Яцун В.О.
студент,
Национальный технический университет Украины
«Киевский политехнический институт»

ПОВЫШЕНИЕ НАДЕЖНОСТИ ОБНАРУЖЕНИЯ ОШИБОК ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ

Расширяющееся использование компьютерных технологий для управления производственными процессами, в том числе связанными с техногенным риском, требуют адекватного повышения надежности всех компонент автоматизированного управления, в том числе, надежности передачи данных между компонентами управляющей системы.

Непрерывный рост скоростей в линиях передачи цифровых данных имеет следствием увеличение ошибок, вызванных межсигнальной интерференцией, а расширяющееся использование беспроводной связи сопряжено с ростом интенсивности внешних электромагнитных помех. Большинство факторов, влияющих на достоверность передачи цифровых данных, прямо зависит от длины линии передачи. Это обуславливает необходимость постоянного повышения надежности средств обнаружения ошибок передачи данных в системах компьютеризованного управления.

Большая часть линий передачи цифровых данных компьютерных систем управления не использует групповой модуляции передаваемых данных: они передаются с применением импульсно-кодовой модуляции [1]. В теоретическом плане такие линии соответствуют модели двоичного симметричного канала. Доминирующим типом ошибок для указанного канала являются независимые друг от друга ошибки относительно небольшой кратности.

Для обнаружения ошибок передачи данных в компьютерных системах управления преимущественно используются [2]:

– циклические избыточные коды (CRC – Cyclic Redundancy Codes)

– контрольные суммы (CS – Check Sum);

– эхоплекс (EH – Echoplex).

Поскольку ошибки нечетной кратности гарантированно обнаруживаются как CRC и CS, наиболее важным типом необнаруживаемых ошибок в системах управления являются ошибки четной малой кратности: от 2 до 6. Этот класс ошибок вероятностно обнаруживается с использованием CS, равно как ошибки кратности 4 и 6 – при применении CRC. Целью исследований является разработка модификации контрольной суммы, использование которого позволило бы гарантировать обнаружение 2-6 кратных ошибок. Поскольку расширение класса гарантированно обнаруживаемых ошибок с помощью модифицированной взвешенной контрольной суммы сопряжено с увеличением разрядности контрольного кода, представляется оправданным разработать способ, который бы позволял гибко менять кратность гарантированно обнаруживаемых ошибок. Это позволило бы обеспечивать ту или иную

надежность передачи цифровых данных в компьютерных системах в зависимости от специфики их практического использования.

Для гарантированного обнаружения ошибок четной кратности, не превышающей h, предлагается способ модификации взвешенной контрольной суммы.

Сущность способа состоит в том, что для формирования компонент контрольной суммы предлагается использование опорного множества частично-ортогональных кодов.

Опорным m-компонентным множеством Ω_m частично-ортогональных кодов порядка h будем называть множество $\Omega_m=\{U_1,U_2,\ldots,U_m\}$, состоящее из m k–битовых кодов $U_1,U_2,\ldots,U_m$ таких, что сумма по модулю 2 любого их подмножества ϑ, которое включает в себя не более h таких кодов не равно нулю.

$$\forall \vartheta = \{V_1, V_2, ..., V_{q_\vartheta}\} \subset \Omega_m, q_\vartheta \le h : V_1 \oplus V_2 \oplus ... \oplus V_{q_\vartheta} \neq 0 \qquad (1)$$

Фактически, это означает, что любое подмножество $\vartheta \subset \Omega_m$, $|\vartheta| \le h$ представляет собой ортогональный базис в h-мерном пространстве.

Пусть контролируется правильность передачи блока B данных, состоящего из m битов: $B=\{b_1,b_2,\ldots,b_m\}$, $b_i\in\{0,1\}$, $i=1,\ldots,m$. Для заданной четной кратности h ошибок, которые должны быть гарантировано обнаружены, всегда возможно сформировать множество $\Omega=\{U_1,U_2,\ldots,U_m\}$ частично-ортогональных кодов.

Согласно предлагаемому способу модифицированная взвешенная контрольная сумма CS на приемнике и передатчике формируется, как сумма по модулю 2 m (k+1)-разрядных ее компонент $W_1,W_2,\ldots,W_m$:

$$CS = W_1 \oplus W_2 \oplus ... \oplus W_m \qquad (2)$$

Значение каждой j–той компоненты контрольной суммы – W_j, $j\in\{1,\ldots,m\}$ определяется значением одноименного бита b_j контролируемого блока и j-тым частично-ортогональным кодом U_j. При этом компонента W_j формируется как конкатенация j–того бита b_j блока B и логического произведения этого бита на каждый из разрядов кода U_j:

$$\forall j \in \{1,...,m\} : W_j = b_j \parallel b_j \cdot U_j \qquad (3)$$

Контрольная сумма, определяемая в соответствии с (2) и (3) вычисляется отдельно на передатчике и приемнике. Блоки данных на передатчике и приемнике, равно как и составляющие их биты, обозначим как $B_S=\{b_{1S},b_{2S},\ldots,b_{mS}\}$ и $B_R=\{b_{1R},b_{2R},\ldots,b_{mR}\}$ соответственно. После передачи блока данных, контрольная сумма CS_S передатчика передается на приемник, где сравнивается с контрольной суммой CS_R, вычисленной на приемнике.

Решение о наличии ошибок при передаче блока данных принимается, если отличен от нуля (k+1)-разрядный код Δ разницы контрольных сумм передатчика CS_S и приемника CS_R: $\Delta = \{\delta_1, \delta_2, ..., \delta_{k+1}\} = CS_S \oplus CS_R$, причем компоненты кода Δ разности определяются в виде:

$$\delta_1 = \bigoplus_{j=1}^{m} (b_{jS} \oplus b_{jR}), Z = \{\delta_2, \delta_3, ..., \delta_{k+1}\} = \bigoplus_{j=1}^{m} (b_{jS} \oplus b_{jR}) \cdot U_j \qquad (4)$$

Покажем, что предложенная модификация взвешенной контрольной суммы обеспечивает гарантированное обнаружения ошибок нечетной

кратности и ошибок, четная кратность которых не превышает заданной порогового значения *h*.

При возникновении в процессе передачи нечетного числа битовых искажений, δ_1 кода Δ разницы контрольных сумм передатчика и приемника в силу (4) представляет собой сумму по модулю 2 нечетного количества единичных компонент, которые соответствуют несовпадающим одноименным битам блоков данных на приемнике и передатчике. Соответственно, δ_1=1. Это означает, что нечетное число ошибок, возникших в процессе передачи блока данных, гарантированно обнаруживается при использовании предложенного варианта взвешенной контрольной суммы.

При возникновении в процессе передачи *m*-битового блока данных ошибок четной кратности $d \le h$, номера *d* искаженных битов образуют множество Θ: $|\Theta| \le h$. Бит δ_1 кода Δ разности контрольных сумм передатчика и приемника принимает нулевое значение в силу того, что $d \bmod 2 = 0$, а значение *k*-битовой компоненты Z кода Δ определяется следующим выражением:

$$Z = \bigoplus_{i \in \Theta} (b_{iS} \oplus b_{iR}) \cdot U_i = \bigoplus_{i \in \Theta} U_i$$

В силу свойства (1) сумма по модулю 2 не более, чем *h* частично-ортогональных кодов не может быть равна нулю, а поскольку $|\Theta| \le h$, то $Z \neq 0$, а соответственно и разность контрольных сумм приемника и передатчика $\Delta \neq 0$. Это означает, что любое искажение не более, чем *h* битов будет гарантированно обнаружено при использовании предлагаемого варианта взвешенной контрольной суммы.

Например, если контролируется правильность передачи блока длиной 1 Кбит (*m*=1024) и при этом необходимо обеспечить гарантированное обнаружения ошибок четной кратности, не превышающей 4 (*h*=4), то разрядность частично-ортогональных кодов, составляющих опорное множество равна 23, а длина контрольного кода составляет *k*+1=24 бита. При возникновении 4-кратной ошибки передачи, пусть, например, подвергнутся искажению следующие биты блока: $b_{59}, b_{767}, b_{768}, b_{1000}$. Соответственно, 23-битовая компонента Z разности Δ взвешенных контрольных сумм приемника и передатчика будет представлять сумму по модулю 2 одноименных частично-ортогональных кодов множества Ω_{1024}: $Z = (U_{59} \oplus U_{767} \oplus U_{768} \oplus U_{1000}) = 0x1175 \oplus 0x40997D \oplus 0x409F7B \oplus 0x82CB99 = 0x82DCEA \neq 0$.

Таким образом, доказано, что ошибки четной кратности, не превышающей заранее заданного значения $h > 2$ гарантированно обнаруживаются при использовании предложенной модификации взвешенной контрольной суммы, в отличие как от CRC, так и от известных разновидностей контрольных сумм [3]. Следовательно, предложенный способ обеспечивает существенное расширение класса гарантированно обнаруживаемых ошибок передачи данных по сравнению с известными способами контроля.

При возникновении ошибок четной кратности *d*, большей, чем *h*: $d > h$, вероятности их обнаружения примерно равны как при использовании CRC, так и при применении контрольной суммы (предложенной модификации и известных разновидностей).

Список использованных источников:

1. Markovskyi O. P. Synchronization Error Detection of Data Transmission Errors in Asynchronous Channels / Markovskyi O. P., Fedorechko O., Doukas N., Bardis N. // Recent Advances in Electrical Engineering Series – 37. Latest trends on Systems. – Vol. 1. – Proceeding of the 18-th International Conference on Systems – CSCC-14. – Santorini Island, Greece, July 17-21. 2014. – ISSN: 1790-5117, ISBN: 978-1-61804-243-9. – P. 179-183.

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

3. Bardis N. G., Markovskyy A. P. Utilization of Avalanche Transformation for Increasing of Echoplex and Checksum Data Transmission Control Reliability// International Symposium on Information Theory and its Application. – ISITA2004. – Parma, Italy, Oktober 10-13, 2004. – PP. 134-139.