Программно-аппаратная реализация системы защищенной передачи данных с хаотической несущей и наблюдателем состояния

А. С. Мушенко[1], А. С. Кузубова[2], А. Д. Золкин[3]

Южный федеральный университет, г. Таганрог

[1]asmushenko@sfedu.ru, [2]kuzubova@sfedu.ru, [3]a.d.zolkin@yandex.ru

Аннотация. **В работе рассматриваются вопросы программно-аппаратной реализации системы защищенной передачи данных, построенной на основе явлений динамического хаоса. В основе работы системы положен синергетический наблюдатель состояния, осуществляющий восстановление (реконструкцию) передаваемого полезного сигнала на стороне приемника. На стороне передатчика полезный передаваемый сигнал подмешивается в хаотическую несущую путем модуляции параметров математической модели хаотического генератора. В работе основное внимание уделено программно-аппаратной реализации такой системы на основе модельно-ориентированного подхода к проектированию на базе системы Matlab и одноплатного компьютера Raspberry Pi. В работе приведен пример синтеза синергетического наблюдателя состояния для хаотической системы Генезио-Тези. Получен прототип системы, реализующей передачу и восстановление полезного сигнала с хаотической несущей, работающий на платформе Raspberry Pi.**

Ключевые слова: синергетический наблюдатель состояния, динамический хаос, нелинейная динамика, модельно-ориентированный подход

I. Введение

Использование явлений динамического хаоса для создания и функционирования систем скрытой передачи данных можно выделить в самостоятельную область теоретических и прикладных исследований начиная с последнего десятилетия XX века. В отечественной литературе по этой теме существует ряд значимых публикаций научной школы профессора А.А. Анищенко и других исследователей [1], в которых показано использование хаотических систем в качестве генераторов опорных колебаний для каналов связи. Хаотическими генераторами, в отличие от широко используемого в каналах связи генератора регулярных колебаний Ван-дер-Поля, принято называть нелинейные динамические системы, которые при определенных сочетаниях своих параметров переходят в режим генерации хаотических колебаний с формированием так называемых «странных» аттракторов в своем фазовом пространстве. Существует огромное число публикаций, начиная с работ Лоренца, Реслера и др. [2], в которых выявлены и исследованы модели такого рода нелинейных динамических систем, что обеспечивает богатый выбор хаотических генераторов при создании систем скрытой передачи данных с хаотической несущей. При формировании таких систем могут использоваться различные методы [3] как для внедрения полезной информации в хаотическую несущую (маскирование хаотическими колебаниями, модуляция параметров хаотического генератора путем аддитивного или мультипликативного внедрения полезного сигнала и др.) на стороне передатчика, так и для восстановления или реконструкции информационной составляющей получаемого сигнала на стороне приемника (фильтрация хаотической несущей, хаотическая синхронизация, использование наблюдателей состояния). Хаотическая синхронизация [4] относится в настоящий момент к наиболее популярному принципу как восстановления полезного сигнала, так и формирования структуры системы передачи данных с хаотической несущей в целом благодаря возможности практической реализации. Альтернативой хаотической синхронизации может являться метод восстановления полезного сигнала на стороне приема с помощью наблюдателей состояния. Интерес исследований в этой области [5] может состоять в том, что использование известных наблюдателей состояния (Калмана, Люенбергера) ограничено необходимостью работы с существенно нелинейными системами, моделями которых являются хаотические генераторы.

В работах научной школы профессора А.А. Колесникова Южного федерального университета развита методика синтеза нелинейных синергетических наблюдателей состояния, в основе которых лежит предложенный профессором А.А. Колесниковым метод аналитического конструирования агрегированных регуляторов (АКАР) [6]. С использованием синергетических наблюдателей состояния решены задачи синтеза наблюдателей состояния для одно- и многоканальных систем передачи данных с хаотической несущей [7], [8], которые могут быть применены при создании систем скрытой передачи данных на основе различных хаотических генераторов 2-го и 3-го порядка.

В данной работе рассмотрены вопросы практической реализации достигнутых в [7], [8] результатов. Приведена процедура синергетического синтеза одноканального наблюдателя состояния для хаотического генератора Генезио-Тези [9], выполнена реализация полученной модели системы в MATLAB/Simulink, на основе модельно-ориентированного подхода [10] проведено моделирование и программная реализация системы, готовой к переносу и дальнейшей реализации на одноплатные компьютеры Raspberry Pi.

II. Синтез наблюдателя для канала связи

Для реализации системы связи была выбрана одноканальная конфигурация, в качестве генератора хаотических колебаний использована модель генератора Генезио-Тези, описываемое системой (1) [9]. Фазовый портрет системы изображен на рис. 1.

$$x' = y;\ y' = z;\ z' = -cx - by - az + x^2 \qquad (1)$$

где: x, y, z – динамические переменные, a, b, c – параметры системы.

За наблюдаемый параметр возьмем параметр a. Введем новый параметр генератора Генезио-Тези:

$$a^*(t) = a + \mu(t).$$

За основу передачи возьмем сигнал $z(t)$, сформированный системой (1), который будет передаваться по открытому каналу связи. При этом принимаются следующее: передаваемая по каналу связи информация является дискретной, т.е. модулирующий сигнал $\mu(t)$ будет всегда иметь прямоугольную форму; модулируемый параметр $a > 0$.

С целью восстановления полезного сигнала, маскированного хаотическими колебаниями путем мультипликативного нелинейного подмешивания непосредственно в параметры модели, для системы (1) выполним синтез синергетического наблюдателя состояния для оценки (т.е. восстановления) параметра $a_1 = a + 1$, который мы будем считать ненаблюдаемой величиной, на стороне приемника. Согласно методике, для построения синергетического наблюдателя для считающегося недоступным для изменения параметра a_1 требуется заменить этот неизвестный параметр соответствующей динамической моделью. Допускается использовать модель в виде дифференциального уравнения: $\dot{w}(t) = 0$, решение которого $w(t) = const$ является кусочно-постоянным изменением параметра $a_1(t)$ во времени. Итак, запишем расширенную система (1) в виде:

$$\dot{X} = y;\ \dot{Y} = z;\ \dot{Z} = -cx - by - (w+1)z + x^2;$$
$$\dot{w}(t) = 0,$$

для упрощения последующих аналитических выкладок переобозначим часть третьего уравнения как G_1. В итоге получим:

$$\dot{X} = y;\ \dot{Y} = z;\ \dot{Z} = G_1 - zw;\ \dot{w}(t) = 0, \qquad (2)$$

где $G_1 = -by - cx + x^2 - z$; w – переменная состояния динамической модели для искомого параметра a_1. В системе (2) известными, т.е. наблюдаемыми параметрами являются переменные x, y, z, а ненаблюдаемый (неизвестный) – w.

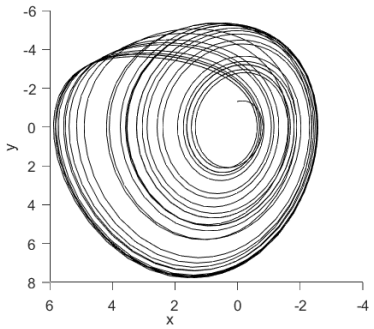


Рис. 1. Фазовый портрет системы Генезио-Тези (1) при a = 1; b = 3.03; c = 5.55; $\{x_0, y_0, z_0\}$ = {0.1, 0.1, 0.1}

Пусть $\widehat{w}$ – является искомой оценкой параметра a_1, т.е. $\widehat{w} = \hat{a}_1$. В этом случае с целью определения оценки нового неизвестного параметра $\widehat{w}$, в процедуре синергетического синтеза необходимо ввести макропеременную:

$$\Psi = w - \widehat{w}. \qquad (3)$$

Далее, согласно процедуре, уравнение редукции будет равно: $\widehat{w} = Q(X, Y, Z) + \upsilon_1$, где $Q(X, Y, Z)$ – новая неизвестная функция от наблюдаемых переменных состояния системы (2); υ_1 – переменная состояния динамического наблюдателя.

Дифференцируя по времени уравнение редукции получим:

$$\frac{d\widehat{w}}{dt} = \frac{\partial Q(X,Y,Z)}{\partial X}\frac{dX}{dt} + \frac{\partial Q(X,Y,Z)}{\partial Y}\frac{dY}{dt} + \frac{\partial Q(X,Y,Z)}{\partial Z}\frac{dZ}{dt} + \frac{d\upsilon_1}{dt}. \qquad (4)$$

Согласно процедуре синтеза, макропеременная (3) должна удовлетворять следующему основному функциональному уравнению метода АКАР, приведенного в виде:

$$\frac{d\Psi}{dt} + L(X, Y, Z)\Psi = 0, \qquad (5)$$

где $L(X, Y, Z) > 0$ – неизвестная функция, которая в случае своей положительной определенности обеспечивает устойчивость основного функционального уравнения (5).

Дифференцируя по времени макропеременную (3) получим:

$$\frac{d\Psi}{dt} = \frac{dw}{dt} - \frac{d\widehat{w}}{dt}.$$

Подставим в уравнение (5) соответствующие выражения из (3), (4) и с учетом (2), согласно процедуре синтеза, получим:

$$-\frac{\partial Q(X,Y,Z)}{\partial X}y - \frac{\partial Q(X,Y,Z)}{\partial Y}z - \frac{\partial Q(X,Y,Z)}{\partial Z} \times$$
$$\times (-zw + G_1) - \frac{d\upsilon_1}{dt} + L(X, Y, Z)(w - \widehat{w}) = 0. \qquad (6)$$

Согласно методике синтеза синергетического наблюдателя, исключим все ненаблюдаемые переменные состояния. Следовательно, из (6) нужно выписать все слагаемые, содержащие ненаблюдаемую переменную w и приравнять их к нулю:

$$w\left(\frac{\partial Q(X,Y,Z)}{\partial Z}z + L(X, Y, Z)\right) = 0. \qquad (7)$$

Так как $w \neq 0$, то равенство в выражении (7) выполняется при выполнении условия:

$$\frac{\partial Q(X,Y,Z)}{\partial Z}z + L(X, Y, Z) = 0 \qquad (8)$$

Выразим из (8) производную по Z функции наблюдаемых переменных состояния системы:

$$\frac{\partial Q(X,Y,Z)}{\partial Z} = \frac{-L(X,Y,Z)}{z} \qquad (9)$$

Исходя из указанных выше условий устойчивости, а также с учетом (9) положим:

$$L(X, Y, Z) = \alpha(-z)^2 > 0, \qquad (10)$$

где $\alpha > 0$ – постоянный коэффициент, который определяет «скорость» оценивания искомого неизвестного параметра a_1.

Далее необходимо проинтегрировать (9) и подставить найденное (10) для получения функции от наблюдаемых переменных:

$$Q(X,Y,Z) = \frac{\alpha z^2}{2}. \quad (11)$$

Теперь, когда известно $Q(X,Y,Z)$ и $L(X,Y,Z)$, исходя из (6) можно вывести уравнение для динамической составляющей наблюдателя:

$$\frac{dv_1}{dt} = -\frac{\partial Q(X,Y,Z)}{\partial X} Z - \frac{\partial Q(X,Y,Z)}{\partial Y} X - \frac{\partial Q(X,Y,Z)}{\partial Z} G_1 - -L(X,Y,Z)\hat{w} = -\alpha byz - \alpha cxz - \alpha x^2 z - \alpha z^2 + \frac{1}{2}\alpha^2 z^4 - \alpha z^2 v_1. \quad (12)$$

Кроме того, оценка параметра a_1 будет иметь следующий вид: $\hat{w} = \hat{a}_1 = -\frac{\alpha z^2}{2} + v_1$.

Таким образом, согласно $a_1 = a + 1$ и (2) имеем:

$$\hat{a} = 1 - \hat{a}_1 = 1 + \frac{\alpha z^2}{2} + v_1. \quad (13)$$

Теперь через (1) можно получить сигнал, который восстанавливается на принимающей стороне. Это разность между оценкой параметра и исходным значением: $\mu_{\text{реконстр}} = \hat{a} - a$.

Согласно приведенной выше процедуре синтеза полученный нелинейный синергетический наблюдатель Исходя из вышеприведённой процедуры, синергетический наблюдатель параметра a_1 состоит из динамической части (6) и статической части (12).

III. Реализация в MATLAB/Simulink

С целью последующей программно-аппаратной реализации на автономной платформе используем принцип модельно-ориентированного проектирования (МОП). Для этого в Simulink создадим схему системы, соответствующую описывающим блоки уравнениям (1), (6), (12) и др., далее с помощью автоматической генерации кода можно создать исполняемый файл для автономной работы или экспортировать программный код для создания независимого приложения под необходимую платформу. Функциональная структура элементов системы передачи данных будет иметь вид согласно рис. 1.

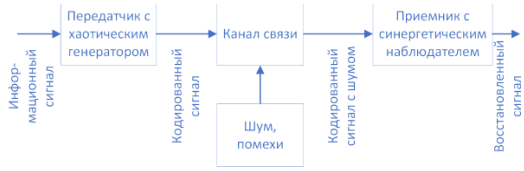


Рис. 1. Функциональная схема системы

Соответствующая рис. 2 и уравнениям (1), (6) и (12) модель в MATLAB/Simulink состоит из трех различных функциональных блоков, реализующих работу передатчика, канала связи и приемника. Общий вид разработанной системы представлен на рис. 3.

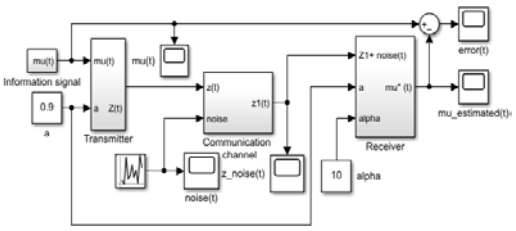


Рис. 2. Общий вид разработанной системы в Simulink

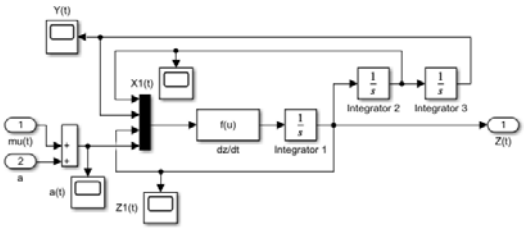


Рис. 3. Блок передатчика системы

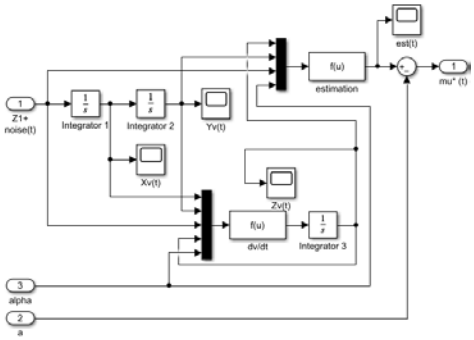
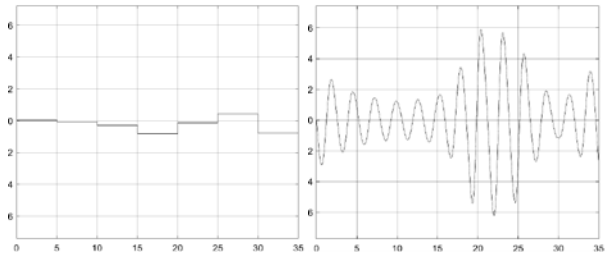


Рис. 4. Блок приемника системы

Система (1) приобретает хаотические свойства при значениях параметров $a \cdot b < c$. Опытным путем были подобраны следующие значения параметров: a =0.9, b =3.55, c = 5.55.

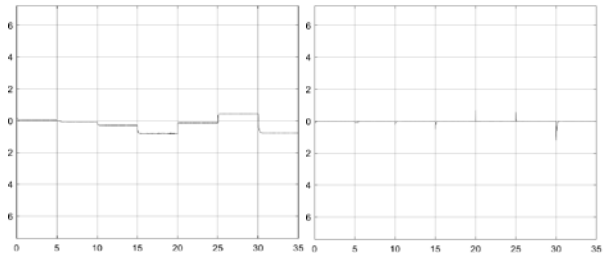
На вход передатчика поступает значение параметра a и информационный сигнал mu(t). В блоке передатчика полезный информационный сигнал подмешивается мультипликативным образом к генерируемой хаотической несущей. На выходе блока передатчика в результате получается сложный сигнал Z(t), содержащий полезный сигнал на хаотической несущей. Общий вид блока передатчика представлен на рис. 4.

Результирующий сигнал $Z_1(t)$ поступает на блок приемника. Здесь выполняется восстановление или извлечение полезного сигнала, в результате на выходе блока приемника образуется восстановленный сигнал mu*(t) и снимается ошибка восстановления error(t). Общий вид приемника представлен на рис. 5. Вид блока dv/dt записывается согласно формуле (12), а блока estimation – согласно формуле (13). Параметр α не может быть универсальным и выбирается в зависимости от настройки системы. В нашем случае положим его равным 10. На рис. 6 и 7 приведены результаты моделирования собранной системы в MATLAB/Simulink. Из результатов моделирования видно, что восстановленный сигнал имеет форму, подобную исходному модулируемому сигналу, что является необходимым признаком работоспособности синтезированного наблюдателя состояния.



(a) **(b)**

Рис. 5. Исходный информационный сигнал (a) и сигнал в канале связи (b)



(a) **(b)**

Рис. 6. Сигнал, восстановленный с помощью синергетического наблюдателя (a), и ошибка восстановления (b)

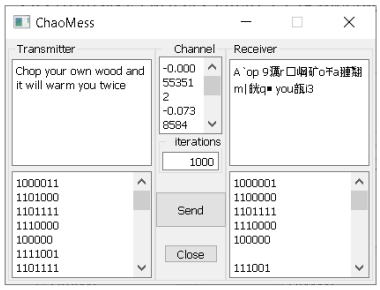


Рис. 7. Сообщение из 37 символов, 1000 итераций

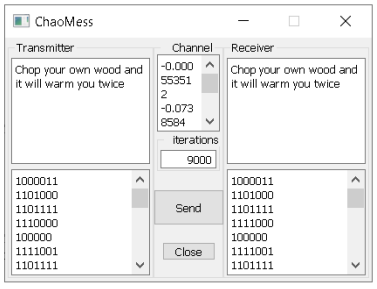


Рис. 8. Сообщение из 37 символов, 9000 итераций

IV. Программно-аппаратная реализация

A. Генерация кода из Matlab/Simulink

Использование МОП и средств MatLab позволяют генерировать C/C++ код из модели Simulink, что значительно облегчает разработку сложных систем на основе нелинейных динамических моделей.

B. Программная реализация

Для независимой программной реализации использованы файлы автоматической генерации кода из пакета MatLab. Необходимы файлы описания работы системы со всеми настройками интеграторов и обработки передачи сообщения, а также некоторые заголовочные файлы. Создание программного продукта на C++ с графическим интерфейсом под платформу Rasbperry Pi выполнено в среде программирования Qt.

С целью коррекции ошибки восстановления, которая неизбежно возникает при работе синтезированного наблюдателя состояния в программный продукт добавлена функциональность многократной передачи тестового сообщения (количество итераций задается пользователем) и стандартной статистической обработкой, позволяющей нивелировать воздействие ошибки восстановления на процесс передачи данных. В данном случае точность обеспечивается многократной повторной передачей шифруемого системой сообщения. На рисунках 8 и 9 показаны результаты восстановления передаваемой информации при разном числе итераций.

V. Заключение

Разработанный прототип программного продукта демонстрирует применимость синтезированного наблюдателя для построения системы защищенной передачи информации с хаотической несущей. Областью применения данного результата может быть передача коротких сообщений, поскольку выбранный метод контроля и восстановления ошибок требует значительного числа повторов процесса передачи. К таким коротким сообщениям можно отнести ключи шифрования или команды управления различных киберфизических систем, для кодирования которых может быть целесообразно применять такие нетрадиционные методы. При использовании других методов контроля и коррекции ошибки восстановления возможно более широкое применение систем на основе синергетического наблюдателя в задачах защищенной передачи данных. Создание программного прототипа для платформы Rasbperry Pi демонстрирует возможность автономной работы системы на промышленном одноплатном компьютере вне среды MATLAB/Simulink.

Список литературы

[1] Anishchenko V.S., Pavlov A.N., Yanson N.B. Reconstruction of dynamic systems as applied to secure communications. *Technical Physics*, **1998**, Vol. 43(12), pp. 1401-1407.

[2] Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, 20, 130-141.

[3] Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. М.: Изд-во ФИЗМАТЛИТ, 2002. 252 с.

[4] Feki, M. An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons Fractals*, **2003**, *18*, pp. 141-148.

[5] Andrievsky B.R., Fradkov A.L. Adaptive-based methods for information transmission by means of chaotic signal source modulation. *Automation and Remote Control*, **2011**, 72:9, pp. 1967-1980.

[6] Колесников А.А. Синергетическая теория управления. М.: Энергоатомиздат, 1994. 344 с.

[7] Колесников А.А., Мушенко А.С., Дзюба Ю.Н., Золкин А.Д. Синергетический наблюдатель переменных состояния в задачах реконструкции систем с хаотической динамикой. Труды Всероссийской научной конференции по проблемам управления в технических системах, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», 2017. С. 58-61.

[8] Mushenko A, Dzuba J, Nekrasov A, Fidge C. A Data Secured Communication System Design Procedure with a Chaotic Carrier and Synergetic Observer. *Electronics*. **2020**; 9(3):497.

[9] Genesio R., Tesi A. Harmonic Balance Methods for the Analysis of Chaotic Dynamics in Nonlinear Systems. *Automatica*, **1992**, Vol. 28, iss.3, pp. 531-548.

[10] Дробинцев П.Д., Котляров В.П., Воинов Н.В., Никифоров И.В. Особенности применения модельно-ориентированного подхода при разработке промышленных приложений. *Моделирование и анализ информационных систем.* **2015**, 22(6), С. 750-762.