

BITT POLYTECHNIC, RANCHI

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

What is Error Detection and Correction?

As we know errors occur to the data during data transmission as well as data processing stages. The errors can occur due to various reasons such as electrostatic interference from nearby circuits, attenuation due to cable or path resistance, distortion due to inductance/capacitance, transmission loss due to leakages etc.

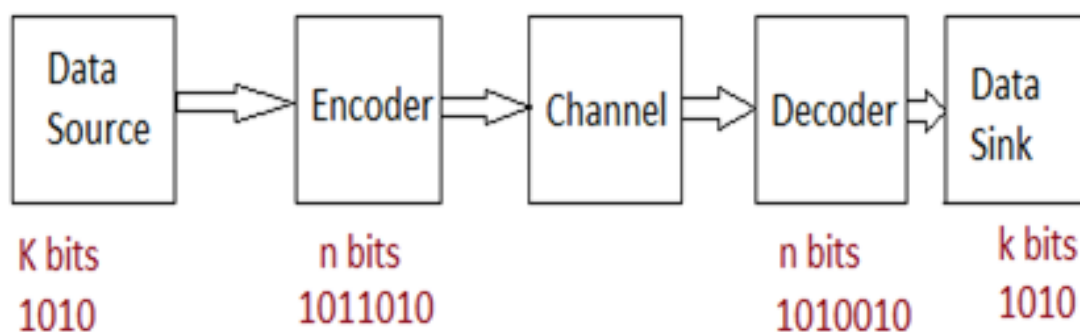
LAN and optical cables introduce less errors than wireless networks. The errors can be of two types viz. single bit error and burst error.

TYPES OF ERROR | SINGLE BIT ERROR, BURST ERROR

Single bit error : Only one bit in the data unit changes in single bit error. Single bit error can happen if we are sending data using parallel transmission.

Burst error : Multiple bits are changed in the burst error. Burst errors can be caused by impulse noise.

Principle of Error Detection



Principle of Error Detection

- When frame is transmitted from transmitter to the receiver. There are two possibilities viz. frame is received without error, frame is received in error (i.e. frame is bad).

- Error detection helps in detecting errors in a received block or frame by the receiver.
- Once the error is detected receiver informs the transmitter to re-transmit the same frame again.
- Error detection can be made possible by adding redundant bits in each frame during transmission. Based on all the bits in the frame (i.e. data + error check bits), receiver is capable of detecting errors in the frame.

Following are the explanation of error detection modules.

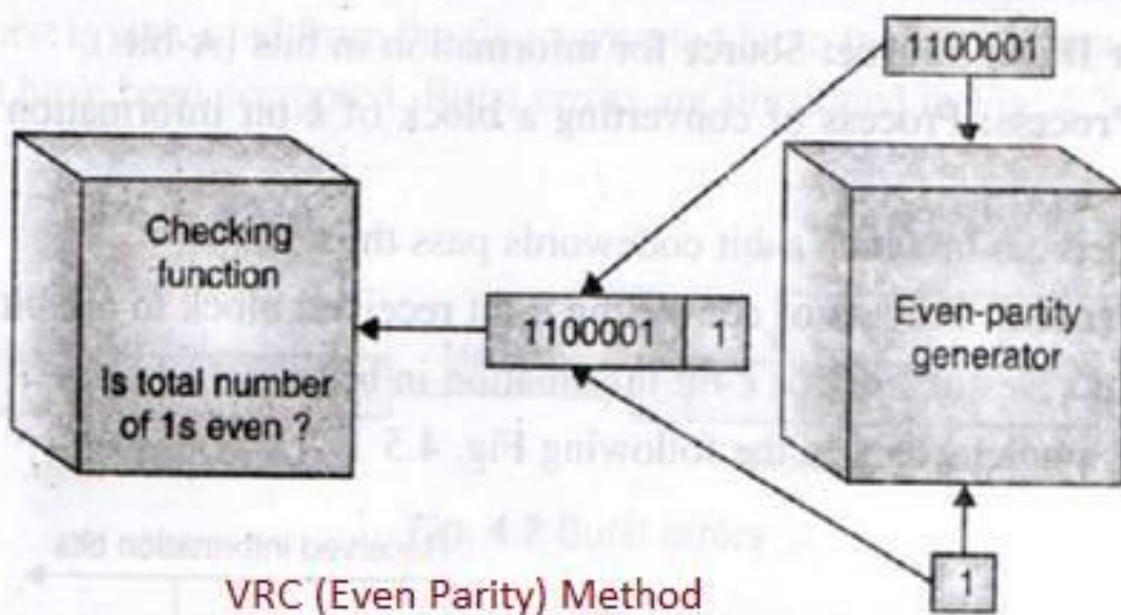
- ▶ Message (or data) source : Source of information in bits (K bits)
- ▶ Encoding process : Process of converting block of k-bit information to n-bit codeword. $n = k + 1$.
- ▶ Channel : Medium in which n-bit codewords pass through.
- ▶ Decoding process : Process of converting n-bit received block to k-bit message.
- ▶ Message sink : Destination for k-bit information in bits.

Error Detection Methods

Following are the **error detection methods** or techniques of error detection in networking.

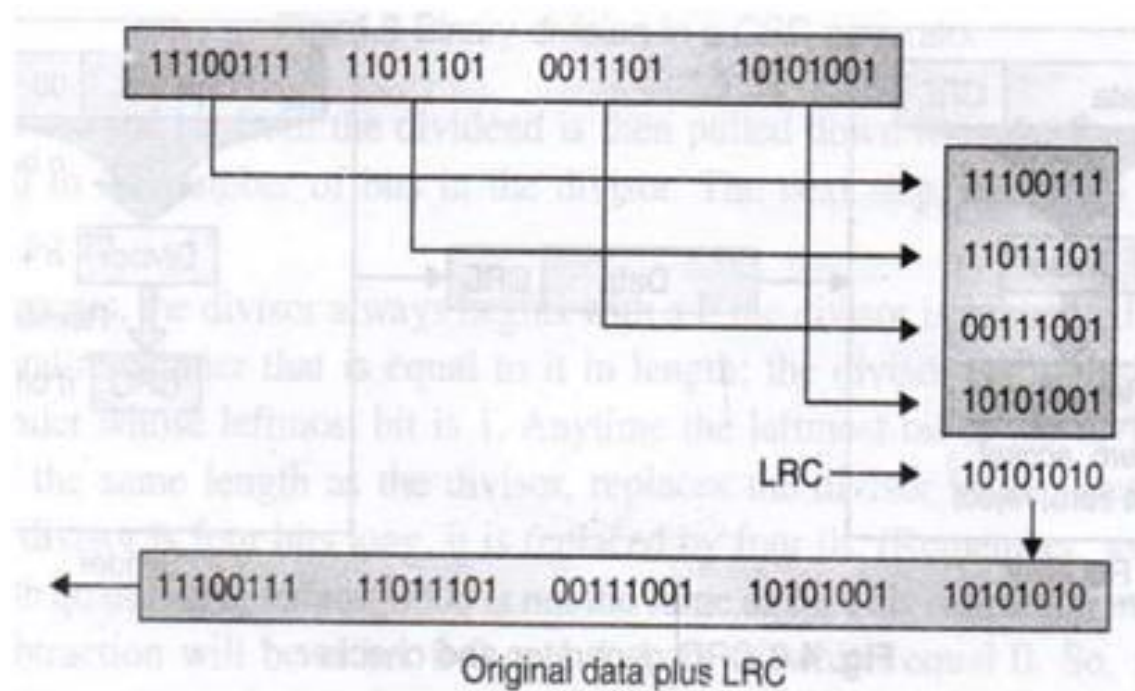
1. VRC Method
2. LRC method
3. CRC method
4. Checksum method

Parity check or vertical redundancy check (VRC) method



In this error detection technique, a redundant bit called parity bit is appended to every data unit so that total number of 1's in the unit (including parity bit) becomes even. The system now transmits entire extended unit across the network link. At the receiver, all eight received bits are checked through even parity checking function. If it counts even 1's data unit passes. If it counts odd number of 1's, it means error has been introduced in the data somewhere. Hence receiver rejects the whole data unit. Similar way odd parity VRC can also be implemented. In this method, total number of 1's in should be odd before transmission.

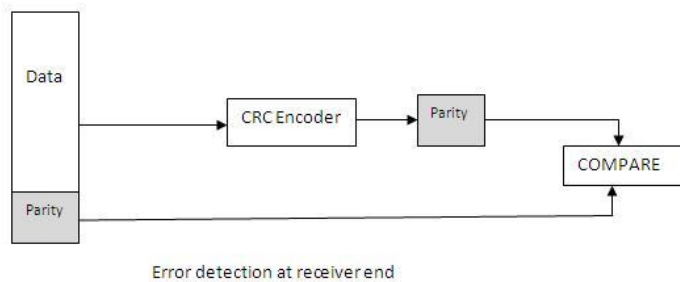
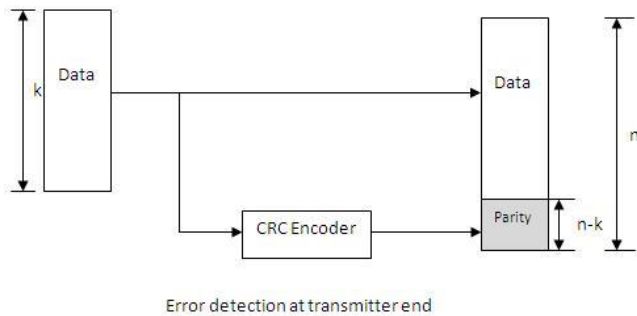
Longitudinal Redundancy Check (LRC) method



In this error detection method, a block of bits are organized in a table (of rows and columns). For example, instead of sending block of 32 bits, first it is organized into four rows and eight columns. Then parity bits for each column is calculated and new row of eight parity bits is formed. These eight parity bits are appended to original data before transmission.

CRC Error Detection and Correction Example

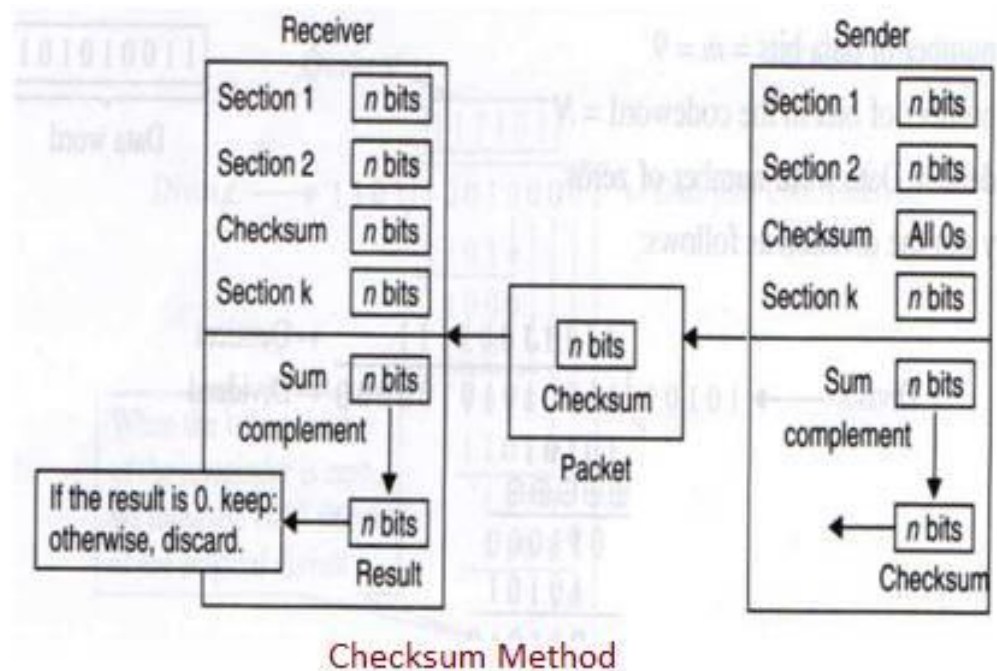
Following figure-2 depicts CRC addition at transmitter end. CRC is calculated based on received block and compared with CRC appended by transmitter. When calculated CRC and original CRC is equal, frame is considered to be error free. When calculated CRC and original CRC is not equal, frame is said to be erroneous.



As shown in the figure, k bits are passed to the encoder block to generate parity bits. This parity bits are added to input data bits and are transmitted as n bits. Hence $n-k$ are parity bits. This happens at the transmitter.

As shown in the figure at the receiver, parity bits along with data bits of total length n bits are passed to the encoder. From the data part crc is again computed and will be compared with the received CRC bits and based on this data is corrupted or not is decided. This process is called error detection and **correction**.

Checksum method



There are two modules in this error detection method viz. checksum generator and checksum checker. In the transmitter, checksum generator subdivides data unit into equal segments of n bits (usually 16). These segments are added together using one's complement arithmetic in such a way that total is also n bits long. The total (i.e. sum) is then complemented and appended to the end of the original data unit as redundancy bits, called checksum field. The extended data unit is transmitted across the network. So if sum of data segment is equal to T , checksum will be $-T$.

The receiver subdivides the data unit as above and adds all segments together and complements the result. If the extended data unit is intact, the total value found by adding all data segments and checksum field should be zero. If the result is not zero, the packet contains error and receiver rejects the packet.