УНИВЕРСАЛЬНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И ОСОБЕННОСТИ ИХ РЕАЛИЗАЦИИ

Крылова В.А.
НТУ «ХПИ», ул. Фрунзе, 21, г. Харьков, Украина, 61002
vika_hpi@mail.ru

В настоящее время при выборе помехоустойчивого кодера его параметры должны быть согласованы с источником сообщения, каналом связи, а также требованиями, предъявляемыми к достоверности доведения информации до получателя. Однако сложно заранее выбирать параметры кода, если качество канала связи неизвестно, а иногда вообще оно может изменяться в процессе эксплуатации системы. Параметры помехоустойчивого кода выбирают исходя из некоторого «среднего» состояния канала связи, что приводит к уменьшению скорости передачи информации, из-за большей избыточности кода. Это может приводить к потере связи при использовании кодов, параметры которых остаются постоянными и не рассчитаны на значительное ухудшение качества канала. Одним из путей устранения этого недостатка является использование систем адаптивного кодирования с автоматической и целенаправленной коррекцией параметров кода по мере изменения качества канала, обеспечивая при этом заданную вероятность доведения сообщения при минимальной избыточности помехоустойчивого кода.

Таким образом, в области унифицированных средства защиты информации существует необходимость в разработке универсальных систем защиты на основе методов адаптивного кодирования. Которые допускают изменения характеристик системы передачи по двум измерениям: энергетический выигрыш за сет кодирования и скорость передачи. При адаптивном кодировании необходимо решить следующие основные задачи: определить качество состояния информационного канала связи; принять решение об изменении значений параметров кодера и декодера, для обеспечения заданной вероятности доведения сообщения при минимальной избыточности кода; установить новые параметры кода в кодирующем и декодирующем устройстве.

Основными параметрами помехоустойчивого кода являются блоковая длина (блоковые коды) или длина кодового ограничения (свёрточные коды) и скорость кода[51]. Однако изменение параметров кода не всегда гарантирует необходимое минимальное кодовое расстояние, и помехоустойчивость может ухудшиться. Т.к. алгоритмы кодирования и декодирования некоторых кодов привязаны к структуре порождающих и проверочных полиномов кода, не все помехоустойчивые коды могут легко менять свои параметры.

Также существует способ расширения любого двоичного (n, k, d) кода до кода со значением $d_{\min} = d + 1$, с помощью добавления к каждой

кодовой комбинации результата суммирования по модулю 2 всех ее символов. Такое повторение кодовых комбинаций обеспечивает повышения минимального расстояния до двух, но при этом скорость кода снижается в два раза. Как правило, такие коды с коррекцией параметров, на приёмной стороне декодируются с помощью алгоритма списочного декодирования, который обеспечивает лучшее соотношение между сложностью и вероятностью ошибки, чем другие алгоритмы.

Для построения адаптивных систем кодирования среди помехоустойчивых кодов наибольший интерес представляют совместимые по скорости, перфорированные сверточные коды (Rate Compatible Punctured Convolutional Codes – RCPC) и гнездовые (вложенные) свёрточные коды (Nested Convolution Codes−NCC). Гнездовые свёрточные коды представляют собой набор кодов со скоростью $R = 1/(n+1)$, которые являются производными от сверточного кода скорости $R = 1/(n+1)$, с помощью поиска лучших генераторных последовательностей $G_{n+1}(D)$. Таким образом, используя технологию разложения материнского свёрточного кода на систему гнездовых (вложенных) свёрточных кодов, можно получить широкий набор кодовых соотношений (ЭВК), при этом сохраняя структуру и алгоритм кодирования материнского кодека. Синтез гнездовых свёрточных кодов, а также их свойства в настоящее время изучаются, также остается открытым вопрос о декодировании гнездовых свёрточных кодов. Однако представляет интерес построение адаптивной системы кодирования, на основе RCPC и NCC кодах, которая допускает изменения по двум измерениям: получение требуемой величины выигрыша за счет кодирования и обеспечение различных требований к информационной и канальной скорости.

Список литературы

1. Жидков И.А. Оценка состояния канала связи по результатам декодирования помехозащищенного кода [Текст] / И.А.Жидков, А.В.Левенец, Ен Ун. Чье. – Х. : Измерительная техника, 2009. − №3(21).

2. Крылова В.А. Оценка информационного состояния канала связи в адаптивных системах кодирования/декодирования [Текст] / В.А. Крылова // Вестник НТУ «Харьковский политехнический институт». – Харьков. : НТУ «ХПИ», 2013. − №8(982). – С. 57

3. Cherubini G. Algorithms for communications systems and their applications/ Cherubini G., Benvenuto N.// Wiley. − 2003.

4. Dieterich H. Partitioning of Convolutional Codes and Applications/ Dieterich H. // Fortschritt-Bericht, VDI R. 10, 2000.

5. Jordan R., Johannesson R., Bossert M. On Nested Convolutional Codes and their application to woven codes/ Jordan R.// IEEE Trans on Inform Theory, Volume 50 Issue 2, February, 2004.− P. 380-384.