MOSCAD CYCLIC REDUNDANCY CHECK (CRC) MECHANISM

INTRODUCTION

Noise and bandwidth limitations of communication channels cause errors in transmission of digital signals. The errors in binary digital transmission are usually measured in Bit Error Rate (BER) which is an average of error bits measured over some statistically significant period of data transmission.

Relatively high BER and burst errors are quite common in radio channels where Signal-to-noise ratio (S/N) is a major factor and is closely linked to the fade margin of the radio channel.

The most common way of dealing with noisy communication channels is to divide the data into frames and send a few extra bytes of check-sum information with each transmitted frame. The check-sum is a numeric value computed from the data being transmitted. The check-sum is then used by a receiver to verify the correctness of the received data. This method of data verification is called error detection.

There are several methods to perform error detection. The most common are:

- transmission of parity bits
- Cyclic Redundancy Check (CRC) code

Byte Parity entails addition of a bit to each byte. This bit is one ("1") if the byte contains an even (odd) number of "1" bits. The method is therefore called Even (Odd) Parity. This method provides some verification, but many of the errors remain undetected.

In a variation of the byte parity method, several bytes of data are grouped into a block. An additional parity byte is appended to each block of data (block parity). This method suffers from limitations similar to Byte Parity.

The most powerful error detection method is the CRC. This method is based on results from the cyclic group theory and is the most reliable means for error detection. The MOSCAD RTU supports the CRC error detection as described below.

The MOSCAD RTU transmits its information and acknowledgments in frames. The length of the frame is variable. This length varies from 7 bytes (excluding CRC) for a short acknowledgment to a maximum of 200 bytes for a full data frame.

MOSCAD CRC ERROR DETECTION

The MOSCAD RTU offers an extraordinary level of error detection and it supports two types of commonly known and internationally acknowledged error detection mechanisms:

- CRC-16 for line communication and RS-232 asynchronous interface
- CRC-32 for radio communication and RS-232 synchronous interface

The MOSCAD RTU has also a built-in efficient Automatic Repeat Request (ARQ) mechanism which causes selective retransmission of a corrupted frame.

CRC-16

CRC-16 is a remainder of a polynomial division, modulo two. This is a 16-bit number defined by the CCITT V.41 standard. The polynom is:

$$X^{16}+X^{15}+X^{5}+1$$

The minimum Hamming distance of this error detection code is 4. It means that any two valid frames of equal length will differ in at least four bits.

The CRC-16 can detect:

- 100% of all single-bit errors
- 100% of all two-bit errors
- 100% of all odd bit errors
- 100% of all burst errors (several adjacent bits are garbled) of length 16 or less
- 99.9969% of all burst errors 17 bits long

- 99.9985% of all burst errors longer than 17 bits

So, in fact, the undetected BER is virtually 0 for most types of errors.

On top of that MOSCAD has a selective re-transmission mechanism (retransmission of error frames only) which improves the throughput immensely.

CRC-32

The CRC-32 bit polynom is (as defined by the IEEE 802.3 standard):

$$X^{32}+X^{26}+ X^{23}+ X^{22}+ X^{16}+ X^{12}+ X^{11}+ X^{10}+ X^{8}+ X^{7}+ X^{5}+X^{4}+ X^{2}+ X+1$$

This polynom is used for protection of frames, where the total number of bits is less than 12,144 (including CRC) as specified by the IEEE 802.3 standard. Under this constraint, the minimum Hamming distance of the code is 4.

In MOSCAD RTUs the maximum length of a frame is 1,632 bits (200 bytes/frame * 8bits/byte + 32 CRC bits). Under this condition, the minimum Hamming distance is 5. The Hamming distance increases with decreasing frame lengths.

The CRC-32 can detect:

- 100% of all single-bit errors
- 100% of all two-bit errors
- 100% of all three bit errors
- 100% of all four bit errors
- 100% of all burst errors (several adjacent bits are garbled) of length 32 or less
- 99.999999953% of all burst errors 33 bits long
- 99.999999976% of all burst errors longer than 33 bits

Therefore Virtually no errors will remain undetected with the use of CRC-32.

References:

Peterson, W. " Cyclic Codes for Error Detection.", Proc. IRE, Jan 1961, pp. 228-235.

Cambell, Joe. C Programmers Guide to Serial Communications. Indianapolis, Ind.: Howard W. Sams, 1988

CCITT V.41: Code Independent Error Control, Blue Book, Volume VIII, Facsile VIII-1, 1988

ANSI/IEEE Standard for Local Area Networks, “Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification”, 1984

T. Fujiwara et al. “Error Detecting Capabilities Of The Shortened Hamming Codes Adopted For Error Detection In IEEE Standard 802.3”, IEEE Transactions on Communications, Vol. 37, No. 9, September 1989, pp 986-989.