

Abstract

Electrooculography (EOG) signals are mapped to control inputs and transmitted to a robotic system, introducing potential cybersecurity risks. AES-GCM authenticated encryption with timestamp-based validation is implemented to prevent malicious attacks. Experimental results show that the secure pipeline for transmitting biosignal commands effectively rejects malicious traffic while maintaining performance.

Keywords: electrooculography, assistive robotics, cyber-physical systems, AES-GCM, authenticated encryption, secure neural data

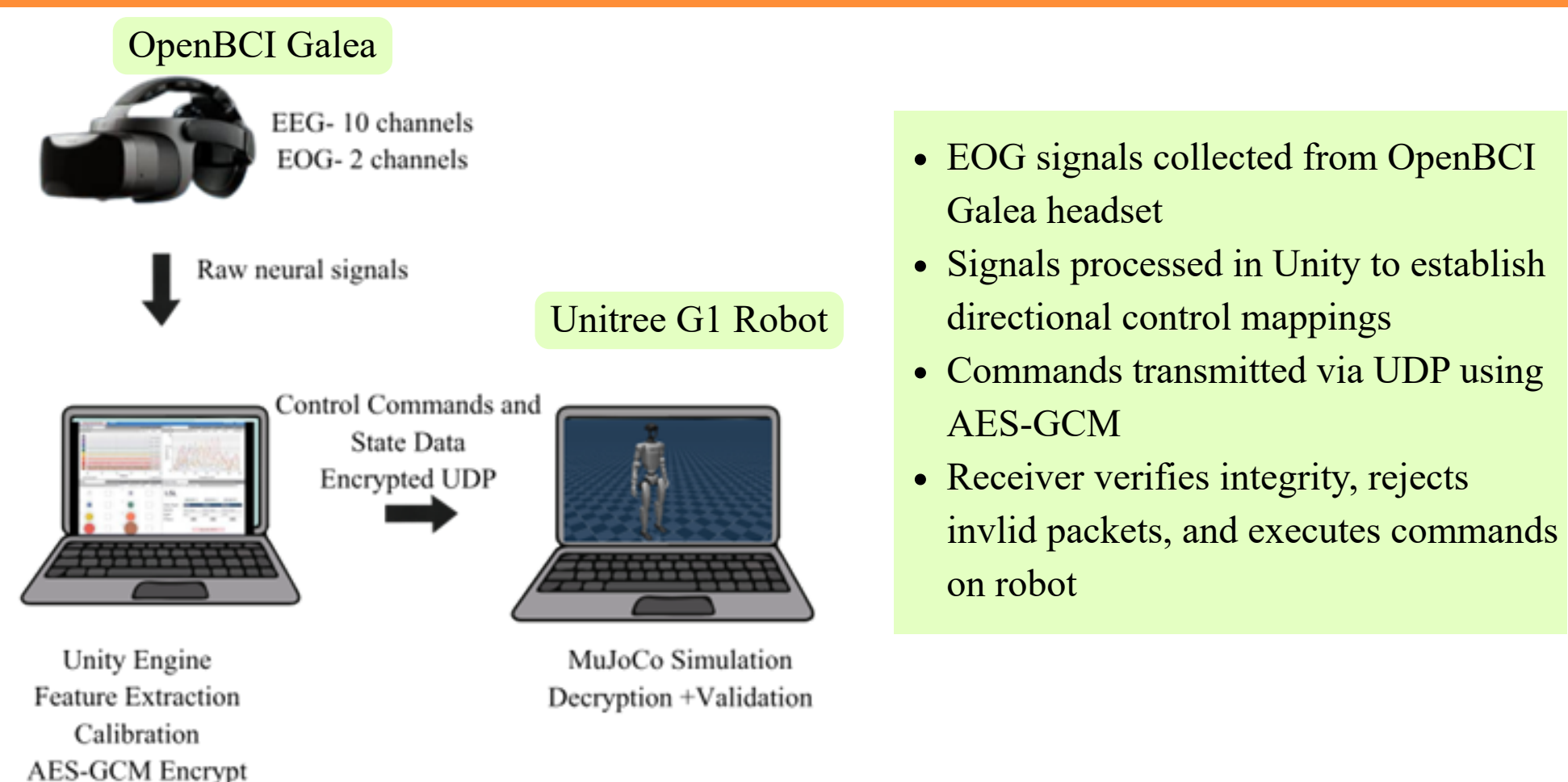
Motivation

Assistive robotics relies more heavily on physiological signals such as electrooculography (EOG) to enable hands-free control. However, transmitting biosignal-derived commands introduces critical cybersecurity risks. Attackers can inject, replay, or flood control packets, potentially causing unsafe robotic behavior

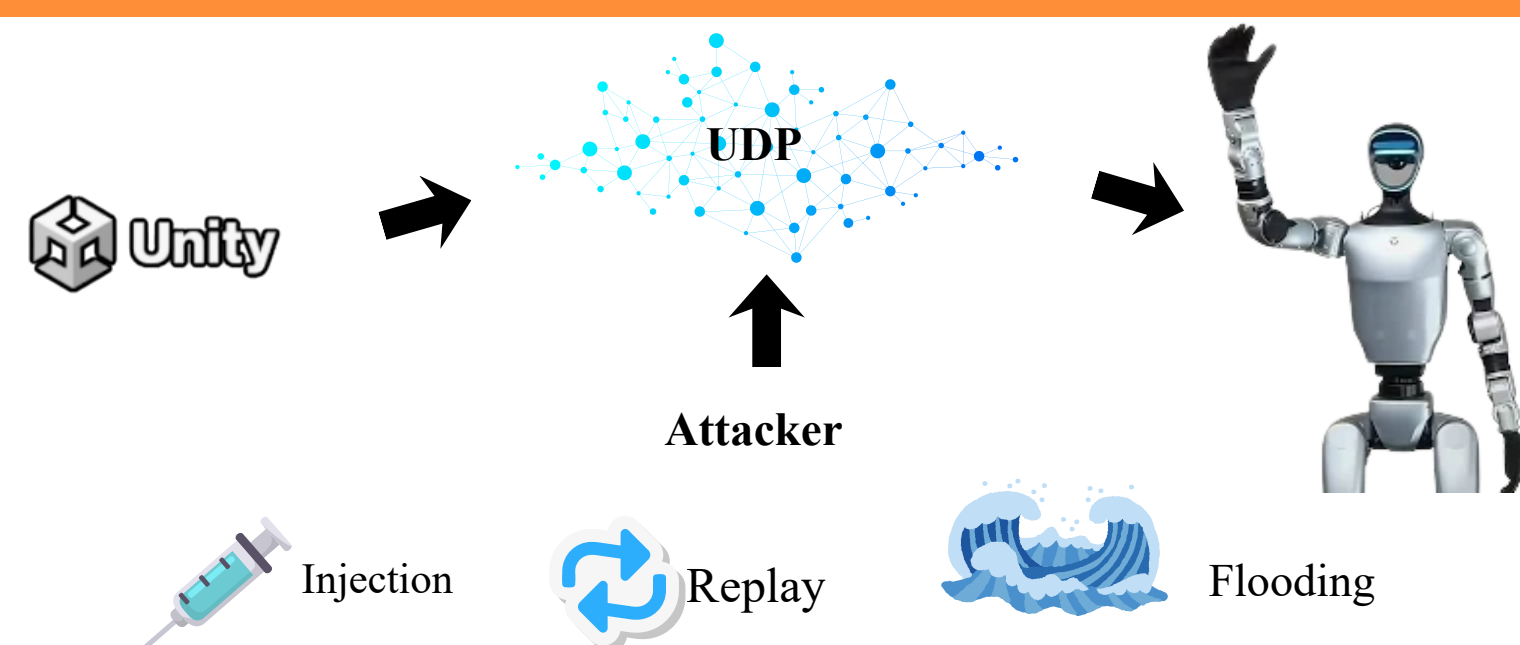
Impact

- Enables a secure technique for hands-free control for motor-impaired individuals
- Prevents harmful robotic behavior caused by malicious or corrupted signals
- Supports deployment of bio-signal based systems in healthcare and assistive environments

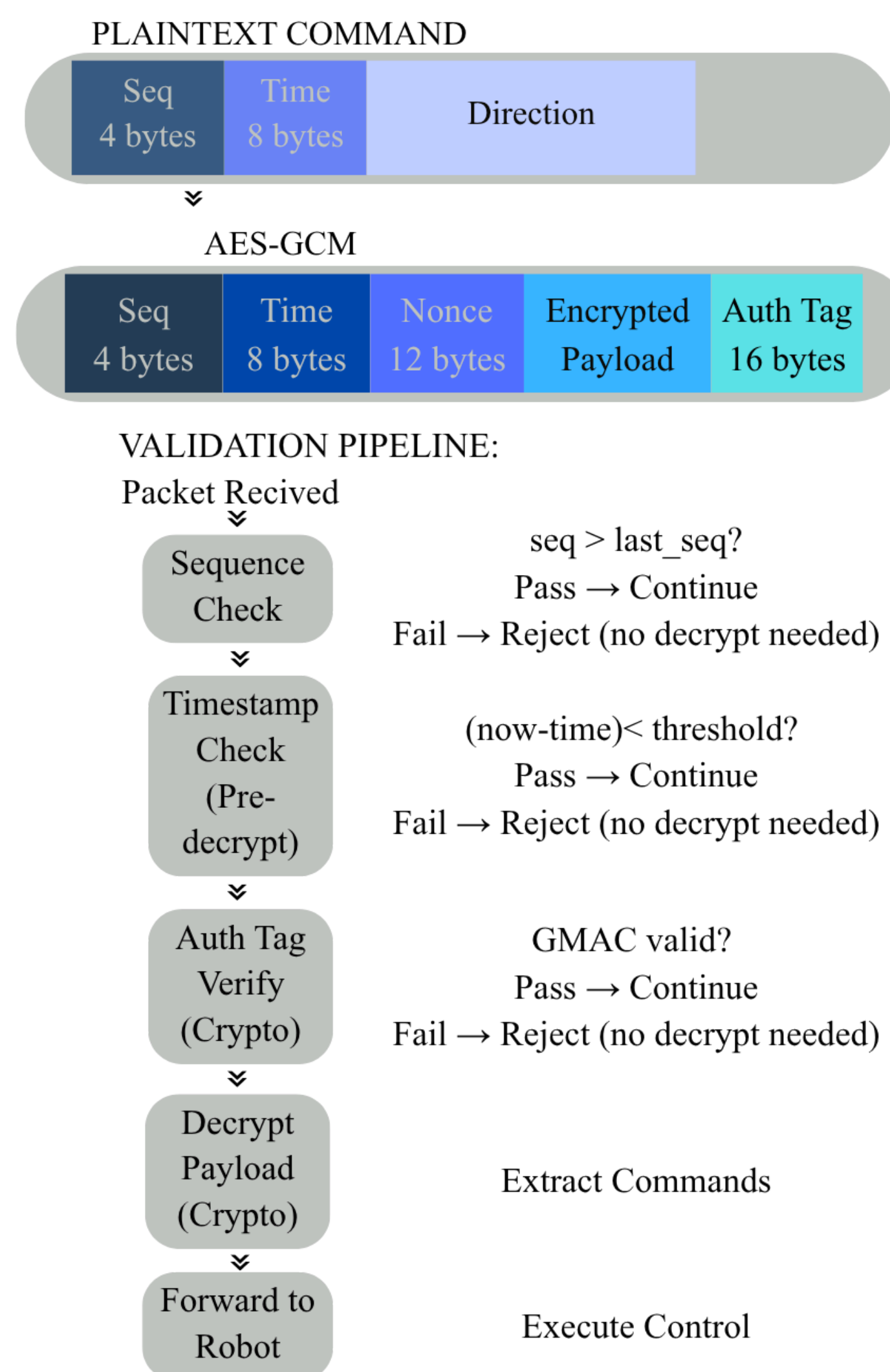
System Overview



Threat Model



Security Design



AES-GCM

$C, T = AES-GCM_K(IV, P, AAD)$
 P = plaintext (command data)
 C = ciphertext
 T = authentication tag
 AAD = additional authenticated data
 Ciphertext C and authentication tag T are generated from plaintext P using key K and IV

Validation Strategy

- Early rejection prevents unnecessary decryption and reduces computational overhead.
- Replay protection enforced by sequence ordering and timestamp constraints.

Experimental Setup

System Configuration

- Pipeline: Galea → Unity → UDP → Mujoco
- Commands transmitted as UDP packets
- Two modes evaluated:
 - Plain (unsecured)
 - Secure (AES-GCM+ Validation)

Attack Scenarios

- **Injection:** Adversarial packets with fake commands
- **Replay:** Retransmission of previously valid packets
- **Flooding:** High-rate packet transmission to overload the receiver

Dataset & Evaluation Setup

- Flood: Sweeps 1-4: progressively increased flood load
- Injection Sweeps 5-7: progressively increased injected packet volume
- Replay: retransmission of previously captured packets

Sweep Details

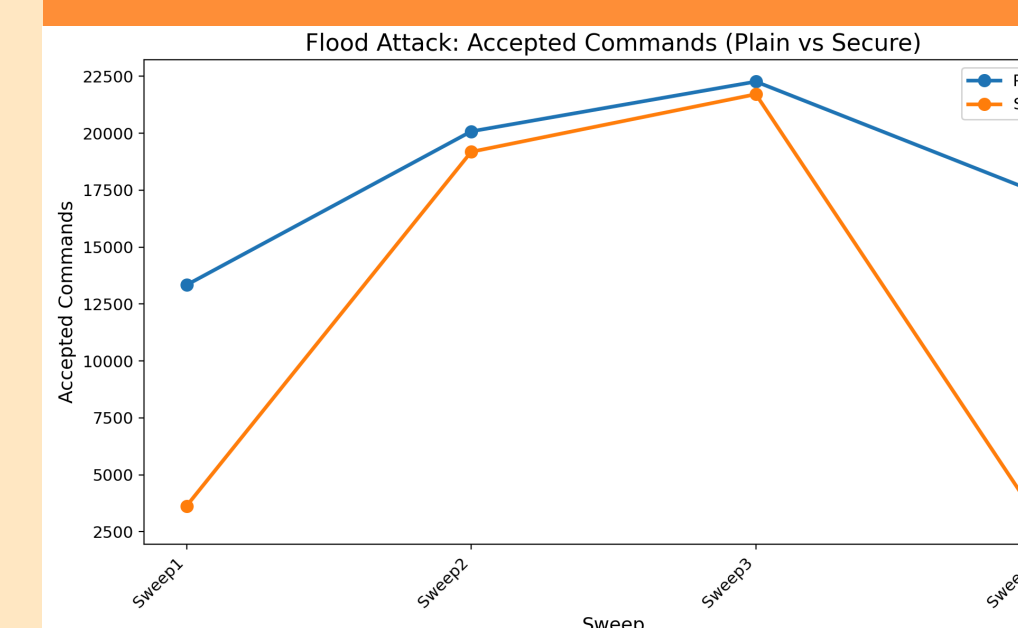
- **Flood**
 - Sweep 1: mixed traffic (valid, malformed, wrong-key) at a moderate rate
 - Sweep 2: malformed packet flooding across varied packet rates
 - Sweep 3: wrong-key packet flooding across varied packet rates
 - Sweep 4: valid traffic at high rate
- **Injection**
 - Sweep 5: wrong-key and tampered packet injection at varying rates and counts
 - Sweep 6: random packet injection at higher rates
 - Sweep 7: valid packet injection

Evaluation Metrics

- Accepted packets (successful command execution)
- Rejected Packets (auth, replay, stale)
- Latency (average and maximum, ms)

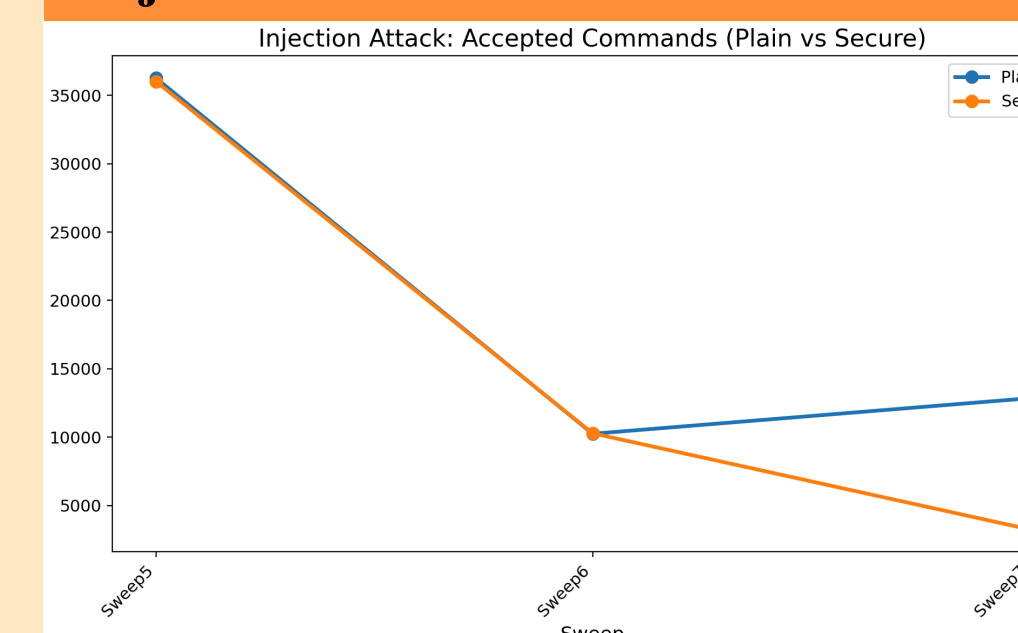
Results

Flood



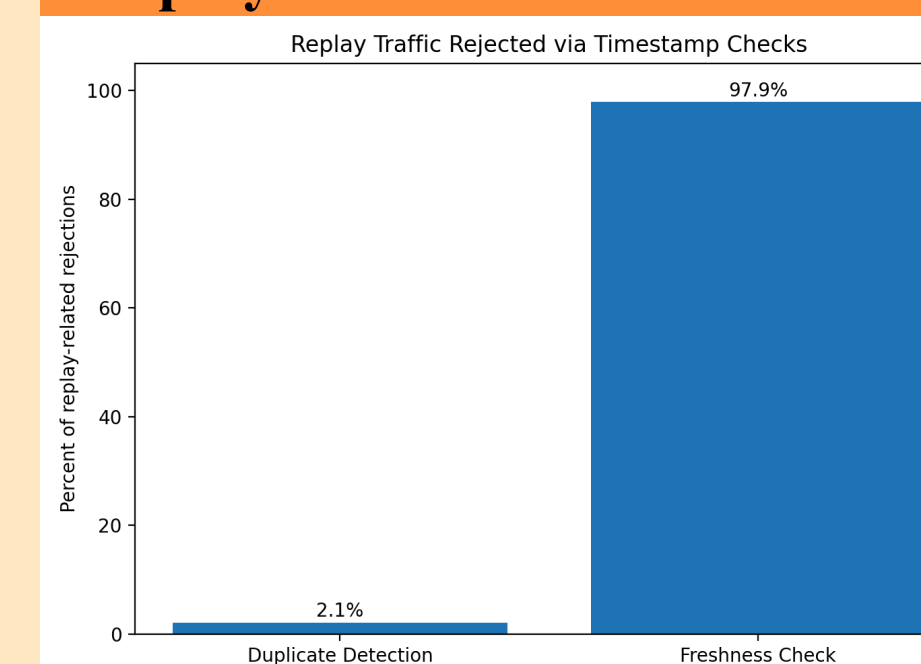
Secure communication maintains comparable throughput at moderate load while filtering traffic under heavier flood conditions. Secure channel reduces accepted traffic by up to 73% under attack conditions.

Injection



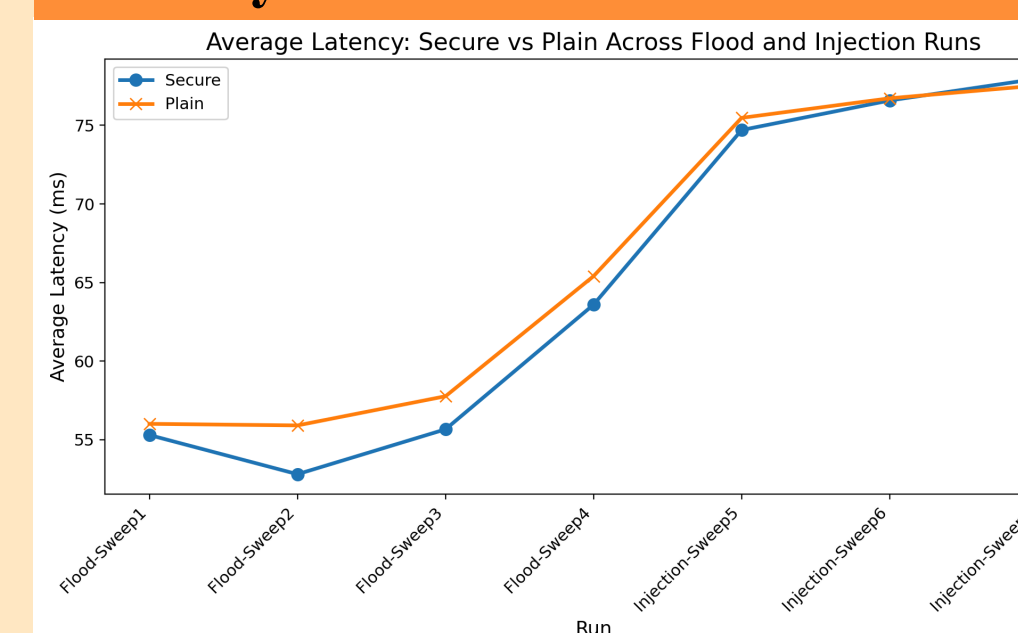
The secure channel rejects unauthorized traffic, while the plain channel continues to accept more commands. Unauthorized commands have been reduced significantly in secure mode.

Replay



Most replay attempts are rejected before decryption via time stamp, over 95%.

Latency



AES-GCM protection preserves real-time performance, with secure and plain latency remaining closely matched across runs. Secure communication reduces the latency overhead by less than 1 ms.

Conclusion

- Secure command transmission prevents injection, replay, and flooding attacks
- Maintain real-time performance with little to no latency overhead (<1ms)
- Feasibility of securing biosignal-driven robotic control

Future Work

- Extend to real world Unitree robotic platform
- Evaluate addition biosignal modalities
- Investigate adaptive network deployments