Comp347: Computer Networks (Revision 7)

Tma2

Assignment 2

Andrew Mackay

ID:3441988

Comp347: Computer Networks (Revision 7)

Assignment 2

1.

Comparing TCP and UDP connections is relatively simple as they are polar opposite in most ways.

UDP or User Datagram Protocol is the more modern network connection protocol although many systems still rely of TCP otherwise known as Transmission Control Protocol for various reasons. Both have distinct differences.

TCP connections are thought of as reliable but slow, UDP being more unreliable while faster, while TCP involves a connection with segment switching and UDP is connection-less. The optimal uses of TCP are for HTTPS, HTTP, POP,SMTP, FTP whereas the optimal uses for UDP are video conferencing, streaming, DNS, VoIP etc.(lifesize, 2017)

2.

TCP establishes a reliable data service by means of assigning a sequence number to an octet(sequence of 8 bits), there is a timeout window where if this data is not received within the time frame it will be sent again. These octets have a limit of 1024 bytes. The timeout intervals are determined by each connection based on total round trip time calculated. Status information is initialized and maintained during this process which includes information on the sockets, sequence numbers and window sizes, which as a whole is called a connection. The receiver in this process sorts through sequence numbers which are received as duplicates or damaged, misplaced data. The amount of data sent is governed by acknowledgments indicating which sequence numbers can be sent according to the last received. Each socket is uniquely identified by means of combination of port number in addition to network and host addresses. (ibm, 2022)

3.

RDT stands for reliable data transfer and is represented in 3 different scenarios being RDT1 2, and 3.

The first RDT is over a perfectly reliable channel, the ideal scenario, but not very realistic. The sending and receiving occur without interruption, the FSM defines operation of the sender and receiver. Both having just one state. This protocol has no difference in a packet of data or a unit of data, and there is no feedback from the receiver at all as there is no reason for it in this seamless scenario.

For RDT2 the second scenario is that there is some bit loss along the way, a medium level of reliability in the scale of RDT. This is not a perfectly seamless scenario of data transfer between sender and receiver but is more realistic. Bit errors occur in the physical components of networks as a packet is transmitted buffers or propagates, and the order they are received may be jumbled. A process of error detection commences where a receiver will communicate with the sender over missed or corrupted packets through positive and negative acknowledgments, or use check sums to allow the sender to detect and recover without needing feedback from receiver, or for sender to resend the whole packets when receiving feedback.

In RDT3 this is the most non ideal scenario, where data is transferred over a lossy channel with bit errors. In addition to bits being corrupted, this scenario presents a new element where they can also be entirely lost. In this scenario the issue of how to detect lost packets and also what to do after detection. There would likely be no ACK or NAK from a receiver if the data was entirely lost so the sending time frame would time out, eventually the data will be re transmitted.

4.

The Go-Back-N protocol allows the sender to transmit multiple packets without acknowledgement, but has a limit of N unacknowledged packets within the pipeline. The sender keeps track of the packets sent and denotes that when receiving ACK from receiver they then change their sequence number to [0, -1] where the packets that are not yet ACK are [base, nextseqnum-1] and packets next in interval are [nextseqnum,base +N - 1] which is for packets that are available to send. The sequence numbers which are >=base+N need to have NAK with sequence number base is ACK. The GBN sender must be able to respond to three main types of events which are invocation from above, receipt of an ACK, and A timeout event.

5.

Error detection is important in message transmission, as there are many things that can happen along the way such as data corruption, lost packets, mixed order of messages.

These are 4 basic error detection techniques: Simple parity check, two dimensional parity check, cyclic redundancy check, and checksum. (Geeksforgeeks, 2016)

A parity of 1 or 0 is added when a block of data is sent and then checked for a match upon being received. It can either be an odd number of 1’s and 0’s or even. If the number of received bits doesn’t match the initial parity number then communication can be stopped until the issue is identified. (Techopedia, 2022)

The two dimensional parity check is a kind of parity check where the blocks of bits are organized in a table and check bits are calculated in each row, and column thus creating the 2 dimensions, as a regular parity check is equivalent to only one row so to say. It is more likely to detect a burst of errors with this method. However there are still situations where this is flawed such as the situation where there are 2 damaged bits in one unit parallel to another unit within the same situation, none of these will be detected. (generalnotes, 2022)

In a cyclic redundancy check there is binary division where a sequence of redundant bits. CRC are also known as polynomial codes because of the bit strings polynomial arithmetic involved in the binary its interpretation. Each piece of data is represented as D, and the bits are represented as R, the calculation is d+r in binary pattern. Where the sender and receiver agree upon a generator, which is a r + 1 bit pattern known as G. D+ R are exactly divisible by G using modulo operator. The receiver divides the received bits by G and if the remainder is not 0 than it is known an error has occurred.

Check summing is somewhat of an overarching term where more than one technique falls into this category. In all check summing techniques D bits of data are equivalent to K bit integers which can be summed and then using the sum as the error detection bit based on the expected value.

6.

In virtual circuits the networks provide a connection only at the network layer which is an alternative to the more popular datagram based network. ATM and Frame relay fit into the category of VC networks.The centralized node can at the most contain 65535 bits as each 16 bit port has this limit. Using the centralized pathway, the node restricts the boundary within a 16 bit field of 2^16 which is equal to 65536 bits/number of virtual circuits.

Q2.1

To convert a binary number into 1s compliment we simply invert the numbers..(tutorialspoint, 2022) It is noted that inversion is different than simply reversing the order of numbers, it is switching each number that is 0 to 1 or 1 to 0 in the sequence. In this case the numbers given are “11011001, 01010010, 11001010, 10100100 and 01011001.” So 1s compliment versions of these comma seperated binary sequences is 00100110, 10101101, 00110101, and 10100110

In order to sum the bytes we take the first 2 binary sequences given (01010011) + (01100110) which = 10111001

This result is than added to the leftover sequence.

(10111001) + (01110100) = 100101101 carry +1, which is then added to the last significant digit within the sum.

00101110 which is then finally inverted to 1s compliment version 11010001

B)

There are uncertainties when sending data and also the links along the path even checking for errors, and even if successful transfer occurs there could still be bit errors upon storing bits. The 1s compliment provides the checksum of the UDP which is valuable in that it is not error prone or has processed errors within the checksum. The checksum is done regardless but 1s compliment simplifies the process, and enhances the chances of detecting an error.

C)

UDP at sender side first performs 1s compliment of 16 bit words then the result is put in the checksum within the UDP segment. If any bit is 0 it detects errors whereas finally if there are no errors it will be converted to all 1’s after this whereas otherwise there would be no error detection.

D)

1 bit errors with this method are always detected however it is possible that 2 bit errors can go undetected. They can still be detected but there is the possibility that there will still be errors.

Q2.2

A)

The link state routing algorithm is an effective way to show the paths between different nodes and which will be the path of least resistance vs the most, comparatively. The least cost path from node to all other nodes in the network is known as “u” . After iterating through the network it is then known which are the most effective paths to other nodes.

The total number of nodes searched to find

This table tells us that the minimum distance is 1, as there is a direct path from v,w,x from u.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B)

Q2.3

Ross, J.F.K.K. W. (2013). Computer Networking: A Top-Down Approach (6th ed.). Pearson Learning Solutions. https://online.vitalsource.com/books/9781269392488

IBM Documentation. (2022). Retrieved 21st October 2022, from https://www.ibm.com/docs/ro/aix/7.1?topic=protocols-transmission-control-protocol

Cook, M. (2017). TCP vs. UDP: What’s the Difference?. Retrieved 1st October 2022, from <https://www.lifesize.com/blog/tcp-vs-udp/>

Error Detection in Computer Networks - GeeksforGeeks. (2016). Retrieved 12th November 2022, from https://www.geeksforgeeks.org/error-detection-in-computer-networks/

What is a Parity Check? - Definition from Techopedia. (2022). Retrieved 12th November 2022, from <https://www.techopedia.com/definition/1803/parity-check#:~:text=A%20parity%20check%20is%20an,bit%20scheme%20as%20the%20sender.>

note, g. (2022). Two-dimension Parity Check to detect error. Retrieved 12th November 2022, from <https://generalnote.com/Computer-Network/Error-Detection-and-Correction/Two-dimension-Parity-Check.php>

One’s Complement. (2022). Retrieved 14th November 2022, from https://www.tutorialspoint.com/one-s-complement#:~:text=To%20get%201's%20complement%20of,least%20significant%20bit%20(LSB).