Increase of Error Detection Effectiveness in the Data Transmission Channels with Pulse-Amplitude Modulation

Akram A. Mustafa

***Abstract*—**In this paper an approaches for increasing the effectiveness of error detection in computer network channels with Pulse-Amplitude Modulation (PAM) has been proposed. Proposed approaches are based on consideration of special feature of errors, which are appearances in line with PAM. The first approach consists of CRC modification specifically for line with PAM. The second approach is base of weighted checksums using. The way for checksum components coding has been developed. It has been shown that proposed checksum modification ensure superior digital data control transformation reliability for channels with PAM in compare to CRC.

***Keywords*—**Pulse-Amplitude Modulation, checksum, transmission, discrete.

I. INTRODUCTION

THIS development of information integration on the basis of computer technologies and telecommunication systems is one of the major factors of the progress in all spheres of human activities. The main issue on technologies improvement in information exchange is the maintenance of more reliable data transmission in the buses of computing systems and in the computer network channels. This issue is becoming more relevant in the current concern. It is determined by the number of factors, amongst of which the most important is the increase of transmission speed, and thus, the increase of negative impact of signal interference. The rise in the number of errors, caused by external electromagnetic fields, is influenced by the rapid growth of their intensity, determined by dynamic expansion of mobile communication means and wireless data transmission channels in the computer networks. On the contrary, there is an ongoing expansion process in the use of information technologies in all spheres of human activities, covering the ones connected with techno genetics risk, which toughens the requirements specified for the reliability of all components of computing systems and computer networks, including digital data transmission means. Taking into account the growth of transmitted in computing systems and networks information volumes, the increase of transmission processes reliability by means of guaranteed detection of the most widespread errors is the most significant. Thus, progressive advance in the way of data transmission needs adequate improvement in means, which provide superior reliability of data transmission in computing systems and networks.

The channels with spectral and amplitude modulation of digital data are widely used in computer networks to increase capacity [1]. The main feature of such modulation is that bit groups of the controlled block are transmitted via channel signal. The spectral modulation of digital data, in particular, is used in phone-, cable and wireless lines of computer networks [1, 2]. The error detection in such lines has specific features, which are not fully taken into account by the currently existing error detection means. Therefore, the analysis of peculiarities of error occurrence in the lines with modulation, and also the development of methods, aimed to increase the effectiveness of control means through their adaptation to detected peculiarities, are important topical issues.

Author is with Department of Computer Science, Al Al-Bayt University, P.O.BOX 922283, 11192, Jordan (e-mail: hamarchi@yahoo.com).

II. ANALYSIS OF THE MODERN STATE OF THE PROBLEM ON MAINTENANCE OF DATA TRANSMISSION RELIABILITY IN THE CHANNELS WITH AMPLITUDE MODULATION

Taking into account relatively low intensity of occurrence of data transmission errors in the buses of computing systems and computer network wire lines, the use of ARQ (Automatic Repeat Request), which implies recurrent transmission of the controlled data block on error detection, is regulated by the current protocols. Cyclic redundancy checks (CRCs) and checksums (CSs) are the most wide-spread means of error detection on digital data transmission through computer systems and networks. CRC with generating polynomial in the n-degree allows to detect all odd errors, all double errors, and also error clusters, the length of which does not exceed n [3]. CS ensures detection of odd errors solely, but unlike CRC, the control with the use of CS is carried out much easier and quicker.

Pulse-Amplitude Modulation (*PAM*) is used quite often to increase capacity in the low-frequency lines for digital data transmission through computer networks. By this type of digital data modulation the group comprised of k adjacent bits, which is called $X=\{x_1,x_2,\ldots,x_k\}$, $\forall j\in\{1,\ldots,k\}:x_j\in\{0,1\}$ code group, is modulated with one channel signal, which can receive 2^k levels: from 0 to $(2^k-1)\cdot s$, where s is discrete interval of the channel signal amplitude.

When *PAM* channel signal is distorted, k bits, which form a code group, can be basically distorted as well. However, according to [1] the errors, which occur in such lines, have the following specific features:

- The errors connected with channel signal transmission through networks are virtually independent and the correlation between their occurrence probability and divisible factor is defined by binomial law.
- by error occurrence on channel signal transmission the distortion probabilities of separate bits of k-level code group, which is modulated with one channel signal, are not equal.

Indeed, if $U(X)$-level of channel signal with pulse-amplitude modulation is specified by binary number, which corresponds to binary value of $X=\{x_1,x_2,\ldots,x_k\}$ code group:

$$U(X)=s\cdot\sum_{j=1}^{k}x_j\cdot 2^{j-1} \quad (1)$$

then, according to [1] by error occurrence on channel signal transmission, caused by Gaussian noise, the most probable distortion of the signal is one, altered by one s-interval of amplitude discrete. We will denote mentioned probability as p_1 (the probability of correct channel signal transmission will be denoted through p_0). Significantly, caused by Gaussian noise channel signal distortion, which is altered by 2 discrete intervals, is less probable (this probability will be denoted as p_2). Similarly, we will denote the probability of caused by Gaussian noise channel signal distortion, which is altered by i-intervals of discrete, as p_i. Pursuant to the data [1] the following in equation is exercised in practice:

$$U(X)=s\cdot\sum_{j=1}^{k}x_j\cdot 2^{j-1} \quad (2)$$

$$p_0 >> p_1 >> p_2 >> p_3 >> \ldots >> p_{2^k-1} \quad (3)$$

Notably, the difference in probability values, which are in the in equation (3), makes several orders.

The bits of X-code group, which corresponds to the distorted channel signal, alter on occurrence of error in channel signal transmission, caused by Gaussian noise. The most important aspect is that the probabilities of distortion of k-bits, which comprise X-code group, are not equal. Thus, on the most probable channel signal distortion, altered by one discrete interval, low bit $x_1$always changes, x_2 bit is distorted with probability 2^{-1}, x_3 bit changes its value with probability 2^{-2} etc. On channel signal distortion, which is caused by Gaussian noise and altered by 2 discrete intervals, the second bit x_2 of the code group completely changes, whereas the third bit x_3 changes with probability 2^{-1}. When the channel signal amplitude alters by $3\cdot s$ value, low bit $-x_1$, as well as after following bit – x_2 of the code group, completely changes. On the assumption of the above mentioned arguments it is clear that high bit $-x_k$ is distorted only under alteration by $2^{k-1}\cdot s$, which is the result of an error in the amplitude of the channel signal. Taking into account probabilities $p_1,p_2,\ldots,p_3$ of channel signal amplitude distortion, caused by Gaussian noise and altered by corresponding number of discrete intervals, probabilities $q_1,q_2,\ldots q_k$ of the distortion of code group bits on occurrence of error in channel signal transmission can be written as follows:

$$\begin{aligned}
q_1 &= p_1+p_3+p_5+p_7+\ldots\\
q_2 &= \frac{1}{2}\cdot p_1+p_2+p_3+\frac{1}{2}\cdot p_5+p_6+p_7+\ldots\\
q_3 &= \frac{1}{4}\cdot p_1+\frac{1}{2}\cdot(p_2+p_3)+p_4+p_5+p_6+p_7+\frac{1}{4}\cdot p_9+\ldots\\
q_4 &= \frac{1}{8}\cdot p_1+\frac{1}{4}(p_2+p_3)+\frac{1}{2}\cdot(p_4+p_5+p_6+p_7)+p_8+\ldots\\
&\ldots\\
q_k &= \frac{1}{2^{k-1}}\cdot p_1+\frac{1}{2^{k-2}}\cdot(p_2+p_3)+\frac{1}{2^{k-3}}\cdot(p_4+p_5+p_6+p_7)+\ldots
\end{aligned} \quad (4)$$

The analysis of (3) and (4) expressions shows that the probabilities of the distortion of different code group bits substantially differ on occurrence of error in the transmission of corresponding channel signal. The distortion of code group low bit - x_1 is the most probable, whereas probability q_2 of the distortion of second bit x_2 is virtually less by half. On the most probable channel signal transmission error (on its amplitude alteration by the value, which is almost equal to s) only one bit (low bit – x_1) of the corresponding code group will be distorted with probability 0.5. The larger number of code group bits will be distorted with probability – 0.5.

Existing error control means, and CRC in particular, do not consider such quite important difference in the possibility of codeword bit distortion, when errors occur in the transmission of modulated channel signal. It is obvious, that an account of the difference appears to be the potential source of increase of the error detection effectiveness. Such possibility can be put into practice by means of optimization of the checking information coding.

The analysis on the possible bit distortion of the digital data, when the latter are transmitted through network lines with pulse-amplitude modulation, must be done with an account of the possibility of channel signal multiple distortions on the transmission of digital data block, which contains m bit.

On one-fold error in the channel signal transmission any bit distortion of the transmitted data block is detected while using CRC, when n-degree of its generating polynomial is larger than the length of k-code group: $n>k$. This is specified by CRC properties, which guarantee the detection of errors, located in the area, the length of which does not exceed the degree of generating polynomial [4].

One can consider, in particular, quite possible on practice [3] case of twofold error in the channel signal transmission. If the possibility of the channel signal erroneous transmission will be denoted through P_c, then possibility P_2 of the given case of large m values will be defined through the following expression:

$$P_2 \approx \frac{m^2}{2\cdot k^2}\cdot P_C^2 \quad (5)$$

In the considered case $2\cdot k$ block bits, which are not located in one area, can be potentially distorted. Keeping within the ongoing analysis, one can concede the most possible case that on distortion of both channel signals, which is caused by Gaussian noise, their amplitude changes for s. Such twofold error in the channel signal transmission is reliably detected by CRC, taking into account that on each error occurrence only one bit of the relevant code group is distorted, and such possibility equals 0.25. When the possibility constitutes 0.75, more than two bits are distorted, though they are not located in one area. The possibility of error non-detecting with the use of CRC constitutes 2^{-n}. Therefore, with the use of CRC twofold error in the channel signal transmission is detected with possibility $\frac{3}{2^{n+2}}$.

Thus, the use of existing error detection means, and CRC in particular, does not allow detecting effectively errors on channel signal transmission in the lines with amplitude modulation. Virtually, only one-fold error can be reliably detected.

The aim of the work is to increase error detection effectiveness in the data transmission channels with amplitude modulation via multiplicity increase of reliably detected errors in the transmission of channel symbols.

III. Modification of CRC for the Increase of Error Detection Effectiveness in the Data Transmission Channels with Amplitude Modulation

Hereafter it is proposed how to increase the effectiveness of CRC use in order to control errors in the network lines with phase-amplitude modulation of digital data through widening of the category of reliably detected error, namely, through twofold error detection on the channel signal transmission, and also through detection acceleration, which is connected with error control. Such method bases on the use of the data, for which the dominant type of pulse distortions is the change of ε amplitude for the value, which does not exceed $3 \cdot s/2$, where s is the value of pulse discrete at pulse-amplitude modulation.

The essence of the proposed method is that the calculation of CRC check code is carried out only with the account of low bit – x_1 of the code group with the omission of other bits. Then, on occurrence of one-fold error in the channel signal transmission, on condition that amplitude distortion will constitute not more than s, such error will be always reliably detected. On occurrence of twofold error in the transmission of the channel signal, which amplitude is distorted not more than on s discrete interval, only two bits are distorted in the bit order, which is checked by CRC. Such distortion is reliably detected while using standardized CRC polynomial. For reliable detection of one-fold errors in the channel signal transmission with the change of ε amplitude by $7 \cdot s/2$, it is proposed to calculate summarizing on module 2 of second bits $-x_2$ of all code groups of the controlled data block as an additional check bit.

Thus, unlike ordinary pattern of CRC use, the category of reliably detected errors widens due to twofold errors in the channel symbol transmission. Moreover, using the proposed method of CRC check code calculation, based on the fact that only every k-bit of the transmitted data block is processed, the speed of detection exercising, which is connected with error control, increases in k-times respectively.

IV. Multiple Error Detection in the Transmission of Channel Symbols with the Use of Weighted Checksum

On error occurrence in the channel signal transmission non-equally probable nature of the distortion of code group bits can be used to increase error detection effectiveness on the basis of weighted checksum application.

Hereafter it is suggested one of the variants how it can be put into practice, taking into account close to real probability distribution on occurrence of diverse errors [2].

It is proposed to calculate modified weighted checksum of $B=\{b_1,b_2,\ldots,b_m\}=\{X_1,X_2,\ldots,X_t\}$ block, where $t=m/k$ is the number of code groups in the block, as summarizing on module 2 of check codes of the code groups: $CS = V_1 \oplus V_2 \oplus \ldots \oplus V_t$. It is also proposed to form the check code of the code group from $\log_2 t+2$ bits, which are organized in three bit fields: $\log_2 t$ – discharge field Z_1 and two one-bit fields z_2 z_3: $V=Z_1 \mid z_2 \mid z_3$. Field Z_1 of V_i, $i=1,\ldots,t$ check code, which corresponds with i-code group X_i in the block, should be formed as the logical product of low bit x_l^i of X_i code group code, and digits of twofold code of W_i serial number of the code group in the block: $V_i= x_l^i \cdot W_i$, where $W_i=\{w_1^i,w_2^i,\ldots,w_l^i\}, l=\log_2 t, \forall e\in\{1,\ldots,l\}: w_e\in\{0,1\}$, noting that $\sum_{e=1}^{l} w_e^i \cdot 2^{e-1}=i$. One can use low bit x_l^i and after following bit - x_2^i of X_i code group as one-fold field z_2 and z_3 respectively. The use of developed weighted checksum modification allows detecting reliably all errors, which dominate in network lines with pulse-amplitude modulation.

On one-fold error occurrence in the channel signal transmission with high probability p_1, the former is caused by Gaussian noise, the amplitude of the channel pulse will change for ε value, which is within $s/2<\varepsilon<3 \cdot s/2$. While in such case low bit x_1 of transmitted code group X will be distorted, the bits of z_2 field of the corresponding V check code, as well as the checksums, will differ in the receiver and transmitter. By this it is meant that such error will be certainly detected.

On occurrence of two errors in channel signal transmission, which cause the change of ε pulse amplitude within $s/2<\varepsilon<3 \cdot s/2$ in both cases, z_2 fields of the checksums will be identical both in the receiver and transmitter. One can illustrate that by this the code of Z_1 field will be different in the receiver and transmitter. Let one concede that the errors took place on transmission of j– and i– channel signals, $i,j\in\{1,\ldots,t\}$ (of – X_i and X_j code groups respectively). While values of x_1^j bits differ in the receiver and transmitter, Z_l field of V_j check code in the transmitter consists of l zero bits (if $x_1^j = 0$ in the transmitter), whereas Z_1 field of V_j check code equals W_j in the receiver, because $x_1^j =1$ (or vice versa, in the case when $x_1^j =1$ in the transmitter, and $x_1^j =0$ in the receiver).

The same matter by analogy is with check codes in the transmitter and receiver for V_i check code: either Z_1 field of this code equals W_i, considering that it equals zero in the transmitter, or vice versa. From the above-mentioned it is obvious that Z_1 field summarizing on module 2 of check codes in receiver V_{jS} and transmitter V_{iR} equals W_j, as well as Z_1 field summarizing on module 2 of check codes in receiver V_{iS} and transmitter V_{iR} equals W_i. For all other channel signals summarizing on module 2 of check codes of the receiver and transmitter equal zero: $\forall u \in \{1,\ldots,t\}, u \neq i, u \neq j$: $V_{uS} \oplus V_{uR}=0$. Consequently, Z_1 field of checksums of the receiver and transmitter for the considered case of twofold error will equal $W_j \oplus W_i \neq 0$. By this it is meant that, unlike CRC application, twofold errors of the considered type, which dominate in comparison with other types of twofold errors, will be reliably detected by the suggested modification of weighted checksum. On one-fold error occurrence in the channel signal transmission with possibility $p_2 << p_1$, the former is caused by Gaussian noise, the amplitude of the channel pulse will change for ε value, which is within $3 \cdot s/2 < \varepsilon < 7 \cdot s/2$. While in such case second bit x_2 of transmitted code group X will be distorted, z_3 field bits of the corresponding V check code, as well as checksums, will differ in the receiver and transmitter. By this it is meant that such error will be reliably detected by the suggested modification of weighted checksum.

The occurrence of two errors in the channel signal transmission will cause the change of ε pulse amplitude within $s/2 < \varepsilon < 3 \cdot s/2$ in one case, and within $3 \cdot s/2 < \varepsilon < 5 \cdot s/2$ in another. In this case the distortion of bits of transmitted block is also reliably detected with the use of suggested modification of weighted checksum. Indeed, let one concede that mentioned errors took place on transmission of j– and i–channel signals, $i,j \in \{1,\ldots,t\}$ (of – X_i and X_j code groups respectively). For instance, one can concede that on transmission of j-channel signal the change of its ε amplitude is within $3 \cdot s/2 < \varepsilon < 5 \cdot s/2$, and on distortion of i-channel signal the change of its ε amplitude is within $s/2 < \varepsilon < 3 \cdot s/2$. Then, on transmission of X_i code group its second bit x_2^j will be distorted, but its low bit x_1^j will not be distorted. On transmission of X_i code group its low bit $-x_1^i$ will be certainly distorted, whereas after following bit x_2^i will be distorted with possibility 0.5. It follows from the abovementioned that bit field z_2 of V_i check code will differ in the transmitter and receiver, whereas for other check codes $V_1,\ldots,V_{i-1},V_{i+1},\ldots,V_t$ the values of bit field z_2 will be equal in the transmitter and receiver. Consequently, z_2 field of Δ code of checksum difference in transmitter and receiver does not equal zero, it means that two-fold errors of the considered type will be reliably detected.

The suggested modification of weighted checksum also allows to detect reliably errors in the transmission of odd channel signals, on condition that the change of ε pulse amplitude is within $s/2 < \varepsilon < 3 \cdot s/2$. As it was illustrated above, it is the most possible amplitude change which results in the distortion of bits of the controlled data block. It is important that on CRC application the detection of errors of such type, on condition that the number of erroneously transmitted pulses is more than one, is not guaranteed: they are detected with the possibility which depends on the degree of CRC generating polynomial [4].

Thus, the suggested modification of weighted checksum, which bases on the use of network lines with pulse-amplitude modulation, allows detecting reliably the types of errors, which dominate in such lines, by means of optimization of the checking information coding. Unlike traditionally used CRC for error detection in such lines, the suggested method has the following advantages:

1. Widening of the category of reliably detected errors by means of two-fold errors in the channel signal transmission, as well as errors in transmission of odd channel signals, which are detected by CRC with possibility $1\text{-}2^n$, where n is the degree of the generating polynomial. Indeed, on most frequently occurred type of errors in the channel signal transmission, when the change of ε amplitude of two distorted pulses is within $s/2 < \varepsilon < 3 \cdot s/2$, more than 2 bits of the controlled block will be distorted with possibility 0.75. According to CRC properties, on its application the distortion of more than two bits can be detected with possibility $1\text{-}2^n$.
2. Decrease of the number of controlled digits for relatively short blocks of transmitted data. On CRC use the number of controlled digits equals n (in practice, depending on application of CRC-16 and CRC-31, n=16 and n=32 respectively), but on the use of the suggested modification of weighted checksum the number of controlled digits equals $2+\log_2 t$. For example, on transmission control of the block with length 64 bites and 8-level pulse-amplitude modulation, $t = 2^{11}$, the required number of controlled digits equals 13.
3. Acceleration of the process of error control on data transmission, considering that, firstly, only 2 low digits of a symbol are controlled in the suggested modification of the checksum, and, secondly, there is a possibility of multi sequencing of detections, which are connected with the control of separate fragments of the transmitted block.

V. Conclusion

The conducted research, aimed at the increase of error detection effectiveness in the digital data transmission channels with pulse-amplitude modulation, has shown that traditionally used CRC technologies for the error detection do not guarantee the detection of important categories of errors, and in particular, bit distortions caused by errors in transmission of channel symbol signals, multiplicity of which exceeds one. Their specific characteristics have been analyzed to increase error detection effectiveness in channels with pulse-amplitude modulation. On this case the errors, which occur in such channels, have been analyzed from two viewpoints: from the point of multiplicity of errors in the channel signal transmission and from the point of possibility characteristics of the change in the amplitude of channel pulse, as well as the influence of the distortion of separate bits of the code group, which is modulated by one channel symbol signal. It has been proved that in channels with pulse-amplitude modulation possibilities of the distortion of code group separate bits greatly differ on occurrence of error in the transmission of modulated channel symbol signal, and the information content, which is connected with bit distortion, greatly differs as well. It opens potential opportunities for the increase of error detection means effectiveness in such lines through the optimization of checking information coding.

It is also suggested how to increase CRC application effectiveness for error control in the network lines with pulse-amplitude modulation of digital data due to category widening of reliably detected errors, namely, due to the detection of twofold (double) errors in the channel signal transmission.

The method of error detection has been developed and researched on the basis of weighted checksum use, which allows to widen the category of reliably detected errors, to decrease the number of controlled bits for relatively short blocks and the time for detections, which are connected with the error control in the speed of digital data transmission in the lines with pulse-amplitude modulation.

REFERENCES

[1] Sklar B. Digital communications. Fundamental and applications. Prentice Hall PTR. – 2001, pp. 1099.
[2] Blahut R.E. Theory and Practice of Error Control Codes. Mass.: Addison-Wesley Publishing Company, 2002, pp 452.
[3] Klove T., Korzhik V. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems. Norwell, MA: Kluwer, 1995, pp 433.
[4] Kounavis M.E., Berry F.L. A Systematic Approach to Building High Performance Software-Based CRC Generators.// 10th IEEE Symposium on Computers and Communications (ISCC'05), – 2005, pp. 855-862.
[5] Mercke R.C., “One-Way Hash Functions and DES” Advances in Cryptology-CRYPTO’89 Proceeding, Berlin: Springer – Verlag, 1990, pp.428-446.
[6] Vinogradov Y.N. Efficient calculation of hash-signatures in systems of data authenticity and information integrity //Visnuk NTUU “KPI” Informatics, management and processing techniques. K. “VEK+”, N36, 2003, pp. 131-143.
[7] Ningping, S., Ryozo, N., Nonbing, Z., Akiro, T., and Wenling, S. "An analysis of average search cost of external hashing with separate chain". Proceedings of 7-th WSEAS International Conference on Circuits, Systems, Communications and Computers (CSCC-2003). 2003, pp 315-324.
[8] Kohonen, T. Associative memory. N.Y. WHP., 2002, p198.
[9] Chang, C.C. The study of an ordered minimal perfect hashing functions // CACM Vol.24, №12, 2000, pp 384-387.
[10] Ramakrishna, M.V., and Bannai, Y. "Direct perfect hashing function of external files", Journal of Database Administration, Vol.2, №.1, 1991, pp 19-28.
[11] Cichelli, R.J. Minimal perfect hash functions made simple // CASM v.23 n.1-, 1980, pp 17-19.