УДК 004.052.42

Самофалов К. Г., чл.-кор. НАН Украины,
Хазем Мохд Саид Абдел Маджид Хатамлех,
Антоненко А. А.

МОДИФИКАЦИЯ КОНТРОЛЬНОЙ СУММЫ ДЛЯ ЭФФЕКТИВНОГО КОНТРОЛЯ ОШИБОК В КАНАЛАХ ПЕРЕДАЧИ ДАННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Национальный технический университет Украины "КПИ"

В статье предложен подход к повышению эффективности обнаружения ошибок с использованием контрольной суммы в каналах компьютерных сетей со спектральной модуляцией. Разработан способ кодирования компонент контрольной суммы. Показано, что предложенная модификация контрольной суммы обеспечивает большую надежность контроля ошибок по сравнению с CRC для каналов со спектральной модуляцией. При этом, реализация предлагаемого способа контроля ошибок с использованием контрольной суммы обеспечивает более высокую скорость выполнения операций контроля по сравнению с CRC.

Введение

Необходимость увеличения скорости передачи информации в компьютерных сетях и системах телекоммуникаций стимулирует расширение использования каналов с эффективной спектральной модуляцией сигналов. В таких каналах, группа смежных бит передаваемых цифровых данных модулируется одним канальным сигналом и при возникновении ошибки передачи такого сигнала возникает потенциальная опасность искажения группы бит.

С другой стороны, рост скорости передачи информации в каналах с эффективной спектральной модуляцией сигналов, обусловленный быстрым совершенствованием цифровых фильтров имеет следствием рост числа ошибок передачи канальных символов, вызванных межсимвольной интерференцией. Характерное для настоящего времени динамичное расширение использования средств мобильной связи имеет следствием многократное увеличение интенсивности высокочастотных полей в окружающем пространстве и, соответственно, увеличение уровня радиопомех в каналах передачи цифровой информации, что вызывает рост ошибок передачи канальных сигналов.

Таким образом, на современном этапе развития систем передачи цифровых данных компьютерных сетей обостряется проблема обеспечения надежности передачи информации в каналах со спектральной модуляцией. Важной составляющей проблемы обеспечения надежности передачи данных в компьютерных сетях является контроль возникающих ошибок.

Это обуславливает актуальность и практическую важность разработки новых методов и средств повышения надежности контроля ошибок при передаче цифровых данных в каналах компьютерных сетей со спектральной модуляцией.

Методы контроля ошибок при передаче данных в сетях и анализ их эффективности для каналов со спектральной модуляцией

В компьютерных сетях информация чаще всего передается блоками, соответственно, наибольшее распространение получили методы блокового контроля ошибок – *CRC* (*Cyclic Redundancy Code*) и контрольная сумма (*CS*).

Основными критериями эффективности контроля ошибок в компьютерных сетях являются надежность обнаружения ошибок различных классов и время, затрачиваемое на выполнение операций, связанных с их обнаружением.

CRC обнаруживает все битовые ошибки нечетной кратности, все 2-кратные ошибки, "пачки" ошибок, если их длина не превышает степень образующего полинома *CRC* [3]. Существенным

недостатком *CRC* является низкое быстродействие, связанное с тем, что операция формирования остатка выполняется побитно. Для устранения этого недостатка в последние годы предложено ряд табличных схем вычисления остатка, которые выполняют операции над байтами и словами. Однако сложность табличной реализации достаточно высока [4].

CS обладает существенно меньшей надежностью контроля, обеспечивая гарантированное обнаружение только битовых ошибок нечетной кратности. Достоинством *CS* является высокая скорость операций контроля, обусловленная как простотой реализуемых в *CS* операций, так и возможностью их распараллеливания.

В современных цифровых каналах передачи информации компьютерных сетей широко используются специальные виды модуляции, обеспечивающие эффективное использование полосы частот. Такие виды модуляции призваны ослабить проблему спектральной перегрузки каналов и соответственно называются спектрально эффективными видами модуляции [2].

Основной особенностью этих видов модуляции является то, что передаваемый по каналу символ принадлежит алфавиту из M символов, что позволяет предавать $k=\log_2 M$ битов за каждый символьный интервал. Это позволяет в k раз повысить скорость передачи цифровой информации. Соответственно значение k называется эффективностью передачи сигналов. К настоящему времени разработаны и активно используются несколько видов такой модуляции, которые ориентированы на различные виды каналов (телефонные, радиоканалы). Параметры большинства из них фиксированы соответствующими протоколами передачи цифровой информации.

Наиболее известным видом спектрально эффективной модуляции является квадратурно-амплитудная модуляция (*quadrature amplitude modulation – QAM*). Существует ряд модификаций *QAM*, отличающихся значениями эффективности k передачи сигналов, лежащих в интервале от 2-х до 10. Так, стандартизированный протокол телефонных модемов V.32 предусматривает использование *QAM* с k=4, протокол V.90 предусматривает применение *QAM* со значением k равным 10 [4].

При возникновении ошибки передачи канального сигнала потенциально могут быть подвержены искажению k бит цифрового кода. Если рассматривать модель канала, в котором предполагается наличие лишь гауссова шума, то возникновение ошибки передачи канального сигнала будет иметь следствием искажение только одного из k бит [1]. Это обусловлено тем, что сигнал *QAM* состоит из двух независимо амплитудно-модулированных несущих. Одна модулирует амплитуду косинусоидальной функции на уровни +1 и –1, а другая – аналогичным образом синусоидальную функцию. В теоретической модели сигналы в каждой из этих двух несущих независимо возмущаются гауссовым шумом. Это означает, что вероятность ошибки по каждой из несущей независима и соответствует бинарной модели. В рамках каждой несущей для амплитудной модуляции используется код Грея – соответственно, ошибка приема амплитуды, вызванная гауссовым шумом будет иметь следствием изменение разрядов кода, причем вероятности количества искаженных бит также подчинены бинарному закону. Таким образом, если рассматривать гауссову модель канала *QAM*, то, с точки зрения возникновения ошибок передачи битов, такой канал идентичен бинарному симметричному каналу.

На практике возникновение ошибок передачи канального символа вызывается рядом факторов (наличие внешних помех, межсимвольная интерференция, наложение отраженных сигналов) и носит более сложный характер [2]. То есть, при ошибках передачи канального символа, может измениться более одного бита k–разрядного кода, кодируемого канальным символом. При этом, закон распределения вероятностей искажения k–разрядного кода при ошибках передачи канального

символа зависит от многих факторов и носит сложный характер. Это важное обстоятельство должно учитываться при организации обнаружения ошибок передачи цифровой информации в каналах компьютерных сетей со спектрально эффективными видами модуляции.

Очевидно, что одиночная ошибка передачи канального символа, вызывающая искажения от одного до k рядом локализованных бит будет всегда обнаруживаться как обычной контрольной суммой, так и *CRC*.

Двойная ошибка передачи канального символа, при условии, что она будет иметь следствием изменение четного числа бит, причем это число больше 2-х, не всегда обнаруживается как обычной *CS*, так и *CRC*.

Например, если при контроле ошибок в 16-*QAM*-канале (k=4) с помощью *CRC* в качестве делителя используется стандартизированный полином *CRC*-16, равный $x^{16}+x^{15}+x^2+1$ (шестнадцатеричное представление имеет вид: G=18005h), то вектор ошибок E=0C000000Fh, содержащий две ненулевые тетрады может быть представлен в виде: $E = G + 2 \cdot G + 16 \cdot G$, то есть вектор E ошибки нацело делится на образующий полином CRC – G: E mod G=0. Это означает, что такая двойная ошибка передачи модулированного сигнала не будет обнаружена *CRC*.

Ошибки передачи канального символа большей кратности – $h \geq 2$, которые потенциально могут вызвать искажения от h до $k \cdot h$ бит также не всегда обнаруживаются *CRC* и обычной *CS*. С учетом того, что все ошибки нечетной кратности выявляются *CRC*, вероятность P_h необнаружения таких ошибок *CRC* с образующим полиномом степени L_{CRC} определяется выражением [4]:

$$P_h = 2^{-L_{CRC}}.$$

Как указывалось выше, в реальных каналах передачи цифровой информации со спектрально эффективной модуляцией ошибки передачи модулированных сигналов вызываются различными причинами и вероятности их появления имеют распределение, близкое к биномиальному [2].

Наиболее распространенные на практике средства обнаружения ошибок: *CRC* и обычная *CS* ориентированы на обнаружение одиночных и многократных битовых ошибок, возникающих в бинарных симметричных каналах и не обеспечивают гарантированного обнаружения многократных ошибок в каналах с модуляцией цифровых данных. В частности, они не обеспечивают гарантированного обнаружения наиболее частных после одиночных, двойных и тройных ошибок канальных сигналов. Кроме того, использование *CRC* сопряжено с проблемой эффективной вычислительной реализации операций контроля в темпе передачи информации, так как процедура вычисления синдрома ошибки в *CRC* носит принципиально последовательный характер.

Из приведенного следует, что современных условиях актуальной задачей является разработка средств повышения эффективности обнаружения ошибок в каналах со спектрально эффективной модуляцией цифровой информации, использование которых в компьютерных сетях постоянно расширяется.

Исходя из этого, целью настоящего исследования является разработка средств повышения надежности обнаружения многократных ошибок передачи канальных символов при использовании спектрально эффективной модуляции цифровой информации. При этом необходимо обеспечить возможность высокоскоростной реализации операций, связанных с контролем правильности передачи информации, за счет, в первую очередь, обеспечения возможности распараллеливания вычислений.

Разработка способа кодирования контрольной суммы для эффективного обнаружения ошибок в каналах со спектральной модуляцией

При создании средств эффективного обнаружения многократных ошибок передачи сигналов в каналах со спектраль-

ной модуляцией представляется целесообразным выбор в качестве основы контрольной суммы. Этот метод контроля обеспечивает широкие возможности для распараллеливания процессов контроля ошибок и, тем самым, решает, в принципиальном плане, проблему производительности обнаружения ошибок.

Контролируемый блок B состоит из m бит: $B=\{b_1,b_2,\ldots,b_m\}$, $b_l\in\{0,1\}$, $l=1,\ldots,m$. Контрольная сумма CS формируется в виде суммы по модулю два $t = m/n$ r-разрядных контрольных кодов $V_1,V_2,\ldots,V_t$: $CS=V_1\oplus V_2\oplus\ldots\oplus V_t$. Каждый j-тый из кодов – $V_j=\{v_1^j,v_2^j,\ldots,v_r^j\}$, $j\in\{1,2,\ldots,t\}$ зависит от группы из n смежных бит контролируемого блока, образующих символ $X_j=\{x_1,x_2,\ldots x_r\}=\{b_{(j-1)r+1},b_{(j-1)r+2},\ldots b_{jr}\}$: $V_j=F(X_j)$, где $F=\{f_1,f_2,\ldots,f_r\}$– система из r булевых функций $f_1,f_2,\ldots,f_r$, определенных на n двоичных переменных. Соответственно, блок B может быть представлен в виде последовательности $t = m/n$ символов: $B=\{X_1,X_2,\ldots,X_t\}$, $X_j\in\{0,1,\ldots,2^n-1\}$. Если обозначить через CS_S контрольную сумму, вычисляемую на передатчике $CS_s=V_{s1}\oplus V_{s2}\oplus\ldots\oplus V_{st}$, а через CS_r – контрольную сумму, вычисляемую на приемнике: $CS_r=V_{r1}\oplus V_{r2}\oplus\ldots\oplus V_{rt}$, то ошибка детектируется по ненулевому значению r-разрядного кода разности контрольных сумм $\Delta=CS_s\oplus CS_r=\bigoplus_{j=1}^{t}(V_{sj}\oplus V_{rj})$. В результате ошибок передачи символов по линии связи они искажаются, то есть при возникновении ошибки передачи j–того символа X_j их коды на приемнике и передатчике не одинаковы: $X_{sj}\neq X_{rj}$. Ошибка не обнаруживается, если существует множество Ξ из h символов блока B, таких, что $\forall l\in\Xi$: $X_{sl}\neq X_{rl}$:

$$\Delta=CS_s\oplus CS_r=\bigoplus_{j=1}^{t}(V_{sj}\oplus V_{rj})=\bigoplus_{l\in\Xi}(V_{sl}\oplus V_{rl})=0\cdot$$

Для обнаружения многократных ошибок передачи канальных сигналов при использовании модуляции, которые потенциально могут вызвать искажения k компактно локализованных битов предлагается длину n кода X выбрать равной длине k кода, который модулируется одним канальным сигналом: $k = n$.

Контрольный код V кода X предлагается формировать из k+1 битовых полей. Каждое i-тое из первых k-х полей, $i=1,\ldots,k$, представляет собой логическое произведение соответствующего i-того бита x_i текущего кода X контролируемого блока на q-разрядный код W_i : $V_i = x_i \cdot W_i$, где $q = \log_2 t$. Каждый из k кодов, используемых при формировании j–го контрольного кода V_j: $W_{ji} = \{w_{ji1},w_{ji2},\ldots,w_{jiq}\}$, $w_{jiy}\in\{0,1\}$, $\forall y\in\{1,\ldots,q\}$, $j\in\{1,\ldots,t\}$, $i\in\{1,\ldots,k\}$, однозначно связан с номером j кода (тетрады) контролируемого блока. Коды W_{j1}, W_{j2}, …, W_{jk} отличны между собой для всех $j\in\{1,\ldots,t\}$.

Одним из возможных вариантов формирования указанных кодов является использование q-разрядного сдвигового регистра с обратной связью, обеспечивающей максимальный период повторения. При этом коды W_{j1}, W_{j2}, …, W_{jk} формируются, как k последовательных значений кода на сдвиговом регистре. Для их хранения, кроме сдвигового регистра необходимо использовать еще k–1 q-разрядных фиксирующих регистров: $RG1,\ldots,RG.k$–1. Сдвиговый регистр может быть выполнен с использованием линейной функции обратной связи, то есть представляет собой классический *LSFR* [3]. Текущий код *LSFR* соответствует W_1, предыдущее значение *LSFR* сохраняется на регистре $RG1$ и соответствует коду W_2. Соответственно, значение кода на *LSFR* предшествующие текущему за два (W_3) и три сдвига (W_4) сохраняются на регистрах $RG2$ и $RG3$.

Последнее, (k+1)-е поле контрольного кода V состоит из k разрядов составляющих символ X: $V_{k+1} = X=\{x_1,x_2,\ldots x_k\}$. Таким образом, общая длина контрольного кода, а соответственно и модифицированной контрольной суммы составляет $L_V = L_{CS} = k\cdot(\log_2(m/k) + 1)$. Например, при длине блока в 2048 байт и использовании 16-*QAM* (k=4), разрядность контрольной суммы составит 4·(12+1) = 52.

Контрольная сумма CS состоит из k-ти полей: $(k+1)$ q-разрядных и одного k-разрядного: $CS = \{CS_1, CS_2, \ldots, CS_k, CS_{k+1}\}$. Каждое из этих полей представляет собой поразрядную сумму по модулю 2 соответствующих полей контрольного кода: $CS_l = \bigoplus_{j=1}^{t} V_{jl}, l = 1,\ldots,k$. Соответственно код Δ разности контрольных сумм передатчика CS_s и приемника CS_r также состоит из $k+1$ полей: $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_k, \Delta_{k+1}\}$: $\Delta_l = CS_{sl} \oplus CS_{rl}$, $l=1,\ldots,k+1$. Ошибка обнаруживается, если хотя бы одной из полей разности Δ не равно нулю.

Оценка надежности обнаружения ошибок передачи модулированных сигналов различной кратности

Поскольку последних k разряда контрольной суммы представляют собой сумму по модулю 2 одноименных бит символов контролируемого блока, то любая одиночная ошибка передачи модулированного сигнала, имеющая следствием искажение от одного до k битов одного символа будет обнаружена.

Предположим, что при передаче блока B имела место двойная ошибка передачи канального сигнала, в результате чего u-тый и g-тый символы: X_u и X_g отличаются на приемнике и передатчике. Обозначим через $X_{su}=\{x_{su1}, x_{su2}, \ldots, x_{suk}\}$ и $X_{ru}=\{x_{ru1}, x_{ru2}, \ldots, x_{ruk}\}$ u-тый символ соответственно на передатчике и приемнике. Обозначим через $X_{sg}=\{x_{sg1}, x_{sg2}, \ldots, x_{sgk}\}$ и $X_{rg}=\{x_{rg1}, x_{rg2}, \ldots, x_{rgk}\}$ g-тый символ соответственно на передатчике и приемнике.

Код i–того поля Δ_i, $i \in \{1,\ldots,k\}$ разности Δ контрольных сумм приемника и передатчика при ошибочной передаче u-того и g-того символов X_u, X_g может быть представлен в виде:

$$\Delta_i = (x_{sui} \oplus x_{rui}) \cdot W_{ui} \oplus (x_{sgi} \oplus x_{rgi}) \cdot W_{gi}.$$

Поскольку $W_{ui} \neq W_{gi}$, то во всех случая, кроме ситуации, когда i-тые биты на приемнике и передатчике равны: $x_{sui} = x_{rui}$ и $x_{sgi} = x_{rgi}$, код i–того поля Δ_i разности контрольных сумм приемника и передатчика не равен нулю: $\Delta_i \neq 0$ и соответственно, ошибочная передача двух кодов будет обнаружена. Однако, указанная исключительная ситуация не может одновременно иметь место для всех k полей $\Delta_1, \Delta_2, \ldots, \Delta_k$ разности контрольных сумм, поскольку в этом случае u-тый и g-тый коды на приемнике и передатчике равны: $X_{su} = X_{ru}$ и $X_{sg} = X_{rg}$, что противоречит принятому предположению о наличии ошибок в передаче этих кодов. Следовательно, предложенный способ формирования контрольной суммы всегда позволяет обнаруживать две ошибки при передаче канального символа с использованием эффективной спектральной модуляции, которые могут вызвать искажения от 2-х до $2 \cdot k$ бит контролируемого блока .

Например, пусть контролируемый блок состоит из 4 байтов и при его передаче используется модуляция 16-QAM (k=4). Общее число передаваемых групп битов (символов) составляет 8 (t=8). Соответственно q=3. Пусть последовательность кодов W формируется 3-разрядным сдвиговым регистром с функцией обратной связи $f(W) = w_1 \oplus w_3 \oplus w_2 \cdot w_3 \oplus 1$. При этом коды W генерируются в следующей последовательности: 0, 1, 2, 5, 3, 7, 6, 4. Пусть, в результате двух ошибок передачи квадратурно-модулированного сигнала искажены 2-й и 8-й группы символов, при этом во второй группе искажены биты x_1 и x_2, а в 8-й – все биты. Соответственно вектор ошибок имеет вид $E=0C000000Fh$. Для второй битовой группы $W_{21} = 1$, $W_{22} = 0$, $W_{23} = 4$, $W_{24} = 6$. Для восьмой битовой группы: $W_{81} = 4$, $W_{82} = 6$, $W_{83} = 7$, $W_{84} = 3$. Значение кода первого поля Δ_1 разности контрольной суммы приемника и передатчика определяется в виде:

$$\Delta_1 = \bigoplus_{j=1}^{8} (x_{sj1} \oplus x_{rj1}) \cdot W_{j1} = W_{21} \oplus W_{81} = 001 \oplus 100 = 101.$$

Аналогично:

$$\Delta_2 = \bigoplus_{j=1}^{8} (x_{sj2} \oplus x_{rj2}) \cdot W_{j2} = W_{22} \oplus W_{82} = 000 \oplus 110 = 110,$$

$$\Delta_3 = \bigoplus_{j=1}^{8} (x_{sj3} \oplus x_{rj3}) \cdot W_{j3} = W_{83} = 111,$$

$$\Delta_4 = \bigoplus_{j=1}^{8} (x_{sj4} \oplus x_{rj4}) \cdot W_{j4} = W_{84} = 011.$$

Значение кода пятого поля Δ_5 разности контрольной суммы приемника и передатчика равно:

$$\Delta_5 = \bigoplus_{j=1}^{8}(X_{sj} \oplus X_{rj}) = \bigoplus_{j=1}^{8} E_j = 1100 \oplus 1111 = 0011.$$

Таким образом, все поля Δ – разности контрольной суммы приемника и передатчика не равны нулю, соответственно рассматриваемая в рамках настоящего примера двукратная ошибка передачи модулированного сигнала, вызвавшая искажение 6-ти бит контролируемого блока обнаруживается, в отличие от *CRC*-16, который эту ошибку не обнаруживает.

При возникновении трехкратной ошибки код Δ разности контрольных сумм передатчика и приемника также не будет равен нулю. Пусть ошибочно переданы коды X_u, X_g, X_e с номерами u,g и e. Каждая i-тая компонента $(k+1)$-го поля $\Delta_{k+1}= \{\delta_{(k+1).1},\delta_{(k+1).2},\ldots,\delta_{(k+1).k}\}$ кода разности контрольных сумм будет равно:

$$\delta_{(k+1)i} = (x_{sui} \oplus x_{rui}) \oplus (x_{sgi} \oplus x_{rgi}) \oplus (x_{sei} \oplus x_{rgi}).$$

Учитывая, что коды, входящие в каждую из пар $<X_{su}, X_{ru}>$, $<X_{sg}, X_{rg}>$ и $<X_{se}, X_{re}>$ различны, то есть $X_{su} \neq X_{ru}$, $X_{sg} \neq X_{rg}$ и $X_{se} \neq X_{re}$, равенство нулю всех битовых компонент $\delta_{(k+1).1}$, $\delta_{(k+1).2},\ldots,\delta_{(k+1).k}$ поля Δ_5 возможно только в случае, если существует бит с номером $\eta \in \{1,\ldots,k\}$ такой, что его значения отличаются на приемнике и передатчике для пары из кодов X_u, X_g, X_e и в одном из этих кодов совпадают. Без нарушения общности можно полагать, что $x_{su\eta} \neq x_{ru\eta}$, $x_{sg\eta} \neq x_{rg\eta}$ и $x_{se\eta} = x_{re\eta}$. Тогда поле Δ_η разности контрольных сумм передатчика и приемника может быть представлено в виде:

$$\Delta_\eta = (x_{su\eta} \oplus x_{ru\eta}) \cdot W_{u\eta} \oplus (x_{sg\eta} \oplus x_{rg\eta}) \cdot W_{g\eta} \oplus (x_{se\eta} \oplus x_{re\eta}) \cdot W_{e\eta} = W_{u\eta} \oplus W_{g\eta}.$$

Поскольку $W_{u\eta} \neq W_{g\eta}$, то в случае равенства поля Δ_k разности контрольных сумм передатчика и приемника нулю: $\Delta_k = 0$, его поле $\Delta_\eta \neq 0$, следовательно, $\Delta \neq 0$. Таким образом, предложенный способ формирования контрольной суммы всегда позволяет обнаруживать три ошибки при передаче канального символа с использованием эффективной спектральной модуляции, которые могут вызвать искажения от 3-х до $3 \cdot k$ бит контролируемого блока. Вполне очевидно, что использование CRC не обеспечивает такой возможности и, следовательно, обладает меньшей надежностью обнаружения трехкратной ошибки передачи модулированного сигнала.

При возникновении ошибки передачи 4-х модулированных сигналов искажаются биты 4-х битовых групп блока. Потенциальная опасность необнаружения искажений в 4-х битовых группах при использовании модифицированной контрольной суммы, существует только в том случае, если в каждой из четырех групп искажению подверглись одни и те же биты. Если один из битов изменился, в результате ошибки, только в трех битовых группах или только в одной, то $\Delta_{k+1} \neq 0$. Если в результате ошибок один бит, например η-тый, $\eta \in \{1,\ldots,k\}$, исказился только в двух битовых группах, то $\Delta_\eta \neq 0$.

Для 4-х k-разрядных кодовых групп существует $2^{k \cdot 4}$ вариантов локализации битовых ошибок. При этом существует k вариантов локализации искаженных бит, когда искажен один бит всех 4-х групп, $\binom{k}{2}$ вариантов локализации искаженных бит когда искажены 2 бита во всех 4-х группах. Аналогично, при искажении i одноименных бит во всех 4-х группах существует $\binom{k}{i}$ вариантов локализации ошибок $(1 \leq i \leq k)$.

Если искажается только один бит во всех 4-х битовых группах, например η-тый, $\eta \in \{1,\ldots,k\}$, то соответствующее η-тое поле Δ_η разности контрольных сумм передатчика и приемника представляет собой поразрядную сумму по модулю 2 4-х различных q-разрядных кодов W. Вероятность того, что эта сумма равна нулю составляет 2^{-q}. Если искажаются два бита во всех 4-х группах, то два соответствующих поля разности Δ контрольных сумм приемника и передатчика являются суммой по модулю 2 4-хразличных q–разрядных кодов W; вероятность того, что

при этом оба упомянутых поля равны нулю составляет $2^{-2 \cdot q}$. Аналогично, вероятность того, что при искажении i, $i \in \{1,\ldots,k\}$, одноименных бит во всех 4-х битовых группах, соответствующие поля разности Δ равны нулю составляет $2^{-i \cdot q}$.

Таким образом, вероятность P_4 того, что искажения контролируемого блока, вызванные 4-х кратной ошибкой модулированного сигнала не будет обнаружена модифицированной контрольной суммой определяется следующим выражением:

$$P_4 = 2^{-k \cdot 4} \cdot \sum_{i=1}^{k} \binom{k}{i} \cdot 2^{-i \cdot q} = 2^{-k \cdot 4} \cdot \left[(1+2^{-q})^k - 1\right] =$$

$$= 2^{-k \cdot 4} \cdot \left[\left(\frac{1+t}{t}\right)^k - 1\right].$$

Например, при передаче 2048 байт и использовании 16-*QAM* (k=4), t=4096 и значение вероятности P_4 того, что ошибка в передаче 4-х канальных сигналов не будет обнаружена при использовании предлагаемого способа формирования контрольной суммы составляет $1.5 \cdot 10^{-8}$.

Если число d ошибок передачи канальных сигналов больше 4-х, то они потенциально могут быть не обнаружены только тогда, когда одноименные биты в d группах, подвергшиеся искажению локализованы в четном числе n_e групп, причем $d \geq n_e \geq 4$.

Вероятность того, что в d группах искажен только один бит (одноименный во всех группах) отлична от нуля только для четных значений d и равна $2^{-d \cdot k}$. Если считать, что искажен только бит с номером η во всех группах ($\eta \in \{1,\ldots,k\}$), то поле Δ_η представляет собой сумму по модулю 2 d q-разрядных кодов W, отличных между собой. Вероятность того, что поле $\Delta_\eta = 0$ равна 2^{-q}. Поэтому, вероятность того, что ошибки, вызвавшие искажение одноименного разряда всех d групп будет не обнаружена равна $2^{-d \cdot k} \cdot 2^{-q}$.

При искажении i бит ($1 < i \leq k$) в d группах в результате d–кратной ошибки передачи модулированного сигнала, ошибка может не быть обнаружена только в ситуации, когда каждый из i бит искажен в четном, большем 2-х числе групп, причем в каждой из групп искажен хотя бы один бит. Количество вариантов выбора четного числа, большего 2-х из d равно $d/2$-1. При фиксированном номере бита в группе, для каждого варианта выбора четного числа l групп, в которых искажается этот бит возможно $\binom{d}{l}$ вариантов локализации искажений по группам. Общее число вариантов локализации ошибок в фиксированном бите, число которых четно и больше 2-х по d группам равно

$$N_d = \binom{d}{4} + \binom{d}{6} + \ldots + \binom{d}{d_p} = 2^{d-1} - \binom{d}{2} - 1,$$

где $d_p = d - d \bmod 2$. Общее число вариантов локализации ошибок в i битах по d группам, при условии, что число групп, в которых искажен каждый из i бит четно и больше 2-х равно N_d^i. Учитывая, что общее число вариантов локализации ошибок по d группам в фиксированном бите равно 2^d, а также то, что число вариантов распределения i ошибок по k разрядам равно $\binom{k}{i}$, вероятность того, что при искажении i бит каждый из них проявляется в виде битовой ошибки в четном числе групп, большем 2-х определяется выражением: $\binom{k}{i} \cdot \frac{N_d^i}{2^{d \cdot k}}$. Очевидно что при выполнении указанных условий поле $\Delta_{k+l} = 0$, а каждое из полей Δ_ε разности контрольной суммы на приемнике и передатчике, номера которых соответствуют номерам i битов в которых произошли ошибки представляет собой сумму по модулю 2 различных q–разрядных кодов, поэтому, вероятность того, что все эти поля окажутся равными нулю и, соответственно, ошибки не будут обнаружены равна $2^{-i \cdot q}$. Таким образом, вероятность P_d того, что ошибка передачи d канальных сигналов (d>4), потенциально вызывающая искажения от d до $d \cdot k$ бит контролируемого блока, не обнаруживается предлагаемой модификацией контрольной суммы определяется следующим выражением:

$$P_d = 2^{-d\cdot k}\cdot\left[\frac{(d+1)\bmod 2}{t}+\sum_{i=2}^{k}\binom{k}{i}\cdot\left(\frac{2^{d-1}-0.5\cdot d\cdot(d-1)-1}{t}\right)^i\right]=$$

$$=2^{-d\cdot k}\cdot\left[\frac{(d+1)\bmod 2}{t}+\left(1+\frac{2^{d-1}-\binom{d}{2}-1}{t}\right)^k-k\cdot\frac{2^{d-1}-\binom{d}{2}}{t}-1\right].$$

В таблице 1 приведены численные значения вероятностей P_d для различных значений d – кратности ошибок передачи модулированного сигнала при передаче 2048 байт и использовании 16-*QAM* (k=4), t=4096.

Таблица 1

Зависимость вероятности P_d необнаружения ошибки передачи модулированного сигнала 16-*QAM* (k=4) от кратности ошибки d при длине контролируемого блока 2048 байт (t=4096)

D	P_d	D	P_d
5	$8.5\cdot10^{-12}$	6	$2.0\cdot10^{-11}$
7	$2.4\cdot10^{-12}$	8	$8.9\cdot10^{-13}$
9	$2.6\cdot10^{-13}$	10	$7.6\cdot10^{-14}$

Приведенные в таблице 1 данные свидетельствуют о том, что для ошибок кратности более 4-х, надежность обнаружения ошибок по предлагаемому способу близка к *CRC*, со степенью образующего полинома равной разрядности *CS*.

Выводы

В результате проведенного анализа эффективности обнаружения ошибок наиболее распространенной в компьютерных сетях технологии *CRC* в каналах со спектральной модуляцией показано, что она не позволяет обеспечить гарантированное обнаружение двукратных ошибок передачи канальных сигналов, вызывающих искажение более чем 4-х бит.

Разработан способ гарантированного обнаружения ошибок указанного класса на основе контрольных сумм. Способ предполагает раздельное формирование контрольных кодов для битовых групп кодов, соответствующих одному канальному символу с последующим суммированием по модулю 2 этих контрольных кодов. Это обеспечивает возможность распараллеливания вычисления модифицированной контрольной суммы и, таким образом, принципиально решает проблему достижения высокой производительности операций контроля ошибок.

Доказано, что предложенный способ позволяет гарантированно обнаруживать ошибки передачи канальных сигналов кратностью до 4-х, что которые потенциально могут вызвать искажения до $4\cdot k$ битовых ошибок. Все битовые ошибки такой кратности не обнаруживаются *CRC*. Следовательно, предложенный способ обеспечивает повышение эффективности обнаружения ошибок для широкого классе каналов передачи данных компьютерных сетей по сравнению с *CRC*, как в плане обеспечения большей надежности, так и в плане повышения производительности операций контроля ошибок.

Список литературы

1. *Али Тауфик Окла Аль-Хавальди.* Оптимизация кодирования эхокода при контроле ошибок передачи данных методом эхоплекса.// Вісник Національного технічного університету "КПІ". Інформатика, управління та обчислювальна техніка. – К.: ВЕК++, 2005. – №43. – С.181-195.

2. *Джонсон Г., Грэхем М.* Высокоскоростная передача цифровых данных. – М.: Вильямс, 2005. – 1016 с.

3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2004.– 1099 с.

4. *Таненбаум Э.* Компьютерные сети. – М.: Питер, 2003. – 991 с.

5. *Partrige C., Hughes J., Stone J.* Performance of Checksums and CRCs over Real Data.// Proc. SIGCOMM'95 Conf., ASM, 1995. – PP. 68-76.

6. *Хелд Г.* Технологии передачи данных. – М.: Питер. 2003. – 715 с.