Report on NS2 Offline: CSE 322

Shamit Fatin: 1805055

January 2023

List of Figures

1 Description on Protocols Used

1.1 MAC 802.11

The MAC 802.11 protocol (WiFi) establishes a set of guidelines that wireless devices must abide by in order to communicate with one another. These guidelines cover data transmission and reception, access to the wireless network, and how to handle device conflicts. The MAC 802.11 protocol functions at the data link layer, serving as a bridge between the physical layer (which controls the actual transfer of data over the airways) and the network layer (which handles the routing of data between devices). The MAC 802.11 protocol comes in a number of variations, each with its own set of features and functionalities. The versions 802.11b, 802.11g, 802.11n, and 802.11ac are some of the most popular ones.

1.2 MAC 802.15.4

Low-power wireless devices must adhere to the 802.15.4 protocol (low-rate wireless personal area network: LR-WPAN) in order to connect with one another. Its low power consumption, low cost, and short-range capabilities make it a popular choice for Internet of Things (IoT) and industrial automation applications. The MAC 802.15.4 protocol offers a standardized method for wireless devices to interact with one another and operates at the data link layer. Since it is so adaptable, the MAC 802.15.4 protocol can be applied in a variety of situations. To meet the unique requirements of various types of devices, it supports several physical layers, as well as various frequencies and modulation methods. The protocol also offers a number of security measures, like as encryption, authentication, and access control, to guarantee the confidentiality and integrity of data transfer.

1.3 DSR

Dynamic Source Routing (DSR) is a routing protocol used in wireless mesh networks and mobile ad hoc networks (MANETs). Because it uses reactive routing, a route is only found when a source node needs to communicate information to a destination node. The DSR protocol's fundamental objective is to identify the fastest, most direct path between any two network nodes. The route discovery procedure is started by the source node and entails broadcasting a route request (RREQ) message to other nodes in the network in order to do this. The RREQ message is broadcast to other nodes in the network once a node gets it and modifies its routing table with the data in the message. The RREQ continues to be broadcasted until it reaches the destination node or a node that has information about the destination node. At this point, the destination node or the intermediate node sends a route reply (RREP) message back to the source node along the reverse path of the RREQ message. The RREP message contains the route information that the source node needs to send data to the destination node. Once the source node has received the RREP message, it can start sending data to the destination node along the route specified in the RREP. The DSR protocol uses source routing, meaning that the complete route from the source to the destination is stored in each packet header. This eliminates the need for intermediate nodes to maintain routing information, reducing the overhead associated with route maintenance.

1.4 TCP

TCP (Transmission Control Protocol) is a communication protocol used for transmitting data over the Internet and other networks. The main goal of TCP is to ensure the reliable and efficient transmission of data between applications running on different devices. It does this by dividing the data into segments, which are then transmitted over the network and reassembled at the destination.

TCP provides a reliable, ordered, and error-checked delivery of data between applications. It ensures that data is transmitted in the correct order and that any errors or lost data are detected and retransmitted.

1.5 TCP Reno

TCP Reno is a congestion control algorithm used in the Transmission Control Protocol (TCP) to manage network congestion and ensure reliable data transfer. It is one of the most widely used congestion control algorithms, along with TCP Vegas and TCP New Reno.

The main goal of TCP Reno is to prevent network congestion by reducing the rate at which data is sent over the network. It does this by monitoring the number of unacknowledged packets (also known as the number of outstanding packets) in the network and adjusting the transmission rate accordingly.

TCP Reno uses a mechanism known as "slow start" to gradually increase the transmission rate until the network becomes congested. At this point, the algorithm enters a "congestion avoidance" phase, where it reduces the transmission rate in response to the increased number of unacknowledged packets.

The specific details of the congestion avoidance phase in TCP Reno are what differentiate it from other congestion control algorithms. In TCP Reno, the transmission rate is reduced by halving the size of the congestion window, which determines the maximum number of unacknowledged packets that can be in the network at any given time.

Once the congestion window has been reduced, the algorithm enters a "fast recovery" phase, where it waits for acknowledgment of the remaining packets. If the number of unacknowledged packets decreases, the congestion window is gradually increased again until it reaches its maximum value. If the number of unacknowledged packets does not decrease, the algorithm enters a "slow start" phase again, gradually increasing the transmission rate until the network becomes congested.

1.6 FTP

FTP (File Transfer Protocol) is a standard protocol for transferring files between computers over a network. It allows users to upload and download files to and from a server, and supports the transfer of large files, including binary files like images, audio, and video, as well as text files like documents and scripts. FTP uses a client-server architecture, with an FTP client connecting to an FTP server to initiate a transfer. FTP supports basic authentication and can also use encryption for secure file transfers.

2 Data Report

The experimentation was done in 2 ways:

- Using 802.11 protocol with no energy model
- Using 802.15.4 protocol with energy model

Report on both experiment is shown below:

2.1 Area Variation on 802.11

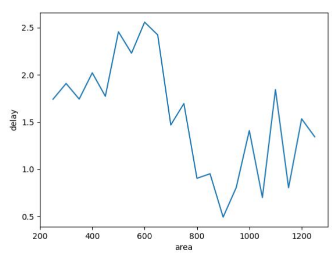

Figure 1: area variation on 802.11: delay calculation

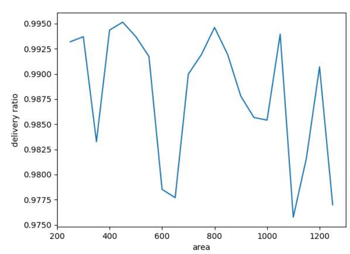

Figure 2: area variation on 802.11: delivery ratio calculation

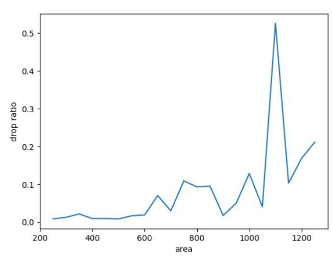

Figure 3: area variation on 802.11: drop ratio calculation

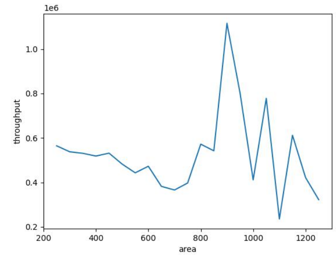

Figure 4: area variation on 802.11: throughput calculation

2.2 Node Variation on 802.11

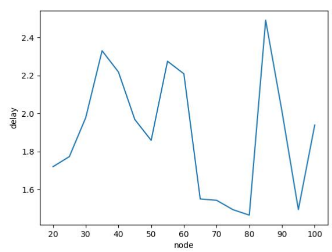

Figure 5: node variation on 802.11: delay calculation

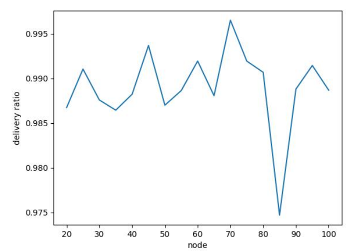

Figure 6: node variation on 802.11: delivery ratio calculation

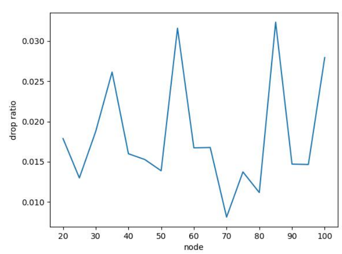

Figure 7: node variation on 802.11: drop ratio calculation

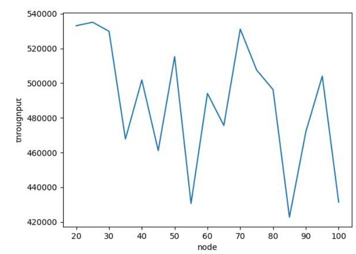

Figure 8: node variation on 802.11: throughput calculation

2.3 Flow Variation on 802.11

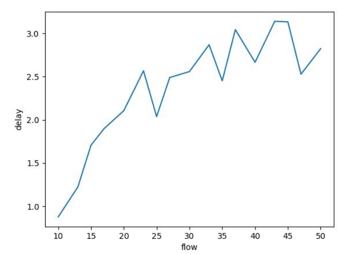

Figure 9: flow variation on 802.11: delay calculation

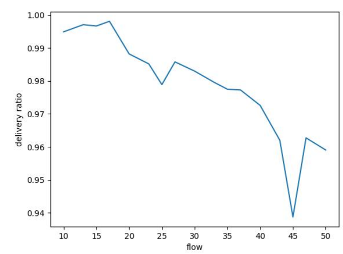

Figure 10: flow variation on 802.11: delivery ratio calculation

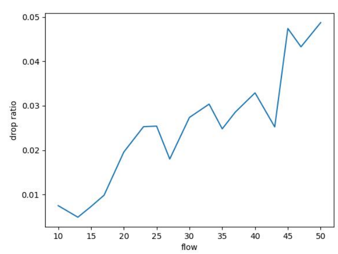

Figure 11: flow variation on 802.11: drop ratio calculation

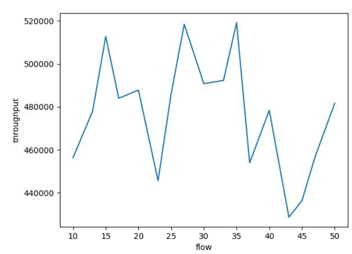

Figure 12: flow variation on 802.11: throughput calculation

2.4 Area Variation on 802.15.4

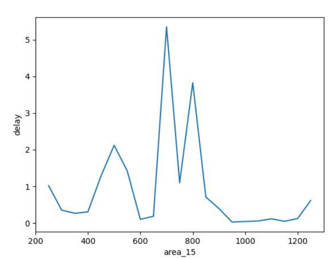

Figure 13: area variation on 802.15.4: delay calculation

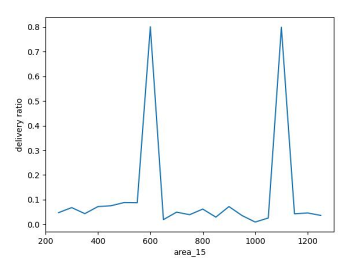

Figure 14: area variation on 802.15.4: delivery ratio calculation

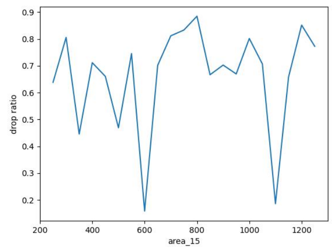

Figure 15: area variation on 802.15.4: drop ratio calculation

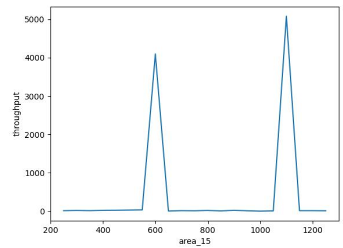

Figure 16: area variation on 802.15.4: throughput calculation

2.5 Node Variation on 802.15.4

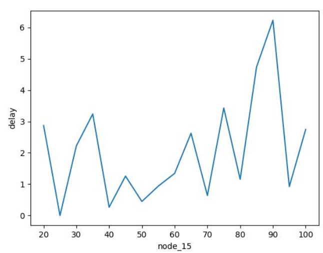

Figure 17: node variation on 802.15.4: delay calculation

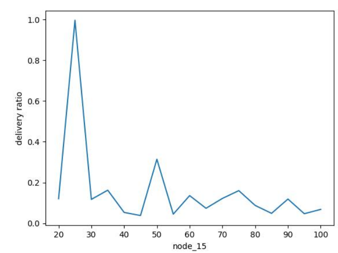

Figure 18: node variation on 802.15.4: delivery ratio calculation

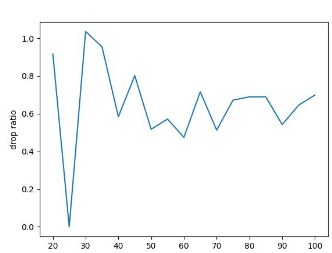

Figure 19: node variation on 802.15.4: drop ratio calculation

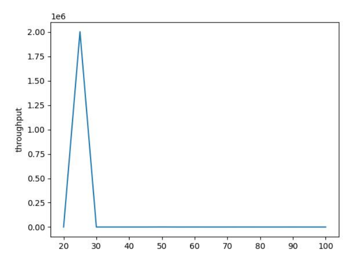

Figure 20: node variation on 802.15.4: throughput calculation

2.6 Flow Variation on 802.15.4

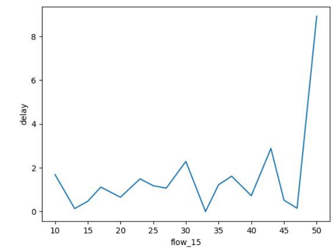

Figure 21: flow variation on 802.15.4: delay calculation

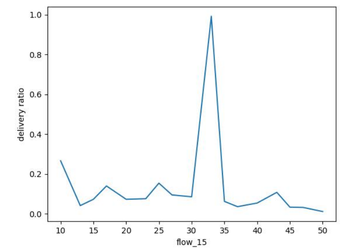

Figure 22: flow variation on 802.15.4: delivery ratio calculation

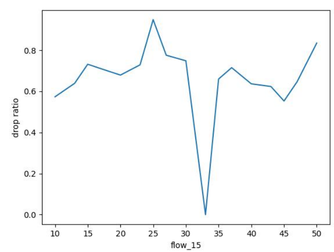

Figure 23: flow variation on 802.15.4: drop ratio calculation

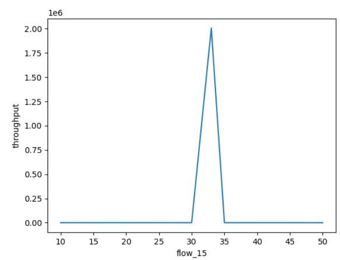

Figure 24: flow variation on 802.15.4: throughput calculation

3 Observation

The results of the experiment measuring network performance in a wireless system did not align with our expectations. Further analysis is necessary to fully understand the deviation from the anticipated outcomes.

3.1 802.11

When examining the effect of changes in the size of an area on throughput, it is generally believed that a decrease in area size will result in an increase in throughput. This hypothesis holds true for areas smaller than 600, but becomes less predictable for larger areas. There have been instances where a performance improvement was observed at a grid size of 900, however, this is not a consistent trend as a decrease in performance has also been observed at a grid size of 1100. This variability suggests that the relationship between area size and throughput is complex and requires further analysis.

Additionally, an increase in the packet drop ratio as the area size increases can be observed, which is a predictable result. However, no correlation has been established between changes in area size and changes in the delivery ratio. These findings indicate that further research is necessary to fully understand the relationship between area size and network performance metrics.

When analyzing the impact of changes in the number of nodes within a 500x500 grid on network performance metrics, no clear correlation has been observed. This lack of relationship is likely due to the consistent flow of data in the network and the random selection of source and destination nodes for each flow. Unless there is a collision in the routing path, the network performance should remain stable and unaffected by changes in the number of nodes. These results suggest that the network's architecture and flow management protocols effectively mitigate the potential impact of changes in node count.

During the course of our experiments, we found that changes in the flow of data were the most predictable factor impacting network performance. Our results show that as the number of flows increases in a fixed environment, network performance decreases. This result is in line with expectations, as a higher volume of flows results in increased inter-node traffic and can lead to congestion, leading to a decrease in overall network performance. These findings highlight the importance of effective flow management in maintaining optimal network performance.

3.2 802.15.4

One challenge encountered when utilizing the 802.15.4 protocol is that it was designed for small-scale networks. In a network with a size of 500x500 meters, where nodes are typically spaced 50 meters apart, there is a high likelihood of packet loss along the transmission path. To address this issue, we attempted to increase the power of the packets to reduce the frequency of packet loss. While this approach did result in improved transmission of some packets, it was insufficient to reliably measure network performance metrics. The dependence on chance for successful packet transmission hindered our ability to gather accurate and meaningful data. Further investigation and optimization of the network design and configuration is necessary to effectively address this issue.