Analyzing Network Performance: Analyzing Delay, Throughput, and Packet Drops with TCP and UDP Protocols

1 Summary

To analyze the network performance, it is first necessary to adopt a circular wireless network topology of at least 10 nodes, 20% of the nodes are assigned to send nodes, 20% of the nodes are assigned to receive nodes, 60% of the nodes are assigned to relay nodes, and the sender and receiver pairs are randomly selected, 10% are assigned to TCP, and 10% are assigned to UDP. After scenario Settings are set as required, perform simulation for 1000 seconds, generate TRACE (.tr) and NAM (.nam) files, and perform 20 simulations of the same topology to obtain the average value for performance analysis. Finally, after the TRACE file and NAM file are generated, the performance analysis is performed. First, the delay analysis needs to be performed to calculate the end-to-end delay of the network and determine the cause of the delay. Then, the total throughput of the network is judged to analyze the causes of high throughput and low throughput. In my awk code, I do network packet processing where the script calculates the latency of the packet and prints out some statistics such as the number of packets sent, the average latency, the number of packets discarded, etc., after a certain period (in this case 20 seconds). After all the data was processed, the END block calculated the final statistics and printed them out, and in awk I also sliced the simulation time.

Finally, when we finish the run and analysis, we will save the values of delay, throughput, and packet drop to an Excel file. Visualize performance metrics with any application for graph generation and data presentation.

2 Introduction

I will introduce the circulator wireless network from the following several aspects. The first one is ring topology in computer networking. The second one is the structure and operation of ring topology. The third one is circulator wireless network.

In computer networking, network topology refers to the physical or logical arrangement of devices and connections in a network. One such topology is the ring topology, which provides simplicity, efficient data transfer, reduced network congestion, and cost effectiveness. However, it also has some limitations, such as the possibility of a single point of failure, limited scalability, slower data transfer as the number of devices increases, and difficulty in troubleshooting the network. Before implementing a ring topology, it is critical to consider the specific needs of the network, the number of devices, and the level of fault tolerance required (Dham, 2023).

In a ring topology, devices are connected in a one-way fashion, forming a continuous circular loop where each device happens to be connected to two other devices, creating a path for the data loop. When a device sends data, it travels along the loop until it reaches the intended recipient. Each device checks the data as it passes through and forwards it if necessary. This helps maintain data integrity and reliability across the network. In addition, ring topologies often include redundancy to enhance fault tolerance. If a node or connection fails, data can still propagate around the ring in the opposite direction, bypassing

the failed node or connection. Overall, this seamless information flow ensures efficient communication within the network and this structure also ensures defined data transmission paths, minimizes conflicts and optimizes information flow for one-way data flow and fault-tolerant communication (Dirk, 2023).

A ring wireless network is a wireless network configuration in which nodes are wirelessly connected to each other to form a closed ring or ring-shaped structure. Each node communicates with its neighbors via wireless signals, and data is transmitted along a ring path, but unlike a wired ring topology, there is no need to physically connect the lines. Data transmission in ring wireless networks is usually achieved through directional antennas.

By analyzing ring topology and circulator wireless network, Circulator wireless network can be regarded as a wireless implementation of ring topology. It uses wireless connection and directional antenna to realize data transmission between nodes in ring topology. Circulator is a key component in the circular wireless network, which ensures the one-way flow of data on the circular path, thereby improving the reliability and efficiency of the network. In general, circulator wireless network is a special ring topology implemented in a wireless environment, using wireless connections and circulator to achieve one-way data transmission between nodes.

In general, compared with the traditional wired ring topology, the ring wireless network has the advantages of wireless connectivity, easy deployment, scalability, fault tolerance, flexibility and cost effectiveness. These benefits make them particularly suitable for a wide range of applications, including outdoor monitoring, industrial automation, smart agriculture, and emergency response.

In my code, I implement a 10-node circular wireless network topology by using the circulator wireless network. In a circulator wireless network, nodes are connected to each other in a circular or ring structure to form a closed loop. Then, TCP and UDP are used as the transport layer protocols for communication between the sender and receiver. Finally, the designed circular wireless network topology is simulated to analyze network performance indicators such as delay, throughput, and packet loss.

3 Proposed Work

According to my TCL file, I first configured the network and defined various parameters of the simulation, such as wireless channel, propagation model, wireless interface, MAC protocol, queue type, link layer type, antenna type, etc. These parameters determine the communication mode between nodes in the simulation network. Second, set up trace files to record simulation events for analysis. This includes a trace file for general events and another trace file for visualizing the network topology using NAM, which visualizes the network topology and node movements. Then, I create a network topology that specifies the size of the simulated area and the number of nodes. Nodes are configured with specific characteristics, such as their mobility model, routing protocols, and so on, as well as the location of the nodes within the simulation area, and then a god function is created to store information about the total number of moving nodes. Nodes are uniformly placed in a circular manner within the simulation area, with each node assigned coordinates according to its Angle within the circle. Thus, a circular wireless topology with radius 200 consisting of 10 nodes is obtained in the ns-2.35 environment. Nodes are not connected by wires, forming a circular wireless network topology, so that the logical arrangement of nodes and connections presents the data transmission process. Use new-trace to open TRACE file to record the data during simulation, and use NAM file to visualize the network transmission process. Configure Node3 and node9 for UDP traffic, follow the UDP protocol, and create a CBR application to

generate the packets. Node1 and node5 configure TCP traffic, follow the TCP protocol, and create FTP applications to simulate file transfer. This configuration allows the network to simulate the network behavior of different types of protocols (UDP and TCP). Next, a simulation is performed, running for the duration it specifies. After the simulation is over, clean up by resetting the node and closing the trace file. At the end of the simulation process, AWK file is used to analyze the TRACE file, and the data is collated to compare the performance of the ring wireless network.

The protocols used in network simulation include: AODV, TCP, and UDP. AODV is suitable for dynamic networks with frequent node mobility and topology changes. TCP is commonly used for applications that require reliable and orderly data transfers, such as web browsing and file transfers. Unlike TCP, UDP does not guarantee the delivery or order of packets. It is suitable for applications that prioritize low latency and minimal overhead, such as real-time multimedia streaming and online gaming. In terms of protocol operation, AODV protocol establishes and maintains routes between nodes according to the current network topology and communication requirements. TCP guarantees reliable data transmission by managing connections, retransmission, and flow control, while UDP enables fast, lightweight communication. In summary, my code sets up a simulated wireless network environment, generates traffic, performs simulations, and provides mechanisms to analyze network behavior and performance.

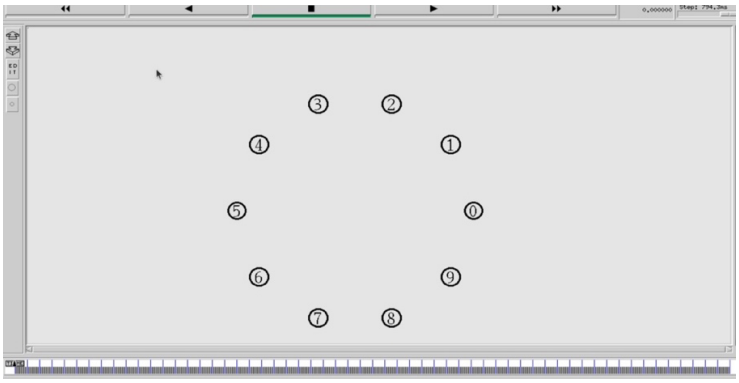

Figure 1: This picture is circle topology with 10 nodes.

4 Results and Discussion

According to the tr file after AWK file analysis, we can see that the Average end to end delay(ms) of TCP is 977.02, and the Total No. of dropped packets of TCP is 217. The Average end to end delay(ms) of UDP is 3302.45, and the Total No. of dropped packets of UDP is 220224. In the line chart, we can also see that compared with UDP, TCP throughput is higher.

In terms of End-to-End Delay, as for TCP, the average end-to-end delay is 977.02 milliseconds, while UDP has a longer average end-to-end delay of 3302.45 milliseconds. The reason of UDP having a longer average end-to-end delay is that UDP does not guarantee the delivery or order of packets. TCP is directly impacted by latency (Boris, 2016). Because it incorporates a mechanism to check that all packets are delivered correctly. It involves the receiver sending a specific packet or flag to the sender to confirm the correct reception of the packet (Boris, 2016).

In general, the delay of UDP is lower than that of TCP, because UDP is a connectionless protocol, which does not need to establish and maintain the connection state, nor does it have congestion control and packet retransmission mechanism. Therefore, the overhead during transmission is relatively small and the latency is usually low. However, in my data, the delay of TCP is lower than that of UDP. This may be because in my network, the network may be congested, and TCP can adjust the sending rate according to the congestion, so the delay of TCP may be smaller than that of UDP.

In terms of Packet Drop, TCP lost 217 packets with a packet drop rate of 1.03%, UDP lost 220,224 packets with a packet drop rate of 91.89%. High packet drop can lead to higher latency, as the sender must retransmit the lost packets, causing additional delays in data transmission. Lost packets can cause delays in data transmission, leading to increased latency or delay times (Alyssa, 2023). The reason of packet drop is that long distances between network devices or multiple network hops can increase the likelihood of packet drop. Another possible cause of packet loss is network congestion. When network traffic is high, packets may be delayed or lost due to limited bandwidth. However, TCP has a packet drop retransmission mechanism during data transmission. When a TCP sender sends a packet, if no acknowledgement is received from the receiver, the retransmission mechanism is triggered to resend the packet. In addition, TCP can reduce the congestion window when the network is congested. In this way, TCP has a lower packet drop rate than UDP.

In terms of Throughput, as for TCP, according to line chart, TCP has a higher throughput than UDP. Because higher throughput values indicate a higher rate of successful packet delivery, TCP has a higher rate of successful packet delivery (Alyssa, 2023). High throughput can be due to ample bandwidth, efficient protocols, and minimal congestion. Instead, low throughput can be caused by congestion, network errors, inefficient routing, or bandwidth limitations. In addition, TCP is a reliable transport protocol that ensures reliable transmission of data through sequence number, acknowledgement, and retransmission mechanisms. In addition, the lost, damaged, or duplicate data will be detected during transmission and appropriate measures will be taken to ensure the integrity and reliability of the data. In contrast, UDP is a connectionless and unreliable transport protocol, so lost or incorrect packets can occur during data transfer. Therefore, the throughput of TCP is higher than that of UDP.

In summary, according to the differences between TCP and UCP in latency, packet loss and throughput, it shows the trade-off between reliability and efficiency in network communication.

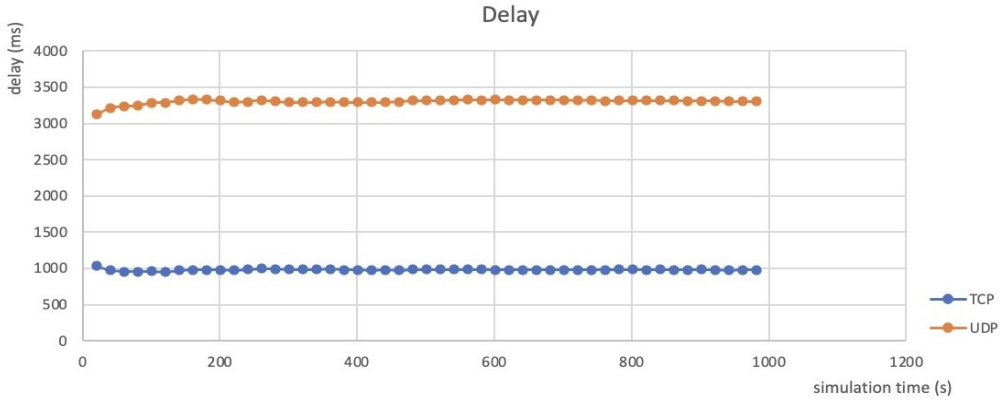

Figure 2: This picture is the value of delay.

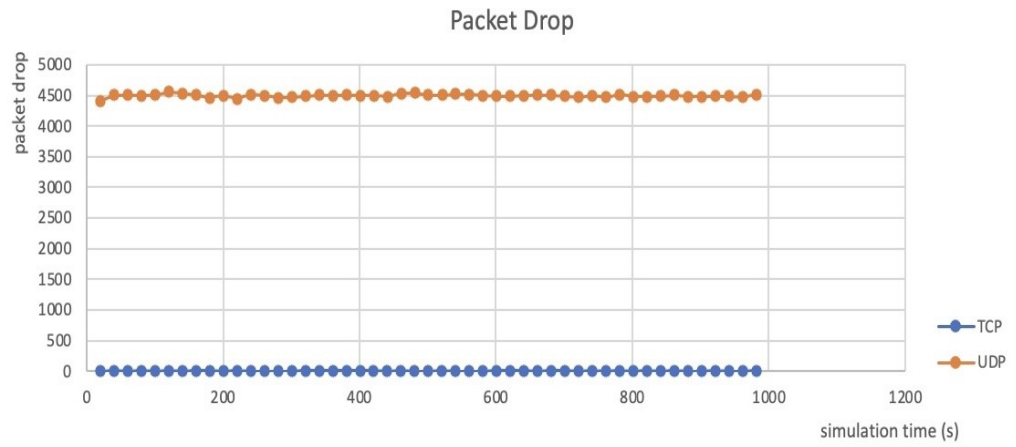

Figure 3: This picture is the value of packet drop.

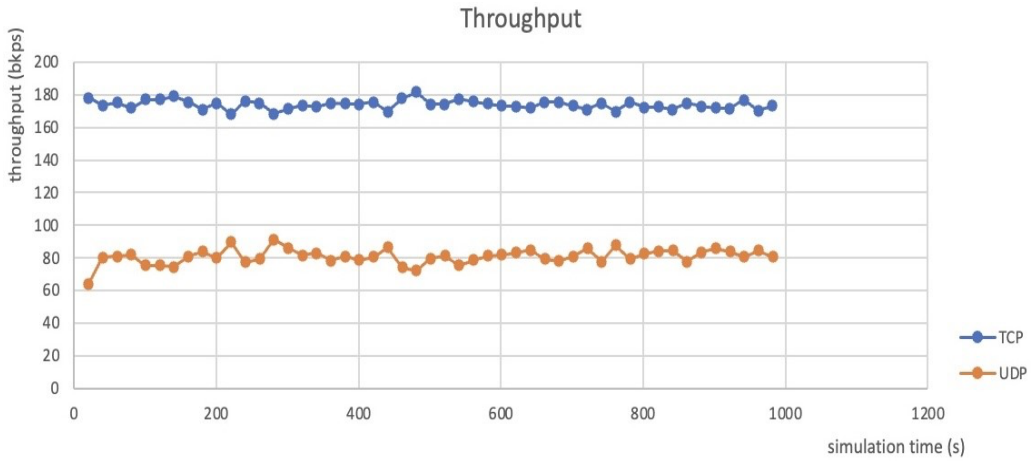

Figure 4: This picture is the value of throughput.

5 Conclusion

In conclusion, this work involved the simulation and analysis of a network using TCP and UDP protocols. Through simulations, we gain an understanding of network performance in terms of latency, throughput, and packet loss. According to the data analysis, because there may be a problem of network congestion, and TCP can adjust the sending rate according to the degree of network congestion, TCP usually shows lower latency compared with UDP. To enhance this work, the effects of different protocol configurations on network simulation performance can be explored. In addition, we can study how to reduce network congestion, which can largely avoid network congestion and improve the efficiency and reliability of the network. Even reducing network congestion can reduce packet loss rates. Secondly, according to the experimental results, it is necessary to reduce the packet loss rate of UDP. Reducing the number of hops and link load between network nodes can reduce the possibility of packet loss. Adjusting the data transfer rate can also prevent packet loss caused by network congestion. Finally, according to the experimental data, to make the network better applied to the actual network usage scenario, the network throughput can be appropriately improved.

6 References

Alyssa, L. (2023) *What is Network Throughput: How to Monitor, Test & Improve It* [online] Available at https://obkio.com/blog/what-is-network-throughput/ [Accessed at 30 April 2024]

Alyssa, L. (2023) *What Is Packet Loss & How Does It Affect Network Performance?* [online] Available at https://medium.com/obkio/what-is-packet-loss-how-does-it-affect-network-performance-c38fe32ce2e7 [Accessed at 30 April 2024]

Boris, R. (2023) *Measuring network performance: links between latency, throughput and packet loss.* [online]Available at: https://accedian.com/blog/measuring-network-performance-latency-throughput-packet-loss/ [Accessed at 30 April 2024]

Dham, M. (2023). *Advantages and Disadvantages of ring topology* [online]. Available at: https://www.prepbytes.com/blog/computer-network/advantages-and-disadvantages-of-ring-topology/ [Accessed at 2 May 2024]

Dirk (2023) *Ring Topology Overview: Exploring the Circular Network Design* [online] Available at: https://network-guides.com/ring-topology/#:~:text=How%20It%20Works%3A%20In%20a%20ring%20topology%2C%20devices,it%20passes%20by%20and%20forwards%20it%20if%20necessary. [Accessed at 2 May 2024]