

Т.С. Филиппова, В.В. Хромов**ОЦЕНКА ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК
ПРОТОКОЛОВ КАНАЛЬНОГО УРОВНЯ**

Филиппова Татьяна Сергеевна, окончила факультет прикладной математики – процессов управления Санкт-Петербургского государственного университета. Ведущий инженер ОАО «НПО «Импульс». Имеет статьи в области алгоритмов передачи данных. [e-mail: tatyana.philippova@gmail.com].

Хромов Валентин Васильевич, кандидат технических наук, окончил радиотехнический факультет Ленинградского политехнического института. Доцент Санкт-Петербургского политехнического университета. Имеет статьи, изобретения в области помехоустойчивого кодирования и передачи данных. [e-mail: khromov1936@mail.ru].

Аннотация

Известны системы кодирования и декодирования с исправлением ошибок, использующие сложные кодовые конструкции, такие как коды – произведения двух линейных кодов с различными кодовыми расстояниями и сверткой части кодированной информации с третьим линейным кодом, либо многоуровневое кодирование относительно слабым кодом с исправлением ошибок с последующим разделением избыточных символов на части и кодированием каждой из этих частей своим кодом с исправлением ошибок. К одним из недостатков этих способов относятся сложность реализации метода и ориентация на передачу потока сообщений. В данной статье будет рассмотрен более простой метод передачи информации, который позволит решить еще и задачу снижения времени передачи за счет использования трех кодов, снижающих вероятность ошибочного приема.

Ключевые слова: блочные коды Боуза-Чоудхури-Хокенгема, Рида-Соломона, Голея, протокол передачи данных.

Введение

При передаче данных в каналах с обратной связью ошибки обычно исправляют, используя механизм переспроса кадров, в которых обнаружены ошибки. Примером такого протокола канального уровня является протокол High-level Data Link Control (HDLC). Хотя HDLC был разработан в 70-х годах XX века, он используется и по сей день (в несколько модифицированной форме) в качестве транспортного протокола для сети Integrated Services Digital Network (ISDN), протокола канального уровня передачи данных в виде пакетов, соответствующих стандарту X.25, и в качестве протокола канального уровня передачи данных, ориентированного на использование модемов [1]. Этот протокол эффективен по скорости, когда невелика канальная задержка и относительно мало ошибок в канале связи ($p < 0,005$).

При большой вероятности ошибки бита $p \approx 0,01 - 0,05$, что часто имеет место в КВ- и УКВ-каналах, используют не только переспрос, но и прямое исправление ошибок.

Предлагается новый протокол передачи данных, который может быть применен для передачи цифровой информации управления по радиоканалу, например в КВ- или УКВ-диапазоне частот. При передаче информации управления наиболее важной характеристикой является время задержки, а известные протоколы по этому критерию не оптимальны. Актуальными являются как задача защиты передаваемых сообщений от случайных одиночных и длинных пакетов ошибок, вызванных различными помехами в канале связи, так и минимизация времени доставки сообщений до получателя.

Протокол передачи с прямым исправлением ошибок

Интересен способ передачи с прямым исправлением ошибок, предложенный в [2]. Он заключается в том, что на передающей стороне к блоку исходной информации добавляют циклическую контрольную сумму (CRC) и полученный блок кодируют внешним кодом Рида-Соломона (РС) и затем внутренним расширенным кодом Голея. Закодированный блок модулируют и передают в канал. После демодулятора принятый блок информации декодируют внутренним кодом. Последовательность декодированных и стертых кодовых слов внутреннего кода запоминают. Если декодирование кодового слова внутреннего кода невозможно, то это некорректируемое кодовое слово сохраняют. Далее декодируют внешний код РС последовательности декодированных и стертых кодовых слов внутреннего кода, вычисляют и проверяют циклическую контрольную сумму упомянутой информационной последовательности. При положительном результате проверки CRC информацию выдают получателю сообщений. При отрицательном результате проверки производят восстановление стертых слов внутреннего кода последовательности. Восстановление стертых слов внутреннего кода и декодирование внешнего кода повторяют до тех пор, пока проверка CRC не даст положительного результата.

Недостатком этого способа является относительно большая временная задержка передачи информации из-за проведения декодирования только после приема всех бит сообщения, как информационных, так и проверочных. Это ограничивает возможность использования данного способа при передаче сообщений в виде команд управления.

Рассматриваемый в данной статье способ отличается тем, что используется более простой по технической реализации внешний код и предлагается другая последовательность передачи бит закодированного сообщения: сначала в канал связи передают все информационные биты, затем биты CRC, проверочные биты внешнего кода и далее проверочные биты внутреннего кода.

В качестве внешнего кода используется блок контроля на четность, в качестве внутреннего – код Голея (23, 12, 7), являющийся совершенным кодом [3]. Данный код позволяет исправлять все векторы ошибок веса 3 или меньшего на кодовом слове из 23 бит (можно использовать и другие блочные коды БЧХ).

Внешний код – это k -битный блок контроля на четность, формируемый следующим образом:

$$m_{J+1} = \sum_{j=1}^J m_j \bmod 2,$$

где $m_j = (a_{j1} a_{j2} \dots a_{js} \dots a_{jk})$,
 a_{js} – информационные биты,
 $j = 1, 2, \dots, J$,

$J = N/k$ – число блоков информации (каждый блок длиной k бит), составляющих передаваемое сообщение из N бит.

Циклический код CRC используется для обнаружения ошибок. Имеется методика выбора циклического кода для обнаружения ошибок, обеспечивающего требуемую вероятность ложного приема сообщения. В качестве примера в предлагаемом способе применяется CRC-16.

На приемной стороне по информационным битам вычисляется и проверяется циклическая контрольная сумма. В случае положительного результата сообщение k бит передается получателю. В противном случае исправляются ошибочные блоки k -битным блоком контроля на четность. Исправление j -го k -битного информационного блока посредством $(J + 1)$ -го блока внешнего кода производится путем замены j -го k -битного блока m_j на m_j^* :

$$m_j^* = m_{J+1} + \sum_{s=1, s \neq j}^J m_s,$$

где суммирование ведется по модулю 2,

$$m_s = (a_{s1} a_{s2} \dots a_{st} \dots a_{sk}),$$

a_{st} – информационные биты N -го блока.

Полученная последовательность из N бит снова проверяется с помощью CRC. При положительном результате проверки принятое сообщение передается получателю, а при отрицательном результате повторяется процедура восстановления блоков до тех пор, пока не будут проверены все J блоков. Если положительный результат проверки CRC все же отсутствует, выполняются операции исправления ошибок внутренним кодом Голея от $j = 1$ до $j = J$. Для этого объединяется j -я информационная k -битная последовательность с j -й проверочной последовательностью кода Голея и декодируется j -й блок. В случае исправления выявленных ошибок вновь выполняется процедура проверки CRC, а при отрицательном результате продолжается операция исправления ошибок в последующих блоках до $j = J$.

Суть предлагаемого протокола передачи данных поясняется системой кодирования / декодирования информации, представленной на рисунке 1. Используются последовательно соединенные блоки: 1 – вычисления и добавления циклической контрольной суммы, 2 – кодирования информации внешним кодом (код контроля четности), 3 – кодирования внутренним кодом, 4 – модулятора, 5 – канала связи,

6 – демодулятора, 7 – вычисления и проверки циклической контрольной суммы, 8 – декодирования внешним кодом (восстановление информационных бит внешним кодом контроля четности), 9 – исправления ошибок внутренним кодом. Блок 7 вычисления и проверки CRC имеет три выхода, второй выход задействуется после приема бит информации и проверочных бит внешнего кода, а третий выход – по мере приема проверочных бит внутреннего кода.

Расчет вероятностно-временных характеристик

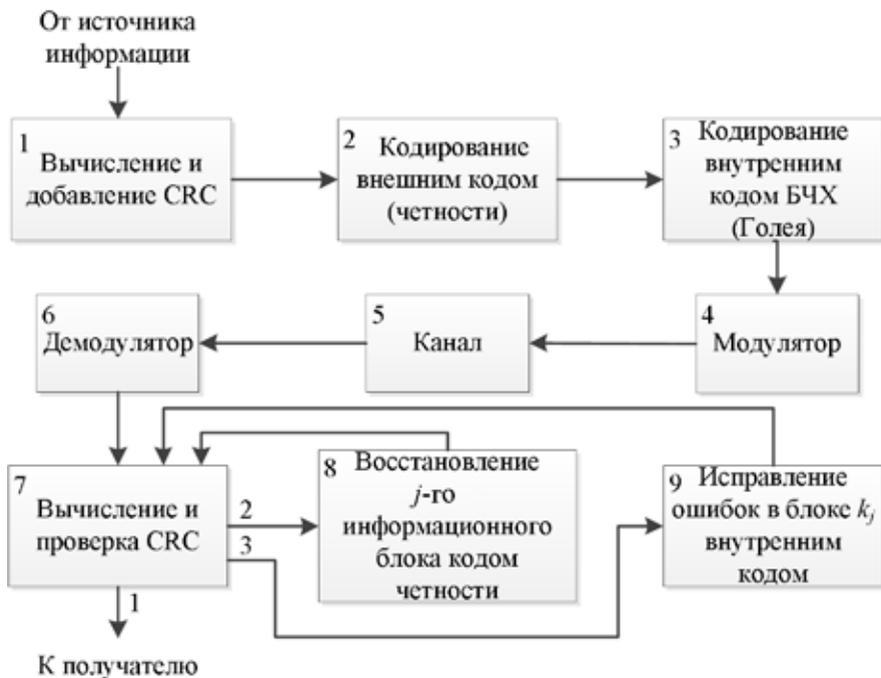


Рис. 1. Система кодирования / декодирования информации

Решение о корректной доставке сообщения может быть принято на разных этапах приема кадра.

На рисунке 2 приведены формулы для расчета вероятностных характеристик, основанные на теории вероятности и комбинаторике. Информационные блоки обозначены k_j , где j – номер блока от 1 до J ,

k – длина блока,

P_j – вероятность того, что сообщение будет принято после приема циклической контрольной суммы (или, что то же самое, после приема $k \cdot J$ бит) равна P_0^j , где P_0 – вероятность того, что на блоке длиной k бит нет ошибок,

J – количество информационных блоков, включая циклическую контрольную

сумму. Блок контроля четности обозначен $k(J+1)$, а вероятность приема сообщения после приема $k(J+1)$ бит равна $JP_0^{J-1}(1-P_0)$. Если проверка по CRC не прошла и ошибки не были исправлены с использованием блока контроля четности, то продолжается прием блоков Голя rj . Вероятности приема сообщения после получения каждого блока Голя указаны на рисунке 2, где P_u – вероятность того, что ошибки есть на блоке длиной k бит и они могут быть исправлены кодом Голя,

P_l – вероятность того, что на блоке длиной k бит есть ошибки и они не исправляются кодом Голя.

Для реальных коротковолновых каналов вероятность приема ошибочного бита P часто равна 0.01–0.05. При использовании предлагаемого способа возможен прием сообщения с задержками, приведенными ниже. В таблице 1 также приведены и вероятности приема с этими задержками.

Таблица 1

Вероятность приема сообщения с различными задержками в канале ДСК

№ п/п	Задержка бит	Вероятность приема P_j		
		$P = 0.01$	$P = 0.03$	$P = 0.05$
1	144	0.245	0.011	0.000
2	156	0.564	0.053	0.003
3	167	0.612	0.077	0.009
4	178	0.650	0.097	0.014
5	189	0.700	0.133	0.020
6	200	0.734	0.181	0.031
7	211	0.778	0.234	0.046
8	222	0.818	0.293	0.078
9	233	0.868	0.396	0.117
10	244	0.904	0.504	0.193
11	255	0.933	0.604	0.303
12	266	0.962	0.740	0.450
13	277	0.985	0.866	0.639
14	288	1.000	0.980	0.848
15	299	1.000	0.999	0.957

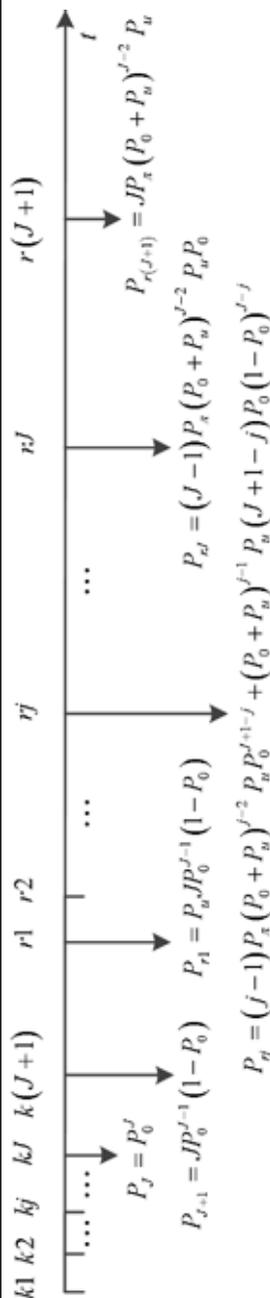


Рис. 2. Формулы для расчета вероятностных характеристик

Таблица 2

Вероятность приема сообщения
с различными задержками в канале ОПП

№ п/п	Задержка бит	Вероятность приема P_j		
		$P = 0.01$	$P = 0.03$	$P = 0.05$
1	144	0.449550	0.278721	0.217782
2	156	0.583417	0.348651	0.250749
3	167	0.608392	0.362637	0.261738
4	178	0.641359	0.382617	0.274725
5	189	0.655345	0.402597	0.289710
6	200	0.688312	0.427572	0.305694
7	211	0.725275	0.457542	0.324675
8	222	0.759241	0.486513	0.345654
9	233	0.800200	0.532468	0.363636
10	244	0.840160	0.579421	0.391608
11	255	0.871129	0.642358	0.430569
12	266	0.915085	0.711289	0.485514
13	277	0.961039	0.817183	0.543457
14	288	1.000000	0.916084	0.640360
15	299	1.000000	0.970030	0.733267

Вероятность и время задержки зависят от структуры потока ошибок в канале связи. В таблице 1 приведены результаты расчета для канала с независимыми ошибками (ДСК). В реальных каналах связи ошибки пакетируются. В таблице 2 приведены результаты, полученные моделированием потока ошибок в виде обобщенного Пуассоновского потока (ОПП) [4]. Для примера использованы следующие параметры канала: $a = 50$, $a = 18$, $a = 10$, при $\nu = 1.5$, которые задают эквивалентный ДСК-канал по вероятности ошибки $P = 0.01$, $P = 0.03$, $P = 0.05$ соответственно.

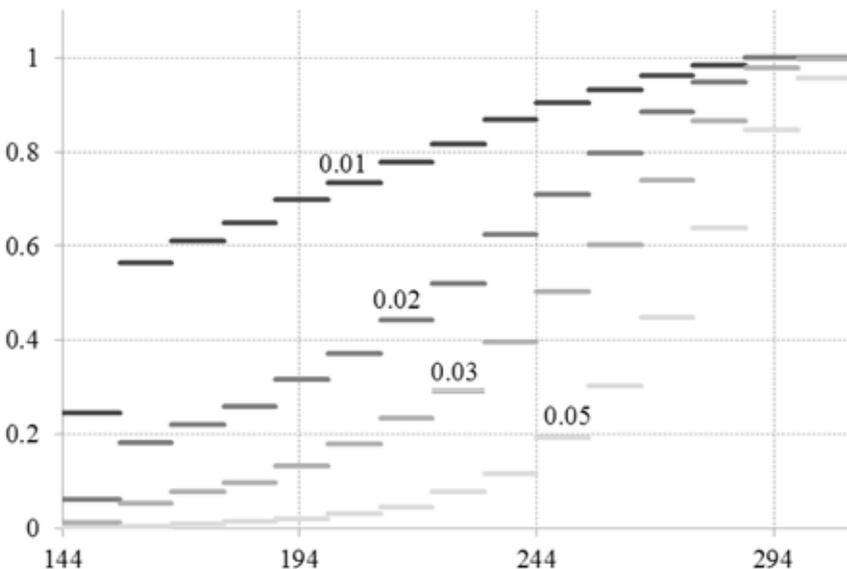


Рис. 3. Функция распределения времени задержки приема (ДСК)

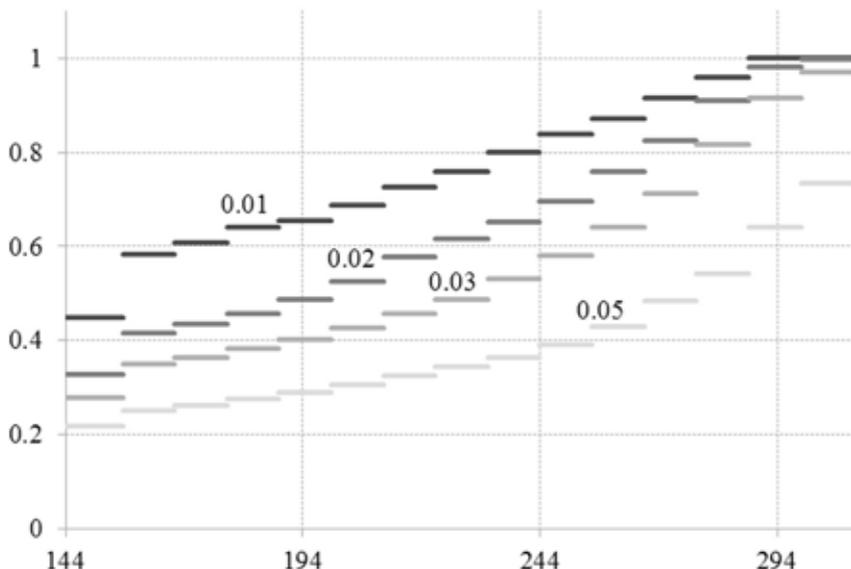


Рис. 4. Функция распределения времени задержки приема (ОПП)

На рисунке 3 представлен график функции распределения времени задержки приема в канале, полученный при моделировании потока ошибок в виде ДСК. Так, при вероятности приема ошибочного бита $P = 0.01$ из 1000 переданных сообщений нет ни одного неприятого, а при $P = 0.05$ нет ни одного сообщения, которое было бы принято сразу после проверки CRC.

На рисунке 4 представлен график функции распределения времени задержки приема при наличии пакетов ошибок в канале. В таком канале из-за группирования ошибок задержка в приеме сообщения в целом меньше, чем в канале с равномерным распределением ошибок.

Заключение

При моделировании выяснилось, что среднее время задержки приема сообщения в канале в виде ОПП меньше, чем в канале в виде ДСК на 7–17 процентов при вероятности ошибки на бит от 0.02 до 0.05.

Таким образом, можно констатировать, что особенно эффективным является применение предлагаемого способа кодирования с восстановлением блоков по блоку четности и исправлением независимых ошибок кодом Голя при передаче коротких команд управления по каналам, в которых вероятность ошибки бита сообщения меньше 0.03, что позволяет иметь распределенный по времени прием.

СПИСОК ЛИТЕРАТУРЫ

1. Хелд Г. Технологии передачи данных. – СПб. : Питер, К. : Издательская группа ВНУ, 2003. – С. 382–383.
2. Патент РФ № 2310273, МПК НОЗМ 13/0020.
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М. : Мир, 1986. – 576 с.
4. Аксенов Б.Е., Александров А.М. Повышение достоверности передачи информации в системах управления. – Л. : изд. ЛПИ им. М.И. Калинина, 1981. – 65 с.