**Phase 4 Report: Covert Channel Mitigation**

**1. Objective** The aim of Phase 4 is to develop and evaluate a mitigation strategy against covert channels identified in Phase 3. The strategy targets covert data transmission using IP timestamp options and consistent packet timing, aiming to degrade covert channel capacity while preserving acceptable communication performance.

**2. Mitigation Strategy** A Mitigator class was implemented to perform three actions:

- **Strip IP Options:** Removes IP timestamp fields that could carry covert bits.
- **Add Random Delays:** Introduces randomized forwarding delays (1-5ms) to disrupt consistent timing used in covert channels.
- **Drop Suspicious Packets:** (Optional) Discards packets with detectable covert indicators like option type 68 (timestamp).

**3. Implementation Details** The mitigator is integrated into the processor from Phase 3. Key features:

- Per-packet delay with statistics tracking.
- Optional metadata removal and packet dropping.
- Environment variables control each mitigation feature:
    - MITIGATE_STRIP_OPTIONS
    - MITIGATE_ADD_DELAY
    - MITIGATE_DROP_SUSPICIOUS

**4. Experimental Setup**

- Environment: Same NATS and Scapy setup as Phase 3.
- ENABLE_COVERT=1 to simulate covert transmission.
- ping -c 100 insec was executed to analyze RTTs and covert traffic behavior.

**5. Results**

**5.1 Ping Summary:**

100 packets transmitted, 95 received, 5% packet loss
rtt min/avg/max/mdev = 6.390/10.443/14.076/1.649 ms

**5.2 Detection Metrics:**

True Positives: 0
False Positives: 0
True Negatives: 0
False Negatives: 207

Accuracy: 0.00%
Precision: 0
Recall: 0
F1-Score: 0

**5.3 Covert Channel Capacity:**

- Capacity: 9.63 bits/sec
- Despite mitigation, covert sender retained some ability to transmit data, likely by redundancy or resilience.

**5.4 Mitigation Statistics:**

Packets Processed: 207
Packets Stripped: 5
Packets Delayed: 195
Packets Dropped: 0
Total Delay Added: 0.579 sec
Average Delay per Packet: 2.80 ms

**6. Analysis**

- **Detection Breakdown:** All covert packets went undetected. The mitigator obscured identifiable metadata and timing features.
- **Performance Cost:** RTT increased noticeably, but within acceptable real-time limits. Random delays increased jitter.
- **Covert Impact:** Capacity increased slightly (from 7.56 to 9.63 bps), likely due to improved packet retention and adjusted sender behavior.

**7. Conclusion** The mitigation approach effectively evaded the Phase 3 detector. It introduces moderate delay and slight overhead. Although it didn't fully eliminate covert transmission, it substantially reduced detectability. A combination of mitigation and adaptive detection may be necessary for robust security.

---

**Appendices**

- Full logs in results.json
- GitHub repo includes code and experiment data
- Mitigator code includes toggleable strategies and runtime metrics tracking