CENG519 - Phase 2

Covert Channel Using TCP MSS Field

Yahya Sungur - 2375723

March 27, 2025

1 Introduction

In this phase of the project, a covert channel was implemented by embedding data into the TCP MSS option field. The sender and receiver communicated over SEC and INSEC containers, respectively, with a processor forwarding the packets. The objective was to measure the performance and capacity of this covert channel.

2 Experiment Setup

- **Sender:** Python script using Scapy (sec container)
- **Receiver:** Python listener script (insec container)
- **Processor:** NATS-based packet forwarder
- **Total Packets Sent:** 500
- **Packet Interval:** 0.0001s
- **MSS Covert Data:** 65535

3 Results

3.1 Benchmark Metrics

Table 1: Performance Metrics

Metric	Value
Total Packets Sent	500
Total Packets Received	500
Packet Loss (%)	0%
Mean Latency (s)	0.0144
95% Confidence Interval	[0.0140, 0.0148]
Throughput (bps)	812.83
Channel Capacity (bps)	812.83

3.2 Latency Distribution

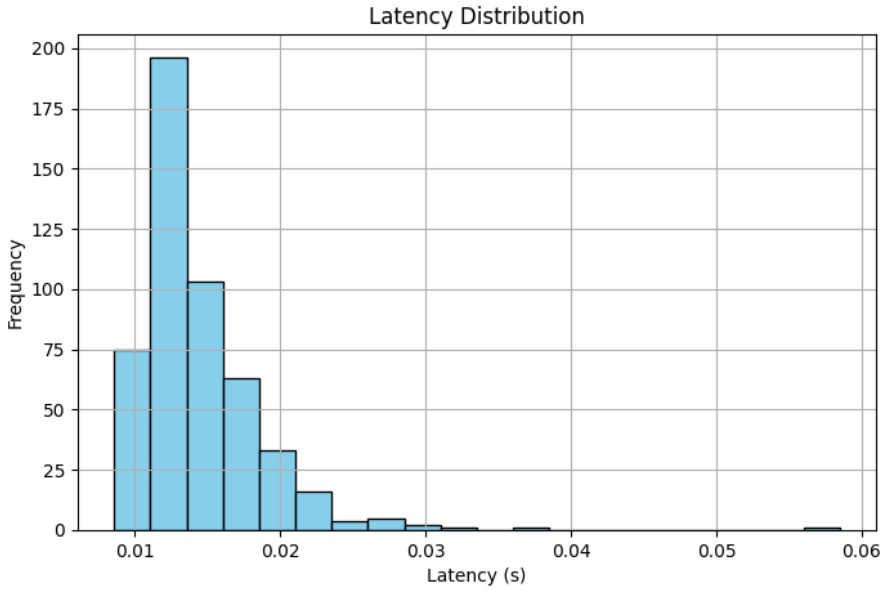

Figure 1: Latency Distribution of Received Packets

3.3 Throughput Over Time

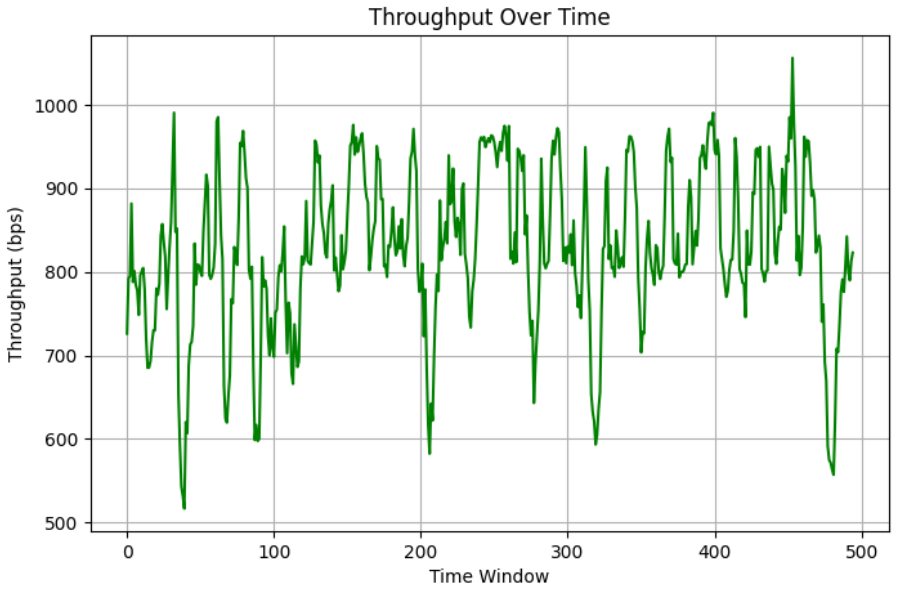

Figure 2: Throughput Variation Over Time

4 Conclusion

The experimental results demonstrate the effectiveness and limitations of embedding data in the MSS option field as a covert channel. Despite the simplicity, the channel achieved a capacity of 812.83 bps with an average latency of 0.0144 s and a packet loss of 0%. These results provide insight into the feasibility of such covert channels in real-world scenarios.