Ceng 519 Phase 2 Report

(TCP Flags: Using control flags like SYN, ACK, FIN, and RST to convey information)

1. Introduction

The covert channel encodes information by manipulating specific TCP flags (ACK+URG for '1' and ACK+PSH for '0') The goal of this study is to characterize the channel's capacity under varying inter-packet delays and quantify its reliability and performance.

2. Experimental Setup

The sender transmits a fixed-length message ("CovertChannelTest") repeatedly, and the receiver attempts to decode it.

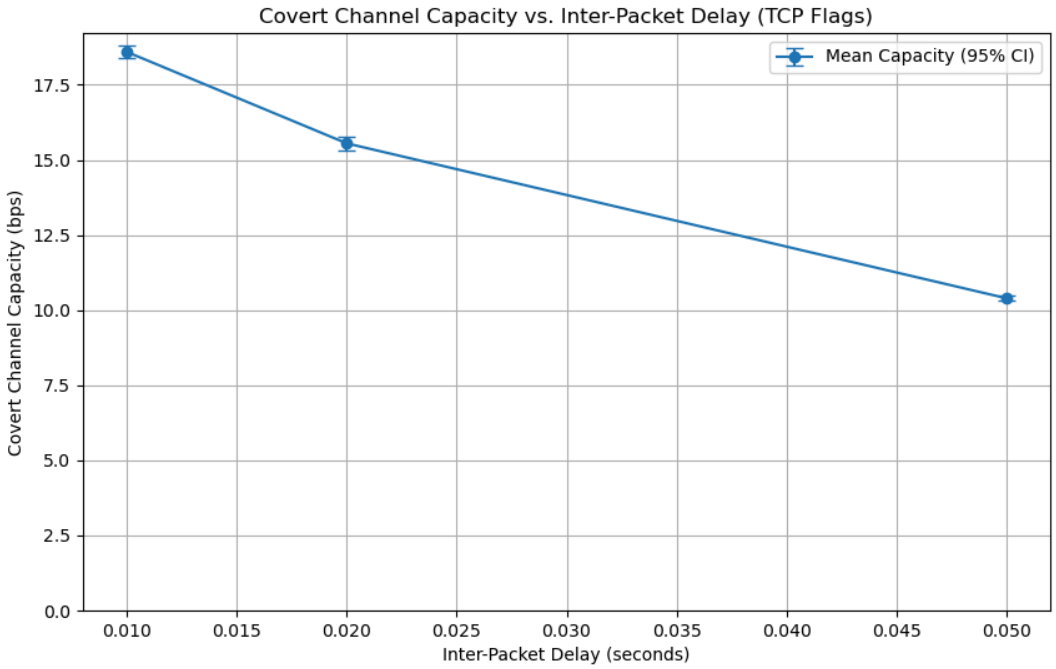
The primary parameter varied in this experiment is the inter-packet delay, which is the time interval between sending consecutive TCP packets, each encoding one bit of the message. The following delay values were tested: [0.010, 0.020, 0.050] seconds. For each delay value, 10 independent trials were conducted.

The key performance metric measured is the covert channel capacity, defined as the number of bits successfully transmitted per unit of time (bits per second, or bps). The transmission time is measured from the moment the sender sends the first packet of the message (SYN+ACK) to the moment the receiver successfully decodes the last bit of the message and receives the End of Message (FIN+ACK).

3. Results

The results of the experimentation campaign are summarized in the table below and illustrated in figure.

Delay (s)	Mean Capacity (bps)	Std Dev	95% CI Margin
0.010	18.59	0.33	0.21
0.020	15.55	0.37	0.23
0.050	10.40	0.13	0.08



The error bars in the figure represent the 95% confidence intervals for the mean capacity.

4. Analysis

The results show a clear trend: as the inter-packet delay increases, the covert channel capacity decreases. This is an expected result, as longer delays directly reduce the number of bits that can be transmitted per second.

- **Confidence Intervals:** The 95% confidence intervals are relatively narrow, indicating that the measured mean capacities are reasonably precise.
- **Reliability:** In all the conducted experiments, the covert channel successfully transmitted the message, demonstrating high reliability.

5. Conclusion

The TCP flag-based covert channel can achieve a moderate capacity. Shorter delays lead to higher capacity but potentially increase the risk of errors or dropped packets.