УДК 004.052.42

АБУ УСБАХ А.Н.,
МЕЛЬНИК А.П.,
ПОНОМАРЧУК Д.С.

ОБ ОДНОМ ПОДХОДЕ К ОБНАРУЖЕНИЮ ОШИБОК ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ СИСТЕМ ОСТАТОЧНЫХ КЛАССОВ

Статья посвящена решению проблемы повышения эффективности выявления ошибок передачи данных в каналах со спектральной модуляцией за счет учета природы их возникновения. С целью гарантированного обнаружения канальных ошибок одной и более кратности был предложен подход, использующий модульное представление на основе Китайской теоремы об остатках. Проведенные теоретические исследования предложенного подхода позволили доказать гарантированность обнаружения символьных ошибок кратностью менее или равной числу контрольных символов в рассматриваемом модульном представлении.

The paper is dedicated to solving the efficiency increasing problem for data transmission error detection in spectrum modulation channel by properties such errors appearance accounted. For the guaranteed errors detection in one and more channel symbols the approach based on Chinese Reminder Theorem has been proposed. In the course of the theoretical researches of proposed approach the guaranteed error detection has been proved for errors quantity less or equal to number of the check symbols in modular representation.

Введение

Развитие и интеграция средств передачи цифровых данных играет важную роль на современном этапе развития компьютерных и информационных технологий. Передача данных в цифровом виде находит применение в таких областях как мобильная связь (EDGE, CDMA2000, 1xEV-DO), цифровое телевидение (DVB-T/H/C/S/S2, ATSC), телекоммуникационных системах беспроводной передачи данных (Wi-Fi, Wi-MAX, Bluetooth), компьютерные сети и др [1]. Характерной особенностью современных средств передачи данных является использование различных видов спектральной модуляции (фазовой-PSK, квадратурно-амплитудной-QAM) для повышения пропускной способности канала. При этом одно изменение фазы/амплитуды может нести в себе более одного информационного бита – канальный символ. Например: QPSK – канальный символ 2 бита, 8-PSK – 3 бита, 16-,32-,64-,128- и 256-QAM – 4,5,6,7 и 8 бит соответственно.

Рост пропускной способности каналов передачи цифровых данных осложняется помехами при передаче и требует адекватного развития средств обнаружения ошибок. Для значительной части систем передачи цифровых данных исправление ошибок выполняется путем повторной передачи блока. Для таких систем, в отличие от корректирующих кодов, фазы обнаружение ошибок и их исправления разнесены. При использовании спектральной модуляции доминируют многократные битовые искажения данных, поскольку одиночная ошибка передачи канального сигнала может изменить произвольное число бит канального символа. Эту особенность битовых искажений необходимо учитывать при создании средств контроля ошибок в каналах со спектральной модуляцией.

Таким образом, проблема повышения эффективности обнаружения многократных битовых искажений в каналах со спектральной модуляцией является актуальной и имеющей практическую значимость.

Анализ существующих средств обнаружения многократных ошибок

В каналах передачи данных со спектральной модуляцией цифровая информация фактически передается символами, каждый из которых модулируется одним канальным сигналом.

Контролируемый блок B, содержащий m бит: $B=\{b_1,b_2,\ldots,b_m\}$, $b_l\in\{0,1\}$, $l=1,\ldots,m$ можно рассматривать состоящим из $t = m/k$ канальных символов: $B=\{X_1,X_2,\ldots,X_t\}$. Каждый j-тый из этих символов X_j, $j\in\{1,2,\ldots,t\}$ включает k смежных бит $X_j=\{x_1,x_2,...,x_k\}=\{b_{(j-1)\cdot k+1},b_{(j-1)\cdot k+2},...,b_{j\cdot k}\}$ контролируемого блока.

При передаче цифровых данных для обнаружения ошибок наиболее часто используют циклические коды и в частности CRC (Cyclic Redundancy Check – циклическая избыточная

проверка). Как и контрольные суммы, CRC относятся к средствам блокового контроля.

Сущность контроля с использованием CRC состоит в том, что блок $B=\{b_1,b_2,\ldots,b_m\}$ представляется полином $P(B)$ степени $m+k$: $P(B)=b_1\cdot x^k+b_2\cdot x^{k+1}+b_3\cdot x^{k+2}+\ldots+b_{m-1}\cdot x^{k+m-1}+b_m\cdot x^{k+m}$. Контрольный код $R(B)$ вычисляется как остаток от деления полинома $P(B)$на образующий полином $Q(X)$ степени k CRC.

По основному критерию эффективности – надежности обнаружения ошибок, циклические коды превосходят контрольные суммы. Ошибки при передаче блока данных не обнаруживается, если полином $E(X)$, соответствующий вектору ошибки делится на образующий полином $Q(X)$ CRC без остатка. Показано [3], что все полиномы $E(X)$, соответствующие указанным ниже ошибкам не делятся на специальным образом выбранный базовый полином $Q(X)$, а следовательно, они обнаруживаются гарантированно:

1. Все искажения битов $b_1,b_2,\ldots,b_m$ нечетной кратности, если базовый полином $Q(X)$ может быть представлен в виде произведения полиномов: $Q(X)=(x+1)\cdot S(X)$;
2. Все двукратные искажения битов $b_1,b_2,\ldots,b_m$ контролируемого блока, если базовый полином $Q(X)=q_0+q_1\cdot x+q_2\cdot x^2+\ldots+q_k\cdot x^k$ содержит не менее трех ненулевых компонент.
3. Группа ошибок, локализованные в рамках k разрядов.

Для остальных ошибок показано [3], что остаток $R(B)$ представляет собой результат хеширования блока B данных в пространство 2^k всех возможных контрольных кодов. Соответственно, вероятность P_{CRC} того, что эти ошибки не будут обнаружены с использованием CRC с образующим полиномом $Q(X)$ степени k определяется как $P_{CRC}=2^{-k}$.

В каналах со спектральной модуляцией, CRC позволяет гарантированно обнаружить только однократную ошибку передачи модулированного сигнала, поскольку искажаемые при этом биты локализованы в рамках группы из k битовых позиций, а значение k на практике меньше степени образующего полинома CRC. При большей кратности ошибок модулированного сигналов, CRC не гарантирует их обнаружения.

Наряду с высокой надежностью, CRC обладает рядом недостатков, наиболее важным из которых является принципиально последовательный характер вычисления контрольного кода, что обуславливает существование ограничений на скорость выполнения операций, связанных с контролем ошибок. Этот недостаток особенно актуален в современных условиях быстрого роста скоростей передачи данных.

Другим эффективным средством обнаружения ошибок в каналах со спектральной модуляцией являются взвешенные контрольные суммы (Weighed Check Sum – WCS) [4]. В отличие от CRC, использование технологии WCS учитывает особенности возникновения битовых искажений в каналах со спектральной модуляцией и позволяет гарантированно обнаруживать битовые искажения, возникающие в двух символах. Недостатком WCS является то, что она не позволяет гарантированно обнаруживать битовые искажения, вызванные ошибочной передачей более 2-х канальных сигналов. Существенным недостатком WCS является также значительно большее по сравнению с CRC число контрольных разрядов, равное $k\cdot(1+\log_2 t)$.

Таким образом, существующие средства обнаружения многократных ошибок в каналах со спектральной модуляцией не обеспечивают эффективное решение обнаружения битовых искажений, вызванных ошибочной передачей более 2-х канальных сигналов.

Целью работы является создание эффективного способа обнаружения битовых искажений, вызванных многократными ошибками передачи канальных сигналов.

Организация контроля ошибок при представлении передаваемых данных в системах остаточных классов

Для гарантированного обнаружения ошибок в одном и более канальном символе необходимо учитывать символьную структуру передаваемых данных. Для этого предлагается использовать метод, основанный на представлении целых чисел в системах остаточных классов – СОК.

Пусть существует система n взаимнопростых чисел $\{p\}^n=\{p_1,p_2,\ldots,p_n\}$ и число P, равное их произведению:

$$P=\prod_{j=1}^{n}p_j \qquad (1)$$

Тогда, согласно Китайской теореме об остатках [1] любое число M, принадлежащее интервалу $[0\ldots P\text{-}1]$ может быть однозначно представлено множеством остатков от деления на взаимно-простые числа, образующие систему $\{p\}^n$.

$$\forall M \in \{0,...,P-1\} : \{r_1, r_2, ..., r_n\} \Leftrightarrow M, r_j = M \bmod p_j,\ j = 1,...,n \quad (2)$$

где $\Leftrightarrow$ символ, обозначающий взаимно-однозначное соответствие. представление числа M (2) называется представлением числа M в системе остаточных классов (СОК). Всегда можно выбрать такую систему взаимно-простых чисел, что ее элементы $p_1,\ldots,p_n$ будут удовлетворять условию:

$$\forall j \in \{1,...,n\} : p_j \geq 2^k \quad (3)$$

Пусть число элементов системы $\{p\}^n$ будет больше числа символов в блоке: $n>t$ $\{p\}^t = \{p_1,p_2,\ldots,p_t\} \subseteq \{p\}^n$. Тогда, согласно (2) и (3) последовательность символов $X_1,X_2,\ldots,X_t$, составляющих контролируемый блок B данных можно рассматривать как представление в системе остаточных классов некоторого числа A:

$$B = \{X_1,...,X_t, X_{t+1},...,X_n\} \Leftrightarrow A, \quad \forall i \in \{1,...,t\} : X_i = A \bmod p_i \quad (4)$$

То же число A может быть представлено в системе остаточных классов на основе $\{p\}^n$:

$$\{X_1,...,X_t, X_{t+1},...,X_n\} \Leftrightarrow A, \quad \forall j \in \{1,...,n\} : X_j = A \bmod p_j \quad (5)$$

Изложенные теоретические положения могут быть положены в основу метода контроля ошибок, возникающих в последовательных интерфейсах со спектральной модуляцией.

Сущность предлагаемого метода состоит в следующем:

1. Выбирается система $\{p\}^n$ взаимно-простых чисел, в зависимости от типа спектральной модуляции определяется число k бит, модулируемых одном сигналом, протоколом определяется число t пересылаемых символов в блоке.

2. Согласно (5) передаваемый блок B данных представляется в выбранной системе $\{p\}^n$ числом A. При этом символы $X_1,X_2,\ldots,X_t$ являются информационной частью передаваемого блока B, а символы $X_t,\ldots,X_n$ образуют контрольные символы. Обозначим через T передаваемый блок, представляющий собой конкатенацию информационного блока B и блока Z контрольных символов: $T = B \,||\, Z$.

3. Информационная и контрольная части блока передаются приемнику.

4. Принятый блок представляет собой посимвольную сумму переданного блока T и n-символьного вектора ошибки $E=\{e_1,e_2,\ldots,e_n\}$, где e_j – k-битовый символ: $e_j = \{\xi_{1j}, \xi_{2j},\ldots,\xi_{kj}\}$, компоненты которого $\xi \in \{0,1\}$:

$$R = \{Y_1,...,Y_n\} = T + E \quad (6)$$

5. Проверка отсутствия ошибок в передаче блока состоит в восстановлении, согласно Китайской теореме об остатках, некоторых чисел C_1 и C_2 [2]:

$$\{Y_1, Y_2,..., Y_t\} \Leftrightarrow C_1, \{Y_1, Y_2,...., Y_n\} \Leftrightarrow C_2 \quad (7)$$

При этом, информация считается переданной без ошибок, если выполняется равенство указанных чисел C_1 и C_2: $C_1=C_2$.

Можно показать, что предложенный метод контроля гарантирует обнаружение ошибок в передаче до (n-t) символов, если выполняются следующие условия:

а). Система $\{p\}^n$ является монотонно возрастающей последовательностью.

б). Произведение модулей $p_{t+1},p_{t+2},\ldots,p_n$ контрольных символов не сравнимо с единицей по любому из модулей символов данных блока B:

$$\prod_{i=t+1}^{n} p_i \bmod p_j \neq 1, \forall j \in \{1,...,t\} \quad (8)$$

Действительно, ошибки в передаче канальных символов могут вызвать искажения битов символов информационного блока B, контрольного блока Z, информационного и контрольного блоков одновременно. Это требует доказательства для ряда частных случаев.

Частный случай А: Искажению подверглись символы только контрольного блока. В этом случае, поскольку, ошибки не затронули символов информационного блока B, то справедливо следующее:

$$\{X_1, X_2,..., X_t\} = \{Y_1, Y_2,..., Y_t\} : C_1 = A \quad (9)$$

В соответствии с Китайкой теоремой остатках, представление в системе остаточных классов однозначно, следовательно, двум различным множествам остатков соответствуют различные целые числа:

$$\{X_1,...,X_n\} \Leftrightarrow A, \{X_1,...,X_t, Y_{t+1},....,Y_n\} \Leftrightarrow C_2 \neq A \quad (10)$$

Исходя из (9) и (10) справедливо следующее: $C_1 = A \neq C_2$. Из этого следует, что $C_1 \neq C_2$,

то есть ошибка гарантированно обнаруживается, если число неверно переданных канальных сигналов не превышает *n-t*.

Частный случай B: ошибки имеют место как при передаче информационных символов, так и при передаче символов контрольного блока. В этом случае, не нарушая общности, можно рассматривать вариант локализации ошибок, при котором ошибки произошли при передаче *d* последних символов и *q* последних символов контрольного блока.

$$\begin{aligned} &A \Leftrightarrow \{X_1,...,X_t\} \\ &A \Leftrightarrow \{X_1,....X_n\} \\ &C_1 \Leftrightarrow \{X_1,...,X_{t-d},X_{t-d+1}+e_{t-d+1},...,X_t+e_t\} \\ &C_2 \Leftrightarrow \{X_1,...,X_{t-d},X_{t-d+1}+e_{t-d+1},....,X_t+e_t, \\ &X_{t+1},...,X_{n-q},X_{n-q+1}+e_{n-q+1},X_n+e_n\} \end{aligned} \quad (11)$$

Согласно Китайской теореме об остатках справедливо следующее:

$$M=\sum_{i=1}^{n} c_i,g_i,r_i \bmod P,\{r_1.r_2,...,r_n\} \Leftrightarrow M, \quad (12)$$

$$c_i = P/p_i; g_i \cdot c_i = 1 \bmod p_i$$

Выражения (11) можно представить, с учетом (12), в следующем виде:

$$A=(\sum_{i=1}^{t} c_i \cdot g_i \cdot X_i) \bmod P^t$$

$$A=(\sum_{i=1}^{t} c_i' \cdot g_i' \cdot X_i) \bmod P \quad (13)$$

$$C_1=(\sum_{i=1}^{t} c_i \cdot g_i \cdot X_i + \sum_{j=t-d+1}^{t} c_j \cdot g_j \cdot e_j) \bmod P^t$$

где $P^t=\prod_{i=1}^{t} p_i$, $P=P^t \cdot \prod_{j=t+1}^{n} p_j = P^t \cdot P^{C_1} \cdot P^{C_2}$,

$P^{C_1}=\prod_{l=t+1}^{n-q} p_l$ – произведение модулей, соответствующих символам контрольного кода, которые переданы без ошибок.

$P^{C_2}=\prod_{h=n-q+1}^{n} p_h$ – произведение модулей, соответствующих символам контрольного кода, переданных с ошибками.

Если предположить, что ошибки не обнаруживаются, то тогда верно:

$$C_1 = C_2 \Rightarrow C_1 - A = C_2 - A \quad (14)$$

Подставив (13) в (14) получим следующее:

$$\begin{aligned} &(\sum_{j=t-d+1}^{t} c_j \cdot g_j \cdot e_j) \bmod P^t = \\ &=(\sum_{j=t-d+1}^{t} c_j' \cdot g_j' \cdot e_j + \sum_{l=n-q+1}^{n} c_l' \cdot g_l' \cdot e_l) \bmod P \end{aligned} \quad (15)$$

Согласно (13) и (14) справедливо:

$$\begin{aligned} &P = P^t \cdot P^{C_1} \cdot P^{C_2} \\ &c_j' = c_j \cdot P^{C_1} \cdot P^{C_2}, \forall j \in \{1,...,t\} \\ &c_l' = P^t \cdot P^{C_1} \cdot \frac{P^{C_2}}{p_l} = P^t \cdot P^{C_1} \cdot P^{C_2/l}, \forall l \in \{t+1,...,n\} \end{aligned} \quad (16)$$

где $P^{C_2/l}$ – произведение модулей, соответствующих символам контрольного блока, переданным с ошибками, за исключением *l*-того символа.

Пусть произведение модулей символов информационного блока, при передаче которых не произошло ошибок, равно P^{tr}, а произведение модулей символов информационного блока, при передаче которых произошли ошибки равно - P^{te}:

$$\begin{aligned} &P^t = P^{tr} \cdot P^{te} \\ &P = P^{tr} \cdot P^{te} \cdot P^{C_1} \cdot P^{C_2} \\ &c_j = P^{tr} \cdot \frac{P^{te}}{p_j} = P^{tr} \cdot P^{te/j} \end{aligned} \quad (17)$$

где $P^{te/j}$– произведение модулей, соответствующих символам информационного блока, при передаче которых произошли ошибки, кроме *j*–го.

С учетом ранее полученных выражений (15) – (17) справедливо следующее:

$$\begin{aligned} &(P^{tr} \cdot \sum_{j=t-d+1}^{t} P^{te/j} \cdot g_j \cdot e_j) \bmod P^{tr} \cdot P^{te} = \\ &=(P^{C_1} \cdot (P^{C_2} \cdot \sum_{j=t-d+1}^{t} P^{te/j} \cdot g_j' \cdot e_j + \\ &+ P^{te} \cdot \sum_{l=n-q+1}^{n} P^{C_2/l} \cdot g_l' \cdot e_l)) \bmod P^{tr} P^{te\bullet} \cdot P^{C_1} \cdot P^{C_2} \end{aligned} \quad (18)$$

В выражении (18) левая и правая части могут быть сокращены на P^{tr}, поскольку оба модуля и подмодульных выражения делятся на P^{tr}:

$$(\sum P^{te/j} \cdot g_j \cdot e_j) \bmod P^{te} =$$

$$= (P^{C_1} \cdot (P^{C_2} \cdot \sum_{j=t-d+1}^{t} P^{te/j} \cdot g_j' \cdot e_j + \quad (19)$$

$$+ P^{te} \sum P^{te/l} \cdot g_l' \cdot e_l)) \bmod P^{te} P^{C_1} P^{C_2}$$

Согласно свойству сравнений в выражении (19) правая часть делится на P^{C1}, поскольку и модуль и подмодульное выражение делятся на P^{C1}. Следовательно, и левая часть выражения (19) делится на P^{C1}.

Одним из возможных решений уравнения (19) является нулевое значение левой и правой части. Множители как левой, так и правой частей (19) не равны нулю, поскольку из (12) следует, что:

$$\begin{aligned} g_j &= 1..p_j - 1 \\ e_j &= 1..p_j - 1 \end{aligned} \quad (20)$$

Следовательно, равенство нулю левой и правой частей уравнения (19) выполняется при справедливости следующей системы:

$$\begin{aligned} g_j \cdot e_j &= p_j, \forall j \in \{t-d+1,...,t\} \\ g_j' \cdot e_j &= p_j, \forall j \in \{t-d+1,...,t\} \\ g_l' \cdot e_l &= p_l, \forall l \in \{n-q+1,...,t\} \end{aligned} \quad (21)$$

Из (21) следует: $g_j = g_j', \forall j \in \{t-d+1,...,t\}$. Из этого очевидным является следующее: $c_j \bmod p_j = c_j' \bmod p_j = c_j \cdot P^{C_1} \bmod p_j$. Из последнего следует, что $P^{C_1} \bmod p_j = 1$. Однако это противоречит условию (7). Следовательно, левая и правая части уравнения (19) не могут быть равными нулю. Левая часть выражения (19) не может превышать модуль, равный P^{te}. Достаточным условием того, чтобы выражение (19) не выполнялось является условие:

$$P^{te} < P^{C_1} \quad (22)$$

По условию а) последовательность модулей монотонно возрастает, следовательно, неравенство (22) будет иметь место, если число модулей в произведении левой части (22) не превышает число модулей в произведении правой части (22). Таким образом, будут гарантированно обнаружены ошибки передачи канальных сигналов, кратность которых не соответствовать контрольным разрядам (16 бит контроля), следовательно, разрядам данных будет сопоставлен 51 модуль. Это позволяет контролировать блок данных длиной 51*4=204 бита. Следует отметить, что рост α приводит к экспоненциальному увеличению

превышает $u<n-t$ ошибок в контрольных символах и $n-t-u$ ошибок передачи символов информационного блока. Таким образом, количество h гарантированно обнаруживаемых ошибок передачи символов определяется следующей формулой:

$$h = n - t \quad (23)$$

Важным аспектом эффективности предложенного метода является анализ количества контрольных разрядов, используемых для обнаружения битовых искажений, вызванных ошибками передачи канальных сигналов.

Следует учитывать, что в предложенном методе разрядность контролируемых символов и символов контроля может быть различной, при условии, что обе указанные величины кратны разрядности канального символа. Это условие обеспечивает локализацию ошибок – ошибка в одном канальном символе приведет к ошибке только в одном символе данных или контроля. В простейшем случае контролируемый символ совпадает с канальным, а разрядность контрольных символов кратна разрядности канальных символов.

Проведенный анализ показал, что предложенный метод имеет ряд ограничений накладываемых необходимостью иметь монотонно возрастающую последовательность взаимно простых модулей удовлетворяющих (8). Объективно, длина такой последовательности, а значит, и размер контролируемого блока данных непосредственно зависит от разрядности символов контроля, которая определяет верхнюю границу для модулей. Все члены последовательности должны быть $p_j < 2^{\alpha}$, $j=1..n$, где α – разрядность символов контроля. Также влияет на длину последовательности модулей разрядность контролируемых символов данных, поскольку минимальный член последовательности должен быть больше любого контролируемого символа, т.е. все члены последовательности должны быть $p_j \geq 2^k$, $j=1..n$. Значение h определяет какое число модулей будет использовано для функций контроля, следовательно уменьшает число модулей для данных. Таким образом, например, при h=2, k=4, α=8 последовательность модулей будет иметь 53 члена, из которых 2 старших будут

длинны контролируемых данных. Так, при увеличении α в два раза (32 бита контроля) можно контролировать блок данных длиной 26156 бит. Другим способом увеличения размера контролируемого блока является использование разрядности контролируемых символов кратной разрядности канальных символов. Однако при этом рост будет линейным.

Таким образом, предложенный метод обнаружения ошибок в модемных интерфейсах со спектральной модуляцией эффективен при относительно больших значениях α и k. Учитывая, что с развитием технологии передачи цифровых данных значение k увеличивается, перспективность предложенного метода обнаружения ошибок в перспективе увеличивается. Не взирая на то, что предложенный метод не позволяет контролировать блоки данных произвольной длины, он, в отличие от CRC, обеспечивает гарантированное обнаружение ошибок и может адаптироваться под качество канала передачи путем использования большего или меньшего числа контрольных разрядов.

Выводы

Предложен метод контроля ошибок в каналах со спектральной модуляцией, основанный на представлении информационных и проверочных символов в СОК.

Метод позволяет повысить эффективность обнаружения ошибок в каналах со спектральной модуляций благодаря тому, что учитывается символьная природа таких ошибок. Предложенный метод позволяет гарантированно обнаруживать пачки битовых ошибок любой длины, а также адаптировать процедуру контроля под качество линии передачи.

Метод может использоваться при модификации существующих и разработке новых протоколов передачи цифровых данных в различных отраслях – мобильной связи, цифровом телевещании, беспроводной передачи и др.

Наиболее перспективным направлением развития предложенного подхода является разработка методов коррекции ошибок с использованием представления в СОК.

Список литературы

1. Анісімов А.В. Алгоритмічна теорія великих чисел. –К.: Академперіодика.–2001.–153 с.
2. Бєйкер А. Введение в теорию чисел. Мн.: Вышєйш. шк., –1999.–340 с.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом ”Вильямс”, 2004.– 1104 с.
4. 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: Випуск 3(14).–К.,НАУ.– 2008.– С.121-128