УДК 004.056

Самофалов К.Г., чл.-кор. НАН Украины,
Абу-Усбах А.Н., к.т.н.,
Рябыкина В.А.

ОБНАРУЖЕНИЕ ЧЕТЫРЕХКРАТНЫХ ОШИБОК В ДВОИЧНОМ СИММЕТРИЧНОМ КАНАЛЕ С ИСПОЛЬЗОВАНИЕМ МИНИМАЛЬНОГО ЧИСЛА КОНТРОЛЬНЫХ РАЗРЯДОВ

Национальный технический университет Украины «КПИ»

Предложен способ гарантированного обнаружения четырех ошибок в двоичном симметричном канале с использованием нелинейных взвешенных контрольных сумм. Предложенный способ предполагает формирование компонент контрольной суммы с использованием специальных нелинейных булевых преобразований. Показано что предложенный способ гарантирует обнаружения более широкого класса ошибок и обеспечивает большую скорость контроля при аппаратной реализации по сравнению с CRC.

Введение

Краеугольным фактором совреме - нного этапа развития инфор-мационной интеграции является прогресс средств передачи данных. Наряду с повышением пропускной способности современных средств телекоммуникаций, важное значение в их совершенствовании принадлежит повышению надежности передачи данных.

Современный этап развития средств телекоммуникаций связан с рядом факторов, негативно влияющих на достоверность передачи информации. Так, повышение скорости передачи сопряжено с ростом ошибок, вызванной явлениями межсигнальной интерференцией [1], интенсивное расширение использования эфирных каналов имеет следствием рост числа ошибок, вызванных внешними помехами. С другой стороны, непрерывное расширение сферы использования информационных технологий, в том числе в сферах, связанных с техногенными или иными рисками, диктует необходимость радикального повышения надежности средств передачи данных.

Известно, что обеспечение высокой достоверности передачи данных достигается как за счет повышения надежности работы канала, так и за счет совершенствования средств контроля и коррекции возникающих при передаче ошибок.

Таким образом, задача повышения эффективности контроля ошибок передачи данных является актуальной и важной для современного этапа развития информационных технологий.

Анализ проблемы обнаружения четырех кратных ошибок

Одним из важнейших направлений повышения эффективности средств обнаружения ошибок передачи данных в современных условиях является расширение класса гарантированно обнаруживаемых ошибок. Важность этого направления повышения эффективности средств контроля ошибок обусловлена, в первую очередь, ростом объемов передаваемой в компьютерных системах и сетях информации.

Для значительной части современных каналов передачи данных характерно использование низкочастотная передача цифровой информации. При такой передаче данных, они кодируются перепадами напряжения, которое может принимать два уровня.

В теоретическом плане такие каналы соответствуют модели двоичного сим-метриичного канала. Доминирующим типом ошибок для указанного канала являются независимые друг от друга ошибки относительно небольшой кратности. Поскольку ошибки нечетной кратности гарантированно обнаруживаются с использованием бита четности,

наиболее важным типом необнаруживаемых ошибок являются ошибки четной малой кратности: 2 и 4.

Основными источниками ошибок являются:

- тепловой шум, вызывается тепловым движением электронов во всех проводящих элементах. Такой шум носит полностью случайный характер. Спектральная плотность мощности шума постоянна для всех частот. Тепловой шум вызывает одиночные ошибки [2];

- межсимвольная интерференция – влия-ние предшествующего импульсного сигнала на прием последующего. Вследствие большой длины линии передачи и ограниченной мощности каскада формирования передаваемого импульса возникает явление размывания (скалывания) фронтов [3]. В результате принятые импульсы перекрываются; хвост одного импульса "размывается" на соседние символьные интервалы, что мешает процессу их детектирования. Даже при отсутствии теплового шума, неидеальная фильтрация, ограничение полосы системы и замирание в каналах приводят к возникновению межсимвольной интерференции [2]. Интенсивность ошибок, вызванных межсимвольной интерференцией существенно зависит от скорости передачи сигналов: чем больше скорость – тем большая вероятность наложения смежных импульсных сигналов. В современных условиях роста скорости передачи информации, межсимвольная интерференция является одним из наиболее доминирующих факторов возникновения ошибок [1]. Такие ошибки носят одиночный характер [4];

- внешние помехи – сигналы, генери-руемые в проводнике под воздействием внешних электромагнитных полей. В современных условиях интенсивность внешних электромагнитных полей непрерывно возрастает. Это вызвано расширяющимся использованием средств мобильной связи, а также компьютерных средств беспроводной передачи информации. Учитывая близость источ-ников электромагнитного излучения к проводным линиям передачи данных вычислительных систем и сетей, рассматриваемый источник ошибок представляется весомым [3] и имеет место тенденция к росту числа ошибок, вызванных внешними помехами. Влияние внешних помех на величину ошибки зависит от интенсивности внешнего электромагнитного поля. Анализ, проведенный в [5] показывает, что электромагнитные поля средств беспроводной передачи данных вызывают импульсные помехи, приводящие к одиночным ошибкам в последовательных линиях передачи данных и групповым ошибкам в параллельных. Другим источником внешних помех являются атмосферные явления. Вызванные атмосферными явлениями помехи имеют существенно большую длительность и приводят к появлению "пачек" ошибок [5].

Наиболее распространенным способом контроля правильности передачи данных является *CRC* (cyclic redundancy code, циклический избыточный код). Этот вид контроля регламентирован для использования в последовательных портах компьютеров, в частности, в порте *USB* [4]. Протоколами *HDLC, SDLC* установлено использование *CRC* для контроля ошибок при передачи информации в сетях [2]. *CRC* относятся к средствам блокового контроля. Если передаваемому блоку B соответствует полином m-степени $B(x)=b_1 \cdot x^m + b_2 \cdot x^{m-1} + \ldots + b_{m-1} \cdot x + b_0$, то контрольный код *CRC* формируется как результат деления полинома $B(X) \cdot x^k$ на образующий полином CRC степени k: $P(x) = x^k + p_{k-1} \cdot x^{k-1} + \ldots + p_1 \cdot x + p_0$.

Ошибки при передаче блока данных не обнаруживается, если полином $E(X)$, соответствующий вектору ошибки делится на образующий полином $P(X)$ *CRC* без остатка. Показано [4], что все указанные ниже ошибки не делятся на соответствующим образом выбранный полином $P(X)$, а следовательно, они гарантированно обнаруживаются:

- все отдельные однобитовые

ошибки;

- все двукратные, если полином $P(X)$ содержит не менее трех единиц;

- любое нечетное количество ошибок, если полином $P(X)$ содержит множитель $(X+1)$.

- любая группа ошибок, длина которой меньше длины полинома-делителя;

Кроме того, показано [4], что если все распределения ошибок считаются равновероятными, то вероятность P_{CRC} того, что эти ошибки не будут обнаружены с использованием *CRC* с образующим полиномом $P(X)$ степени n определяется следующей формулой:

$$P_{CRC} = \frac{1}{2^n}. \qquad (1)$$

Таким образом, наиболее распространенный вид контроля ошибок - *CRC* не гарантирует обнаружения четырехкратных ошибок.

Вместе с тем, существует ряд методов обнаружения ошибок, которые гарантируют обнаружения четырехкратных ошибок. Для анализа их эффективности представляется целесообразным выполнить оценку теоретически минимального числа контрольных разрядов, необходимых для решения задачи гарантированного детектирования четырехкратных ошибок.

Очевидно, что для гарантированного обнаружения четырехкратных ошибок, возникающих при передаче m-разрядного информационного блока, минимальное число k контрольных разрядов должно быть таким, чтобы наименьшее хемминговo расстояние между $(m+k)$-битовыми передаваемыми кодами равнялось пяти. Это означает, что если выбрать любой из 2^m возможных кодов m-битового информационного блока и обозначить через ξ соответствующий ему передаваемый $(m+k)$-разрядный код, то существует m соседних кодов, отличающего от ξ в одном информационном разряде. Для того, чтобы хеммингово расстояние между разрешенными кодами было равным пяти, необходимо, чтобы для кода ξ существовало $r_1 = m$ недопустимых кодов, отличающихся от ξ только в одном разряде, $r_2 = m\cdot(m-1)/2 \approx m^2/2$ кодов, отличающихся от ξ в двух разрядах. Кроме того, должно существовать $r_3 = m\cdot(m-1)\cdot(m-2)/3! \approx m^3/6$ кодов, отличающихся от ξ и соседних с ним m кодов в трех разрядах. Таким образом, для кода ξ должно существовать $r_1 + r_2 + r_3/m$ недопустимых кодов. Из этого следует, что минимальное число k контрольных разрядов, обеспечивающих гарантированное обнаружение четырехкратных ошибок в m-битовом информационном коде, соответствует минимальному k, при котором выполняется условие:

$$2^{m+k} \geq 2^m \cdot (1 + m + \frac{m^2}{2} + \frac{m^2}{6}). \qquad (2)$$

После сокращения и логарифмирования обоих частей неравенства (2) минимальное k можно представить в виде:

$$k \geq \left\lfloor \log_2 (1 + m + \frac{m^2}{2} + \frac{m^3}{6}) \right\rfloor. \qquad (3)$$

Поскольку

$\frac{m^2}{2} > 1 + m + \frac{m^2}{6}$, то справедливо:

$$k = \left\lfloor \log_2 2 \cdot \frac{m^2}{2} \right\rfloor = 2 \cdot \log_2 m. \qquad (4)$$

Так, например, для гарантированного обнаружения четырехкратных ошибок в блоке длиной 1 Кбит (m=1024) требуется согласно (4) k=2·log$_2$1024 = 20 контрольных разрядов.

Так, для решения этой задачи с использованием трехмерных кодов Хемминга требуется $k_3 = 3\cdot(\sqrt[3]{m})^2 = 3\cdot m^{2/3}$. Это означает, что для гарантированного обнаружения четырехкратных ошибок в блоке длиной 1 Кбит требуется 305 контрольных разрядов, что более чем на порядок превышает определенный выражением (4) теоретический минимум.

Существует способ [4] гарантированного обнаружения четырех кратных ошибок с использованием взвешенных контрольных кодов. Сущность этого способа состоит в том, что контрольный код V передаваемого блока B формируется в виде конкатенации суммы по модулю 2 всех битов блока и суммы по модулю 2 логических произведений битов блока на опорные коды W_1, W_2 ,$\ldots W_n$ в виде:

$$V = \bigoplus_{j=1}^{m} (b_j \cdot W_j \mid b_j). \qquad (5)$$

Опорные коды W_1, W_2 ,$\ldots W_n$ по числу бит в передаваемом блоке B формируются таким образом, чтобы сумма по модулю 2 любого их подмножества, включающего не более четырех кодов не равна нулю. При возникновении не более, чем четырех ошибок, разность контрольных кодов приемника и передатчика будет равна сумме по модулю 2 опорных кодов, соответствующих переданных с ошибками битов блока. Такая ошибка всегда будет обнаруживаться в силу свойств опорных кодов.

Число k_0 контрольных разрядов, используемых для обнаружения четырех кратной ошибки определяется следующей формулой [4]:

$$k_0 = 2.3 \cdot \log_2 m. \qquad (6)$$

Сравнение значения k_0, определяемого формулой (6) со значением теоретического минимума (4) показывает, что известный способ, использующий опорные весовые коэффициенты не обеспечивает решение коррекции четырехкратной ошибки с минимальным числом контрольных разрядов.

Целью исследований является создание метода, использующего для гарантированного обнаружения четырех ошибок в двоичном симметричном канале теоретически минимального числа контрольных разрядов.

Использование нелинейных кодов для обнаружения ошибок

Проведенный анализ показал, что достичь поставленной цели можно только с использованием нелинейных преобразований.

В качестве способа применения такого преобразования предлагается модификация взвешенной контрольной суммы, состоящей из трех компонент. Первая компонента C_1 взвешенной контрольной суммы информационного блока B представляет собой сумму по модулю 2 логических произведений битов блока на их порядковые номера в блоке:

$$C_1 = 1 \cdot b_1 \oplus 2 \cdot b_2 \oplus \ldots \oplus m \cdot b_m. \qquad (7)$$

Вторая компонента C_2 блока B представляет собой сумму по модулю 2 логических произведений битов блока на результат нелинейного преобразования F их порядковых номеров:

$$C_2 = b_1 \cdot F(1) \oplus b_2 \cdot F(2) \oplus \ldots \oplus b_m \cdot F(m). \qquad (8)$$

Третья компонента C_3 контрольной суммы вычисляется, как бит четности информационного блока:

$$C_3 = b_1 \oplus b_2 \oplus \ldots \oplus b_m. \qquad (9)$$

Функциональное преобразование $F(X)$ выбирается таким образом, чтобы для любой пары битов блока сумма по модулю 2 конкатенации их номеров и функциональных преобразований номеров двух не повторялась. Формально это означает, что для любых четырех различных номеров битов: $q,l,g,r \in \{1,\ldots.m\}$ всегда выполняется неравенство:

$$\forall q,l,g,r \in \{1,\ldots,m\}:$$
$$< q, F(q) > \oplus < l, F(l) > \neq \qquad (10)$$
$$\neq < g, F(g) > \oplus < r, F(r) > .$$

Описанный выбор функционального преобразования $F(X)$ иллюстрируется следующим простым примером. Если блок содержит 15 бит (m=15), то одним из преобразований $F(X)$, при котором

выполняется (10) является преобразование, представленное в табл.1.

Таблица 1.

X	$F(X)$	X	$F(X)$
0	0	8	5
1	1	9	13
2	2	10	12
3	3	11	7
4	4	12	11
5	6	13	14
6	9	14	8
7	10	15	15

Если выбрать, например, четыре номера: q=3, l=6, g=11 и r=14, то конкатенации их номеров и функциональных преобразований номеров равны: $<q,F(3)>=<3,3>$, $<l,F(l)> = <6,8>$, $<g,F(g)> = <11,7>$ и $<r,F(r)> = <14,9>$. Легко убедиться, что для выбранных номеров неравенство (10) выполняется: $<q,F(q)> \oplus <l,F(l)> = <5,11> \neq <g,F(g)> \oplus <r,F(r)> = <5,14>$.

Трехкомпонентный контрольный код $<C_{1S},C_{2S},C_{3S}>$ в соответствии с формулами (7)-(9) вычисляется на передатчике и по тем же формулам (7)-(9) вычисляется приемником по принятому блоку: $<C_{1R},C_{2R},C_{3R}>$. На приемнике также вычисляются три компоненты разностей контрольных кодов приемника и передатчика:

$$\begin{aligned} \Delta C_1 &= C_{1S} \oplus C_{1R} \\ \Delta C_2 &= C_{2S} \oplus C_{2R} \\ \Delta C_3 &= C_{3S} \oplus C_{3R} \end{aligned} \qquad (11)$$

Если все три компоненты разности контрольных сумм приемника и передатчика равны нулю: ΔC_1=0, ΔC_2=0 и ΔC_3=0, то считается, что блок передан без ошибок.

Если при передаче блока ошибочно передано нечетное число битов, то такая ошибка обнаруживается в силу того, что $\Delta C_3 \neq 0$.

При ошибочной передаче 2-х бит, имеющих номера q и l, где $q,l \in \{1,..,m\}$, $q \neq l$, код ΔC_1 представляет собой сумму по модулю 2 двух различных кодов - номеров искаженных битов q и l. соответственно он не равен нулю: $\Delta C_1 = q \oplus l \neq 0$. Это означает, что двукратная ошибка гарантированно обнаруживается.

При ошибочной передаче четырех битов, номера которых равны q,l,g и r разность контрольных сумм приемника и передатчика $\Delta C = <q,F(q),1> \oplus <l,F(l),1> \oplus <g,F(g),1> \oplus <r,F(r),1>$.В силу (9) $\Delta C \neq 0$. что означает гарантированное обнаружение любой четырехкратной ошибки в информационном блоке B.

Узловым вопросом практического применения предложенного подхода к обнаружению четырехкратных ошибок передачи данных с использованием нелинейных взвешенных контрольных сумм является получение функциональных преобразований $F(X)$. обеспечивающих выполнение условия (11).

Если $q \oplus l \neq g \oplus r$, то условие (11) выполняется. Если $q \oplus l = g \oplus r$, то для того, чтобы выполнялось условие (11) необходимо, чтобы:

$$F(q) \oplus F(l) \neq F(g) \oplus F(r) \ . \qquad (12)$$

Если считать, что $q \oplus l = g \oplus r = \delta$, то условие (12) можно представить в виде:

$$\begin{aligned} &F(q) \oplus F(q \oplus \delta) \neq \\ &\neq F(g) \oplus F(g \oplus \delta) \end{aligned} \ . \qquad (13)$$

Булево функциональное преобразование $F(X)$ представляет собой систему из n булевых функций: $F(X) = \{f_1(X),f_2(X),.. .,f_n(X)\}$. Код δ - являет собой n-разрядный двоичный код $\delta=\{\xi_1,\xi_2,..,\xi_n\}$, $\forall i \in \{1,..,n\}$: $\xi_i \in \{0,1\}$. Единичные разрядные компоненты $\xi_1,\xi_2,...,\xi_n$ кода δ соответствуют битам, в которых коды X_q и X_l (равно как и коды X_g , X_r) отличны между собой. Очевидно, что код δ однозначно определяет множество ϑ переменных, значениями которых отличаются коды X_q и X_l Левую часть неравенства (13) можно рассматривать как значение дифференциала функционального преобразования $F(X)$ по переменным множества ϑ на наборе X_q.

Аналогично, правая часть (13) представляет собой значение дифференциала $F(X)$ по переменным множества ϑ на наборе X_g.

Дифференциал функционального преобразования $F(X)$ по переменным, соответствующим единичным компонентам кода δ представляет собой функциональное преобразование $d(F(X),\delta)$ определяемое в виде:

$$d(F(X),\delta) = F(X) \oplus F(X \oplus \delta). \quad (14)$$

Поскольку на наборах переменных, хеммингово расстояние между которыми равно δ, преобразование $d(F(X),\delta)$ принимает одинаковые значения, то n-битовый код $d(F(X),\delta)$ на 2^n наборах входных переменных может принимать не более 2^{n-1} различных значений.

Поскольку на выбор наборов X_q и X_g не накладывается никаких ограничений, кроме того, что эти наборы должны быть разными: $X_g \neq X_q$, не равными нулю и δ: $X_q \neq 0$, $X_g \neq 0$, $X_q \neq \delta$, $X_g \neq \delta$ и не отличаться друг от друга на код δ: $X_q \neq X_g \oplus \delta$, то неравенство (13) должно выполняться для любых двух наборов, удовлетворяющих означенным выше условиям. С учетом изложенного, неравенство (13) может быть представлено через дифференциал преобразования $F(X)$ в следующем виде:

$$\begin{aligned} &\forall q, g \in \{1,\ldots 2^n - 1\}, \\ &g \neq q, X_g \neq \delta, X_q \neq \delta: \\ &d(FX_g),\delta) \neq d(F(X_q),\delta) \end{aligned} \quad (15)$$

Суть неравенства (15) состоит в том, что значения дифференциала $d(F(X),\delta)$ на любых двух, не нулевых, не равных между собой или отличающихся на δ наборах, должны быть различными. Это означает, что дифференциал $d(F(X),\delta)$ должен на всех наборах, кроме оговоренных выше, принимать различные значения. Общее число наборов для n булевых переменных равно 2^n. На каждой паре наборов, отличающихся на δ дифференциал $d(F(X),\delta)$ принимает одинаковые значения в силу симметричности выражения (14). Поэтому максимальное число возможных значений дифференциала ограничено 2^{n-1}. Поскольку нулевой набор не используется (нумерация битов блока начинается с единицы), то при возникновении 4-кратной ошибки (в битах с номерами $q,l,g,r > 0$) не может возникнуть ситуации, при которой ошибочно переданы биты с номерами 0 и δ. Поэтому значение дифференциала $d(F(X),\delta)$ на наборе $X=\delta$ не имеет значения. Исходя из этого, сделанный выше вывод о том, что дифференциал $d(F(X),\delta)$ должен на всех наборах, кроме нулевого и равного δ, принимать различные значения, можно уточнить в виде: дифференциал $d(F(X),\delta)$ на наборах, отличных от нулевого и равного δ, должен принимать в точности $2^{n-1}-1$ разных значений.

Если принять во внимание то, что в приведенных выше рассуждениях код δ полагался любым, отличным от нуля, то можно обобщить сделанный выше вывод для любого значения δ следующим образом:

Для того, чтобы в рамках предлагаемого подхода функциональное преобразование $F(X)$ обеспечивало возможность гарантированного обнаружения двух и четырех кратных ошибок, его дифференциал по любому непустому подмножеству переменных должен принимать в точности $2^{n-1}-1$ различных значений.

Выводы

С целью повышение эффективности обнаружения ошибок передачи данных в линиях, моделью которых является симметричный двоичный канал доказано, что для гарантированного обнаружения четырех-кратных ошибок в m-битовом блоке при его передаче в двоичном симметричном канале при использовании теоретически минимального числа контрольных разрядов - $\log_2 m$, необходимо использовать нелинейные преобразования. На основе двухкомпонентной нелинейной взвешенной

контрольной суммы разработан способ построения контрольного кода, обеспечивающий, в отличие от известных методов гарантированное обнаружение четырехкратных ошибок и исправление двухкратных при использовании теоретически минимального числа контрольных разрядов. Предложенный способ по характеристикам обнаружения ошибок нечетной кратности и пачек ошибок идентичен *CRC*. Определены свойства нелинейного преобразования, которые обеспечивают возможность последнего для гарантированного обнаружения четырехкратных ошибок при использовании теоретически минимального числа контрольных разрядов.

В отличие от *CRC* предложенный способ обрабатывает каждый бит контролируемого блока независимо, а, значит, позволяет распараллелить вычисление контрольного кода при аппаратной реализации, тем самым, не накладывает ограничений на возможность выполнения контроля ошибок в темпе передачи данных.

Список литературы

1. Самофалов К.Г., Марковский А.П., Мулки Яссин Ахмед Ал Бадайнех. Обнаружение и исправление ошибок передачи данных с использованием взвешенных контрольных сумм // Проблеми інформатизації та управління. Збірник наукових праць: Вип. 3(14). – К.: НАУ. – 2008. – С.121 – 128.

2. Марковский А.П., Аль-Хавальди Али, Драгунов Н.В. Использование дифференциального кодирования для повышения надежности контроля передачи данных // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. – Київ: ВЕК+ – 2004 – № 42. – С. 198 – 205.

3. Троян О.С. Применение лавинных преобразований для повышения надежности обнаружения ошибок с использованием контрольных сумм // Вісник Національного технічного університету „КПІ". Інформатика, управління та обчислювальна техніка. К.:ВЕК+. – 2004. - № 41. – С.141 – 154.

4. Klove T., Korzhik V. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems. Norwell, MA: Kluwer, 1995. – 433 p.