Алгоритмическая модель канала связи

И. А. Козинов[1], Я. О. Саклаков[1], А. С. Костарев[1], С. Г. Бурлуцкий[2]
[1]*Военно-космическая академия имени А.Ф. Можайского*
[2]*Санкт-Петербургский государственный университет аэрокосмического приборостроения*

***Аннотация*. Предложена алгоритмическая модель канала связи, с заданной на нем сложностной (алгоритмической) мерой, которая может быть использована при обосновании требований к выбору сигнально-кодовых конструкций для радиосистем передачи информации, функционирующих в каналах с преднамеренными помехами.**

Ключевые слова: канал связи; модель; кодовая конструкция

I. Введение

Теорию кодирования можно рассматривать как раздел теории информации, посвященный проблеме достижения пределов скорости передачи информации, предугаданных Клодом Шенноном.

Традиционная теория кодирования основана на вероятностной модели канала связи. Для вероятностной модели декодирование определяется в терминах распределения вероятностей $p(x)$ на входных последовательностях канала связи. Декодер при этом настраивается на вероятности, которые, на самом деле, известны неточно и могут менять я в процессе передачи информации, особенно в канале с преднамеренными помехами, когда структура помехи подстраивается под сигнал. Изменившаяся статистика ведет к снижению эффективности декодирования и его неоптимальности для новых условий.

В. Гоппой развит алгебраический подход к теории информации. Теория информации трактуется как абстрактная теория слов со своими специфическими задачами, связанными с хранением слов в памяти компьютера, обработкой слов и их передачей по каналам связи. На множестве слов канонически присутствует алгебраическая структура, связанная с действием симметрической группы на словах. Эта структура используется для определения информации слова с различными приложениями к информатике [1, 2].

Введенная В.Гоппой [1] алгебраическая модель канала связи с информационной метрикой, заданной на симметрической группе перестановок кодовых слов, позволяет строить не вероятностную теорию кодирования, для которой возможно устойчивое (оптимальное) декодирование для целого класса распределения вероятностей. Однако в этой теории не учитываются алгоритмические зависимости между символами кодовых слов, и алгоритмическая сложность задания кодовых слов, определяющие возможности постановщика помех по более эффективному подавлению радиолиний.

II. Алгоритмическая модель канала связи для каналов с преднамеренными помехами

При помехоустойчивом кодировании в поток передаваемых символов вводятся дополнительные (избыточные) символы для исправления возникающих на приемной стороне ошибок. Это требует увеличения скорости передачи по каналу, что при выбранном типе модема эквивалентно расширению полосы частот сигнала и уменьшению энергии посылки. Поэтому может возникнуть правомерный вопрос о целесообразности использования избыточного кодирования.

На этот вопрос дает ответ теорема Шеннона о пропускной способности непрерывного канала связи, из которой следует, что пропускная способность непрерывного канала увеличивается с расширением его полосы, но при оптимальном (в широком смысле) кодировании. Поэтому следует ожидать повышения достоверности передачи при заданной скорости и отношении сигнал/шум в канале при внесении избыточности. Однако не существует оптимального кодека для сообщения, не фиксированного по длительности [3].

Введем в рассмотрение алгоритмическую модель канала связи с заданной на нем сложностной (алгоритмической) мерой.

Алгоритмическую меру определим, как количество информации, необходимое для того, чтобы переработать слово $\boldsymbol{x}$ в кодовое слово $\boldsymbol{y}$ (или наоборот).

По Колмогорову [4] она определяется как минимальная длина программы (например, состоящей из «0» и «1»), которая позволяет построить (предсказать) кодовое слово **y**, имея в своем распоряжении слово **x**:

$$K\left(\frac{y}{x}\right) = \min_{B(p,x)} \left(l(p)\right),$$

где $B(p,x)$ – функция, для которой имеется вычисляющий ее значение алгоритм; p – программа, реализующая этот алгоритм.

Любая кодовая конструкция с избыточными символами есть результат работы некоторого алгоритма, где x – это поступающие на вход кодирующего устройства (с вероятностью $P(x)$) слова сообщения, а y – кодовые слова на выходе кодирующего устройства. Таким образом, чем больше избыточных символов содержит кодовое слово, тем больше в нем «алгоритмической» части. Для кодов с проверкой на четность это один символ, а для кодовых

последовательностей, используемых в системах с расширением спектра сигналов – это все кодовое слово. Кодовые слова с большей сложностью формируются более длинной «программой», следовательно, чем больше «программа» $l(p)$, тем большее количество информации переносит кодовое слово.

Необходимость введения алгоритмической модели канала связи обусловлена несколькими причинами.

Во-первых, важной характеристикой помехозащищенности является структурная скрытность. Она характеризует способность противостоять мерам радиотехнического анализа, направленным на раскрытие сигнала. Это означает распознавание формы сигнала, определяемой способами его кодирования и модуляции, т. е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов. Следовательно, для увеличения структурной скрытности необходимо иметь по возможности большую мощность используемых кодов и достаточно часто изменять форму сигналов.

При оценке структурной скрытности кодов и связанной с ней сигнальной имитостойкости (свойство характеризующее способность противостоять активным действиям помехопостановщика целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных), возникает вопрос о влиянии сложности алгоритмов формирования кодов и длине сегмента идентификации кодовых слов на системные характеристики каналов связи, в частности на пропускную способность канала связи, на который в рамках традиционной вероятностной модели канала связи ответа получить не удается.

Канал связи с преднамеренными помехами, в котором помехопостановщик имитирует структуру кодовых слов, пытаясь передать ложные сообщения, либо создает имитирующие помехи (вскрывая алгоритм формирования кодовых слов) является алгоритмическим каналом связи, на котором может быть задана алгоритмическая мера и «алгоритмическая память» канала [5].

Во-вторых, при использовании в канале связи так называемого «бегущего кода» (смены алгоритмов формирования кодовых слов), возникает проблема снятия неопределенности относительно алгоритма смены кодовых слов. При передаче больших массивов информации алгоритмическая неопределенность снимается в начале сеанса связи при помощи «синхроключа» и является пренебрежимо малой по сравнению с вероятностной энтропией источника. При передаче же информации короткими пакетами алгоритмическая неопределенность сравнима с вероятностной и ее обязательно нужно учитывать.

Пару «кодер источника – кодер канала» можно рассматривать как новый источник дискретных сообщений при формировании «бегущего кода». Использование для передачи информации кодов с большей алгоритмической сложностью эквивалентно дополнительному эффективному кодированию «источника» кодового словаря, устраняющему алгоритмическую избыточность кодовых слов. Такое «сжатие» кодовых слов должно приводить к увеличению скорости передачи информации. Кроме того, алгоритмическая сложность манипуляционного кода, формирующего «бегущий код», также оказывает влияние на пропускную способность канала связи.

Наконец, третьей причиной является толкование термина «случайность» и «псевдослучайность» применительно к кодовым словам переносчикам информации.

Наиболее эффективным переносчиком информации является случайный процесс, поскольку он является самым неожиданным для получателя. В алгоритмической теории информации доказано, что последовательность символов может считаться «случайной», если она случайна и по вероятностной и по сложностной мере. Только в этом случае последовательность является максимально сжатой и не содержит избыточности. Применительно к теории кодирования это означает, что более сложные кодовые слова являются «более случайными» и обеспечивают более высокую скорость передачи информации.

Алгоритмическую меру на множестве кодовых слов можно вводить над вероятностной мерой, расширяя вероятностную модель канала с преднамеренными помехами. В этом случае синтез кодовых слов производится традиционно по $d_{\min}$, а сложность кодовых слов учитывается только для каналов с преднамеренными помехами, путем введения алгоритмической памяти канала (через меняющуюся статистику помех для кодов с различной сложностью), а также учитывается при обосновании минимальной длины «синхроключа» при передаче пакетов, состоящих из нескольких кодовых слов, передаваемых в режиме «бегущий код».

При таком подходе доказывается, что постановка имитирующих помех для систем, использующих коды с большей сложностью слов, менее эффективна, поскольку возникающая в канале «алгоритмическая память» пропорциональна алгоритмической сложности кодовых слов. Повышение скорости передачи, при использовании кодовых слов с большей сложностью, обеспечивается за счет сокращения длины «синхроключа», так как появляется возможность снизить требования к сложности и длине манипулирующей последовательности «бегущего кода» [6].

Увеличение сложности кодовых слов, является аналогом эффективного кодирования источника, в качестве которого выступает «кодовый словарь». В этом случае можно говорить об алгоритмическом эффективном кодировании «кодового словаря», в ходе которого устраняется алгоритмическая избыточность.

Синтез нелинейных кодовых последовательностей в настоящее время производится именно по $d_{\min}$, а характеристика сложности (линейной, квадратичной и т. д. [5, 7]) выступает в качестве дополнительного

показателя. Критерий, которым здесь пользуются – чем больше сложность кодовых слов, тем лучше.

При задании алгоритмической меры на множестве кодовых слов как самостоятельной меры требуется развитие направления теории кодирования, основанного на алгоритмической модели канала связи.

Для того, чтобы задать модель канала необходимо задать:

1) множество кодовых слов на входе канала и входной алфавит;

2) множество слов на выходе канала и выходной алфавит;

3) переходную матрицу канала, показывающую число переходов *i*-й буквы входного слова в *j*-ю букву слова на выходе канала;

4) взаимную информацию между входными и выходными словами, максимум которой характеризует пропускную способность канала: уровень помех в канале.

Зададим разбиение множества двоичных кодовых слов длины n на классы эквивалентности по мере $l(p)$. Каждый алгоритм формирования кодовых слов можно характеризовать своей длиной программы $l(p)$, $i = 1...m$ (где m – число классов эквивалентности). Тогда множество всех двоичных кодовых слов длины **n** разбивается на непересекающиеся классы эквивалентности:

$$2^n = 2^{l_1(p)} + 2^{l_2(p)} + ... + 2^{l_1(p)} + 2$$

Пусть множество кодовых слов задается алгоритмами различной сложности. Зададим для алгоритмического канала два кодовых расстояния, по которым будем различать кодовые слова с различной сложностью.

Минимальным алгоритмическим расстоянием $\Delta l_{\min} = l_i(p) - l_j(p)$ назовем минимальную разность между длинами программ формирования кодовых слов. Можно показать, что минимальное алгоритмическое расстояние обладает всеми метрическими свойствами, превращающими множество кодовых слов в метрическое пространство.

Минимальным алгоритмическим хеммингловым расстоянием $dl_{\min}$ назовем число позиций, в которых различаются кодовые слова с различной сложностью для заданного $\Delta l_{\min}$.

Множество входных ходовых слов задается словами, принадлежащими различным классам эквивалентности (с *различной* $l(p)$) с заданным минимальным расстоянием $\Delta l_{\min}$. Переходная матрица канала задается числом переходов входного кодового слова с $l_i(p)$ в слово $l_j(p)$, $l_i(p) \neq l_j(p)$.

Пропускная способность алгоритмического канала задается как максимум взаимной алгоритмической энтропии между входными и выходными словами канала.

III. Заключение

Предложенная алгоритмическая модель канала связи может быть использована при обосновании требований при выборе сигнально-кодовых конструкций для радиосистем передачи информации, функционирующих в каналах с преднамеренными помехами.

Список литературы

[1] Гоппа В.Д. Введение в алгебраическую теорию информации. Москва : Наука : Изд. фирма «Физ.-мат. лит.», 1995. 106 с.

[2] Гуров И.П. Основы теории информации и передачи сигналов. СПб.: BHV-Санкт-Петербург, 2000. 97 с.

[3] Хромов Л.И. Теория информации и теория познания. 2-е изд., доп. Спб., Изд. Русского философского общества, 2021. 310 с.

[4] Колмогоров А.Н. Теория информации и теория алгоритмов. М.: Наука, 1987. 304 с.

[5] Тараненко П.Г. Псевдослучайные и кодовые последовательности. Методы синтеза и анализа. СПб.: ВИКУ им. А.Ф.Можайского, 1999. 110 с.

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

[7] Вернер М. Основы кодирования: Учеб. для ВУЗов. Москва: Техносфера, 2004. 288с.