CENG-519 Term-Project

Berke Can Ünlü - 2381028

Contents

1 Phase 1 **2**
1.1 Setup . . . 2
1.2 Experiments . . . 2
1.2.1 Results . . . 2

2 Phase 2 **2**
2.1 Setup . . . 2
2.2 Development . . . 3
2.2.1 Default Parameter Values . . . 3
2.3 Experiments . . . 4
2.3.1 Changing Padding Length . . . 4
2.3.2 Changing Message Length . . . 7
2.3.3 Changing Noise rate . . . 10

3 Phase 3 **13**
3.1 Development . . . 13
3.1.1 Analysis Functions . . . 13
3.2 Experiments . . . 14
3.2.1 Default Parameter Values . . . 14
3.2.2 Secret Message Length . . . 15
3.2.3 Noise Rate . . . 17
3.2.4 No Covert Packet Count . . . 19
3.2.5 Padding Length . . . 21
3.2.6 TP, TN, FP, FN, F-Scores . . . 23

4 Phase 4 **24**
4.1 Development . . . 24
4.2 Experiments . . . 24
4.2.1 Parameter Values . . . 24
4.2.2 Detector Results . . . 24
4.2.3 The Covert Message Received . . . 24

1 Phase 1

1.1 Setup

I have created a folder ***term-project-python-processor*** inside code folder. It adds a random delay for every packet received from subscribed subjects which are *inpktsec* and *inpktinsec*. I have followed the instructions on the *README* file to send ping packets from the sec container to the insec container.

1.2 Experiments

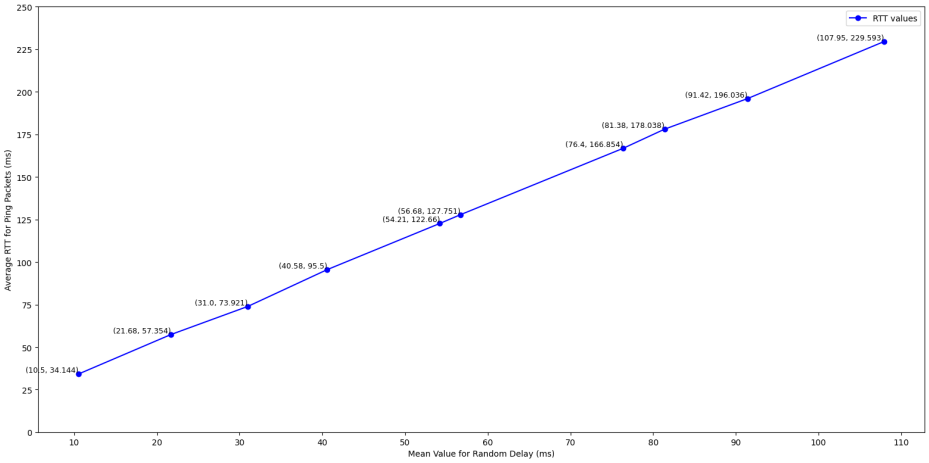
```
ping -c 100 insec
```

I used the command above to create 100 ping packets to send them insec container from sec container.

```
python main.py --delay-mean {desired mean value}
```

I conduct 10 experiments with random values ranging from 10 to 100, increasing by 10, using the command above.

1.2.1 Results



2 Phase 2

2.1 Setup

I have changed the Dockerfiles of sec and insec containers to install the scapy library for Python. There was a misunderstanding about the covert channel I was using. Because of this, the Phase 2 document will be different from the current one. In the first version, I used the IP options field directly to carry the covert data. However, I later realized that the covert data should actually be placed in the padding bytes of the IP options, which are used to make the IP header length a multiple of 4 bytes.

2.2 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. If size of the options header are less than 40 bytes and not multiple of 4 bytes, then it is required to add padding bytes to make it multiple of 4 bytes.

The Sender has four inputs, which are secret message, noise rate, padding length, and number of packets when there is no secret message. Noise rate parameter is a float between 0 and 1, which is used to send noise packets with given rate. Padding length is between 1 and 4, which is used to divide secret message in chunks and send these chunks with covert channel.

2.2.1 Default Parameter Values

- **Noise rate:** 0.3
- **Padding length:** 4
- **Sleep time after receiving/sending packets:** 1 sec

The receiver has one input, which is padding length. When it receives the packets, it controls whether these packets have the IP Options header. If it exists, then it extracts the padding bytes from the packet and adds them to an array to concatenate these values later on to construct the secret message.

Note that some values of IP option type are reserved.[1] Therefore, I used a set of unassigned option types to send covert information.

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

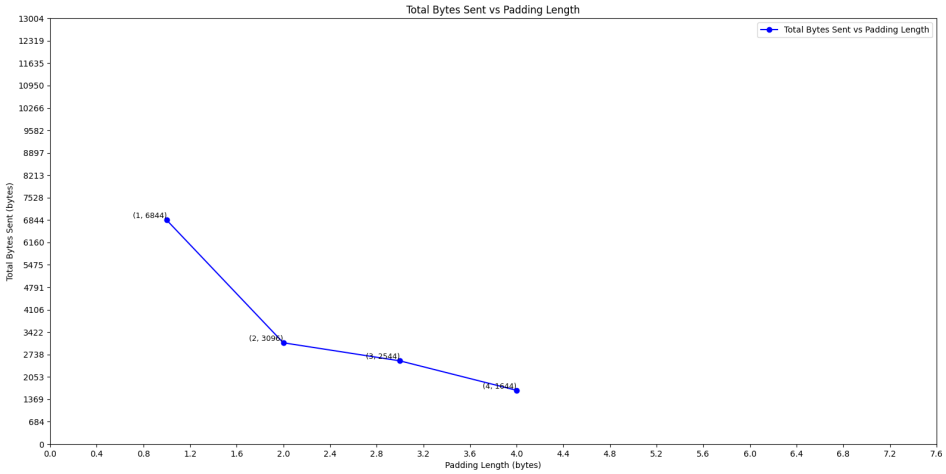
2.3 Experiments

There are three different experiment category. Python processor worked with 5 ms mean delay.

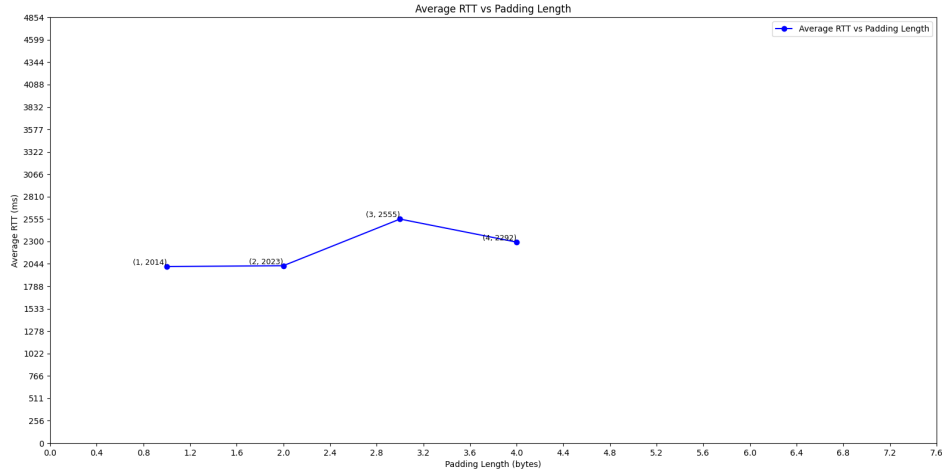
2.3.1 Changing Padding Length

I conducted four experiments using padding lengths of 1, 2, 3 and 4 bytes.

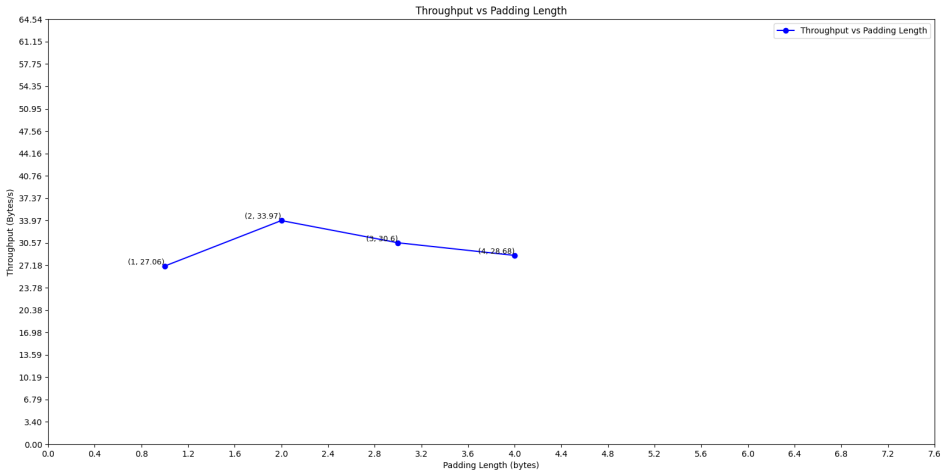
2.3.1.1 Total Bytes Sent



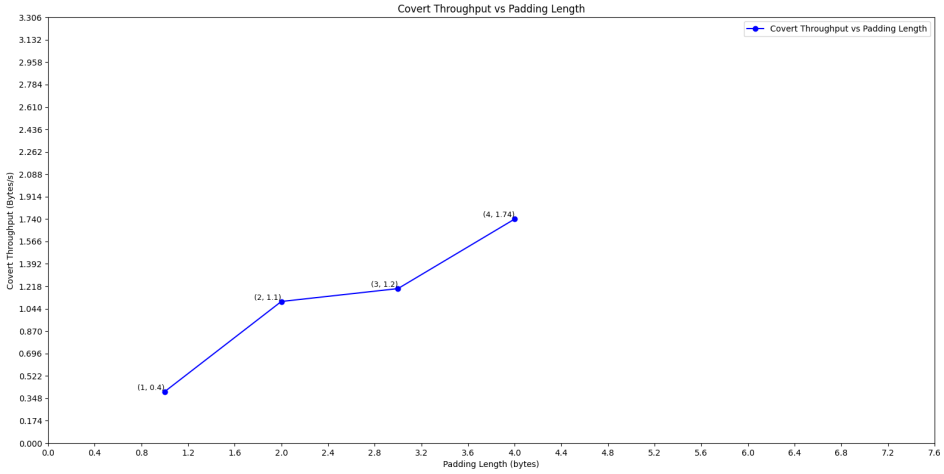
2.3.1.2 Average RTT



2.3.1.3 Throughput



2.3.1.4 Covert Throughput



2.3.1.5 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 2221.0 ms
  - *95% Confidence Interval:* (1866.39, 2575.60) ms
- **Total Bytes Sent:**
  - *Mean:* 3532.0 bytes
  - *95% Confidence Interval:* (379.51, 6684.48) bytes
- **Throughput:**
  - *Mean:* 30.0775 bytes/sec
  - *95% Confidence Interval:* (25.98, 34.17) bytes/sec
- **Covert Throughput:**
  - *Mean:* 1.11 bytes/sec
  - *95% Confidence Interval:* (0.35, 1.86) bytes/sec

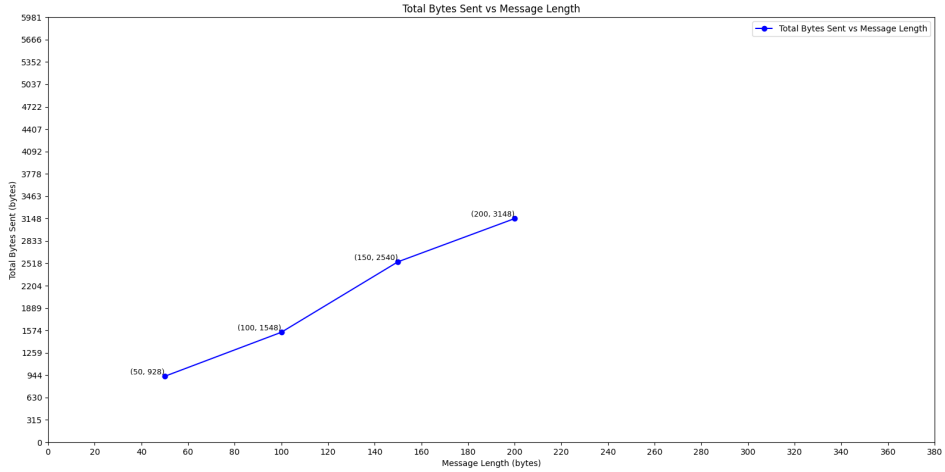
2.3.1.6 Results

Changing the padding length has minimal impact on average RTT and throughput, indicating stable channel performance. However, increasing padding length leads to a lower total number of bytes sent since more data sent by each packet. The reason why Covert throughput less than padding length is the default value of noise rate.

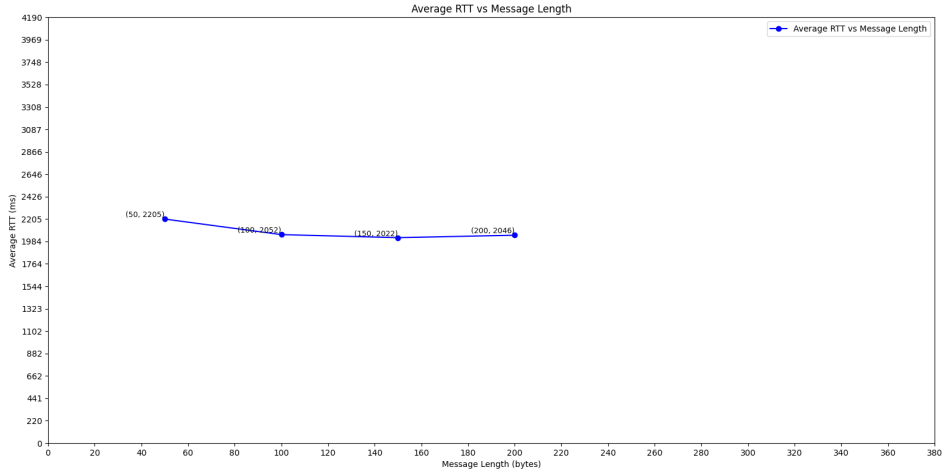
2.3.2 Changing Message Length

I conducted four experiments using message lengths of 50, 100, 150, and 200 bytes.

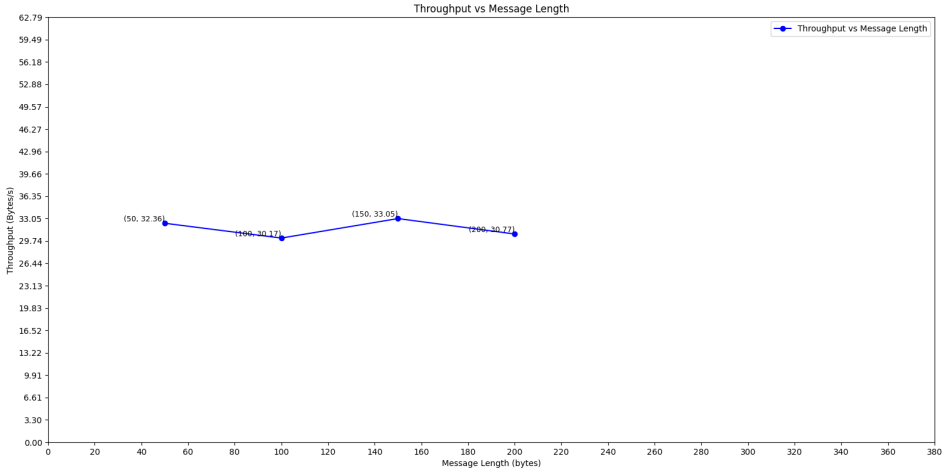
2.3.2.1 Total Bytes Sent



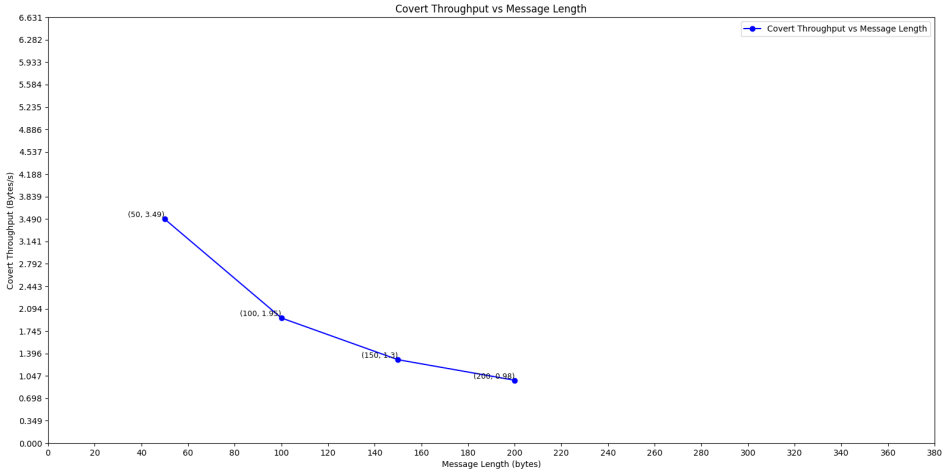
2.3.2.2 Average RTT



2.3.2.3 Throughput



2.3.2.4 Covert Throughput



2.3.2.5 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 2081.25 ms
  - *95% Confidence Interval:* (1966.16, 2196.33) ms
- **Total Bytes Sent:**
  - *Mean:* 2041.0 bytes
  - *95% Confidence Interval:* (673.04, 3408.95) bytes
- **Throughput:**
  - *Mean:* 31.5875 bytes/sec
  - *95% Confidence Interval:* (29.73, 33.43) bytes/sec
- **Covert Throughput:**
  - *Mean:* 1.93 bytes/sec
  - *95% Confidence Interval:* (0.39, 3.46) bytes/sec

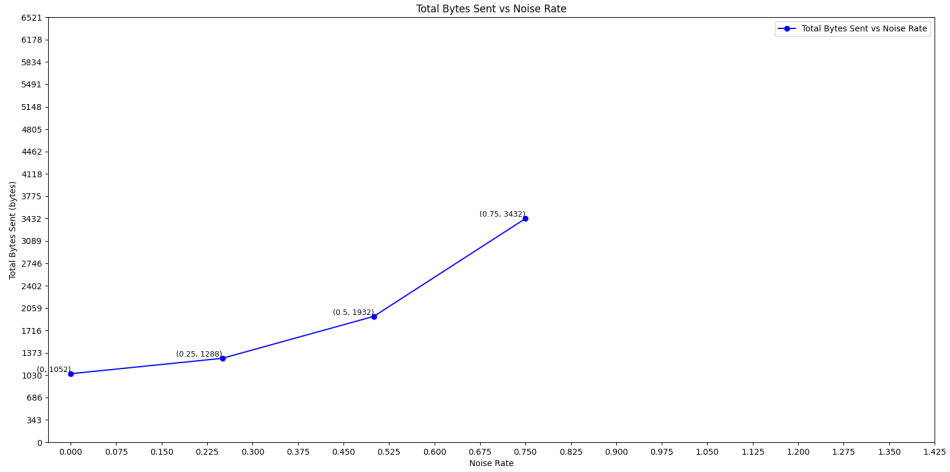
2.3.2.6 Results

Changing the secret message length has minimal impact on average RTT and throughput, indicating stable channel performance. However, increasing secret message length leads to a higher total number of bytes sent since more packets are sent. The reason why Covert throughput less than padding length is the default value of noise rate.

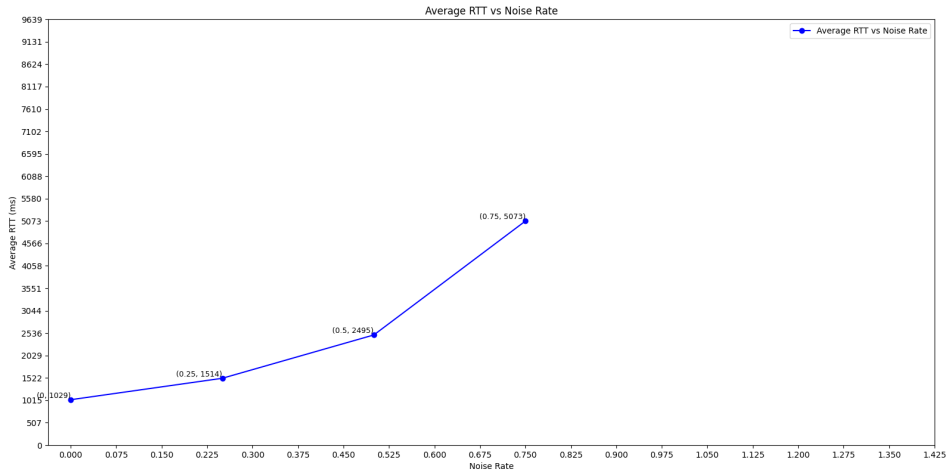
2.3.3 Changing Noise rate

I conducted four experiments using packet rate values of 0, 0.25, 0.5, and 0.75.

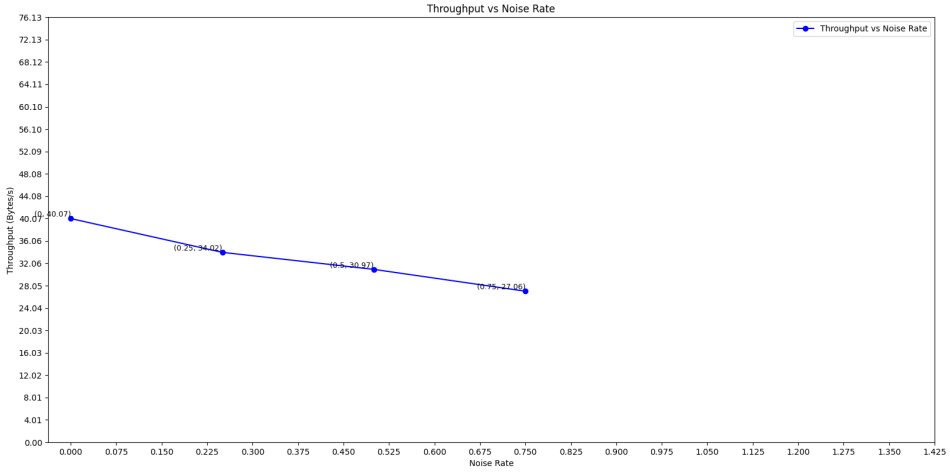
2.3.3.1 Total Bytes Sent



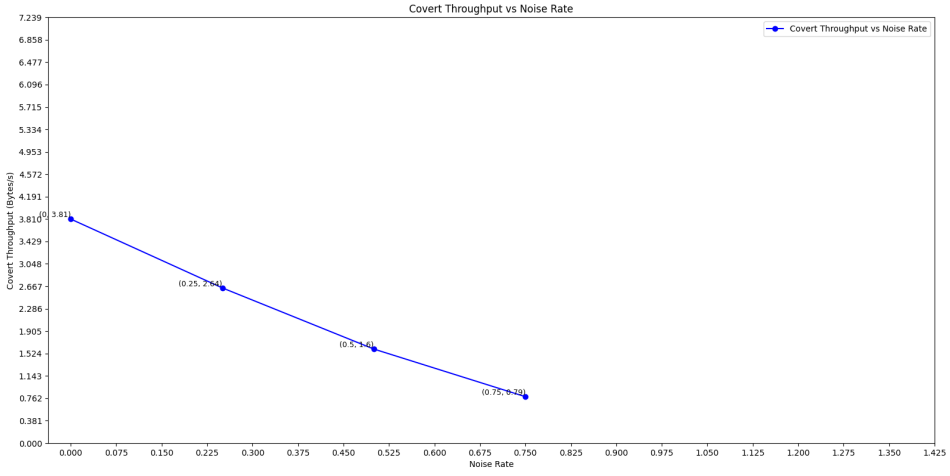
2.3.3.2 Average RTT



2.3.3.3 Throughput



2.3.3.4 Covert Throughput



2.3.3.5 Averages and Confidence Intervals

- **Average RTT:**
  - *Mean:* 2527.75 ms
  - *95% Confidence Interval:* (43.03, 5012.46) ms
- **Total Bytes Sent:**
  - *Mean:* 1926.0 bytes
  - *95% Confidence Interval:* (450.57, 3401.42 bytes
- **Throughput:**
  - *Mean:* 33.03 bytes/sec
  - *95% Confidence Interval:* (25.46, 40.59) bytes/sec
- **Covert Throughput:**
  - *Mean:* 2.21 bytes/sec
  - *95% Confidence Interval:* (0.40, 4.01) bytes/sec

2.3.3.6 Results

The results show that changing the noise rate significantly affects all metrics. The extremely wide confidence intervals, especially for RTT, indicate high variability and potential instability caused by increased noise.

3 Phase 3

3.1 Development

I have created a class for covert channel detection in the Python processor. This class has a parameter called *suspicion_threshold* which is the minimum suspicion score to decide whether the channel is covert or not.

There are three analysis function inside of this class. Each analysis returns a floating-point number between 0 and 1 as suspicion score.

3.1.1 Analysis Functions

- **Option Frequency Analysis**
  - IP Options header is rarely used in IP packets. I divided the number of packets with IP Options by the number of all packets to create a detection metric.
  - $R = \frac{N_{IPOptions}}{N_{total}}$
  - **Criteria:**
    - If frequency = 0, return 0.0
    - If frequency less than 0.2, return 0.25
    - If frequency less than 0.4, return 0.5
    - If frequency less than 0.6, return 0.75
    - Otherwise, return 1.00
- **Option Type Frequency Analysis**
  - IP Options header has some unassigned types. I divided the number of packets with uncommon option types by the number of all packets to create a detection metric.
  - $R = \frac{N_{UncommonTypes}}{N_{total}}$
  - **Criteria:**
    - If frequency = 0, return 0.0
    - If frequency less than 0.2, return 0.2
    - If frequency less than 0.4, return 0.4
    - If frequency less than 0.6, return 0.6
    - If frequency less than 0.8, return 0.8
    - Otherwise, return 1.00
- **Option Padding Entropy Analysis**
  - I used Shannon Entropy to measure the entropy of padding bytes.
  - $H(X) = -\sum_i p(x_i) \log_2 p(x_i)$
  - **Criteria:** There are 256 different byte options for padding bytes. Therefore, maximum entropy is 8.0.
    - If entropy less than 3.5, return 1.0
    - If entropy less than 4.5, return 0.75
    - If entropy less than 5.5, return 0.5
    - If entropy less than 6.5, return 0.25
    - Otherwise, return 0

3.2 Experiments

I've conducted four experiments for each parameter, which are message length, noise rate, no covert packet count and padding length.

3.2.1 Default Parameter Values

- **Noise rate:** 0.3
- **Padding length:** 4
- **Sleep time after receiving/sending packets:** 1 sec
- **Suspicion Threshold:** 0.4
- **Secret Message:** "Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi dignissim ultricies nisl, quis ornare lacus pulvinar eu. Sed a malesuada nibh, quis lacinia ligula. Pellentesque rutrum, lorem sed metus."

3.2.2 Secret Message Length

3.2.2.1 Experiment 1
Secret message length is 200 bytes.

3.2.2.2 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.71
- **Low average entropy of padding lengths:** 4.24
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.75
- **Total Suspicion Score:** 0.85

3.2.2.3 Experiment 2
Secret message length is 300 bytes.

3.2.2.4 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Moderate average entropy of padding lengths:** 4.65
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

3.2.2.5 Experiment 3
Secret message length is 400 bytes.

3.2.2.6 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.71
- **Moderate average entropy of padding lengths:** 4.66
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

3.2.2.7 Experiment 4

Secret message length is 500 bytes.

3.2.2.8 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.73
- **Moderate average entropy of padding lengths:** 5.01
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

3.2.3 Noise Rate

3.2.3.1 Experiment 1
Noise rate is 0.

3.2.3.2 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.71
- **Very Low average entropy of padding lengths:** 2.23
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.93

3.2.3.3 Experiment 2
Noise rate is 0.25.

3.2.3.4 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Moderate average entropy of padding lengths:** 4.73
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

3.2.3.5 Experiment 3
Noise rate is 0.5.

3.2.3.6 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Low average entropy of padding lengths:** 4.35
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.75
- **Total Suspicion Score:** 0.85
- **Suspicious activity detected:** Score = 0.85

3.2.3.7 Experiment 4

Noise rate is 0.75.

3.2.3.8 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Low average entropy of padding lengths:** 4.42
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.75
- **Total Suspicion Score:** 0.85

3.2.4 No Covert Packet Count

3.2.4.1 Experiment 1
50 packet has been sent without secret message.

3.2.4.2 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.71
- **Very Low average entropy of padding lengths:** 1.82
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.93

3.2.4.3 Experiment 2
100 packet has been sent without secret message.

3.2.4.4 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.59
- **Very Low average entropy of padding lengths:** 1.53
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.60
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.90

3.2.4.5 Experiment 3
150 packet has been sent without secret message.

3.2.4.6 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.70
- **Very Low average entropy of padding lengths:** 1.84
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.93

3.2.4.7 Experiment 4

200 packet has been sent without secret message.

3.2.4.8 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.70
- **Very Low average entropy of padding lengths:** 1.84
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.93

3.2.5 Padding Length

3.2.5.1 Experiment 1
Padding length is 1.

3.2.5.2 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.71
- **Very Low average entropy of padding lengths:** 2.23
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 1.00
- **Total Suspicion Score:** 0.93

3.2.5.3 Experiment 2
Padding length is 2.

3.2.5.4 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Moderate average entropy of padding lengths:** 4.73
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

3.2.5.5 Experiment 3
Padding length is 3.

3.2.5.6 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Low average entropy of padding lengths:** 4.35
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.75
- **Total Suspicion Score:** 0.85

3.2.5.7 Experiment 4

Padding length is 4.

3.2.5.8 Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Low average entropy of padding lengths:** 4.42
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.75
- **Total Suspicion Score:** 0.85

3.2.6 TP, TN, FP, FN, F-Scores

In the conducted experiments, there were a total of 16 cases, consisting of 12 True Covert Channels (positive cases) and 4 False Covert Channels (negative cases). The heuristic detector successfully identified all True Covert Channels without missing any, demonstrating perfect sensitivity. However, it also incorrectly classified all False Covert Channels as positive. The F-Score (also called F1-Score) is the harmonic mean of precision and recall, calculated as:

$$F - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

where

$$Precision = \frac{TP}{TP + FP}, \quad Recall = \frac{TP}{TP + FN}$$

- **True Positives (TP):** 12
- **True Negatives (TN):** 0
- **False Positives (FP):** 4
- **False Negatives (FN):** 0
- **F-Score:** 0.86

This performance indicates the heuristic detector is highly sensitive but has a tendency to produce false positives, which may need to adjustments such as adding new analysis or fine-tuning the criteria of current analysis.

4 Phase 4

4.1 Development

I have created a class for covert channel mitigation in the Python processor. This mitigator is triggered when the detector identifies a covert channel. To ensure meaningful detection, I have set a packet count threshold in the detector; it does not run if there are fewer than 50 packets. Additionally, the detector runs periodically, with a period of 5 seconds.

When the mitigation strategy is active, the processor handles packets received from the sec container, modifies the IP option header and padding bytes, and then publishes the updated packets. The IP option header is replaced by 4 IP No Operation Option. Padding bytes are replaced by 'x00' bytes.

4.2 Experiments

I have conducted 1 experiment since it is enough to show that receiver do not receive the whole covert message.

4.2.1 Parameter Values

- **Noise rate:** 0.3
- **Padding length:** 4
- **Sleep time after receiving/sending packets:** 1 sec
- **Suspicion Threshold:** 0.4
- **Secret Message:** "Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras eget augue lectus. Quisque tempus neque eu ante fermentum vulputate. Mauris id sem quis velit tempor gravida. Suspendisse pulvinar congue rhoncus. Sed eu vehicula nisl, vel aliquam ipsum. Sed lacinia vehicula ullamcorper. Mauris molestie."

4.2.2 Detector Results

- **High frequency of IP options:** 1.00
- **Very high frequency of uncommon IP option types:** 0.72
- **Moderate average entropy of padding lengths:** 4.65
- **Option Frequency:** 1.00
- **Option Type Frequency:** 0.80
- **Option Padding Entropy:** 0.50
- **Total Suspicion Score:** 0.77

4.2.3 The Covert Message Received

"Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras eget augue lectus. Quisque tempus neque eu ante fermentum vulputate. M"