CENG 519 Term Project Phase 2 Covert Channel Analysis Report

1. Introduction

This report explains the implementation and evaluation of performance of the covert channel using the IPv4 Timestamp Option. The covert channel was integrated into the existing Phase I development environment by modifying the packet processor. In this context, the secure container (sec) sends normal packets, which are intercepted and modified by the middlebox for covert insertion, and these packets are then forwarded toward the insecure container (insec). This serves as the basis for covert communication, whereas performance metrics provide means for quantification.

2. Methodology

The covert channel method has been selected through the IPv4 Timestamp Option. It is based on the very fact that the option is underused in the current networks, which makes changes to this header less likely to be noticed by typical network monitoring tools. The covert data will thus be embedded in a field that is normally reserved for routing timestamps; hence, the phantom with a controlled way of channel capacity evaluation will occur.

The system is fully parametrized using environment variables such as ENABLE_COVERT, COVERT_MESSAGE, and MEAN_DELAY. Channel performance is measured by capturing the round-trip time (RTT) and random delays for each packet. The following metrics were computed from the experimental data:

- Average RTT and its 95% Confidence Interval (CI).
- Average Delay and its 95% CI.
- Covert Channel Capacity in bits per second.

Some experimentation campaigns were run where the configuration parameters were varied and the performance metrics were taken. The outcomes were then saved in 'results.json' and plotted accordingly.

3. Results

3.1 Summary Statistics

Following is a summary of the key performance metrics collected during these experiments, summarized for easy reference.

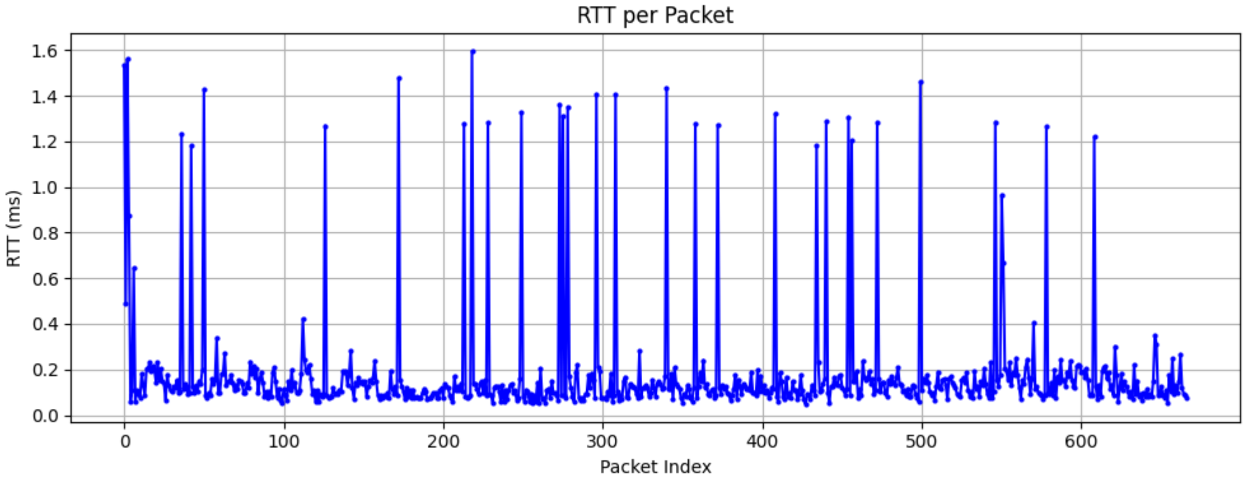
Summary Statistics:

- RTT Average: 0.182 ms
- RTT 95% Confidence Interval: 0.020 ms
- Delay Average: 4.888 µs
- Delay 95% Confidence Interval: 0.369 µs
- Covert Channel Capacity: 19.155 bps

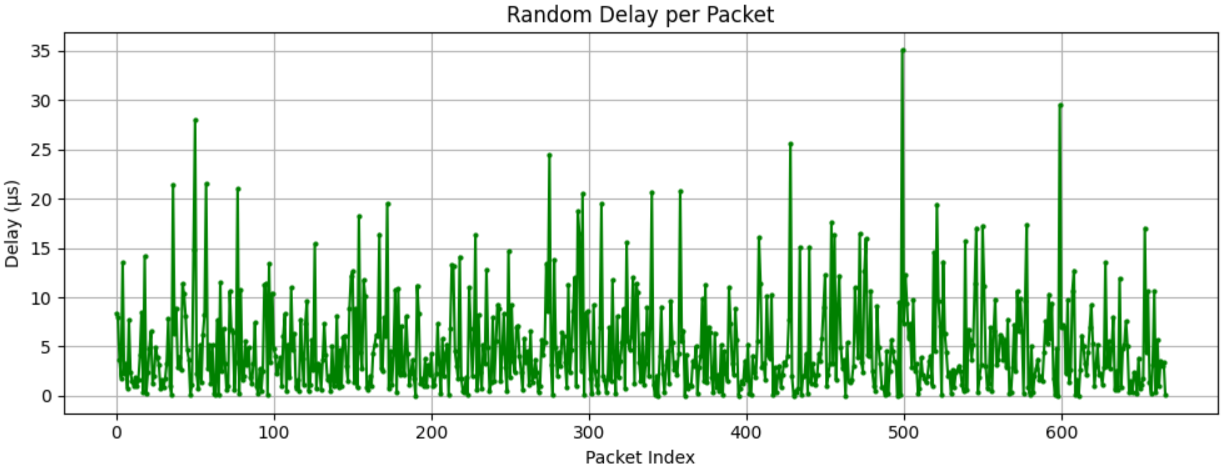
3.2 Plots

The following plots were generated from the experimental data:

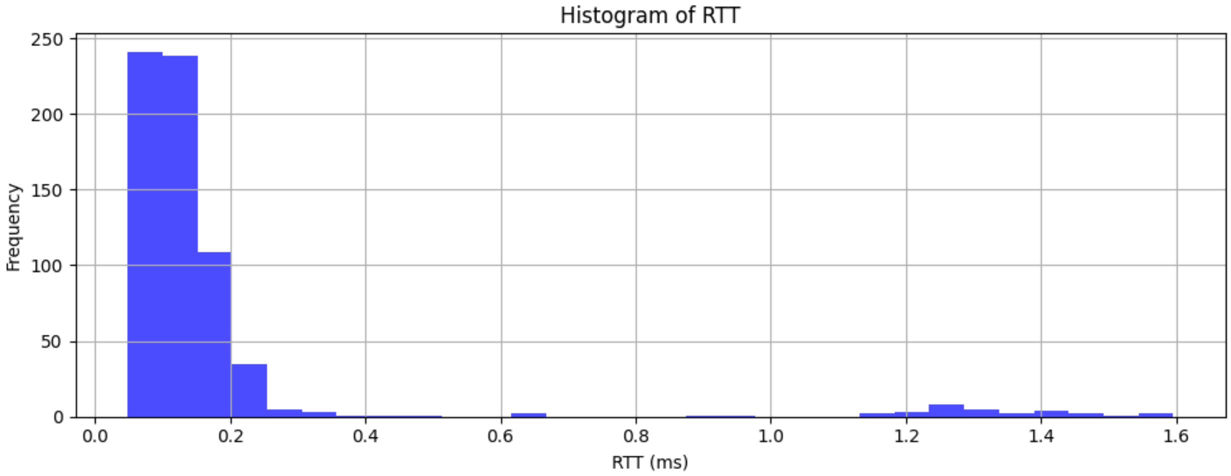
1. RTT vs. Packet Index



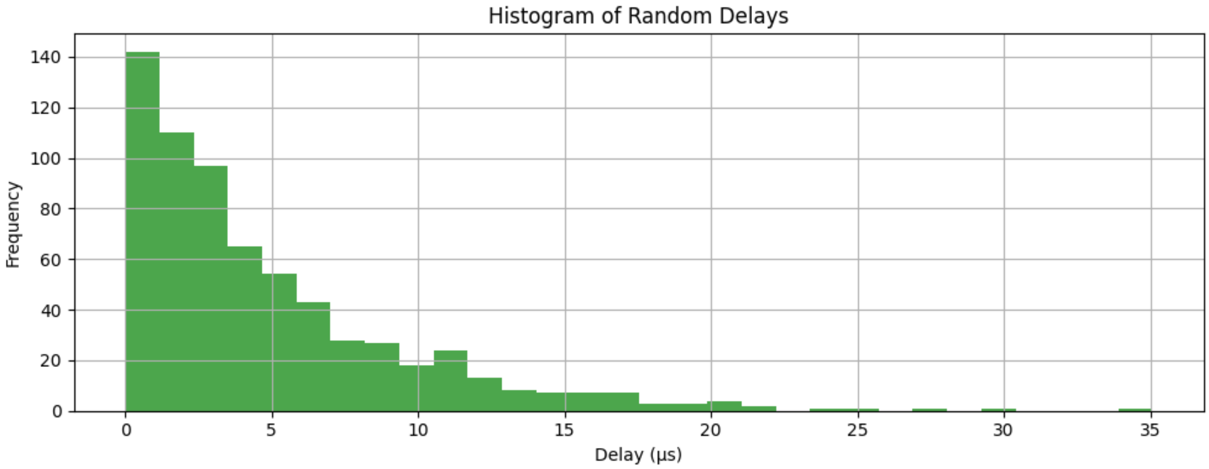
2. Random Delay vs. Packet Index



3. Histogram of RTT values

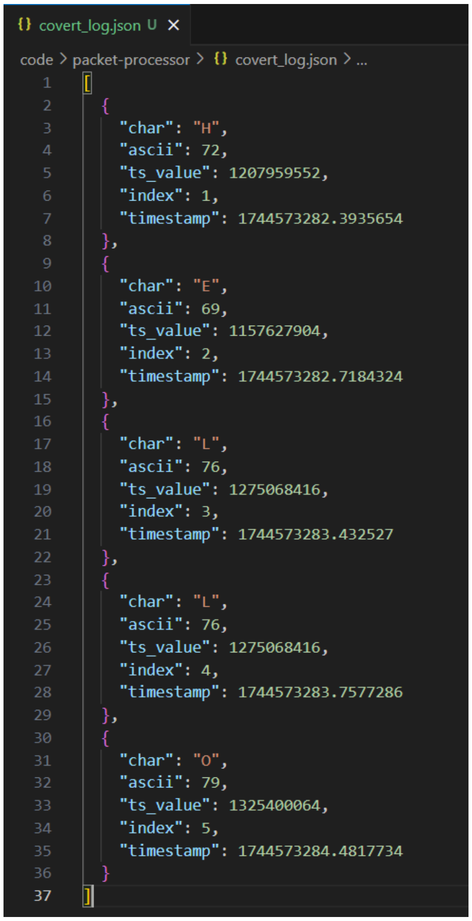


4. Histogram of Random Delays



3.3 Covert Log Data

A covert log was maintained throughout the experimentation to log all the details of each covert injection event. The log records information on the injected character, its ASCII value, the computed timestamp value injected into the IPv4 Timestamp Option, packet index, and injection time. A section from the covert log data is shown below in JSON format:



```json
[
  {
    "char": "H",
    "ascii": 72,
    "ts_value": 1207959552,
    "index": 1,
    "timestamp": 1744573282.3935654
  },
  {
    "char": "E",
    "ascii": 69,
    "ts_value": 1157627904,
    "index": 2,
    "timestamp": 1744573282.7184324
  },
  {
    "char": "L",
    "ascii": 76,
    "ts_value": 1275068416,
    "index": 3,
    "timestamp": 1744573283.432527
  },
  {
    "char": "L",
    "ascii": 76,
    "ts_value": 1275068416,
    "index": 4,
    "timestamp": 1744573283.7577286
  },
  {
    "char": "O",
    "ascii": 79,
    "ts_value": 1325400064,
    "index": 5,
    "timestamp": 1744573284.4817734
  }
]
```

4. Analysis

The results indicate that the covert channel itself effectively embeds hidden data into the IPv4 header while generally leaving the packets to be passed undisturbed. RTT and delay values with their confidence intervals are reliable features to evaluate the performance of the covert channel. At 19.15 bps, the covert channel capacity allows for transmitting small amounts of sensitive data covertly. Such capacity is typical for channels relying on timing or header alterations that would evade detection from common network-monitoring tools. More tuning of parameters like mean delay can be used either to increase throughput or to make the channel more stealthy.

5. Conclusion

In the Phase 2 implementation, the covert channel using the IPv4 Timestamp Option was successfully integrated into the existing packet processor. The experimental campaign showed that the channel was working with stable timing characteristics and that key performance metrics were obtained. Although at low capacity (~19.15 bps), the channelsemploys such fewer augmentations of delay, hence posing as a least to Ms-updaria network traffic interrogation.