Computer Networks - CS 204

Rishit Saiya - 180010027, Summary

April 17, 2020

1 Data Error

Transmitted data over a cable/channel always has a chance that some of the bits will be changed/flipped (0 to 1 or 1 to 0) due to noise, signal distortions, attenuation or intrusion into the network by an outsider.

Random Errors change the bits in an unpredictable fashion. Each bit has a certain probability of being changed. These errors are in general due to the thermal noise, exhaustion in servers, etc.

Burst Errors change a certain segment of bits in succession. They are often caused due to faulty registers in the electrical components, etc.

2 Error Detection

The error in transmission are inevitable and result in changes in one or more bits in a transmitted frame.

Some of the notations we use here are as follows:

- F : The number of bits in the frame.
- p_b : It denotes the probability of a single bit error, which is called as *Bit Error Rate*.
- p_1 : It is the probability that a frame arrives with no bit errors in it.
- p_2 : It is the probability that a frame arrives with one or more undetected bit errors.
- p_3 : It is the probability that a frame arrives with one or more detected bit errors but no undetected bit errors.

If no Error Detection scheme is used, we can conclude the following:

$$p_1 = (1 - p_b)^F$$

$$p_2 = 1 - p_1$$

$$p_3 = 0$$

WLOG, we can say that higher the length of the frame i.e., higher F, results in high p_b and low p_1 and higher p_2.

Error detection is not 100% reliable. The protocols may miss some errors but rarely though. Larger the error detection and correction bits redundancy will yield better results and detection.

2.1 Hamming Distance

The Hamming Distance is calculated for 2 bit patterns. The Hamming Distance H is the number of positions where the two bit patterns differ. Those positions are calculated by checking the positions of 1s when we XOR the two bit patterns.

For example: Consider 2 bit patterns: 11010, 01011.
The resulting hamming code when we XOR the above 2 codes are:

$$(11010) \text{ XOR } (01011) = 10001$$

Since there are 2 1s in these, so the H = 2. For a group of codes, the Hamming Distance H, is decided by selecting the minimum of all Hamming Distances calculated from the Transmitted Code. Once the H of a group of bit patterns is known, we try to detect the error involved till there from Transmitted Code.

By using this idea and theory of Hamming Code, we can use this concept for Error Detection.

2.2 Parity Check

This is one of the simplest error detection techniques. It appends a parity bit to the end of a block of data. The odd number of bit errors can be detected. If an even number of bits are inverted due to error, an undetected error occurs.

This technique is also not 100% reliable, as noise impulses are often too long enough to destroy more than 1 bit, particularly at high data rates. **Even Parity** So if our data has odd number of 1s we add 1 at the end to make even number of 1s in the data. Whereas if there are even number of 1s in the data, we simply add 0 at the end. **Odd Parity** So if our data has odd number of 1s we add 0 at the end to make odd number of 1s in the data. Whereas if there are odd number of 1s in the data, we simply add 0 at the end.

2.3 Checksum Testing

This is another way of checking for errors. This is a number calculated from the data and sent along with the data. If any errors occur during transmission, then checksum for the received data will differ from the transmitted data.

A simple checksum technique is adding all the data. In general this is done for 16-bit long data. If the checksum turns out to be longer than 16-bit, then it only transmits the 16-bit.

2.4 Cyclic Redundancy Code

This is essentially a more sophisticated type of checksum where it is extremely unlikely that any errors will go undetected.

The data is regarded as being one very long binary number. Place holder digits are added onto end and it is divided by a generator polynomial using modulo 2 division. The remainder at the end of this division is the CRC.

2.5 Cyclic Redundancy Check

When given a k- bit block of bits, the transmitter generates an n-bit sequence, known as the Frame Check Sequence (FCS), so that the resulting frame, consisting of k+n bits, is exactly divisible by some predetermined number. The receiver then divides the incoming frame by the number and, if there is no remainder, it is assumed that there was no error.