# CENG-519 TPPhase-2

Berke Can Ünlü - 2381028

## 1 Setup

I have changed the Dockerfiles of sec and insec containers to install the scapy library for Python.

## 2 Development

I have created covert-channel-sender.py and covert-channel-receiver.py in sec and insec containers, respectively. ”Padding Bytes: Using padding areas in IP packets to store covert messages.” is the covert channel that I choose. I decided to pad IP Options header which has maximum size of 40 bytes.[1]. The first byte is reserved for type and the second byte is reserved for the length of the packet[2] Therefore, I have 38 bytes to send covert messages and padding.

The Sender has 4 inputs, which are secret message, option type, padding length, and packet rate. The option type indicates the IP option type and some of these values are reserved.[3]. The sender creates chunks from the secret message length of 38 - padding length. The rest of these bytes are filled with padding value, which is b'xc8'. Then, it starts to send IP packets to the receiver.

The receiver has 2 inputs, which are option type and padding length. When it receives the packets, it controls whether this has IP Option header. If it exists, then it appends the decoded message to an array to concatenate these values later on to construct secret message.

[1] https://www.tutorialspoint.com/options-field-in-ipv4-header

[2] https://net.academy.lv/lection/net_LS-08ENa_ip-options.pdf

[3] https://www.tutorialspoint.com/options-field-in-ipv4-header

## 3 Experiments

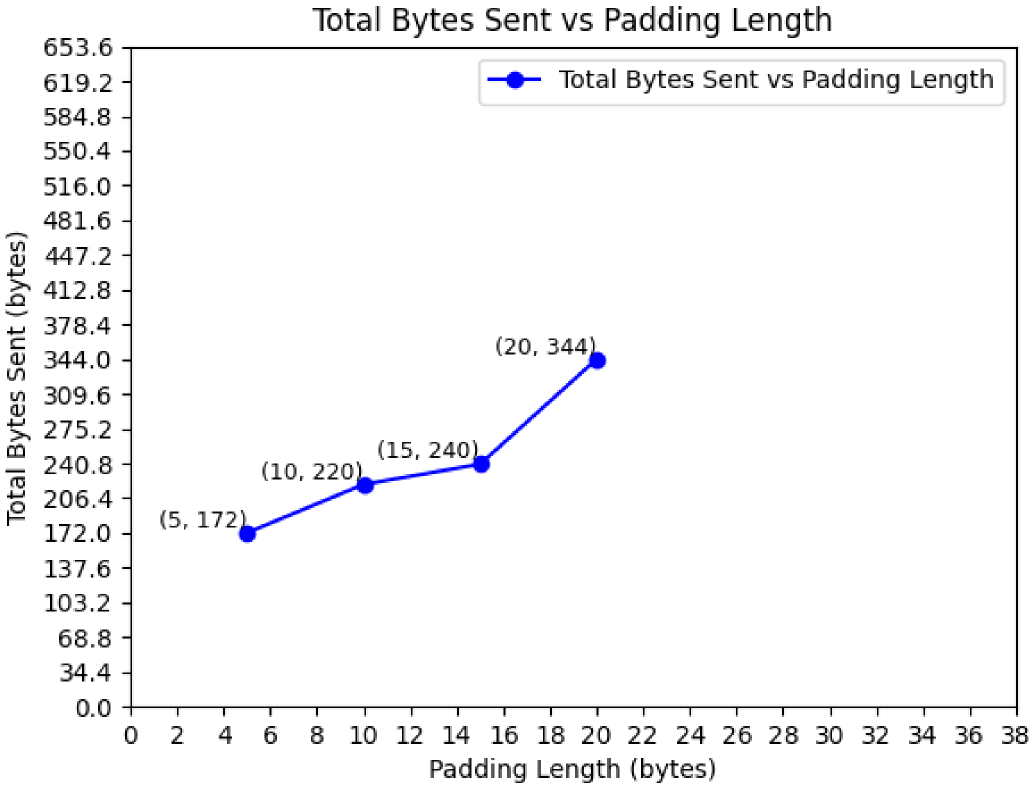
I have created a bash script to run experiments with different input values. I have 3 different experiment category. Python processor worked with mean 5 ms delay.

```
docker compose exec -d term-project-python-processor python3 main.py
echo "Started main.pyin term-project-python-processor"

docker compose exec -d insec  \
python3 covert-channel-receiver.py --pad-len 5
echo "Started covert-channel-receiver.py in insec"

docker compose exec sec \
python3 covert-channel-sender.py --pad-len 5 \
--secret-message \
"Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor."
\
> ./test-results/pad-len-sec-5.txt 2>&1 &

echo "Started covert-channel-sender.py in sec"
sec_pid=$!

wait $sec_pid
echo "sec container exited, logs are written"
docker compose restart
```

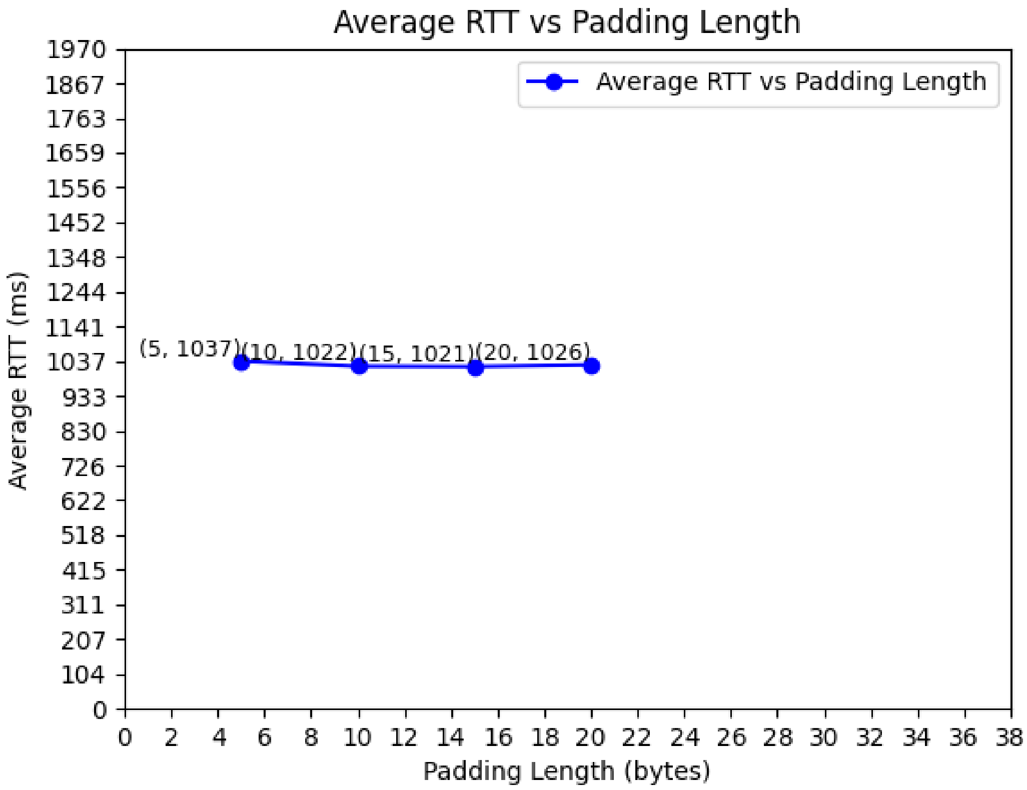
## 3.1 Changing Padding Length

I conducted four experiments using padding lengths of 5, 10, 15, and 20 bytes.

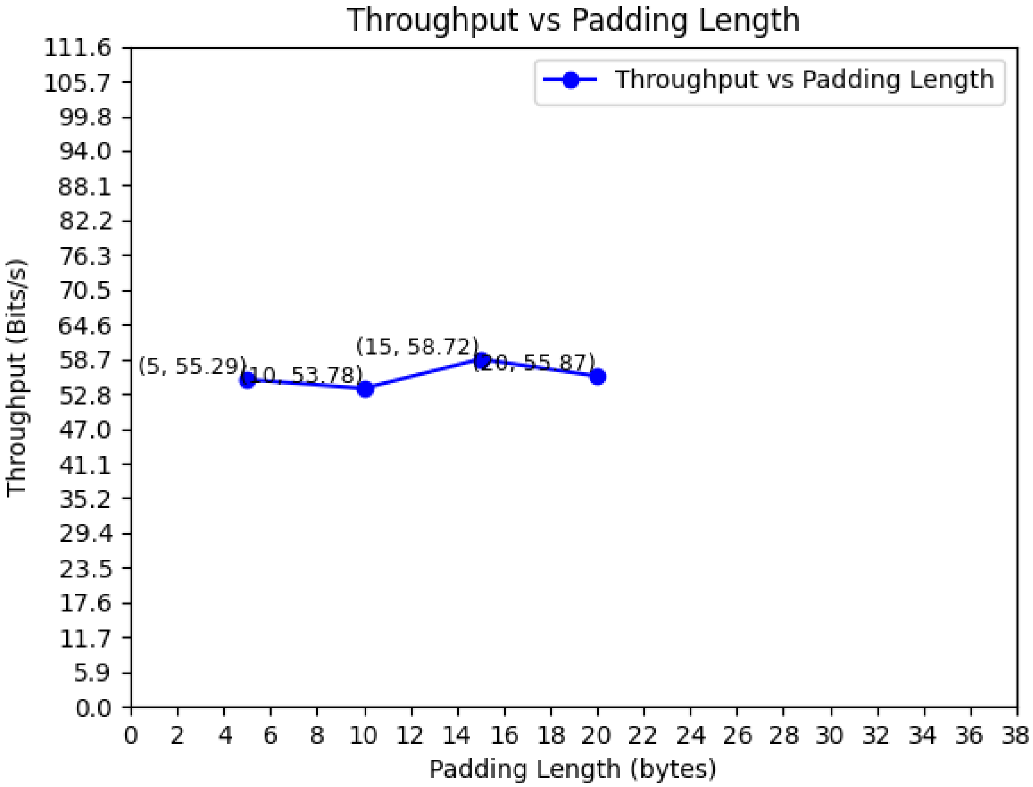
### 3.1.1 Total Bytes Sent



#### 3.1.2 Average RTT



#### 3.1.3 Throughput



### 3.1.4 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 1026.5 ms
  - *95% Confidence Interval:* (1016.40, 1036.60) ms
- **Total Bytes Sent:**
  - *Mean:* 244.0 bytes
  - *95% Confidence Interval:* (144.07, 343.93) bytes
- **Throughput:**
  - *Mean:* 55.915 bytes/sec
  - *95% Confidence Interval:* (53.07, 58.76) bytes/sec

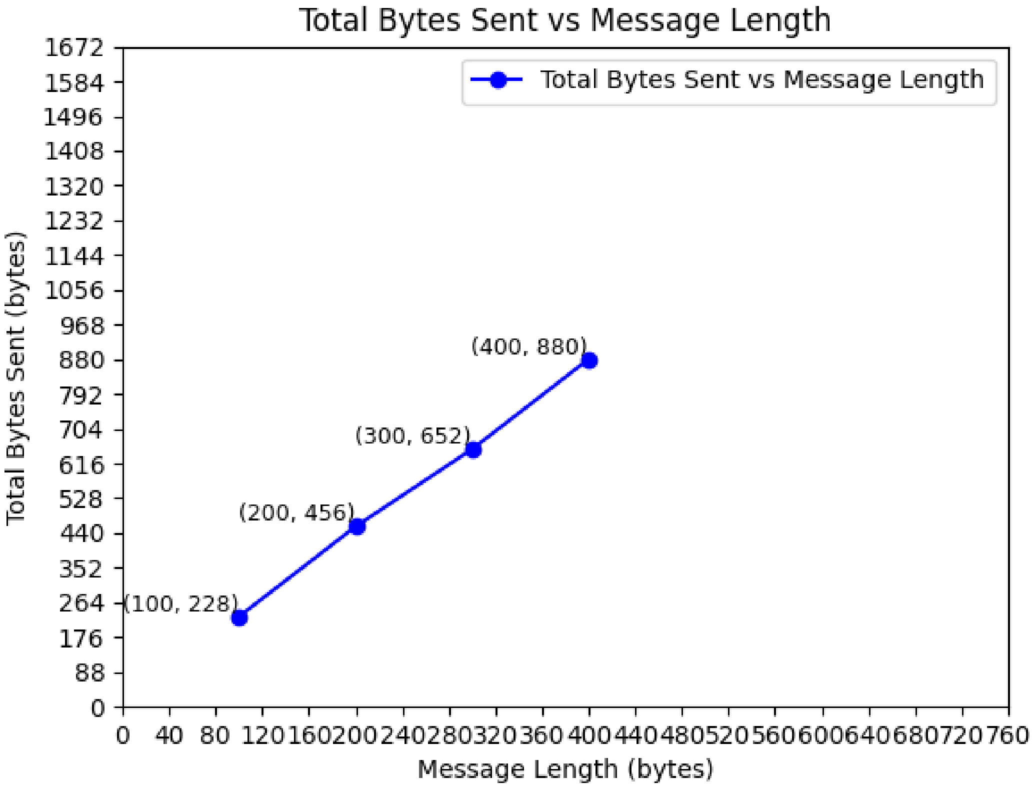
### 3.1.5 Results

The results indicate that changing the padding length has no significant impact on average RTT or throughput. However, since IP options are limited to a maximum size of 40 bytes, increasing the padding length leads to a corresponding increase in the total number of bytes sent.

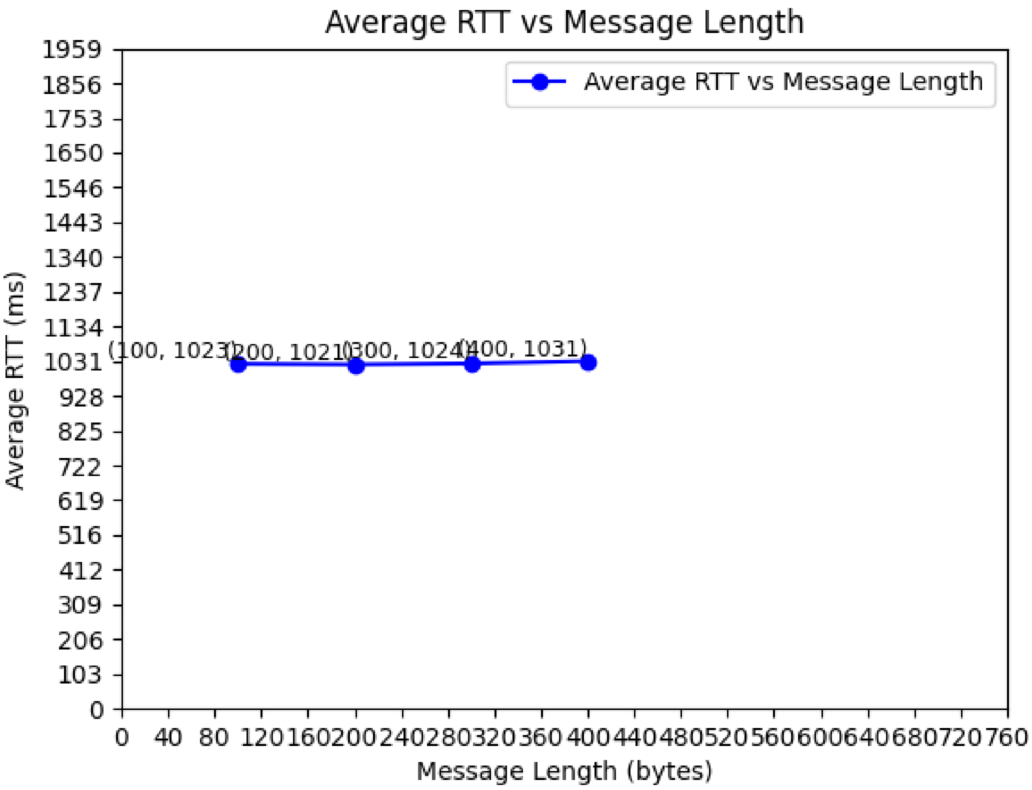
## 3.2 Changing Message Length

I conducted four experiments using message lengths of 100, 200, 300, and 400 bytes.

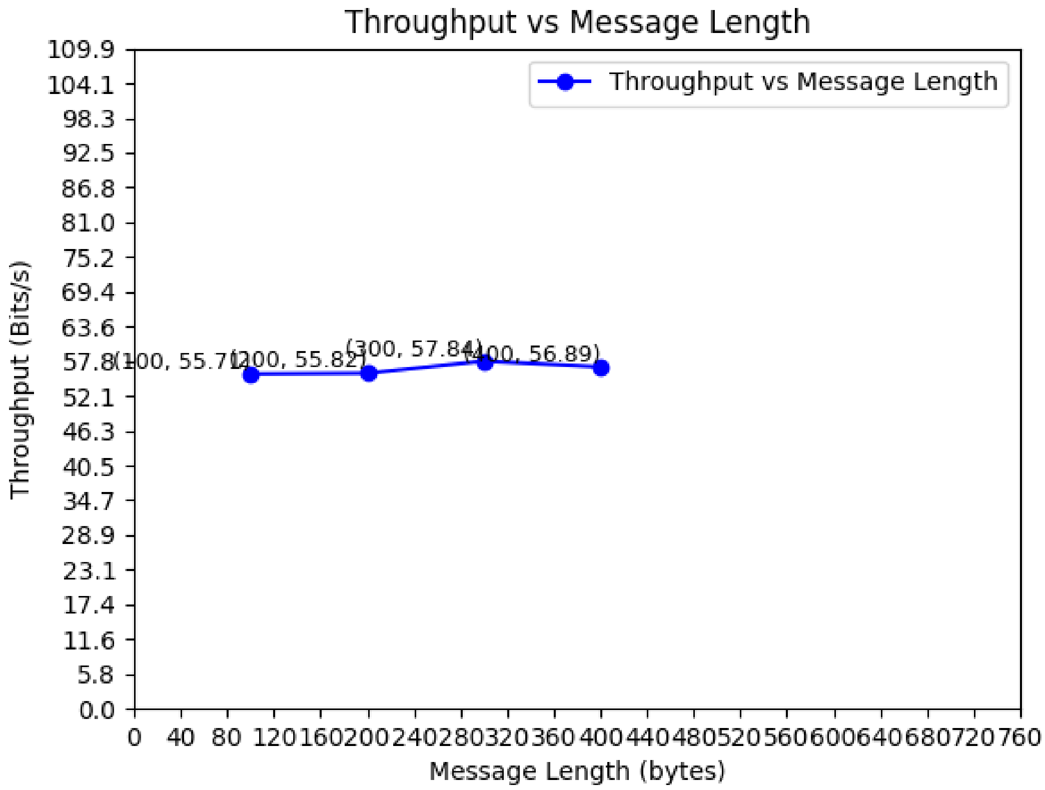
### 3.2.1 Total Bytes Sent



#### 3.2.2 Average RTT



#### 3.2.3 Throughput



#### 3.2.4 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 1024.75 ms
  - *95% Confidence Interval:* (1018.76, 1030.74) ms
- **Total Bytes Sent:**
  - *Mean:* 554.0 bytes
  - *95% Confidence Interval:* (170.98, 937.02) bytes
- **Throughput:**
  - *Mean:* 56.565 bytes/sec
  - *95% Confidence Interval:* (55.18, 57.95) bytes/sec

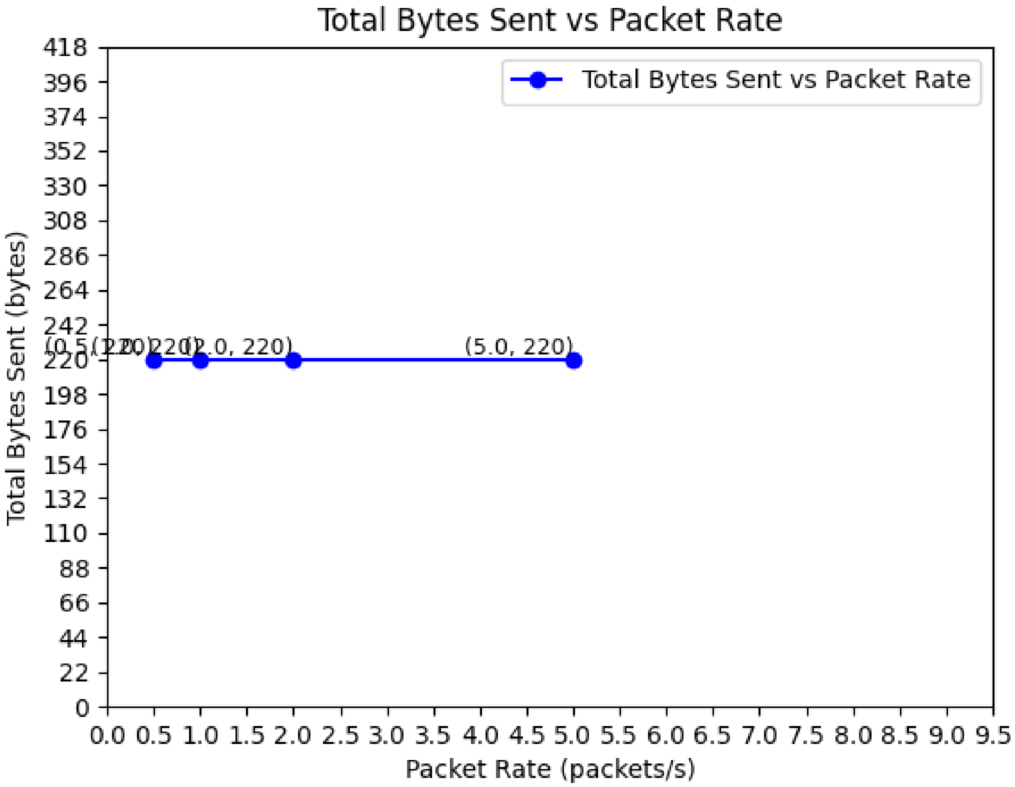
#### 3.2.5 Results

The results indicate that changing the message length has no significant impact on average RTT or throughput. However, since IP options are limited to a maximum size of 40 bytes, increasing the message length leads to a corresponding increase in the total number of bytes sent.

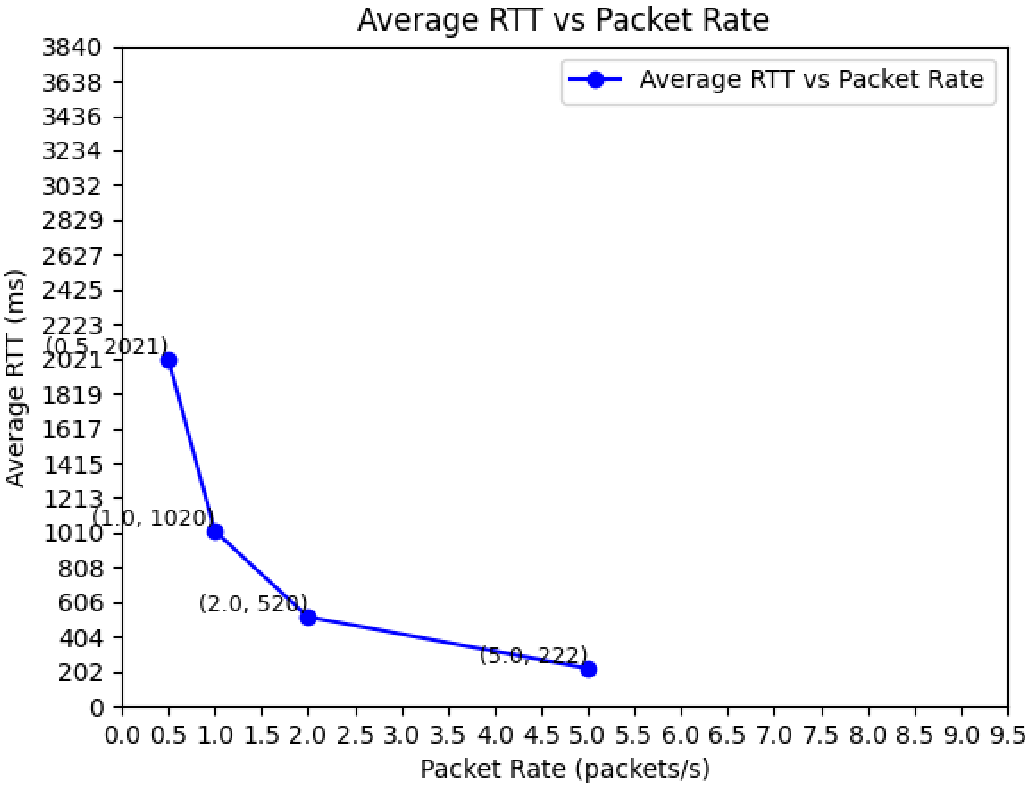
## 3.3 Changing Packet Rate

I conducted four experiments using packet rate values of 0.5, 1.0, 2.0, and 5.0.

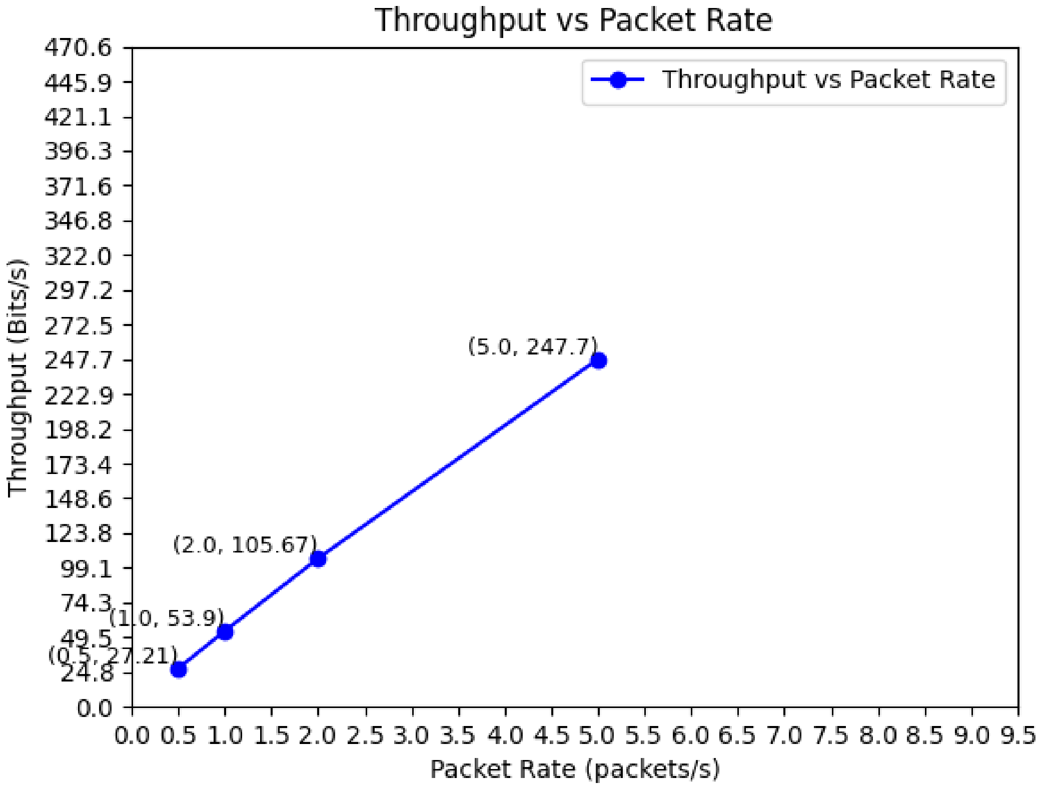
### 3.3.1 Total Bytes Sent



#### 3.3.2 Average RTT



### 3.3.3 Throughput



### 3.3.4 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 945.75 ms
  - *95% Confidence Interval:* (-141.29, 2032.79) ms
- **Throughput:**
  - *Mean:* 108.62 bytes/sec
  - *95% Confidence Interval:* (-26.81, 244.05) bytes/sec

### 3.3.5 Results

The results indicate that changing packet rate affects Average RTT and Throughput significantly. Since message length and padding length are the same during these experiments, total bytes sent is 220 bytes. The wide range with negative lower bound indicates that there is high variability in both Average RTT and Throughput. Potential instability and inconsistency may happen at certain rates.