Министерство образования и науки Российской Федерации

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

Кафедра теоретических основ компьютерной безопасности и криптографии

Каскадные коды

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Морарь Эдуарда Николаевича

Научный руководитель

доцент, к.ф.-м.н. _____ А.Н. Гамова

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

В настоящее время огромное число систем связи основывается на передаче большого количества сообщений в цифровом виде. Однако в канале связи возможно возникновение помех, из-за которых может произойти сбой при приёме сообщения. В результате, это влечёт за собой искажение передаваемых данных. Это приводит к высокой вероятности наличия ошибок в принятом сообщении. Тем временем для большинства приложений допустимо лишь небольшое количество ошибок в обработанных дискретных данных. В результате возникает проблема осуществления надёжной передачи данных по каналам связи с шумами.

Существует несколько решений данной проблемы. Наиболее оптимальным является помехоустойчивое кодирование, которое основывается на введении искусственной избыточности в передаваемое сообщение. Применение данного способа кодирования позволяет получить энергетический выигрыш, который может быть использован для улучшения параметров и характеристик систем передачи данных, например, повышения дальности связи уменьшения размеров антенн, увеличения скорости передачи информации, снижения мощности передатчика и так далее.

Для достижения лучших результатов в конструировании избыточных кодов прибегают к, например, их модификации и комбинированию (последовательное соединение, прямая сумма, произведение кодов). Наилучшие на сегодня коды получены не как представители того или иного семейства кодов, а с помощью данной процедуры. Одними из таких кодов являются каскадные коды. В них используются комбинации как блочных, так и непрерывных кодов.

Целью своей работы ставлю исследование каскадных кодов и анализ алгоритмов, применяемых в них. Для этого выполню следующие задачи:

1) построение каскадных кодов;

2) их программная реализация;

3) тестирование и выявление закономерностей при различных параметрах.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 85 страниц, из них 41 страница – основное содержание, включая 11 рисунков и 15 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1 Каскадные коды

В этом разделе рассматриваются каскадные коды, их построение, кодирование и декодирование, а также приводится классификация данных кодов.

В подразделе 1.1 описан принцип построения каскадных кодов и представлена общая схема. Каскадные коды были введены Форни в качестве линейных блочных помехоустойчивых кодов со сравнительно высокой корректирующей способностью и возможной большой длиной блока n. Эти цели достигаются благодаря применению нескольких сравнительно простых уровней, или, так называемых каскадов, кодирования и декодирования. Наиболее распространенной является схема с двумя уровнями кодирования. Один код при этом называется внешним, а другой – внутренним. Также в этом подразделе описаны обобщённые каскадные коды, в которых может быть больше уровней, и коды, которые используются для построения каскадных, являются разложимыми.

В подразделе 1.2 подробно описана общая структура кодирования и декодирования каскадных кодов, представлена формула расчета относительной скорости, описаны чаще всего используемые коды в качестве внешних и внутренних. В качестве внутреннего кода используются двоичные блоковые или непрерывные коды. Внешний код – это, чаще всего, (N, K)-код Рида-Соломона. Коды Рида-Соломона широко распространены на практике, поскольку являются кодами с максимальным кодовым расстоянием ($D = N - K + 1$) и имеют в качестве кодовых символов k-элементные двоичные последовательности.

В подразделе 1.3 описывается использование перемежителя и его основные функции. Основные две это:

1) для преобразования кодовых слов в векторы, размерность которых соответствует размерности (информационным символам) внутреннего кода;

2) для разбиения пакетов ошибок.

В подразделе 1.4 приводятся классификации каскадные кодов по виду используемых кодов, по области применения и по использованию перемежения символов.

2 Коды, применяемые на внешнем и внутреннем уровнях каскадного кода

В данном разделе рассмотрены коды, которые чаще всего применяются в структурировании каскадных кодов в качестве внешнего или внутреннего уровня.

В подразделе 2.1 описаны коды Боуза-Чоудхури-Хоквингема (БЧХ-коды). Были рассмотрены принципы построения этих кодов, систематическое кодирование и способы декодирования, в частности, с помощью алгоритма Берлекэмпа-Мэсси и алгоритма Евклида.

В подразделе 2.2 проиллюстрированы коды Рида-Соломона (РС-коды). Они являются важным частным случаем БЧХ-кодов, корни порождающего полинома которых лежат в том же поле, над которым строится код. Также рассмотрены алгоритмы кодирования и декодирования РС-кодов.

В подразделе 2.3 рассмотрены коды Хэмминга и его основные свойства. Код Хемминга – это блочный код, позволяющий исправлять одиночные и фиксировать двойные ошибки. К нему относятся коды с минимальным кодовым расстоянием $d_{min} = 3$. Также были изучены алгоритмы кодирования и декодирования данных кодов.

В подразделе 2.4 показаны свёрточные коды. Были рассмотрены его структура (имеет сумматор по модулю 2, регистр сдвига и коммутатор) и процессы кодирования и декодирования.

3 Практическая часть

В этом разделе показана моя реализация каскадного кода на языке Python версии 3.6. Разобран интерфейс данной программы и проиллюстрирован

тестовый пример. Далее с помощью этой программы с сообщениями различной длины и различными параметрами внешних и внутренних кодов были проведены множество испытаний. Также произведён анализ результатов полученных при выполнении тестов по следующим характеристикам: максимальное количество исправленных ошибок, время выполнения кодирования и декодирования, относительная скорость кода. Были сделаны выводы по тому, какую структуру, внутренние и внешние коды и параметры нужно выбрать, чтобы построенный каскадный код более эффективно кодировал и декодировал данные разного объёма.

ЗАКЛЮЧЕНИЕ

Каскадные коды играют заметную роль в теории и практике кодирования. Интерес к ним определяется следующим: достоинством каскадных кодов является относительно низкая сложность кодирующих и декодирующих устройств, так как данные коды позволяют выполнить процедуры кодирования и декодирования по этапам, применяя на каждом этапе достаточно короткие по сравнению с результирующим коды. При этом корректирующие способности кода довольно высокие. Недостатком же является высокая избыточность передаваемой информации.

В данной работе я рассмотрел построение каскадных кодов. Была изучена схема двухуровневого каскадного кода и структура двухступенчатой системы каскадного кодирования и декодирования.

Также были рассмотрены возможные внутренние и внешние коды каскадных кодов. Это коды Рида-Соломона, Боуза-Чаудхури-Хоквингема, Хэмминга и свёрточные. Также были изучены способы кодирования и декодирования данных кодов.

Далее была написана программа, написанная на языке Python, включающая в себя реализацию двухуровнего каскадного кода, который состоит из внешнего кода Рида-Соломона с систематическим кодированием и декодированием с помощью алгоритма Берлекемпа – Месси, и внутреннего кода в трёх вариантах: БЧХ-код с систематическим кодированием и декодированием с помощью алгоритма Берлекемпа – Месси, код Хэмминга с систематическим кодированием и синдромным декодированием, свёрточный код с декодером Витерби, и выполняющая его тестирование (успешность декодирования, количество исправленных ошибок, время кодирования и время декодирования)..

Итогом моей работы стали тестирование и выявление оптимальных характеристик при различных параметрах описанных кодов, в чем и

заключается анализ алгоритмов, используемых в данных каскадных кодах. С помощью написанной мною программы были получены таблицы с результатами тестирования, с помощью которых были сделаны следующие выводы:

- если наиболее важной характеристикой является количество исправляемых ошибок (например, в каналах с сильными помехами), то:
    a. для сообщений маленькой длины более предпочтительны коды, у которых внешними являются РС-коды с малой длиной кодового слова, а внутренними – БЧХ-коды с малой длиной кодового слова и свёрточные с кодовым ограничением 7;
    b. для сообщений средней длины более предпочтительны коды, у которых внешние – коды Рида-Соломона с большой длиной кодового слова (255), а на внутренние – БЧХ-коды с параметрами (15, 5) или (63, 18);
    c. для сообщений большой длины более предпочтительны коды, у которых внешние – коды Рида-Соломона с различной длиной кодового слова, а внутренние – БЧХ-коды с параметрами (15, 5) или (63, 18);
- если наиболее важной характеристикой является скорость декодирования, то:
    a. для сообщений малой длины более предпочтительны коды, у которых на внешнем уровне коды Рида-Соломона с малой длиной кодового слова, а на внутреннем – коды Хэмминга;
    b. для сообщений средней длины более предпочтительны коды, у которых на внешнем уровне РС-коды с малой длиной кодового слова, а на внутреннем – коды Хэмминга с длиной кодового слова 31 или 63, и свёрточные коды с кодовым ограничением 3;

c. для сообщений большой длины более предпочтительны коды, у которых внешние РС-коды с большой длиной кодового слова, а внутренние – Хэмминга и свёрточные с кодовой длиной 3.

- если наиболее важной характеристикой является относительная скорость кода (например, для ограничения объёма посылаемых данных), то:
    a. для сообщений малой длины более предпочтительны коды, на внутреннем уровне которых расположены коды Хэмминга и БЧХ с малой длиной кодового слова (7 или 15);
    b. для сообщений средней и большой длины более предпочтительны коды, на внешнем и на внутреннем уровне которых расположены коды Рида-Соломона и коды Хэмминга соответственно с большой длиной кодового слова (63 – 255).

Таким образом, первоначально поставленные задачи можно считать выполненными, а цель работы достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. М. : Техносфера, 2005. 320 с.

2 Касами, Т. Теория кодирования / Т. Касами, Н. Токура, Ё. Ивадари, Я. Инагаки: пер. с японского А. В. Кузнецова. М. : Мир, 1978. 576 с.

3 Форни, Д. Каскадные коды / Д. Форни: пер. с английского В. В. Зяблова, О. В. Попова. М. : Мир, 1970. 207 с.

4 Блох, Э. Л. Линейные каскадные коды / Э. Л. Блох, В. В. Зяблов. М. : Наука, 1982. 229 с.

5 Вернер, М. Основы кодирования. Учебник для ВУЗов / М. Вернер. М. : Техносфера, 2004. 288 с.

6 Шувалов, В. П. Передача дискретных сообщений. Учебник для ВУЗов / В. П. Шувалов, Н. В. Захарченко, В. О. Шварцман. М. : Радио и связь, 1990. 464 с.

7 Гладких, А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи [Электронный ресурс] / А. А. Гладких. Ульяновск : УлГТУ, 2010. 379 с.

8 Никитин, Г. И. Свёрточные коды. Учебное пособие / СПб. : СПбГУАП, 2001. 80 с.

9 Питерсон, У. Коды, исправляющие ошибки. [Электронный ресурс] : учебное пособие / У. Питерсон, Э. Уэлдон: пер. с английского Р.П. Добрушина, С.И. Самойленко. М. : Мир, 1976. 594 с.

10 Берлекэмп, Э. Алгебраическая теория кодирования [Электронный ресурс] : учебное пособие / Э. Берлекэмп. М. : Мир, 1971. 478 с.

11 Зяблов, В.В. Высокоскоростная передача сообщений в реальных каналах [Электронный ресурс] / В.В. Зяблов, Д.Л. Коробков, С.Л. Портной. М. : Радио и связь, 1991. 288 с.

12 Колесник, В.Д. Декодирование циклических кодов / В.Д. Колесник, Е.Т. Мирончиков. М. : Связь, 1968. 251 с.

13 Зиновьев, В.А. Обобщённые каскадные коды [Электронный ресурс] / В.А. Зиновьев // Проблемы передачи информации. 1976. Т. 12. Выпуск 1. С. 5–15

14 Золотарёв, В.В. Помехоустойчивое кодирование. Методы и алгоритмы [Электронный ресурс] : справочник / В.В. Золотарёв, Г.В. Овечкин. М. : Горячая линия – Телеком, 2004. 126 с.

15 Кудряшов, Б.Д. Основы теории кодирования [Электронный ресурс] : учеб. пособие / Б.Д. Кудряшов. СПб. : БХВ-Петербург, 2016. 400 с.

16 Золотарёв, В.В. Коды и кодирование [Электронный ресурс] / В.В. Золотарёв. М. : Знание, 1990. 64 с.

17 Блейхут, Р. Теория и практика кодов, контролирующих ошибки [Электронный ресурс] : учебно – справочное издание / Р. Блейхут. М. : Мир, 1986. 576 с.

18 Егоров С.И. Коррекция ошибок в информационных каналах периферийных устройств ЭВМ [Электронный ресурс] : учеб. пособие / С. И. Егоров. Курск : КурскГТУ, 2008. 252 с.

19 Евсеев, Г.С. О сложности декодирования линейных кодов [Электронный ресурс] / Г.С. Евсеев // Проблемы передачи информации. 1983. Т. 19. Выпуск 1. С. 3–8

20 Нейфах, А.Э. Свёрточные коды для передачи дискретной информации [Электронный ресурс] / А.Э. Нейфах. М. : Наука, 1979. 222 с.