t)$ в устройстве 6, представим так, что $x(t) = 0$ при $t < t_0 + T_P + T_0$ и $x(t) = A_C [1 + s(t)] \cos(\omega_C t)$ при $t \geq t_0 + T_P + T_0$, где A_C , ω_C - амплитуда и частота несущих колебаний, T_0 - задержка сигнала сообщения относительно момента поступления запускающего импульса на генератор 4. Тогда для сигнала $z_1(t)$ на выходе сумматора 5 можно записать $z_1 = x_1(t) + x(t) + (1 - \gamma_P) f(t)$, а для сигнала на выходе усилителя 7 (обладающего коэффициентом усиления G) - $G z_1(t)$. Эти колебания излучаются антенной 8.

В приемном устройстве колебания с антенны 9 подаются на разветвитель 10. С одного его выхода (первого) принятые колебания поступают на электронный коммутатор 11, который, пропуская пилот сигнал, запирается, так что на ждущий генератор 13, который подобен генератору 4, воздействует только радиоимпульс, прошедший через линию задержки 12, а хаотические колебания, сформированные в передатчике, «отсекаются». При этом в коммутаторе 11 при разветвлении радиоимпульса на две равные части компенсируются потери на разветвление так, что колебания радиоимпульса на каждом из двух выходов равны колебаниям радиоимпульса на входе коммутатора. Если на входе разветвителя 10 колебательный процесс (при компенсации потерь в передающем тракте) определяется величиной $G z_1(t)$, то на первом его выходе (на входе коммутирующего устройства 11) реализуются колебания $G \gamma_R z_1(t)$, где γ_R – коэффициент разветвления. В втором его выходе имеем сигнал $(1 - \gamma_R) G z_1(t)$. После прохождения коммутирующего устройства имеем $G \gamma_R (1 - \gamma_P) f(t)$, а после задержки в линии 12 на время T_R (при условии $T_R = T_P$) – $\varphi_2(\tau) = G \gamma_R (1 - \gamma_P) f(\tau)$. В результате воздействия этого сигнала генератор 13 возбуждается. При этом его колебания $x_2(t)$ определяются решением уравнений, получающихся из системы (2), (3) при замене индекса 1 на индекс 2; постоянные параметры ($\omega_2, Q_2, B_2, \delta_2, \sigma_2, T_2$) имеют тот же смысл, что и аналогично обозначенные параметры с индексом 1 в системе (1), (2).

Колебания $x_2(t)$ подаются на один из входов сумматора 14. На другой его вход поступает сигнал, равный величине $(1 - \gamma_P) \gamma_R G f(t)$. Суммарный колебательный процесс, определяемый выражением $z_2(t) = x_2(t) + (1 - \gamma_P) \gamma_R G f(t)$, попадает на один из входов (на первый) вычитающего устройства 15. На второй его вход подаются колебания (с выхода разветвителя 10), равные $G (1 - \gamma_R) z_1(t)$. Разностные колебания $z(t) = G (1 - \gamma_R) z_1(t) - z_2(t)$ воздействуют на детектирующее устройство 16, с которого снимается выходной сигнал после процессов нелинейного преобразования, интегрирования и фильтрации, описываемых уравнениями

$$u = \xi_0 + \xi_1 z + \xi_2 z^2,$$

$$dv/dt = \zeta (u - v),$$

$$d^2w/dt^2 + (\omega_0/Q_0) dw/dt + \omega_0^2 (w - \beta v) = 0,$$

где $\xi_0, \xi_1, \xi_2, \zeta, \omega_0, Q_0, \beta$ – постоянные, $u(t), v(t), w(t)$ – сигналы на выходах нелинейного, интегрирующего и фильтрующего устройств соответственно.

На рис. 2 приведены характерные спектры мощности при передаче информации. При численном анализе математической модели генераторы 4 и 13 полагались идентичными, а их параметры (при $i = 1, 2$) равными следующим значениям: $\omega_i = 4, Q_i = 1, B_i = 8, \delta_i = 0.1, T_i = 2$. Передаваемый сигнал $s(t)$ задан в виде $s(t) = A_\Omega \cos \Omega t$. При этом $A_{PS} = 2, \omega_{PS} = 4, t_0 = 10, t_P = 20, T_P = T_R = 2, T_0 = 1, G = 2, \gamma_P = \gamma_R = 0.5, A_\Omega = 0.2, \Omega = 0.6, A_C = 0.4, \omega_C = 4, \xi_0 = 0.1, \xi_1 = 0.2, \xi_2 = 2, \zeta = 1, \omega_0 = 0.4, Q_0 = 1, \beta = 0$. На рис. 2,а иллюстрируется спектр мощности S_1 на выходе устройства 6 и спектр мощности S_3 на выходе приемного устройств, а на рис. 2,б – спектр мощности S_2 на выходе усилителя 7.

Как видно (рис. 2,б), спектр мощности на выходе передатчика отображает хаотический характер колебаний. При этом передаваемый регулярный сигнал надежно замаскирован. В приемном устройстве передаваемый сигнал четко выделяется (кривая S_3 на рис.2,а). Спектр несущих регулярных колебаний просматривается на выходе (незначительный резонансный пик по уровню – 70 dB на частоте $\omega = 4$) лишь вследствие выбора низкого (для наглядности) значения добротности фильтрующего устройства.

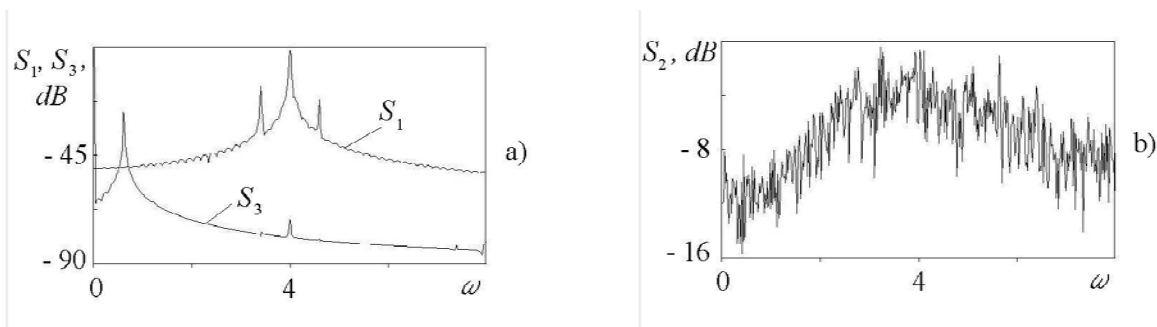


Рис. 2

Проведенный анализ свидетельствует о возможности использования рассмотренного способа для передачи конфиденциальной информации. Его особенностью является то, что используются не аналоговые хаотические генераторы, а программы, обеспечивающие моделирование на компьютерах элементов передатчика и приемника с соответствующими устройствами ввода и вывода, которые применяются при обычной пакетной радиосвязи.

Работа выполнена при финансовой поддержке РФФИ (проект № 00-07-90147).

Литература

1. Pecora L.M. and Carroll T.L. Synchronization in chaotic Systems // Phys. Rev. Letters., 1990. V. 64. № 8. P. 821-824.
2. Садченков Д.А. Техника и возможности СиБи радиосвязи. М.: Изд-во «СОЛОН-Р», 2001. 272 с.



BATCH TRANSFER OF THE INFORMATION AT ITS MASKING BY MULTYMODE CHAOS

Kal'yanov Er.

Institute of the radio Engineering and Electronics of the Russian Academy of Science (Fryazino branch).
pl. Vvedenskogo 1, Fryazino, Moscow oblast, 141120, Russia, e-mail: kalyan@ms.ire.rssi.ru. Tel.: (095)
5269049

Abstract. The circuit of latent transfer of the digital signal with reference to batch communication is considered. The mathematical model of way of masking of information by multimode chaotic oscillations is investigated.

The masking of the information by chaotic oscillations is widely investigated, since work [1]. It is interest with reference to a batch communication [2]. In the present work the new way of chaotic masking with reference to a batch radio communication is considered. This way is based on use identical chaotic auto oscillatory systems with rigid excitation in the transmitter and receiver.

In the transmitting device the managing a radio pulse ("pilot-signal") is formed. After a branching the part of oscillations of radio pulse acts on an output of the transmitter. Other part of a radio pulse lingers over and moves on the expecting generator with chaotic dynamics. To chaotic oscillations of the generator the information signal is mixed. The resulting oscillations also act on an output of the transmitter.

In the reception device the accepted signal branches. The part it acts on the switchboard, which passed only oscillations of pilot-signal. These oscillations (after their delay) raise the chaotic generator of the reception device. Other part of the accepted oscillations moves on the subtracting device, on which the oscillations of the chaotic generator move also. After detecting the information signal is allocated.

The numerical analysis of mathematical model of the considered way of transfer of information shows, that at the appropriate choice of parameters of transmitting and reception devices the reliable masking of the information by multimode chaos is possible. Feature of the considered way is that not analog chaotic generator, and their mathematical models are used. Devices of input and output same as well as at use of a usual batch radio communication.

The work is executed at financial support RFFI (project no. 00-07-90147).

References

1. Pecora L.M. and Carroll T.L. Synchronization in chaotic Systems // Phys. Rev. Letters., 1990. V. 64. № 8. P. 821-824.
2. Садченков Д.А. Техника и возможности СиБи радиосвязи. М.: Изд-во «СОЛОН-Р», 2001. 272 с.