**Networking Assignment**

Student name

Institutional Affiliation

Table Contents

[Data Communication Error detection and recovery 3](#_Toc70435917)

[Cyclic redundancy codes 3](#_Toc70435918)

[Hamming Code 4](#_Toc70435919)

[Digital modulation techniques and encoding schemes. 4](#_Toc70435920)

[Digital modulation techniques 4](#_Toc70435921)

[Amplitude-shift keying (ASK), 5](#_Toc70435922)

[Frequency-shift keying (FSK) 5](#_Toc70435923)

[Phase-shift keying (PSK) 5](#_Toc70435924)

[Digital data encoding schemes. 5](#_Toc70435925)

[Non-Return to Zero (NRZ) 6](#_Toc70435926)

[Bi-phase Encoding 6](#_Toc70435927)

[Manchester encoding 7](#_Toc70435928)

[Deferential Encoding 7](#_Toc70435929)

[The TCP/IP model suite 7](#_Toc70435930)

[Network interface layer 9](#_Toc70435931)

[Internet layer 9](#_Toc70435932)

[Transport layer 10](#_Toc70435933)

[Application Layer 10](#_Toc70435934)

[Analysis of User Datagram Protocol (UDP) 10](#_Toc70435935)

[IP addressing 12](#_Toc70435936)

[Principles of IP addressing 12](#_Toc70435937)

[Class A 13](#_Toc70435938)

[Class B 13](#_Toc70435939)

[Class C 14](#_Toc70435940)

[Subnetting 14](#_Toc70435941)

# Data Communication Error detection and recovery

The transmission of data or information between a source and a receiver is referred to as data communications. The data is sent by the source and received by the receiver. The actual generation of information, as well as the resulting action of the information at the receiver, is not included in Data Communications (Bardis, 2017). In today's world of high-speed computers, dependable data communication is critical. In real-world communication systems, however, perfect data transmission does not exist. Errors, no matter how minor, will always be present.

Errors are caused by one of two factors. First, there may be a component malfunction, causing the data to be altered. The second, and by far the most common, type of error occurs when the communication channel picks up noise. Communication lines are located outside of the computer and are subjected too much worse conditions than data paths found inside the computer (Bardis, 2017). Errors don't usually happen one by one. It's more likely that they'll happen in bursts. That is, if there is any noise on the communications line, more than one bit of the received data would most likely be incorrect. To make matters worse, errors do not occur in a predictable pattern over time.

Errors, as well as data, are transmitted between digital communication systems. Data will be lost until these errors are identified and corrected. Data should be transferred with great precision for efficient communication (Panem et al, 2019). This can be accomplished by identifying and correcting errors first. The method of detecting errors in data transmitted from transmitter to receiver in a communication device is known as error detection. To detect these errors, we add redundancy codes to the data as it is transmitted from the source (transmitter). These codes are known as error detection codes. The most popular and effective method of error detection codes are cyclic redundancy codes and hamming codes.

## Cyclic redundancy codes

The most effective and simple to implement error detection mechanism is cyclic redundancy codes. CRC is based on binary division, while checksum is based on addition. A series of redundant bits called cyclic redundancy check bits is appended to the end of the data unit in CRC. A second, set binary number divides the resultant data unit exactly. The inbound data unit is separated by the same binary number at the recipient end. The data packet is approved if the balance is zero. A remainder suggests that the data packet experienced an error during delivery and was thus rejected by the recipient. The technique of generating the CRC bit is explained below:

If we can consider that there is an n bit message to be transmitted from source to destination, the sender device generates a k-bit sequence known as frame check sequence (FCS). The k bits are attached to the n bits so that (n+k) bits are transmitted as a package. The k-bit frame check order is produced by splitting the n bit message, attached by k zeros, by a set number. This number is (k + 1) bit segment, and it is considered as coefficient of a generator polynomial. The r-bit Frame check sequence is produced as the balance of binary division. Once the (k + r) bit frame is acknowledged, it is divided by similar set number. If the remainder part is zero, it indicates that there was no error, and the frame is accepted by the receiver. CRC is a powerful tool for identifying errors in data that is commonly used in data transmissions, data storage space, and data compression. It's also used for detecting logical faults and checking integrated circuits.

## Hamming Code

This code not only detects but also corrects the error bit in the entire data sequence. This code employs a variety of parity bits at strategic locations in the code word. The number of parity bits is calculated by the number of data bits. The hamming code makes use of the relationship between redundancy bits and data bits, and it can be used for any number of data bits. The redundancy bits in Hamming code are put at specific calculated locations to avoid errors. The Hamming gap is the distance between the two redundancy bits.

# Digital modulation techniques and encoding schemes.

## Digital modulation techniques

The method of encoding a digital data signal into the transmitted signal's amplitude, phase, or frequency is known as digital modulation. The encoding process has an effect on the transmitted signal's bandwidth and robustness to channel degradation. The aim of spectral efficiency is to determine how quickly data can be transmitted within a given bandwidth. The most popular digital modulation techniques include;

### Amplitude-shift keying (ASK),

ASK is a type of amplitude modulation in which bit values are assigned to non-continues amplitude levels. To transmit information, the carrier signal is modulated among the members of a set of discrete values.

### Frequency-shift keying (FSK)

FSK is a type of frequency modulation in which bit values are assigned to distinct frequency levels. There are two types of FSK: noncoherent and coherent. The gradual frequency shifts between two distinct values known as the "mark" and "room" frequencies in noncoherent forms of FSK. There is no phase break in the output signal of coherent FSK. FSK modulation formats produce modulated waveforms that are purely real values, so they don't have the same characteristics as quadrature modulation schemes.

### Phase-shift keying (PSK)

## PSK is a form of angle modulation used in digital transmissions, in which the carrier's phase is independently varied to represent data, either in relation to a reference phase or the phase of the signal unit immediately preceding it. Some PSK systems have only two possible carrier phase angles; each phase shift carries one bit of data, so the bit rate is equal to the modulation rate.

## Digital data encoding schemes.

Until information can be transmitted through communication channels, it must first be encoded into signals. The waveform pattern of voltage or current used to represent the 1s and 0s of a digital signal on a transmission connection is known as digital to digital line encoding.

### Non-Return to Zero (NRZ)

The NRZ Codes have a high voltage level of 1 and a low voltage level of 0. The voltage level remains constant during bit intervals, which is the key characteristic of NRZ codes. If the value of the previous bit and the value of the current bit are the same, the end or start of a bit will not be shown, and the voltage state will remain the same.

Figure 1 Non-Return to Zero (NRZ)

### Bi-phase Encoding

Three voltage levels are used in bipolar. Positive, negative, and zero are the three options. Bit 0 happens when the amplitude is zero. Bit 1 is also known as Alternate Mark Inversion because it happens alternately when the voltage mark is either positive or negative (AMI). Since the pulses for Is are polarized differently, there is no DC part.

Figure 2 Bi-phase Encoding

### Manchester encoding

Manchester encoding is a synchronized clock encoding technique that the physical layer uses to scramble the clock and a synchronous data bit stream (Jameel, 2018). A logic 0 is identified by a 0 to 1 transition in the middle of the bit, and a logic 1 is identified by a 1 to 0 transition in the middle of the bit in this encoding. It's worth noting that signal transitions don't always happen at the 'bit borders' (the line separating one bit from the next), but there is always one in the middle of each bit.

Figure 3 Manchester encoding

### Deferential Encoding

Differential encoding is a digital encoding technique that uses a signal shift rather than a specific signal state to represent a binary value. Binary data in any user-defined I/Q or FSK modulation can be encoded during the modulation process using differential encoding. Data is expressed by changes rather than levels in this encoding scheme. Rather than stage, it is a more accurate and error-free method of change detection. It's easy to lose track of polarity in complicated transmission layouts.

# The TCP/IP model suite

The TCP/IP model, is a group of communication protocols that are used to link network nodes on the internet. In a local area network, TCP/IP can also be used as a networking protocol (an intranet or an extranet). Davidson (2012) affirms that TCP/IP defines how data is shared over the internet by defining

End-to-end communications that define how packets should be broken down, handled, distributed, routed, and received at their destination. TCP/IP is designed to make networks stable, with the ability to recover automatically from the failure of any computer on the network, and it needs little central management. The TCP/IP suites comprise of two main protocols; TCP and IP.

TCP specifies how applications can establish communication pathways through a network. It also controls how a message is broken down into data packets and sent over the internet, where it is reconstructed in the correct order at the destination address. This IP address is checked by each gateway device on the network to decide where the message should be forwarded.

The TCP/IP protocol suite consisting up of four layers namely; Network interface layer, internet layer, transport layer and application layer (Mundra & El Taeib, 2015).

Figure 4 TCP/IP Model

### Network interface layer

The Network Interface layer is in control of sending and receiving TCP/IP packets on the device medium. TCP/IP was designed to be system-agnostic in terms of system access, casing organization, and medium. This layer consist of protocols such as ARP, IP and RARP

**ARP** – Address resolution protocol. This protocol binds an ever-changing IP address to a media access control address also known as physical address of the machine.

**IP** - Internet protocol. This protocol determines the source and destination address of the machines in a network.

**RARP** – Reverse Address resolution protocol. This networking protocol is used by client machine to request IP address given the physical address of the machine also known as media access control address.

### Internet layer

This layer's primary function is to transfer packets from any network or device to their destination, regardless of the path they take. With the support of different networks, the Internet layer provides a practical and procedural mechanism for transmitting variable length data sequences from one node to another. The major protocol in this layer is IP, ICMP, IGMP and ARP.

**IP** protocol is concerned with routing the packets from source to destination on the internet layer of TCP/IP model.

**ICMP** – Internet control message protocol. The Internet Control Message Protocol is responsible of providing symptomatic capabilities and reporting errors caused by failed IP parcel delivery.

**IGMP** - The Internet Group Management Protocol (IGMP) is in charge of managing IP multicast groups.

### Transport layer

The Transport layer is in charge of providing session and datagram information to the Application layer. TCP and UDP are the two most important protocols in this layer.

**TCP**- Transmission Control Protocol is an internet protocol suite that decomposes messages into smaller data packets and reassembles them on the receiving end. It is a secure, one-to-one, connection-oriented communications service.

**UDP** – User datagram protocol is a connectionless and unreliable communication service that facilitates exchange of both broadcast and multicast type of data transmission.

### Application Layer

The application layer is the fourth and final layer in the four-layer TCP/IP model. The Transport layer is mounted on top of the Application layer. The Application layer switches between layers and defines the protocols that applications use to exchange data. The protocols in this layer include HTTP, FTP, SMTP, and Telnet

**HTTP** – The Hypertext Transfer protocol is concerned with the exchange of web documents over the internet in World Wide Web system.

**FTP** – the File Transfer protocol is used to transfer file in a computer network. It's a widely used standard protocol for sending files from one computer to another.

**SMTP** – the Simple Mail Transfer protocol is used to send and receive messages over the e-mail system.

**Telnet** - this protocol that allow remote communication between computers over the network.

# Analysis of User Datagram Protocol (UDP)

UDP is a Transport layer protocol that provides connectionless and unreliable communication services between different network devices. In this practical we will capture and analyze UDP traffic, identify source and destination Media access control address, source and destination IP address using wireshark network analyzer.



Figure 5 Analysis of User Datagram Protocol (UDP)

Identifying source and destination media access control address



Figure 6 Identifying source and destination media access control address

Identifying source and destination IP address



Figure 7 Identifying source and destination IP address

# IP addressing

### Principles of IP addressing

An IP address is a number that tells you how to get to a particular host, usually outside the LAN. An IP address is a 32 bit number having an address space of 232. IP addresses are binary numbers, so they're usually written in decimal (IPv4) or hexadecimal (IPv6) thus making them easier to read and use for humans (Garcia-Jimenez et al, 2009). The Internet Protocol (IP) is a group of standards and specifications for generating and distributing data messages, across networks. The Internet Protocol (IP) is a component of the Internet protocol suite's Internet layer.

IP was created to function in a complex network. This means that IP must function without the use of a central catalogue or display, and it cannot depend on the existence of certain links or nodes. Since IP is a connectionless, datagram-oriented protocol, each data packet must include the source IP address, destination IP address, and other information in the header to be transmitted successfully. IPv4 and IPv6 are the two variants of IP currently in use.

On the internet and in several business networks, the original IPv4 protocol is still in use today. The IPv4 protocol, on the other hand, only allowable for 232 addresses. This, combined with the way addresses were assigned, resulted in a situation where there would be insufficient unique addresses for all internet-connected devices (Sisat et al, 2012). The Internet Engineering Task Force (IETF) created IPv6 and formalized it in 1998. This update significantly expanded the address space available, allowing for a total of 2128 addresses.

Notably, an IP address is typically represented as four octets of numbers ranging from 0-255 in decimal form rather than binary form. There are two pieces of IPv4 addresses. The network is specified by the first numbers in the address, while the host is specified by the last numbers. A subnet mask defines which part of an address is used for networking and which part is used to address a particular host. IP version 4 is grouped into five classes; A, B, C, D, and E.

### Class A

In a Class A network, the network part of the address is the initial eight bits, or the first octet, and the host portion of the address is the remaining portion of the address. There are 128 different Class A networks to choose from. However the address 127.0.0.0 is referred to as loopback address.

### Class B

The first 16 bits of an address in a Class B network addresses are the network component. The first bit of a Class B network is set to 1 and the second bit is set to 0. Class B networks are defined as 128.0.0.0 to 191.255.0.0 in dotted decimal notation. There are 16,384 different Class B networks to choose from.

###

### Class C

**Class D** addresses are not used for normal networking operation since the addresses are used for multicasting applications.

**Class E** addresses are reserved and their usage was never defined.

## Subnetting

References

Bardis, N. G. (2017). Efficient Error Detection and Correction in Block Data Transmission. In *Green IT Engineering: Concepts, Models, Complex Systems Architectures* (pp. 161-184). Springer, Cham.

Davidson, J. (2012). *An introduction to TCP/IP*. Springer Science & Business Media.

Garcia-Jimenez, S., Magana, E., Izal, M., & Morato, D. (2009, October). IP addresses distribution in Internet and its application on reduction methods for IP alias resolution. In *2009 IEEE 34th Conference on Local Computer Networks* (pp. 1079-1086). IEEE.

Mundra, S., & El Taeib, T. (2015). TCP/IP protocol layering. *International Journal of Computer Science and Information Technology*, *3*(1), 415-417.

Jameel, L. W. (2018). Manchester Coding and Decoding Generation Theortical and Expermental Design. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, *42*(1), 130-138.

Panem, C., Gad, V., & Gad, R. S. (2019). Polynomials in Error Detection and Correction in Data Communication System. In *Coding Theory*. IntechOpen.

Sisat, S. N., Bhopale, P. S., & Barbudhe, V. K. (2012). IP Subnetting. *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, *2*(5), 5.