Министерство образования и науки Республики Казахстан

Евразийский национальный университет им. Л.Н.Гумилева

Институт информационной безопасности и криптологии

СБОРНИК ТРУДОВ

III Международной научно-практической конференции

«Информационная безопасность в свете Стратегии Казахстан - 2050»

15-16 октября 2015 года, г. Астана

5. Горбатов В.С. Контроль защищенности речевой информации в помещениях. – М.: НИЯУ МИФИ, 2014. – 248 с.

6. Горшков Ю.Г. Анализ и маскирование речи. Учебное пособие. – М.:МГТУ им. Н.Э. Баумана, 2006. – 58 с.

7. АдамянА. Защита речевой информации руководителя организации от скрытой записи посетителем. http://daily.sec.ru, 17.08.2007.

8. Джурунтаев Д.З. Схемотехника. Учебник. – Алматы: Эверо, 2005. – 276 с.

Золотарев В.В., Овечкин Г.В., Ташатов Н.Н.

ПРИМЕНЕНИЕ ПРИНЦИПА ДИВЕРГЕНЦИИ ПРИ ДЕКОДИРОВАНИИ СВЁРТОЧНЫХ КОДОВ

Институт космических исследований РАН, Москва,РФ

Рязанский государственный радиотехнический университет, Рязань, РФ

Евразийский национальный университет, Астана, РК

Помехоустойчивое кодирование стало неотъемлемой частью современных систем передачи и хранения информации. Это стало возможным благодаря существенным прорывам, достигнутым теорией кодирования за последние годы. Представленные в [1] основные достижения оптимизационной теории кодирования свидетельствуют о том, что построенные на новых постулатах этой теории многопороговые декодеры (МПД) к настоящему моменту достигли уже весьма высокого уровня эффективности при умеренной сложности. В гауссовских каналах эти алгоритмы работают с вероятностью ошибки на бит $P_b(e)<10^{-5}$ при уровне битовой энергетики E_b/N_0~1,3 дБ. Организовать столь же эффективную работу декодеров низкоплотностных (LDPC) кодов, при таком уровне шума уже весьма сложно, а для высокоскоростных каналах и невозможно.

С другой стороны, возможность реализации декодеров МПД на основе технических решений [2] позволяет сохранять хорошие энергетические характеристики декодирования на высокие скоростях передачи канала, в том числе выше, чем 1 Гбит/с [3, 4]. К тому же ресурсы улучшения характеристик для МПД алгоритмов ещё не полностью исчерпаны, что позволяет и в дальнейшем ожидать от них дальнейшего улучшения эффективности работы при больших уровнях шума. Представленные в [5, 6] результаты исследований показывают, что символьные многопороговые декодеры (QMПД) существенно перекрывают по своей эффективности коды Рида-Соломона и практически реализуемые QLDPC коды, оставаясь столь же простыми в реализации, как и их прототипы – двоичные МПД.

Главная причина столь высокой степени преимущества МПД декодеров всегда заключается в том, что и для весьма высоких уровней шума канала они обеспечивают такое же декодирование, как и оптимальные переборные методы, но при линейной сложности. Для многих сочетаний характеристик кодов и каналов эффективность МПД разных модификаций при малой энергетике канала столь значительна, что других методов, которые работоспособны в этих условиях, вообще назвать нельзя. Таким образом, преодолев уровень эффективности реальных декодеров LDPC кодов, алгоритмы МПД фактически заявили о своём первенстве по эффективности и сложности реализации вообще для всех значимых приложений в системах передачи, хранения, контроля и восстановления цифровых данных.

Однако в настоящее время недостаточно применения в декодерах итеративного типа только простых средств обработки цифровых потоков на базе мажоритарной логики. Использование только мажоритарной логики, видимо, не даст существенно приблизиться к пропускной способности канала. В настоящей работе предлагаются новые направления развития итеративных алгоритмов, которые могут помочь значительно приблизить допустимые уровни кодовых скоростей к пропускной способности каналов.

Рассмотрим схему простого свёрточного кодирования с кодовой скоростью R=1/2, представленную на рис. 1. Она состоит из регистра сдвига, в левой части которого сгруппированы ячейки, с выходов которых поступают значения их содержимого на входы полусумматора (mod 2 сумматор), с выхода которого проверочные символы кода отправляются в канал. Для упрощения описания будем полагать код систематическим. Поэтому вместе с проверочным символом кода в канал на каждом такте работы кодера уходит и один информационный символ из нулевой ячейки регистра сдвига.

Принципиальным моментом для описания работы данного кодера является наличие далеко в правой части кодирующего регистра ещё одной ячейки, содержимое которой также поступает на вход полусумматора, с которого данные уходят в канал.

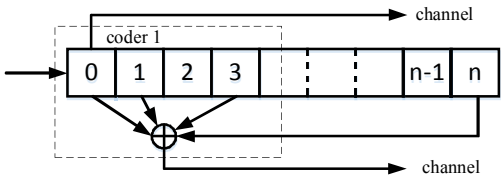

Рисунок 1 – Кодер дивергентного кода

На рис. 2 показан декодер свёрточного кода, соответствующий кодеру, представленному на рис.1. Он построен по идеям МПД и содержит 2 пороговых элемента (ПЭ), находящихся в левой и правой частях декодера. Левый ПЭ (ПЭ 1) и соответствующие части информационного и синдромного регистров, с которыми он взаимодействует, выделены пунктирным квадратом и названы Decoder1 (D1).

Полный декодер со вторым пороговым элементом (ПЭ 2) в правой части регистров декодеров подобен D1. Но на вход ПЭ 2 поступает ещё и

дополнительная проверка кода, которая появляется в декодере намного позже символов компактной группы проверок, связанных с первым ПЭ1.

При работе в канале первый ПЭ1 принимает решения об информационных ошибках на основании только своей группы проверок. Если шум канала и код выбраны правильно, то после первого ПЭ 1 плотность таких ошибок будет меньше, чем до этого порога, а достигнув второго ПЭ 2, эти ошибки согласно принципам работы МПД будут подчищены. А поскольку на входы ПЭ 2 поступает на одну большее число проверок, чем в ПЭ 1, то и корректирующие возможности второго ПЭ 2 будут более высокими, что позволит усилить процесс коррекции, так как второй ПЭ 2 работает с кодом, у которого минимальное расстояние d как бы выросло на единичку по сравнению с первым ПЭ 1. Важно, что этого удалось добиться без привлечения методов каскадирования, которые отнимают избыточность у первого кода (и первого ПЭ 1), что заметно уменьшает корректирующие возможности первого декодера.

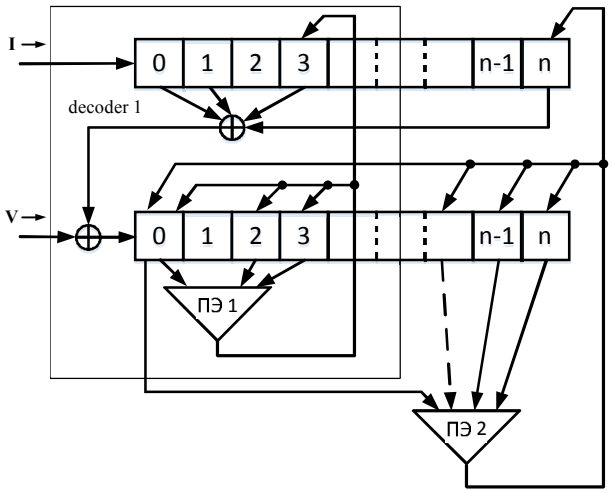

Рисунок 2 – Декодер дивергентного кода

Очевидно, что предложенный код сам может быть первой частью ещё более длинного кода с подобной же структурой. Тогда на двух таких условных

"каскадах" кодирования/декодирования минимальное расстояние d уже будет увеличено на 2 и т.д.

Получившаяся схема декодирования стала намного более сложной, так как эффект роста кодового расстояния, крайне ценного ресурса, не может быть получен просто так. Первый декодер на рис. 2 часть ошибок, которые он не исправил, пропускает направо ко второму ПЭ2. И тогда с ячейки *n* через два полусумматора эти ошибки попадают в синдромный регистр. Значит, первый ПЭ1 работает при немного возросшем уровне шума, что ухудшает его характеристики. Но если ПЭ1 справляется с этим возросшим потоком ошибок и ухудшает свои характеристики немного, а второй ПЭ2 помогает первому, то можно ожидать, что вместе они справятся с таким более сложным потоком ошибок, что и позволяет продолжить анализ этой схемы для определения её возможностей при высоком уровне шума.

Рассмотрим характеристики такой дивергентной схемы (с растущими, "расходящимися" значениями d), представленные на рис. 3. На нём также представлены приближённые зависимости вероятности ошибки декодеров $P_b(e)$ от уровня шума канала для алгоритма Витерби (VA) и для МПД декодеров с кодами, имеющими некоторое кодовое расстояние d и d+1. Характеристики имеют типичные изгибы, которые находятся в точках, где вероятности ошибки МПД при уменьшении уровня шума (вправо) достигают оптимальных минимальных значений для используемых кодов. Левее точек перегибов алгоритмы уже не могут работать из-за высокого шума канала. Рисунок демонстрирует принцип дивергентного кодирования, при котором МПД, работающий в такой схеме с кодом, имеющим расстояние d+1 обеспечивает декодирование при уровне шума ~1,7 дБ, хотя сам МПД работает в обычном режиме только при уровне шума порядка 1,8 дБ.

Характеристики МПД с кодом, имеющим минимальное расстояние *d,* близки к оптимальным до энергетики 1,6 дБ. Установим уровень шума для него 1,7 дБ. Это точка 1 на диаграмме. Теперь подключим в кодере и декодере

дополнительную далёкую проверку, влияние которой мы обсуждали по рис. 1 и 2. Если дополнительный шум от этой проверки невелик и может быть выражен как увеличение шума канала примерно на 0,1 дБ, с которым первый МПД с кодом, имеющим расстояние *d*, ещё справляется, то характеристики этого МПД сместятся из точки 1 в точку 2 и пока останутся оптимальными. Но тогда во второй декодер с ПЭ2 действительно попадает поток информационных ошибок из первого декодера с гораздо меньшей плотностью, чем вероятность ошибок в канале. А это и создаёт условия, при которых второй ПЭ2 действительно тоже дополнительно снизит плотность ошибок, пришедших к нему от первого ПЭ1 (точка 3). Но это произойдёт уже при уровне шума, примерно на 0,1 дБ большем, чем тот, при котором ПЭ2 мог работать без поддержки ПЭ1. Разумеется, применяя этот принцип несколько раз, можно значительно продвинуться в область более высоких шумов канала.

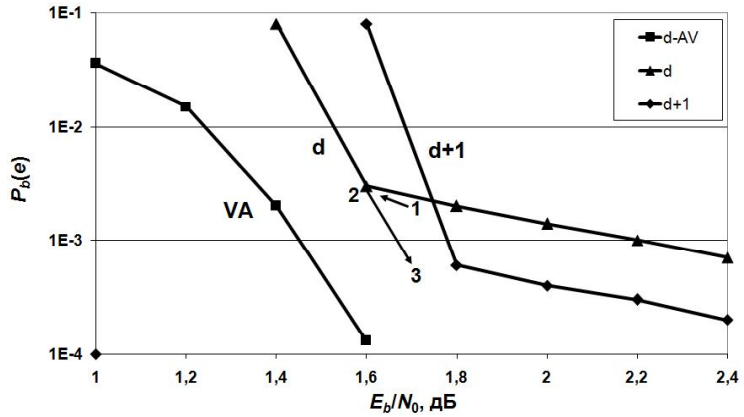

Рисунок 3 – Характеристики дивергентного кода

Обращаясь далее к графику для АВ, который приведён на рис. 3, можно заметить, что он не имеет таких перегибов, как кривые для МПД. Кроме того, обычно графики для длинных, но ещё реализуемых в плане сложности декодеров АВ лежат левее графиков для МПД, как это и показано на рис. 2. Это значит, что если вместо первого ПЭ1 поставить достаточно эффективный декодер АВ, то применение принципа дивергенции может быть ещё более эффективным.

Разнообразные сопоставления эффективности многих алгоритмов декодирования показали также, что единственной группой методов, которые измеряют расстояние своих решений до принятого сообщения, являются МПД, QМПД (декодеры символьных кодов) и алгоритм Витерби. В работе показано, что они успешно применяются совместно, в том числе для дивергентного кодирования.

Литература

1. В.В. Золотарёв, Ю.Б. Зубарев, Г.В. Овечкин. Многопороговые декодеры и оптимизационная теория кодирования. // Под редакцией академика РАН В.К. Левина. М., «Горячая линия – Телеком», 2012, 238 с.

2. Патент РФ №2377722.

3. Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В. Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // Научно-технический сборник «Техника средств связи», серия «Техника телевидения», юбилейный выпуск, МНИТИ, 2010, с.41–43.

4. В.В. Золотарёв. Г.В. Овечкин. Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // "Электросвязь, М., 2014, №12, с.10-14.

5. Zolotarev V.V., Averin S.V. Non-Binary Multithreshold Decoders with Almost Optimal Performance. 9-th ISCTA’ 07, July, UK, Ambleside, 2007.

6. Ovechkin G.V., Zolotarev V.V. Non-binary multithreshold decoders of symbolic self-orthogonal codes for q-ary symmetric channels – 11-th ISCTA’09, July, UK, Ambleside, 2009.

Ибраев Н.С.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФАКТОР УСПЕШНОГО ПЛАНИРОВАНИЯ ВОЕННЫХ (СПЕЦИАЛЬНЫХ) МЕРОПРИЯТИЙ