# CENG519 - Phase 4 Report

Cansu Eskici
2588036

June 15, 2025

## Mitigation Algorithm

The mitigation mechanism implemented in the processor aims to disrupt the covert channel by probabilistically modifying the least significant bits (LSBs) of the TCP timestamp values in transit. For every TCP packet containing a timestamp option, the processor applies mitigation with a probability determined by the mitigation_coef parameter. When mitigation is triggered, a random number of LSBs (between 0 and 4) in the timestamp value (TSval) are cleared (set to zero), and the modified timestamp is written back into the TCP options field. The altered packet is then forwarded to its destination. This approach introduces controlled noise into the timestamp field, making it difficult for a covert receiver to reliably reconstruct hidden data. By tuning the mitigation_coef, the strength of the mitigation can be adjusted, allowing for a balance between normal network operation and the disruption of covert communication The randomization of the number of bits cleared further increases the uncertainty for any covert channel, enhancing the effectiveness of the mitigation strategy.

## Results

Table 1: Receiver correct message rate for various mitigation coefficients and configurations.

| Bits | Mitigation Coefficient | Message Length | Receiver Correct Rate |
|---|---|---|---|
| 3 | 0.01 | 21 | 0.67 |
| 3 | 0.01 | 75 | 0.00 |
| 3 | 0.01 | 141 | 0.00 |
| 4 | 0.01 | 21 | 1.00 |
| 4 | 0.01 | 75 | 0.33 |
| 4 | 0.01 | 141 | 0.33 |
| 6 | 0.01 | 21 | 1.00 |
| 6 | 0.01 | 75 | 0.33 |
| 6 | 0.01 | 141 | 0.33 |
| 8 | 0.01 | 21 | 0.67 |
| 8 | 0.01 | 75 | 0.67 |
| 8 | 0.01 | 141 | 1.00 |
| 11 | 0.01 | 21 | 1.00 |
| 11 | 0.01 | 75 | 1.00 |
| 11 | 0.01 | 141 | 1.00 |
| 16 | 0.01 | 21 | 1.00 |
| 16 | 0.01 | 75 | 1.00 |
| 16 | 0.01 | 141 | 0.67 |
| 3 | 0.10 | 21 | 0.00 |
| 3 | 0.10 | 75 | 0.00 |
| 3 | 0.10 | 141 | 0.00 |
| 4 | 0.10 | 21 | 0.00 |
| 4 | 0.10 | 75 | 0.00 |
| 4 | 0.10 | 141 | 0.00 |
| 6 | 0.10 | 21 | 0.00 |
| 6 | 0.10 | 75 | 0.00 |

Continued on next page

**Table 1 Mitigation Experiment Results**

| Bits | Mitigation Coefficient | Message Length | Correct Receiving Rate |
|---|---|---|---|
| 6 | 0.10 | 141 | 0.00 |
| 8 | 0.10 | 21 | 0.00 |
| 8 | 0.10 | 75 | 0.00 |
| 8 | 0.10 | 141 | 0.00 |
| 11 | 0.10 | 21 | 0.00 |
| 11 | 0.10 | 75 | 0.00 |
| 11 | 0.10 | 141 | 0.00 |
| 16 | 0.10 | 21 | 0.00 |
| 16 | 0.10 | 75 | 0.00 |
| 16 | 0.10 | 141 | 0.00 |
| 3 | 0.20 | 21 | 0.00 |
| 3 | 0.20 | 75 | 0.00 |
| 3 | 0.20 | 141 | 0.00 |
| 4 | 0.20 | 21 | 0.00 |
| 4 | 0.20 | 75 | 0.00 |
| 4 | 0.20 | 141 | 0.00 |
| 6 | 0.20 | 21 | 0.00 |
| 6 | 0.20 | 75 | 0.00 |
| 6 | 0.20 | 141 | 0.00 |
| 8 | 0.20 | 21 | 0.00 |
| 8 | 0.20 | 75 | 0.00 |
| 8 | 0.20 | 141 | 0.00 |
| 11 | 0.20 | 21 | 0.00 |
| 11 | 0.20 | 75 | 0.00 |
| 11 | 0.20 | 141 | 0.00 |
| 16 | 0.20 | 21 | 0.00 |
| 16 | 0.20 | 75 | 0.00 |
| 16 | 0.20 | 141 | 0.00 |
| 3 | 0.30 | 21 | 0.00 |
| 3 | 0.30 | 75 | 0.00 |
| 3 | 0.30 | 141 | 0.00 |
| 4 | 0.30 | 21 | 0.00 |
| 4 | 0.30 | 75 | 0.00 |
| 4 | 0.30 | 141 | 0.00 |
| 6 | 0.30 | 21 | 0.00 |
| 6 | 0.30 | 75 | 0.00 |
| 6 | 0.30 | 141 | 0.00 |
| 8 | 0.30 | 21 | 0.00 |
| 8 | 0.30 | 75 | 0.00 |
| 8 | 0.30 | 141 | 0.00 |
| 11 | 0.30 | 21 | 0.00 |
| 11 | 0.30 | 75 | 0.00 |
| 11 | 0.30 | 141 | 0.00 |
| 16 | 0.30 | 21 | 0.00 |
| 16 | 0.30 | 75 | 0.00 |
| 16 | 0.30 | 141 | 0.00 |
| 3 | 0.40 | 21 | 0.00 |
| 3 | 0.40 | 75 | 0.00 |
| 3 | 0.40 | 141 | 0.00 |
| 4 | 0.40 | 21 | 0.00 |
| 4 | 0.40 | 75 | 0.00 |
| 4 | 0.40 | 141 | 0.00 |

Continued on next page

**Table 1 Mitigation Experiment Results**

| Bits | Mitigation Coefficient | Message Length | Correct Receiving Rate |
|---|---|---|---|
| 6 | 0.40 | 21 | 0.00 |
| 6 | 0.40 | 75 | 0.00 |
| 6 | 0.40 | 141 | 0.00 |
| 8 | 0.40 | 21 | 0.00 |
| 8 | 0.40 | 75 | 0.00 |
| 8 | 0.40 | 141 | 0.00 |
| 11 | 0.40 | 21 | 0.00 |
| 11 | 0.40 | 75 | 0.00 |
| 11 | 0.40 | 141 | 0.00 |
| 16 | 0.40 | 21 | 0.00 |
| 16 | 0.40 | 75 | 0.00 |
| 16 | 0.40 | 141 | 0.00 |

# Discussion

The results indicate that the mitigation mechanism effectively disrupts the covert channel, especially at higher mitigation coefficients. At a mitigation coefficient of 0.01, the receiver's correct message rate is relatively high, particularly for smaller message lengths and fewer bits. However, as the mitigation coefficient increases, the correct message rate drops significantly, indicating that the mitigation is successful in preventing the covert channel from functioning effectively. The results also show that the effectiveness of the mitigation varies with the number of bits used for hiding data. For example, with 3 bits, the correct message rate is higher at lower mitigation coefficients, but it drops to zero as the coefficient increases. This suggests that the covert channel is more vulnerable to disruption when fewer bits are used. The mitigation mechanism's probabilistic nature allows for a balance between normal network operation and the disruption of covert communication. The results demonstrate that the entropy-based detector is highly effective at identifying the presence of a covert channel, as indicated by the consistently high detector rates (often 1.00) across all tested configurations of bit width, entropy threshold, and message length. This suggests that the method is robust and sensitive to the statistical anomalies introduced by covert data embedding in TCP timestamp fields.