TOS Covert Channel: Implementation, Performance Analysis, and Experimental Results

Kerem Recep Gür
Student ID: 2448462

April 13, 2025

Abstract

This report presents the design, implementation, and performance evaluation of a covert channel that exploits the IP Type of Service (TOS) field. The channel uses a header/payload structure with control packets for session delimitation and redundancy for robustness. Experiments were conducted by varying TOS Mapping Bits, redundancy (packets-per-symbol), and sender interval parameters via terminal commands. Combined measurement results from both the sender and receiver sides are summarized in tables and further illustrated with graphical analyses. Additionally, statistical analysis including a 95% confidence interval is computed for key metrics.

1 Introduction

Covert channels enable secret communication by bypassing standard network protocols. In this implementation, the IP TOS field is manipulated to encode covert data. The sender and receiver are fully parameterized to allow experiments with various configurations:

- **TOS Mapping Bits:** The number of bits used from the TOS field (1, 2, 4, or 8).

- **Redundancy (Packets per Symbol):** The number of redundant packets for each symbol (e.g., 1, 2, or 3).

- **Sender Interval:** The inter-packet delay (0.01 s and 0.1 s).

Terminal commands were executed to vary these parameters during testing.

2 Implementation Details

2.1 Sender Implementation

The sender performs the following steps:

1. **Message Encoding:** The message is converted to its 8-bit ASCII binary representation and segmented into symbols based on the specified TOS Mapping Bits; padding is added if necessary.

2. **Header Construction:** A header is constructed to encode the number of payload symbols using at least 16 bits (rounded up to a multiple of the TOS Mapping Bits).

3. **Packet Transmission:** Control packets (`START` and `END`) are sent to mark session boundaries. Data packets (with TOS values corresponding to each symbol) are transmitted with configurable redundancy.

4. **Interval Control:** A user-defined interval is maintained between packet transmissions.

2.2 Receiver Implementation

The receiver:

1. **Packet Filtering:** Listens on a specified UDP port and filters packets with the expected payload and TOS field.

2. **Session Demarcation:** Uses control packets to switch modes. A `START` packet triggers header collection (which determines the number of payload symbols), while an `END` packet signals the end of the session.

3. **Redundancy Resolution:** Applies majority voting on redundant packets to determine the correct symbol for each position.

4. **Performance Measurement:** Computes the message transmission time and channel capacity, where capacity is calculated as the total number of payload bits divided by the elapsed time.

2.3 Statistical Analysis and 95% Confidence Interval Calculation

For each configuration with multiple trials, the mean ($\bar{x}$) and standard deviation (s) of performance metrics (such as transmission time and capacity) are calculated. A 95% confidence interval (CI) for the mean is then computed using:

$$CI = 1.96 \times \frac{s}{\sqrt{n}}$$

where n is the number of experiments.

The following snippet from the implementation shows the exact calculation of the confidence interval:

```
ci_duration = 1.96 * stdev(durations) / (n**0.5)
ci_throughput = 1.96 * stdev(throughputs) / (n**0.5)
```

2.4   Test Methodology

Experiments were conducted by varying terminal command parameters. For instance, the following commands were used for TOS Mapping Bits = 8, redundancy = 3, and sender interval = 0.1 s:

```
python3 tos_covert_sender.py --message "Test Covert Channel" \
  --tos-mapping-bits 8 --interval 0.1 --packets-per-symbol 3 \
  --repeat-message 1 --target-ip 10.0.0.15 --port 8888

python3 tos_covert_receiver.py --tos-mapping-bits 8 \
  --packets-per-symbol 3 --timeout 180 --iface eth0
```

Similar commands were executed to vary TOS Mapping Bits, redundancy, and sender interval.

3   Experimental Results

Combined results for sender and receiver are grouped by TOS Mapping Bits value. The following four combined tables summarize the performance metrics.

3.1   TOS Mapping Bits = 1

Table 1: Combined Results for TOS Mapping Bits = 1 (narrowed version)

Redundancy	Sender Interval (s)	Sender Time (s)	Symbols	Total Pkts	Receiver Time (s)	Capacity (bit/s)
1	0.01	8.748	152	174	8.540	17.798
1	0.1	24.007	152	174	23.441	6.484
2	0.01	16.997	152	342	16.757	9.071
2	0.1	46.740	152	342	46.159	3.293
3	0.01	24.547	152	510	24.353	6.241
3	0.1	69.489	152	510	68.923	2.205

3.2   TOS Mapping Bits = 2

Table 2: Combined Results for TOS Mapping Bits = 2 (narrowed version)

Redundancy	Sender Interval (s)	Sender Time (s)	Symbols	Total Pkts	Receiver Time (s)	Capacity (bit/s)
1	0.01	5.073	76	90	4.830	31.472
1	0.1	12.657	76	90	12.032	12.633
2	0.01	9.196	76	174	8.891	17.096
2	0.1	23.624	76	174	23.048	6.595
3	0.01	12.384	76	258	12.182	12.478
3	0.1	35.492	76	258	34.912	4.354

3.3   TOS Mapping Bits = 4

Table 3: Combined Results for TOS Mapping Bits = 4 (narrowed version)

Redundancy	Sender Interval (s)	Sender Time (s)	Symbols	Total Pkts	Receiver Time (s)	Capacity (bit/s)
1	0.01	2.417	38	48	2.217	68.569
1	0.1	6.589	38	48	5.968	25.469
2	0.01	4.272	38	90	4.014	37.865
2	0.1	12.351	38	90	11.773	12.910
3	0.01	6.548	38	132	6.278	24.210
3	0.1	18.143	38	132	17.574	8.649

3.4   TOS Mapping Bits = 8

Table 4: Combined Results for TOS Mapping Bits = 8 (narrowed version)

Redundancy	Sender Interval (s)	Sender Time (s)	Symbols	Total Pkts	Receiver Time (s)	Capacity (bit/s)
1	0.01	1.363	19	27	1.149	132.274
1	0.1	3.747	19	27	3.132	48.530
2	0.01	2.496	19	48	2.301	66.062
2	0.1	6.548	19	48	5.962	25.493
3	0.01	3.376	19	69	3.201	47.488
3	0.1	9.665	19	69	9.077	16.746

4   Graphical Analysis

The following figures were generated during the experiments. And is described in detail below:
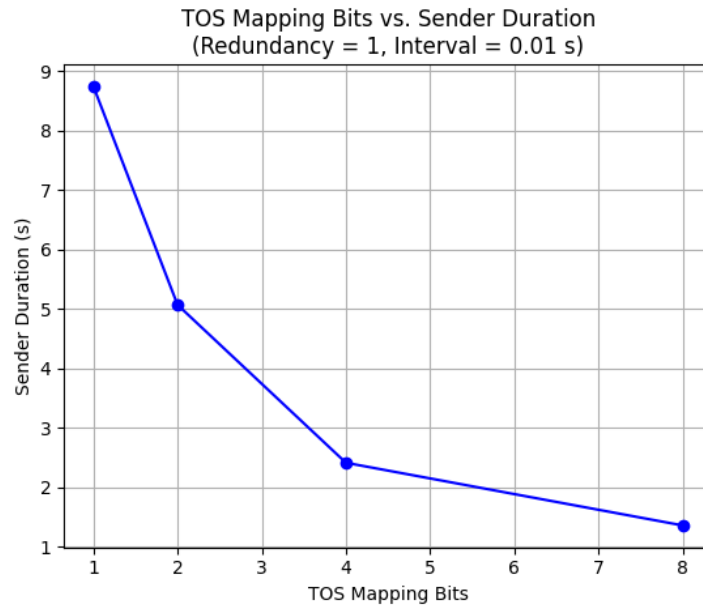
Figure 1: Plot 1: Effect of varying TOS Mapping Bits on Sender Duration. The plot (with redundancy fixed at 1 and sender interval set to 0.01 s) shows that as TOS Mapping Bits increase, the sender duration decreases.
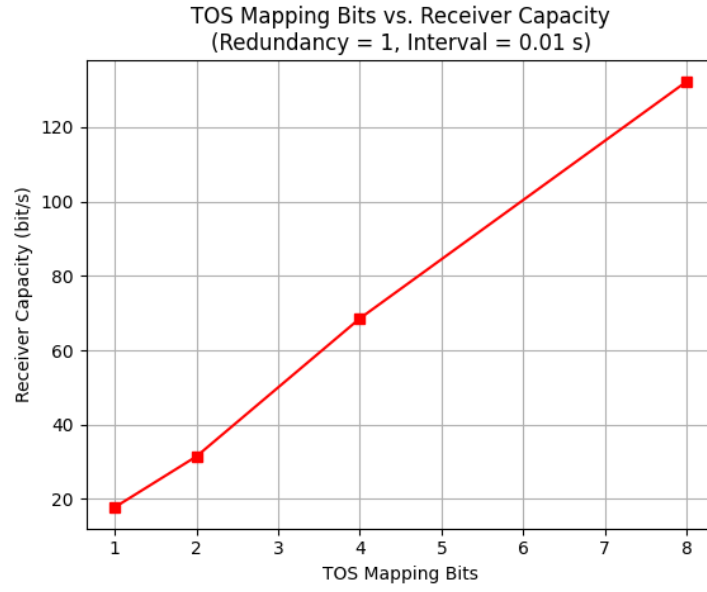
Figure 2: Plot 2: Effect of varying TOS Mapping Bits on Receiver Capacity. With redundancy = 1 and sender interval = 0.01 s, receiver capacity improves as TOS Mapping Bits increase.
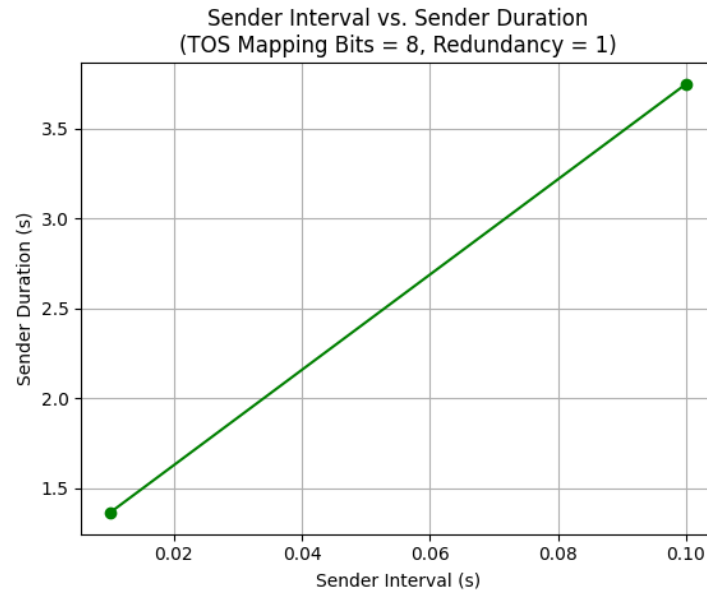

Figure 3: Plot 3: Sender Interval vs. Sender Duration for TOS Mapping Bits = 8 (Redundancy fixed at 1). This plot illustrates how the sender's transmission time varies with different sender intervals when the TOS Mapping Bits is set to 8 and redundancy is maintained at 1.
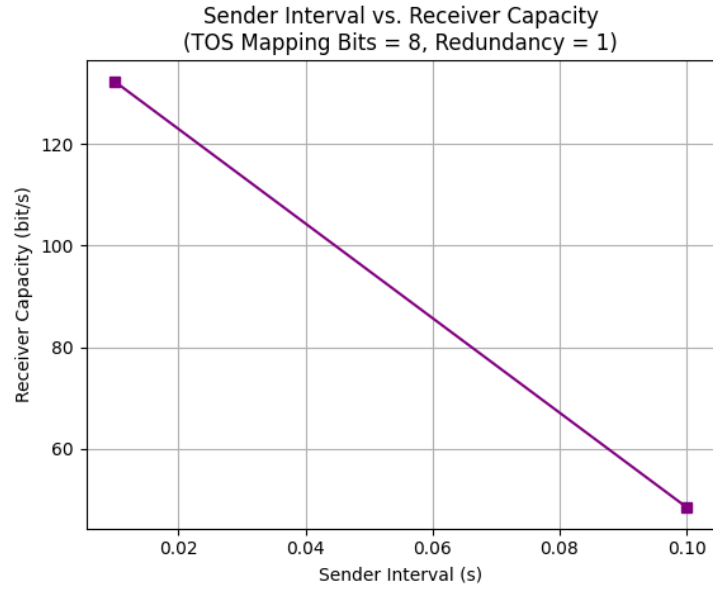
Figure 4: Plot 4: Sender Interval vs. Receiver Capacity for TOS Mapping Bits = 8 (Redundancy fixed at 1). This plot demonstrates the effect of varying the sender interval on the receiver's capacity under the condition that the TOS Mapping Bits is 8 and redundancy remains constant at 1.
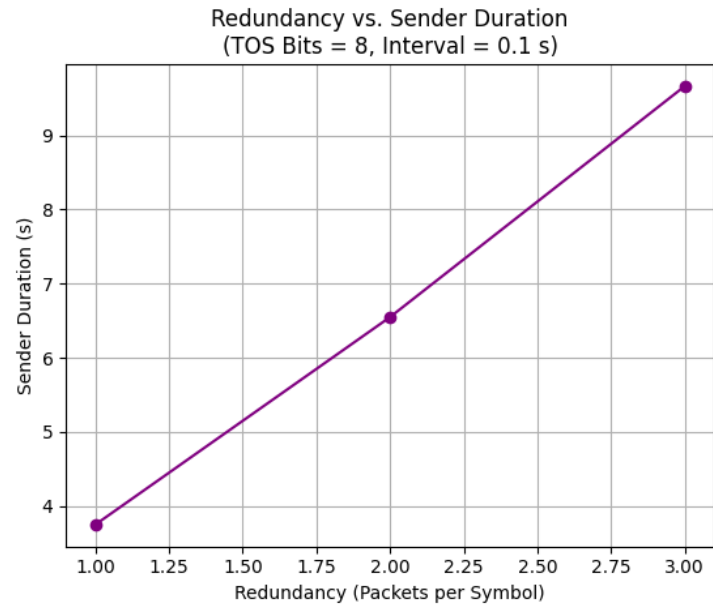

Figure 5: Plot 5: Effect of Redundancy on Sender Duration for TOS Mapping Bits = 8 at a fixed sender interval of 0.1 s. Higher redundancy increases the transmission time.
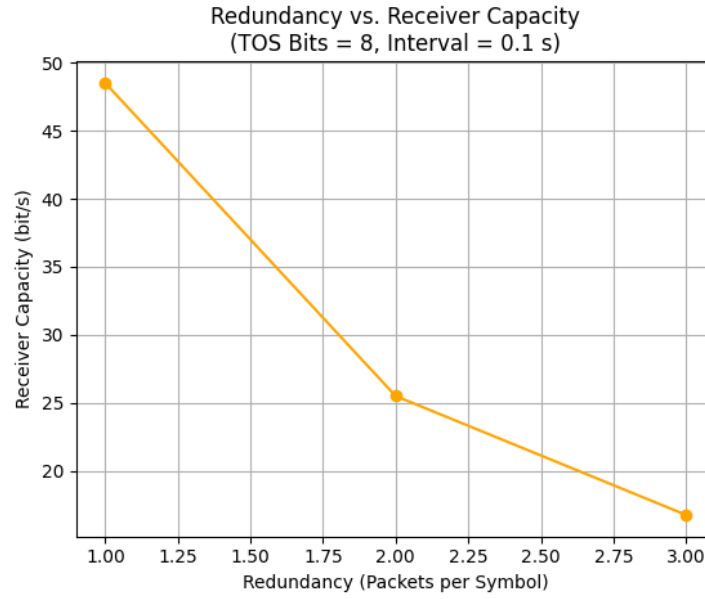
Figure 6: Plot 6: Effect of Redundancy on Receiver Capacity for TOS Mapping Bits = 8 at a fixed sender interval of 0.1 s. As redundancy increases, the effective receiver capacity decreases.

5   Discussion

The experimental results reveal several important trends:

- **Effect of TOS Mapping Bits:** As TOS Mapping Bits increase, fewer payload symbols are needed to represent the message, leading to shorter sender durations and higher receiver capacity.

- **Impact of Redundancy:** Higher redundancy improves reliability via majority voting but increases the overall transmission time and reduces effective channel capacity.

- **Sender Interval Influence:** Shorter sender intervals reduce the total transmission time and increase receiver capacity; however, very aggressive intervals might impact reliability under congested conditions.