УДК 681.38

О. В. Білик[1]

ОГЛЯД МЕТОДІВ ПРИХОВАНОЇ ПЕРЕДАЧІ З ВИКОРИСТАННЯ ГЕНЕРАТОРІВ ДИНАМІЧНОГО ХАОСУ

[1] ТОВ НВП «Дайтекс Технолоджі»

Анотація

У роботі проведено огляд методів прихованої передачі інформації за допомогою генератора динамічного хаосу.

Ключові слова: динамічний хаос, нелінійна система, синхронізація, ведуча-ведена схема.

Abstract

The paper reviews the methods of covertinformation transfer using a dynamic chaos generator.

Keywords:dynamic chaos, nonlinear system, synchronization, master-slave circuit.

Вступ

Хаотичний сигнал є коливальним сигналом в динамічних системах. Тому хаотичні коливання можна використовувати в системах передачі інформації між нелінійними системами: передавачем і приймачем інформації.В основі методів з використанням динамічного хаосу лежить можливість синхронізації. Далі в роботі будуть розглянуті методи прихованої передачі на основі хаосу в режимі повної синхронізації, фазової синхронізації і узагальненої синхронізації, а також схеми передачі інформації, що використовуються в цих режимах. Варто зазначити, що на сьогоднішній день також відомі синхронізація із запізненням і синхронізація індукована шумом. Динамічний хаос - перспективна основа побудови принципово нових систем обробки та зберігання інформації [1]. Нижче перераховані відмінні риси хаотичних процесів, завдяки яким застосування хаосу в передачі інформації є перспективними.

Метою роботи є проведення огляду відомих методів системи прихованої передачі інформації за допомогою генератора динамічного хаосу.

Результати дослідження

Режим повної синхронізації характеризується точним збігом векторів стану ведучої і веденої систем: x(t)=u(t). Це можливо в разі повної ідентичності взаємодіючих систем по керуючим параметрам. Використання такого режиму синхронізації передбачає використання в системі зв'язку, як мінімум, двох односпрямованих зв'язаних ідентичних хаотичних генераторів [2].

В системі зв'язку з хаотичним маскуванням інформаційний сигналm(t) адитивно (в суматорі) підмішується до хаотичного сигналух(t), що генерується ведучою системою, на виході ведучої системи. Після цього результуючий сигнал x+m передається в канал зв'язку і далі на вхід відомої системи. У веденій системі здійснюється повна хаотична синхронізація генератора хаосу, що знаходиться в ній за допомогою приймаючого сигналу, в результаті чого динаміка приймаючого генератора стає ідентичною динаміці передавального. Схема передачі інформації за допомогою хаотичного маскування показана на рисунку 1, дех(t) - хаотичний сигнал,m(t) - інформаційний сигнал, m’(t) - оцінка інформаційного сигналу на виході веденої системи,w- шум в каналі зв'язку, CS- повна хаотична синхронізація. Виділений інформаційний сигнал m’(t) отримується після проходження через віднімач як різниця між приймаючим сигналом і синхронним хаотичним відгуком в генераторі відомої системи.

При хаотичному маскуванні рівень інформаційного сигналу повинен бути нижче на 35-65 дБ рівня хаотичного (маскуючого) сигналу. Ця умова приводить до того, що інформаційний сигнал порівнюється з рівнем шумів в каналі зв'язку. Що може привести до невисокої якості передачі через імовірність невеликого відношення сигнал/шум. Також через це з'являється ймовірність різко ускладнити можливість реалізації передачі інформаційного сигналу через потенційну можливість появи будь-яких збурюючих факторів. Наприклад, розлад параметрів ведучої і веденої систем може привести до появи на виході веденої системи додаткових шумів десинхронізації, що в свою чергу зробить передачу важко реалізовуваною [3].

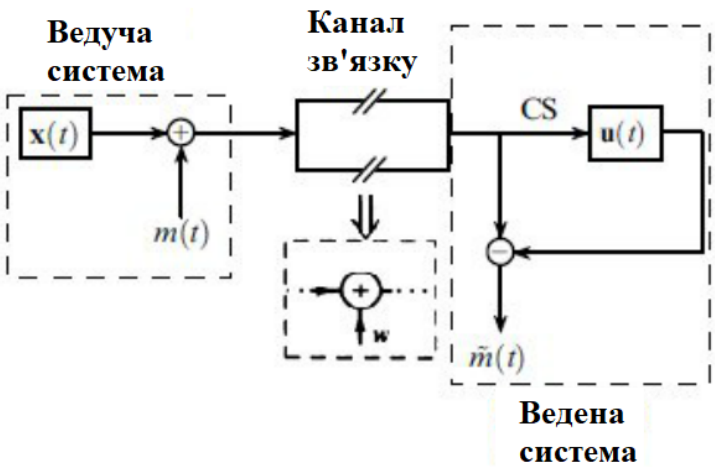

Рис. 1. Схема хаотичного маскування

Також при такій схемі передачі сигналу може виникнути причина порушення конфіденційності передачі інформаційного сигналу. Існує така проблема через можливість відтворити на приймальній стороні вихідний хаотичний сигнал при низькому, як вимагає дана система зв'язку, рівні підмішуючого інформаційного сигналу, що в свою чергу дозволяє виділити передаваний інформаційний сигнал. Для вирішення даної проблеми слід збільшити рівень інформаційного сигналу, тобто збільшити співвідношення сигнал/шум, а це призведе до погіршення якості передачі, тому що в даній системі зв'язку інформаційний сигнал є зовнішнім збурюючим фактором по відношенню до хаотичного сигналу, тобто інформаційний сигнал накладає на хаотичний, а не навпаки.Також до недоліків варто віднести низьку енергетичну ефективність схеми, що передає по каналу зв'язку в основному сигнал, який не містить інформації.

Таким чином, до недоліків хаотичного маскування відносять: ймовірність невисокої якості передачі через невелике відношення сигнал/шуму, який важко буде реалізувати через потенційну можливість появи будь-яких збурюючи факторів, проблему конфіденційності або на противагу цьому погіршення якості передачі, а також низьку енергетичну ефективність схеми.

Застосування хаотичного маскування на практиці малоперспективно, тому що цей метод має обмежену область застосування через ряд вимог, що накладаються при використанні системи. Серед цих вимог: забезпечення високого ступеня ідентичності ведучої і веденої системи, а також забезпечення каналів зв'язку з низьким рівнем шумів при рівні інформаційного сигналу на 35-65 дБ рівня хаотичного сигналу.

Перемикання хаотичних режимів реалізовується блок схемою, зображену на рисунку 2. Це один з можливих варіантів методу передачі інформації за допомогою перемикання хаотичних режимів. Існують і інші види, які відрізняються числом ведучих і ведених систем, а також способом комутації режимів.

На цій блок-схемі S, S’ – вихідний інформаційний сигнал в бінарній формі і його оцінка на виході приймача. Передавач інформації складається з двох ведучих систем, що складаються з генераторів хаосу як однакової, так і різної структури. При однаковій структурі ці генератори відрізняються параметрами, але хаотичні сигнали, що виникають в них, вибираються таким чином, щоб вони мали схожі спектральні і статистичні властивості. Ця умова має виконуватися для забезпечення конфіденційності передачі. Приймач інформації представлений двома веденими системами, кожна з яких утворює з відповідною їй ведучою системою пару «ведуча-ведена». Тобто в основі даного підходу лежить взаємозв'язок двох пар «ведуча-ведена» систем.

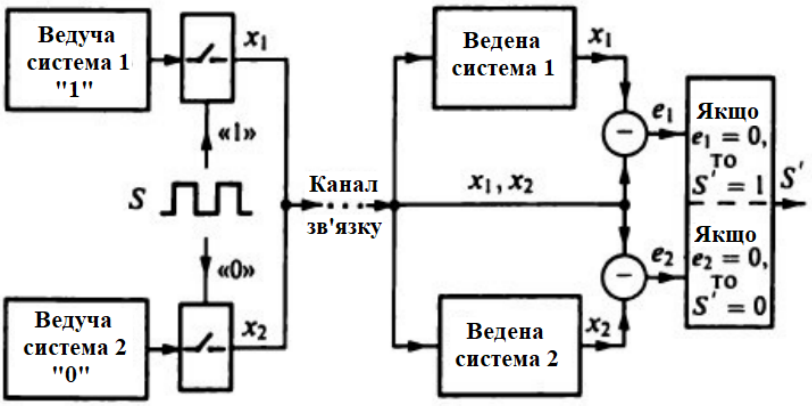

Рис. 2. Перемикання хаотичних режимів

У кожен момент часу в канал зв'язку передається хаотичний сигнал X тільки від однієї з ведучих систем [3]. Для цього на виходах цих ведучих систем розташовані комутуючі пристрої, керовані інформаційним повідомленням в формі бінарного сигналу. Якщо приходить бінарна 1, то один з комутаторів відкривається і пропускає сигналх$_1$, а інший комутатор, який розташований на виході ведучої системи 2, закривається. При бінарному 0 ситуація протилежна. Для організації такої взаємодії важливо, щоб хаотичні режими в ведучих системах були обрані так, щоб при подачі сигналу ними виконувалася синхронізація на виході тільки відповідної їм веденої системи. Отже, по тому, яка ведена система синхронізувалася, можна визначити, який з двох бітів був переданий в певний момент часу.

Внаслідок перемикання режимів у ведучій системі виникають перехідні процеси, які призводять до часових затримок синхронізації ведучої системи з веденої системи. При маленькій частоті перемикання режимів у порівнянні із середньою частотою хаотичного сигналу дана затримка не робить істотного впливу на систему передачі інформації. А при порівняно високих частотах перемикання «затримка може стати співрозмірною з тривалістю передачі інформаційного біта», що в свою чергу викликає помилкові спрацьовування при визначенні «свого-чужого» сигналу.

Висновки

Так як в даному методі для виділення інформації веденої системи, досить тільки визначити який сигнал надійшов на його вхід: від відповідної ведучої її системи або інший, то для реалізації його не потрібно враховувати жорсткі обмеження на ступінь ідентичності використовуваних пар ведуча-ведена система і рівень шумів в каналі зв'язку. Проблеми конфіденційності в даній системі зв'язку відсутня. З одного боку, вибір перемикаючих хаотичних режимів на основі близькості їх характеристик збільшує конфіденційність, але, з іншого боку, можливість відтворення в приймачі сигналу вихідних хаотичних сигналів, як і в хаотичному маскуванні, веде до обмеження приватності. Енергетична ефективність системи передачі досить висока. Це пов'язано з тим, що весь переданий по каналу зв'язку хаотичний сигнал є носієм інформації. Таким чином, схема передачі інформації з перемиканням хаотичних режимів має обмеження по швидкості передачі двійкової інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vadim S. Anishchenko, Tatyana E. Vadivasova, Galina I. Strelkova. Deterministic Nonlinear Systems. A Short Course. Switzerland: Springer International Publishing, 2014. 294 p.

2. Дмитриев А. С., Ефремова Е. В., Максимов Н. А., Панас А. И. Генерация хаоса / под общ. ред. А. С. Дмитриева. Москва: Техносфера, 2012. 424 с.

3. Корчинский В.В. Модель шумового сигнала для передачи конфиденциальной информации. *Вісник НТУ «ХПІ»*. 2013. №11(985). С. 90-95.

Білик Ольга Володимирівна — ТОВ НВП «Дайтекс Технолоджі», Вінниця, e-mail: bilyk@i.ua

Bilyk Olga V. — LLC SPE "Daitex Technology", Вінниця, e-mail: bilyk@i.ua