

Using the generalized synchronization regime for hidden communication

Galiuk Sergii, Kushnir Mykola,
Dmytro Vovchuk

Radio Engineering and Information Security Department, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Storozhynetska Str., 101, UKRAINE.
E-mail: dimavovchuk@gmail.com

The quality of synchronization is one of the main parameters that determine possibility and reliability of information transmission in modern communications technology. In chaotic communication synchronization and information transfer occur simultaneously in analog and digital communication systems, i.e. the transmitted signal is both a synchronizing and information-carrying signal.

Two chaotic systems are said to be in the generalized synchronization regime, if, when connected, there exists the functional dependency $Y = F(X)$ after the states transition process stopped. The notions X and Y – are the vectors of driving and response systems respectively. There are several types of chaotic synchronization: complete, phased, and generalized. For information transfer, complete synchronization is more often used. However, such systems have several drawbacks, among which is the demand of a higher identity degree for chaotic generators of the transmitter and receiver. The generalized synchronization, in comparison with the complete one, does not require system parameters identity and is more resistant to noise.

The author has offered a method of a hidden communication applying the generalized synchronization technique for phase-coherent Resler systems. In the presented paper the Chua system is considered to be suitable and efficient for transmitting information. The dependence of the generalized synchronization boundary is analyzed with respect to the system parameters. It was revealed that for the Chua schemes with some rearrangement, two scenarios of transition to the generalized synchronization regime are possible, relating to the parameters distinction: a) main frequency seizure or b) via full extension of the fluctuations mode of the driving system. The simulation results proved the suitability of the studied generators for efficient information transmitting. To improve the level of communication security the advanced noise generators are usually used (Fig. 1).

Використання режиму узагальненої синхронізації при прихованій передачі інформації

Галюк Сергій, Кушнір Микола,
Вовчук Дмитро

Кафедра радіотехніки та інформаційної безпеки, Чернівецький Національний університет, УКРАЇНА, м.Чернівці, вул.Сторожинецька, 101,
E-mail: dimavovchuk@gmail.com

Ключові слова – узагальнена синхронізація, хаотична система, схема Чуа, одно направлено зв'язані системи, прихована передача інформації, ведучий та ведений генератори.

I. Вступ

В сучасних цифрових системах передавання інформації синхронізація використовується для узгодження тактових частот приймальної і передавальної сторін, а передача власне інформації здійснюється окремо від бітів синхронізації. Синхронізація – це процес встановлення і підтримки функціональної залежності між станами двох чи більше систем. Якість синхронізації є одним з основних параметрів, що визначає можливість та надійність передачі інформації.

В хаотичних аналогових та цифрових системах зв'язку процес синхронізації і передачі інформації відбувається одночасно, тобто передаваний сигнал є синхронізуючим сигналом і одночасно інформаційним (або несучим сигналом).

Вважається, що дві хаотичні системи перебувають в режимі узагальненої синхронізації, якщо при встановленому з'єднанні між системами після закінчення перехідних процесів між станами двох систем існує функціональна залежність $Y = F(X)$, де X та Y – вектори стану відповідно ведучої та веденої систем.

Розрізняють декілька основних видів хаотичної синхронізації: повна, фазова, узагальнена. Серед них для передачі інформації найчастіше пропонують використовувати повну синхронізацію. Проте такі системи володіють рядом недоліків, зокрема вимагають високого ступеня ідентичності хаотичних генераторів передавача і приймача [1, 2, 4]. Узагальнена синхронізація в порівнянні з повною не вимагає високої ідентичності параметрів систем і володіє значною стійкістю до шумів [1, 3, 4].

В [4] запропоновано спосіб прихованої передачі інформації з використанням узагальненої синхронізації для фазо-когерентних систем Реслера.

У представленій роботі ми досліджуємо можливість використання системи Чуа для передавання інформації. Досліджено залежність границі виникнення узагальненої синхронізації в залежності від параметрів системи, промодульовано процес передавання-приймання інформації, продемонстровано стійкість системи передавання інформації до шуму (рис.1).

II. Узагальнена синхронізація

З визначення узагальненої синхронізації слідує, що маючи відомості про стан першої системи X , можна однозначно прогнозувати стан другої системи Y однонаправлено зв'язаної з першою. Функціональна залежність, що описує зв'язок між станами взаємодіючих систем, може бути достатньо складною чи навіть фрактальною, що є важливим для захищеності передаваної інформації.

Існуючі системи на основі повної та фазової хаотичної синхронізації є ефективними лише при передачі інформації через ідеальний канал зв'язку, наявності ідентичних генераторів на передавальній та приймальній сторонах, крім того, вони не завжди характеризуються достатнім рівнем конфіденційності.

До переваг використання узагальненої синхронізації в хаотичних системах зв'язку слід віднести можливість синхронізації неідентичних, параметрично різних систем та систем з різною розмірністю фазового простору. Виявлення узагальненої синхронізації можливе одним із наступних трьох методів: методом найменшої взаємної помилки найближчих траєкторій, методом розрахунку умовних ляпуновських експонент чи методом допоміжної системи. На практиці найпростішим є метод допоміжної системи [5].

Властивості узагальненої синхронізації використовуються у процесі прихованої передачі інформації в присутності шумів.

В роботі [1] автори показали, що границя виникнення узагальненої синхронізації системи Реслера на площині параметрів системи практично не залежить від інтенсивності шуму. Використовуючи виявлену властивість узагальненої синхронізації, автори в [3, 4] запропонували спосіб прихованої передачі цифрової інформації, що базується на використанні двох шляхів встановлення узагальненої синхронізації: захоплення основної частоти ведучого генератора та повного подавлення режиму власних коливань веденого генератора. При малому розлаштуванні власних частот генераторів спостерігається перший сценарій, при великому – другий.

Зауважимо, що система Реслера при використаних значеннях параметрів відноситься до фазокогерентних і тому в ній можливі два способи встановлення режиму узагальненої синхронізації. Питання придатності до використання інших хаотичних систем залишається відкритим.

Дослідимо синхронізацію однонаправлено зв'язаних схем Чуа в залежності від розлаштування параметрів системи.

III. Прихована передача інформації

Спосіб прихованої передачі інформації призначений для передачі цифрових сигналів реальними каналами зв'язку, тобто в присутності шумів.

У представленій схемі 1 – передавальний пристрій, 2 – генератор шуму, 3 – канал зв'язку, 4 – приймаючий пристрій, $m(t)$ – інформаційний сигнал, $x(t)$ – вектор стану передавальної системи, D – інтенсивність шуму,

$\xi(t)$ – шумовий сигнал, $u(t)$ та $v(t)$ – вектори стану ідентичних хаотичних генераторів приймальної системи.

$$s(t) = x(t) + Dx(t) \quad (2)$$

де (2) – сигнал у каналі зв'язку.

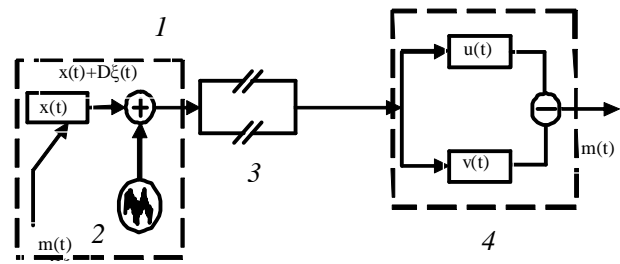


Рис.1. Блок-схема реалізації способу прихованої передачі інформації на основі режиму узагальненої синхронізації в присутності шумів.

Принцип роботи полягає в наступному. Якщо в якості генераторів передавального і приймального пристрою вибрати однонаправлено зв'язані системи Чуа, передавальний генератор буде описуватися системою диференціальних рівнянь:

$$\begin{cases} \dot{x} = a(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = by - gz \end{cases} \quad (3)$$

де $\alpha = 9,237$; $\beta = 17,2$; $\gamma = 0,0042$ – параметри системи.

$f(x) = m_2x + 1/2(m_0 - m_1)[\text{abs}(x + a_1) - \text{abs}(x - a_1)] + (m_1 - m_2)[\text{abs}(x + a_2) - \text{abs}(x - a_2)]$ – нелінійна функція; $a_1 = 1$, $a_2 = 7$, $m_0 = -1,53$, $m_1 = -0,7436$, $m_2 = 572$.

Ведений та допоміжний генератори приймача описуються наступною системою диференціальних рівнянь:

$$\begin{cases} \dot{x}_{2,3} = y_{2,3} - x_{2,3} - f(x_{2,3}) + e(x_1 - x_{2,3}) \\ \dot{y}_{2,3} = x_{2,3} - y_{2,3} + z_{2,3} \\ \dot{z}_{2,3} = -b y_{2,3} - g z_{2,3} \end{cases} \quad (4)$$

де індекси $i = 1, 2$ відповідають веденому та допоміжному генераторам, e = коефіцієнт зв'язку, x_1 – ведучий модульований вхідний сигнал.

Цифровий інформаційний сигнал $m(t)$ здійснює модуляцію параметра генератора передавача. Модуляція параметрів повинна виконуватись таким чином, щоб характеристики сигналу, який передається, змінювались незначно і залишалася можливість виникнення або, навпаки, знищення режиму узагальненої синхронізації. Оскільки границя узагальненої синхронізації володіє значною стійкістю до шуму, то для додаткового маскування використовується генератор шуму. Шум адитивно додається до хаотичного сигналу. Вихідний сигнал передається у канал зв'язку, де зазнає впливу шумів у каналі.

На приймальній стороні розташовані ідентичні генератори, що перебувають в режимі узагальненої синхронізації із передавальним генератором. Почат-

кові умови приймальних генераторів відрізняються, тобто $u(t_0) \neq v(t_0)$.

На практиці різні початкові умови виникають автоматично внаслідок флуктуацій в системах. Нехай передачі біту "0" відповідає наявності режиму узагальненої синхронізації між ведучою і веденою системами. Відповідно передачі біту "1" – режим десинхронізації. Тоді при передачі "0" на виході веденого та допоміжного генераторів ми отримаємо однакові сигнали. На виході пристрою віднімання буде нульовий сигнал. В протилежному випадку (передача біту "1") на виході генераторів приймача отримаємо різні сигнали і на виході пристрою віднімання буде сигнал ненульової потужності.

IV. Синхронізація схем Чуа

Дослідимо границю виникнення режиму узагальненої синхронізації в системі однонаправлено зв'язаних схем Чуа (3) і (4) від значення параметра β_1 , при $\beta = 17,5$. Вважатимемо, що синхронізація має місце, якщо помилка синхронізації між відповідними сигналами веденої та допоміжної систем менша 2% від значення рівня сигналів.

На рис.2 приведена розрахункова залежність

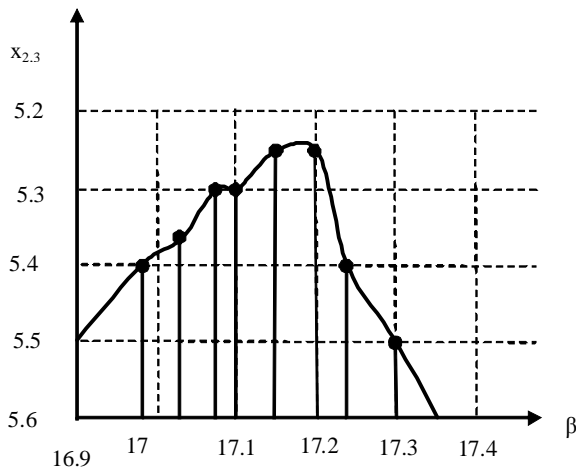


Рис.2. Границя виникнення узагальненої синхронізації в системі однонаправлено зв'язаних схем Чуа при $\beta = 17,5$

З рисунка видно, що при $\beta_{max} \approx 17,2$ поріг синхронізації має максимум і спадає при відхиленні β_{max} . При ідентичних ведучій та веденій системах та $e < 5,6$ узагальнена синхронізація не спостерігається, що відрізняє схему Чуа від системи Реслера.

Від параметра β_1 залежить основна частота ведучого хаотичного сигналу. На рис.3 а, б приведено спектри хаотичного сигналу x_1 ведучої системи відповідно при $\beta_1 = 17,2$ та $17,5$. На рис.3 в, г – спектри сигналу x_2 веденої системи. З порівняння рис. 3 а, в слідує, що має місце захоплення основної частоти ведучого сигналу. Основна частота ведучого сигналу $\omega = 20,51$ рад/с. Зміни параметра β з $\beta = 17,2$ до $\beta = 17,5$ відповідає зміна основної частоти з $\omega = 20,51$ рад/с до $\omega = 20,57$ рад/с. Однак навіть при такій

малій зміні частоти синхронізація між системами втрачається, хоча в спектрі сигналу x_2 веденої системи спостерігається чітка спектральна складова на частоті $\omega = 20,57$ рад/с (рис.3 г).

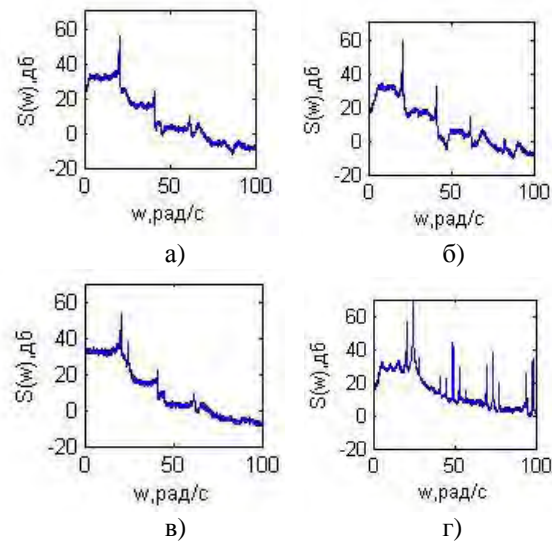


Рис.3. Спектр хаотичного сигналу ведучої (а, б) та веденої (в, г) систем при $\beta_1 = 17,2$ та $17,5$.

Процес синхронізації та десинхронізації при зміні параметра β та $e = 5,4$ показано на рис.4. При зміні параметра у межах досліджуваного діапазону хаотичний режим ведучої системи не змінюється. Для обох вибраних значень β (див. рис 4 а, б) атрактор залишається одновитковим. При $\beta_1 = 17,2$, $e = 5,4$ спостерігається узагальнена синхронізація, при $\beta_1 = 17,2$, $e = 5,4$ – десинхронізація. При десинхронізації ведена система знаходиться в режимі квазіперіодичних коливань, однак для передавання інформації це не має принципового значення.

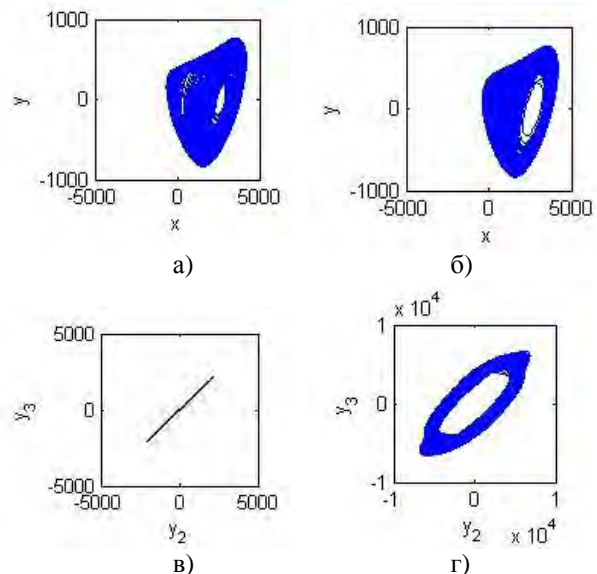


Рис.4. Процес синхронізації та десинхронізації при зміні параметра β та $e = 5,4$ у межах досліджуваного діапазону.

Висновок

У роботі досліджено синхронізацію однонаправлено зв'язаних схем Чуа. Показано, що режим однониткового хаосу між однонапрямлено зв'язаними схемами Чуа можна використовувати для прихованої передачі інформації. Результати моделювання підтвердили теоретичні висновки.

Література

- [1] Короновский А. А. Теоретическое исследование обобщенной синхронизации диссипативно связанных хаотических систем в присутствии шума / А. А. Короновский, О. И. Москаленко, А. А. Овчинников, А. Е. Храмов // Известия РАН. серия физическая. – 2009. – том 73. – № 12. – с. 1726–1730.
- [2] Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А. С. Дмитриев, А. И. Панас. – М.: Издательство Физико-математической литературы. - 2002. – 252с.
- [3] Moskalenko O. I. Generalized synchronization of chaos for secure communication: remarkable stability to noise / O. I. Moskalenko, A. A. Koronovskii, A. E. Hramov // Phys. Lett. A. – 2010. – v. 374. – pp. 2925-2931.
- [4] Короновский А. А. Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов / А. А. Короновский, О. И. Москаленко, А.Е.Храмов // ЖТФ. – 2009. – т. 80. - № 4. – с. 1-8.
- [5] Abarbanel H. D. I. Generalized synchronization of chaos: The auxiliary system approach / H. D. I. Abarbanel, Rulkov N. F., Sushchik M. M. // Phys. Rev. E. – 1996. – v. 53. - № 5. – pp.4528-4535.