МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра радиофизики и нелинейной динамики

Применение хаоса в системах связи

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 4061 группы
направления 11.03.02 Инфокоммуникационные
технологии и системы связи
Института физики
Зуевой Елизаветы Алексеевны

Научный руководитель
доцент, к.ф.-м.н., _____ И.А. Корнеев

Зав. кафедрой радиофизики
и нелинейной динамики,
д.ф.-м.н., доцент _____ Г.И. Стрелкова

Саратов 2025 г.

Введение

Современные системы связи сталкиваются с серьезными ограничениями: традиционные аналоговые методы уязвимы к накоплению шумов и искажений при передаче на большие расстояния, а цифровые системы требуют широкой полосы частот и чувствительны к нелинейным эффектам в канале при использовании сложных схем модуляции. В поиске альтернатив особый интерес представляет *хаотическая связь* — направление, использующее сложные колебания нелинейных систем для передачи информации. Её основу составляют детерминированные хаотические сигналы, которые обладают тремя ключевыми свойствами:

1. Широкополосный спектр, повышающий устойчивость к помехам;
2. Чувствительность к начальным условиям, обеспечивающая сложность и непредсказуемость;
3. Воспроизводимость при точном воссоздании параметров системы.

Физическую основу таких систем образуют нелинейные генераторы, описываемые дифференциальными уравнениями. Их способность генерировать сигналы, статистически похожие на шум, но управляемые по своей природе, открывает уникальные возможности:

- Скрытность передачи: Широкополосные хаотические сигналы маскируют информацию, затрудняя её обнаружение;
- Энергоэффективность: Отдельные методы позволяют передавать полезный сигнал без сильного подавления хаотической составляющей;
- Адаптивность: Хаотические системы могут работать в условиях параметрических нестабильностей.

Пионерские работы Куомо-Оппенгейма и Пекоры-Кэрролла заложили основы синхронизации хаотических систем. Сегодня выделяют четыре основных подхода:

1. Хаотическая маскировка: Информационный сигнал $s(t)$ добавляется к хаотическому носителю $x(t)$: $u(t) = x(t) + s(t)$.

   Приемник, синхронизированный с передатчиком, восстанавливает $s(t)$ вычитанием оцененной копии $x'(t)$. Метод требует высокой точности синхронизации.
2. Переключение хаотических режимов: Бинарные "0" и "1" кодируются переключением между разными хаотическими генераторами. Приемник определяет символ по ошибке синхронизации. Ограничение — низкая скорость из-за переходных процессов.
3. Нелинейное подмешивание: Информационный сигнал встраивается непосредственно в динамику хаотической системы. Приемник использует обратную операцию для демодуляции.
4. Системы на основе ФАП: Фазовые автоподстройки частоты работают в хаотическом режиме. Двухканальные схемы передают аналоговые сигналы, одноканальные — цифровые данные.

Цель выпускной квалификационной работы: Провести обзор методов и подходов применения динамического хаоса в системах связи, проанализировать их преимущества, недостатки и перспективы развития.

Задачи:

1. Изучить основные способы аналоговой и цифровой передачи информации.
2. Составить обзор основных методов применения генераторов хаоса для задач передачи информации.
3. Провести детальный анализ экспериментальных реализаций хаотической передачи сигнала.

Структура дипломной работы соответствует логике проведения исследования и состоит из трех основных глав:

- Глава 1. Классические методы передачи информации - анализирует традиционные аналоговые и цифровые системы связи, описывает их основные принципы работы, ключевые преимущества и фундаментальные ограничения (уязвимость к шумам, требования к полосе, сложность синхронизации и т.д.).
- Глава 2. Методы хаотической передачи информации - представляет основные подходы к использованию детерминированного хаоса для передачи информации, рассматривает различные способы интеграции информационного сигнала с хаотическим носителем или генератором, анализирует принципы работы, потенциальные преимущества (скрытность, широкополосность) и ключевые проблемы (синхронизация, уязвимость безопасности, энергоэффективность) каждого подхода.
- Глава 3. Экспериментальная реализация хаотической передачи информации - фокусируется на практических аспектах и безопасности хаотических систем связи, описывает методы анализа уязвимостей хаотических систем (криптоанализ) и экспериментальные реализации, сравнивает устойчивость разных подходов к атакам и оценивает их реальную скрытность и эффективность.

  В работе представлено:

  - 3 главы;
  - 9 рисунков, иллюстрирующих модели и результаты анализа;
  - 1 таблица, содержащая сравнительный анализ систем;
  - 24 источника в списке литературы, включающих как фундаментальные, так и современные публикации по теме.

Основное содержание

Аналоговая связь основана на непрерывном представлении информации. Исходный сигнал (например, звук) преобразуется микрофоном в электрический сигнал m(t). Для эффективного излучения спектр m(t) переносится на высокочастотную несущую c(t) = A_c * cos(2πf_c t + φ_c) с помощью модуляции:

- Амплитудная (АМ): Амплитуда A_c изменяется пропорционально `m(t)`. Спектр содержит несущую и две боковые полосы. Уязвима к шумам.
- Частотная (ЧМ): Мгновенная частота f_i(t) = f_c + Δf * m(t) изменяется пропорционально m(t). Амплитуда постоянна, спектр сложный, теоретически бесконечен. Устойчивее к амплитудным шумам.
- Фазовая (ФМ): Фаза φ_c изменяется пропорционально m(t). Тесно связана с ЧМ, амплитуда постоянна.

Модулированный сигнал излучается антенной, распространяется (ослабляется, искажается, подвергается шумам). Приемник усиливает, фильтрует и демодулирует сигнал (детектор огибающей для АМ, частотный/фазовый детектор для ЧМ/ФМ), восстанавливая m'(t). Ограничения аналоговой связи: уязвимость к шумам и искажениям (накопление по тракту), снижение качества с расстоянием, сложность мультиплексирования.

Цифровая связь основана на представлении информации дискретными битами. Аналоговый сигнал s(t) преобразуется в цифровой вид:

1. Дискретизация во времени: Измерение s(t) с частотой f_s ≥ 2F_max (теорема Котельникова). Результат: отсчеты s[n] = s(n*Δt).

2. Квантование по уровню: Сопоставление каждого s[n] ближайшему уровню квантования. Результат: квантованные отсчеты s_q[n]. Разность - шум квантования.
3. Кодирование источника: Представление s_q[n] битами (АЦП). Часто применяется сжатие (MP3, JPEG).
4. Помехоустойчивое кодирование: Добавление избыточных бит для обнаружения/исправления ошибок (коды Хэмминга, Рида-Соломона, LDPC).

Битовый поток c[m] группируется в символы по k бит (M = 2^k возможных символов). Цифровая модуляция (манипуляция) ставит в соответствие каждому символу уникальное состояние несущей:

- ASK (амплитудная манипуляция): Символы кодируются разными амплитудами.
- FSK (частотная манипуляция): Символы кодируются разными частотами.
- PSK (фазовая манипуляция): Символы кодируются разными фазами (BPSK: 0°, 180°; QPSK: 0°, 90°, 180°, 270°).
- QAM (квадратурная амплитудная модуляция): Символы кодируются уникальной комбинацией амплитуды и фазы (16-QAM, 64-QAM). Эффективна по полосе, но чувствительна к шумам при высоких M.

Модулированный сигнал передается по каналу (шум, затухание, искажения, межсимвольная интерференция - ISI). Приемник выполняет: 1) Синхронизацию (тактовая, несущей, часто ФАПЧ); 2) Фильтрацию и формирование (согласованный фильтр максимизирует SNR); 3) Демодуляцию и решение: Измеряет сигнал в оптимальный момент, наносит точку (I,Q) на созвездие, выбирает ближайший символ. Далее идет декодирование (обратное группировке, коррекция ошибок канальным декодером, декодирование источника) и цифро-аналоговое преобразование (ЦАП) в s'(t). Преимущества цифровой связи: помехоустойчивость и

регенерация сигнала, интеграция с вычислительными сетями, гибкость обработки, универсальность канала. Вызовы: сложность синхронизации, требования к полосе, чувствительность к нелинейностям при сложных созвездиях.

Хаотическая маскировка (CM) - аддитивное наложение информационного сигнала s(t) на хаотический носитель x(t) передатчика: u(t) = x(t) + s(t). Приемник содержит ведомую систему, синхронизированную с передатчиком, генерирующую оценку x'(t) ≈ x(t). Сигнал восстанавливается вычитанием: s'(t) = r(t) - x'(t) ≈ s(t) (при малой ошибке синхронизации и шуме). Преимущества: Принципиальная скрытность. Недостатки: 1) Высокая чувствительность к рассогласованию параметров (>1-2% ведет к десинхронизации); 2) Низкая энергоэффективность (мощность хаоса P_x должна на 35-65 дБ превышать P_s); 3) Уязвимость безопасности (детектирование по мощности, реконструкция аттрактора при SNR>20 дБ); 4) Чувствительность к шуму канала. Практические реализации (система Лоренца) показывают хорошее качество речи (MOS>4.0) при P_x/P_s=40 дБ и SNR=30 дБ.

Переключение хаотических режимов (CSK) кодирует бинарные символы выбором хаотического аттрактора. Варианты передатчика: 1) Два разных генератора; 2) Один генератор с переключением параметра (μ1 для "1", μ2 для "0"). При передаче "1" выход подключен к Генератору1 (или μ=μ1), при "0" - к Генератору2 (или μ=μ2). Демодуляция в приемнике основана на хаотической синхронизации: 1) По ошибке синхронизации: Принятый сигнал r(t) подается на две ведомые системы (копии Ген1 и Ген2). Переданный символ определяется по меньшей ошибке синхронизации (e1 < e2 => "1"). 2) Корреляционный: После синхронизации r(t) коррелируется с локальными копиями x1'(t) и x2'(t); большая корреляция указывает на символ. Преимущества: Потенциал скрытности (LPI - Low Probability of Intercept), широкополосность. Недостатки: 1)

Крайняя чувствительность к шуму n(t) и рассогласованию параметров; 2) Ограничение скорости из-за переходных процессов при переключении и времени захвата синхронизации; 3) Сложность реализации и калибровки идентичных генераторов. Метод смещает интерес к некогерентным методам (DCSK).

Нелинейное подмешивание глубоко интегрирует s(t) в динамику хаотической системы передатчика (напр., в точку разрыва обратной связи): dx/dt = g(x, s(t)), u(t) = h(x). Приемник использует взаимообратное преобразование (напр., вычитание вместо сложения). При синхронизации ведомой системы s'(t) = r(t) - x'(t) ≈ s(t). Преимущества: 1) Гибкость по уровню сигнала (P_s может быть сравнима с P_x или выше, в отличие от СМ); 2) Повышенная устойчивость к рассогласованию параметров (до ~6%); 3) Потенциально высокая скрытность (глубокая нелинейная обработка); 4) Структурная универсальность (сложение-вычитание, деление-умножение и др.). Ограничения: 1) Зависимость качества от точности синхронизации; 2) Требование полного перекрытия спектров s(t) и x(t) для скрытности; 3) Сложность реализации некоторых обратных преобразований; 4) Требование стабильности хаотической генерации.

Использование структуры ФАП использует петли ФАП, работающие в хаотическом режиме. Двухканальная схема (аналоговая): Три идентичные петли ФАП. ФАП0 генерирует опорный хаос x. ФАП1 (пер.) синхронизируется с ФАП0, формирует x1, смешивает с S -> x1+S. ФАП2 (прм.) синхронизируется с ФАП0, формирует x2≈x1. Демодуляция: S' = (x1+S+w) - x2 ≈ S+w. Недостаток: два канала связи. Одноканальная схема (гибридная): Информационный битовый поток S и хаотический бинарный сигнал x1 комбинируются логическим элементом "Исключающее ИЛИ": u = S ⊕ x1. Демодуляция в идентичном приемнике: S' = u ⊕ x2. При синхронизации (x1=x2) S' = S. Проблемы: 1) Узкие зоны устойчивого

хаоса; 2) Нестабильность ГУН; 3) Чувствительность к шумам; 4) Сложность реализации гибридных систем.

Амплитудно-фазовые возвратные преобразования (APRM) - метод криптоанализа ХСС, превосходящий традиционный ARM (Amplitude Return Map). APRM анализирует совместное распределение амплитуд экстремумов сигнала Z_m и интервалов времени между ними Δτ_m, строя диаграмму (Δτ_m, Z_m). Для модулированного сигнала строятся отдельные диаграммы для символов "0" и "1". Различия оцениваются метрикой D, вычисляемой по 2D-гистограммам точек на диаграммах. Низкое D означает высокую скрытность. Преимущество APRM: Эффективно выявляет скрытые паттерны, особенно при модуляции, слабо искажающей фазовый портрет (напр., модуляция симметрии s в численном интеграторе), где ARM малоэффективен. Для параметрической модуляции (изменение b системы) уязвимость к APRM очень высока.

Система CPPM (Chaotic Pulse Position Modulation) - пример некогерентной ХСС. Генератор создает импульсы с хаотическими интервалами T_k (на основе отображения, напр., логистического). Бинарные символы модулируются сдвигом позиции импульса: "0" - импульс в ожидаемое время t_k, "1" - импульс в t_k + δ. Приемник использует огибающую и предсказание t_k по синхронизированной копии генератора. Преимущества: Некогерентный прием (не нужна точная синхронизация осцилляторов), скрытность (LPI). Недостатки: BER выше классических схем (BPSK, FSK), уязвимость к анализу временных паттернов, низкая скорость.

Сравнительный анализ методов модуляции и их устойчивости к атакам (ARM, APRM):

- Параметрическая модуляция (b): Очень высокая уязвимость к APRM. Защита - сложность динамики, большие вариации Δb. Ограничение - снижение помехоустойчивости (BER↑ при Δb↓).

- Модуляция симметрии (s): Низкая уязвимость к ARM, умеренная к APRM (малое искажение фазового портрета). Защита - слабое искажение фазового портрета. Ограничение - чувствительность к шуму (BER↑ при SNR↓).
- CPPM: Умеренная уязвимость к ARM, высокая к APRM (оценочно). Защита - отсутствие периодичности, широкий спектр. Ограничение - низкая скорость, уязвимость к анализу временных паттернов.

Вывод: Модуляция симметрии (s) обеспечивает максимальную скрытность от возвратных преобразований. APRM - эффективный инструмент криптоанализа. Физические реализации (CPPM) подтверждают компромисс между скрытностью и эффективностью. Необходимо: использование сложных генераторов, комбинирование методов (симметрия + импульсная позиция), дополнительное шифрование.

ЗАКЛЮЧЕНИЕ

Исследование применения детерминированного хаоса в системах связи демонстрирует значительный потенциал для решения ключевых проблем современных телекоммуникаций. В отличие от классических аналоговых и цифровых методов, хаотические системы предлагают уникальные свойства, такие как широкополосный спектр, естественная скрытность передачи и устойчивость к узкополосным помехам. Однако их внедрение сопряжено с фундаментальными компромиссами, требующими глубокого понимания динамики нелинейных систем.

Основные методы хаотической связи — маскировка, переключение режимов, нелинейное подмешивание и системы на базе ФАП — раскрывают разнообразие подходов к интеграции информации в хаотический носитель. Маскировка, несмотря на простоту реализации, страдает от жестких требований к синхронизации и низкой энергоэффективности, так как информационный сигнал должен быть подавлен на 35–65 дБ относительно хаотической составляющей. Метод, основанный на переключении аттракторов, обеспечивает высокую скрытность, но критически чувствителен к параметрическим рассогласованиям и шуму, а также ограничен в скорости из-за переходных процессов при смене режимов. На этом фоне нелинейное подмешивание выделяется гибкостью: оно допускает соизмеримые по мощности информационные и хаотические компоненты, повышая энергоэффективность и устойчивость к отклонениям параметров. Системы с хаотическими ФАП, особенно гибридные одноканальные схемы, открывают путь к цифровой передаче данных без сложной синхронизации, хотя их стабильность зависит от точности настройки генераторов.

Ключевым вызовом для всех методов остается безопасность. Детерминированная природа хаоса создает уязвимости к криптоанализу,

таким как амплитудные (ARM) и амплитудно-фазовые (APRM) возвратные преобразования. APRM, анализируя совместное распределение амплитуд экстремумов и временных интервалов между ними, эффективно выявляет скрытые паттерны даже в сложных системах, подобных CPPM (Chaotic Pulse Position Modulation). Эксперименты подтвердили, что модуляция на основе управляемой симметрии в численных моделях (например, изменение коэффициента симметрии в полуявных схемах интегрирования) обеспечивает наивысшую скрытность, минимально искажая фазовый портрет системы. В то же время традиционная параметрическая модуляция (изменение бифуркационных параметров) легко детектируется APRM.

Перспективы хаотической связи лежат в комбинации её преимуществ с достижениями цифровых технологий. Гибридные системы, сочетающие хаотическую модуляцию симметрии с помехоустойчивым кодированием или шифрованием данных, способны обеспечить как высокую скрытность (LPI/LPD), так и устойчивость к ошибкам. Для практической реализации необходимы:

- Разработка интегрированных генераторов хаоса с адаптивной подстройкой параметров;
- Оптимизация методов некогерентного приёма (например, в CPPM) для снижения зависимости от синхронизации;
- Внедрение APRM-анализа на этапе проектирования систем для оценки их криптостойкости.

Таким образом, хаотическая связь не является универсальной заменой традиционным методам, но предлагает мощные решения для специализированных приложений — от защищённых каналов военного назначения до энергоэффективных IoT-устройств. Дальнейший прогресс в этой области зависит от преодоления инженерных проблем синхронизации и создания стандартизированных, воспроизводимых схем, устойчивых к реалиям зашумленных каналов связи.