# SOUNDBOOST: Effective RCA and Attack Detection for UAV via Acoustic Side-Channel

Haoran Wang*, Zheng Yang*, Sangdon Park^, Yibin Yang*, Seulbae Kim^, Willian Lunardi°, Martin Andreoni°, Taesoo Kim*, Wenke Lee*

Georgia Tech*
POSTECH^
Technology Innovation Institute°

Georgia Tech

# Motivation and Background

- UAV applications: surveillance, delivery, mapping, entertainment
- Dependence on critical sensors: GPS and IMU
- Increasing threats: GPS spoofing and IMU biasing attacks
- Difficulty in distinguishing compromised sensors under conflicting reports
- Current solutions lack effective root cause analysis.

Georgia Tech

# Key Challenges

- Can acoustic signals effectively correlate with UAV kinematics?
- How to reliably identify which sensor (GPS or IMU) is compromised?
- How to accurately identify simultaneous attacks?
- Can acoustic analysis remain robust under adversarial sound spoofing attacks?

Georgia Tech

# Threat Model and Assumptions

- Adversary capabilities:
  - Can spoof either GPS or IMU sensors or both
  - Has full knowledge of UAV flight status
- Attack goals:
  - Cause mission failure by misleading the UAV without crashing it
  - Evade detection by avoiding obviously anomalous sensor values
- System assumptions:
  - Acoustic channel is unforgeable due to physical and operational constraints
  - UAV control loop remains closed-loop and acoustic signal remains observable
  - Adversary cannot arbitrarily manipulate microphone input or motor acoustics

# SOUNDBOOST Overview

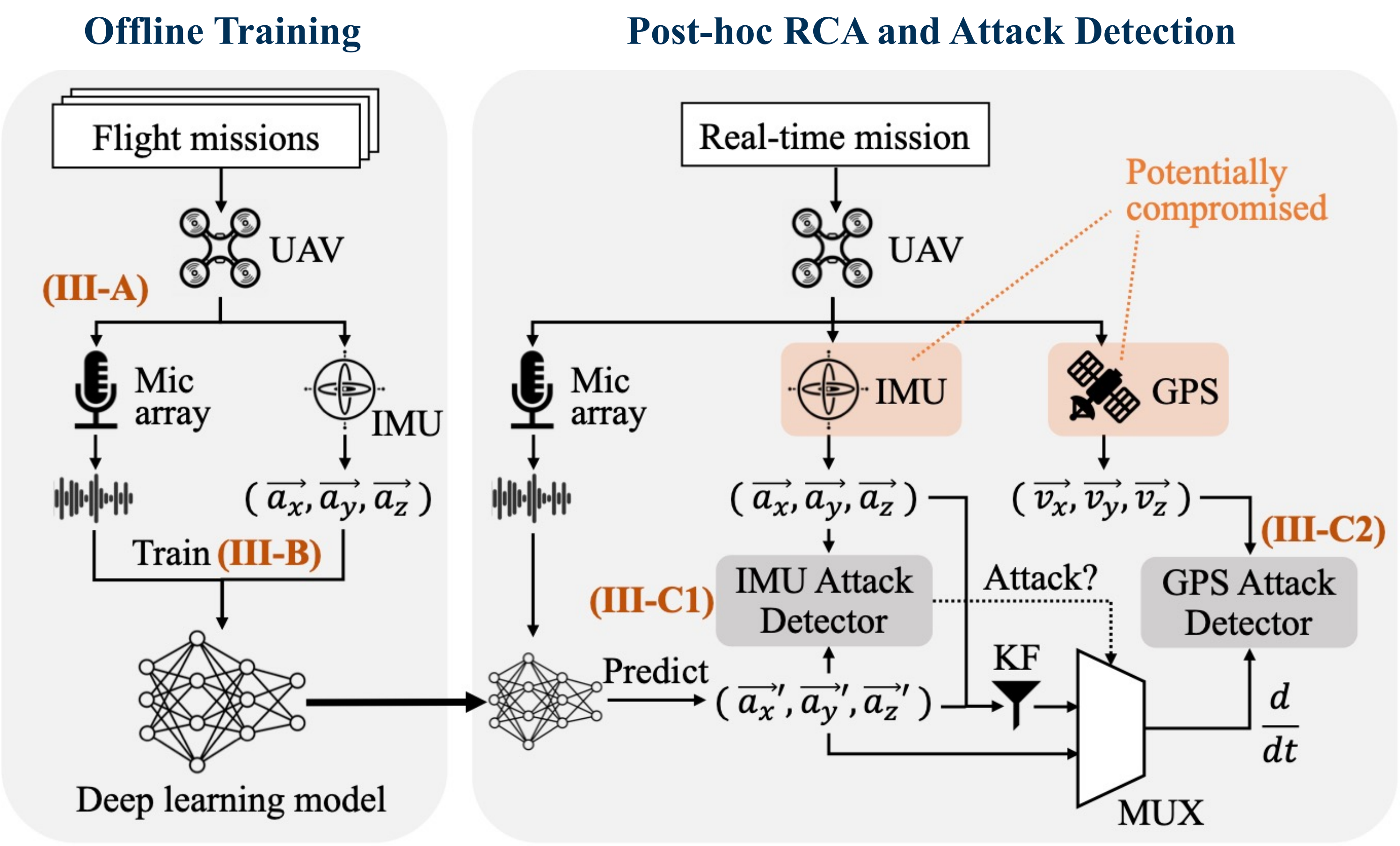
- Utilizing acoustic side-channel for robust RCA
- Post-incident diagnosis with integrated machine learning and sensor fusion
- Workflow:
    A. Acoustic Signature Generation

    B. Deep Learning-based acoustic-kinematics correlations

    C. Post-hoc RCA:

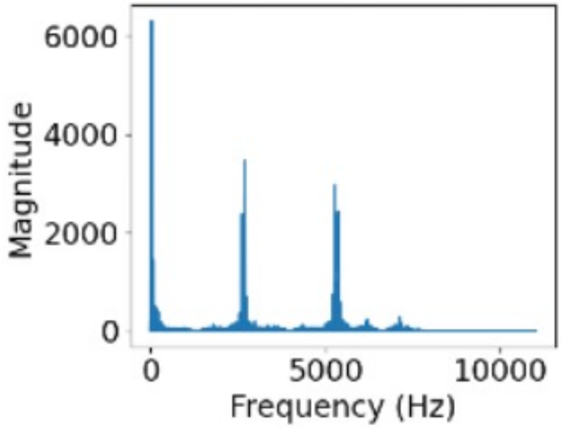
      1. IMU Attack Detection

      2. GPS Attack Detection

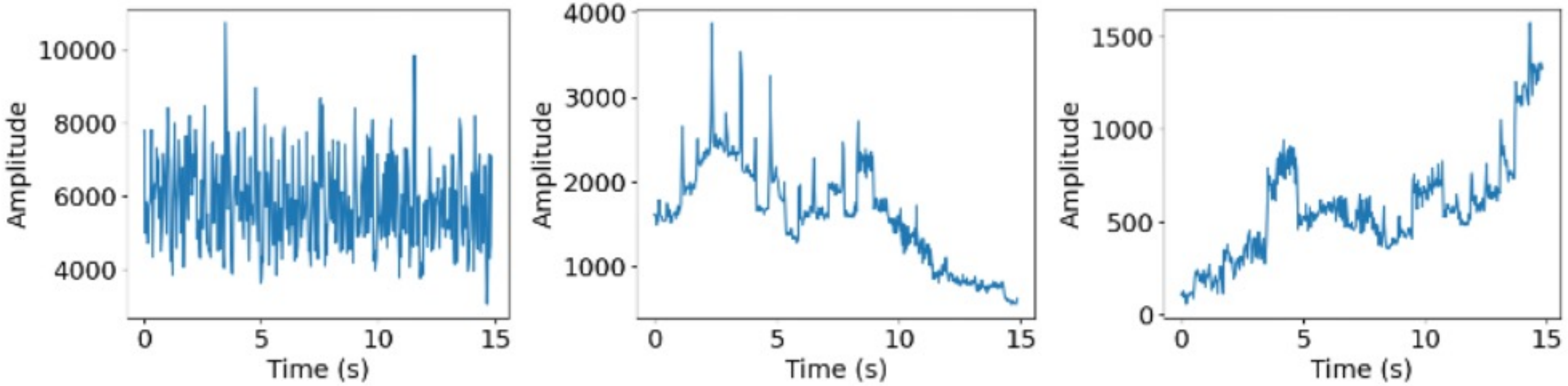


# Acoustic Signature Generation

- FFT analysis of drone motor sounds
- Identifying key frequencies:
  - Aerodynamic: around 5500 Hz
  - Mechanical: around 2500 Hz
  - Blade-passing: around 200 Hz




- Insights: Amplitude of sound provides clear patterns indicating drone acceleration states (hovering, decelerating, accelerating)

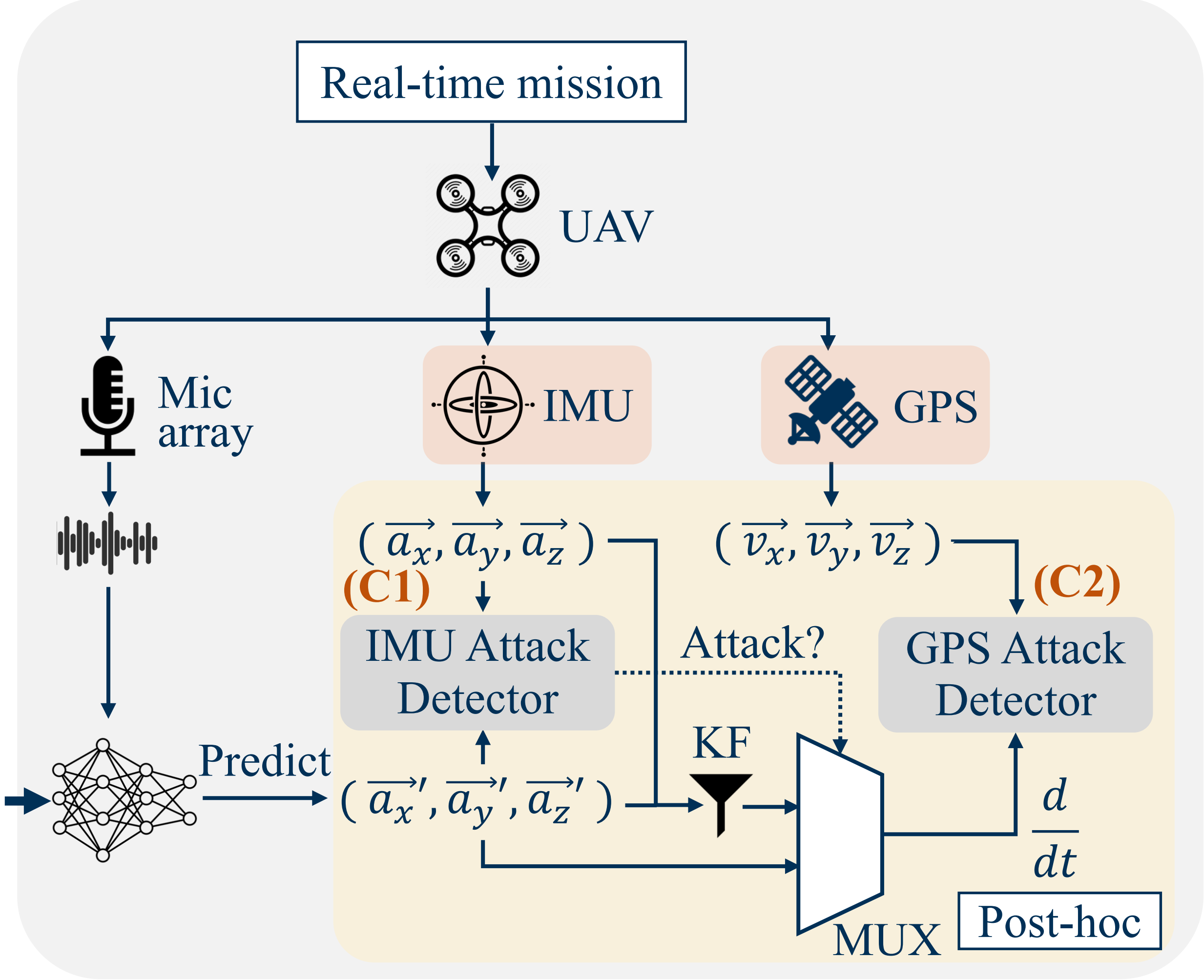


# Kinematics Correlations

- Deep learning-based correlation of acoustic signatures with UAV acceleration vectors
- Model selection and training: MobileNetV2
- Choosing optimal time window
- Data augmentation techniques to handle environmental variability

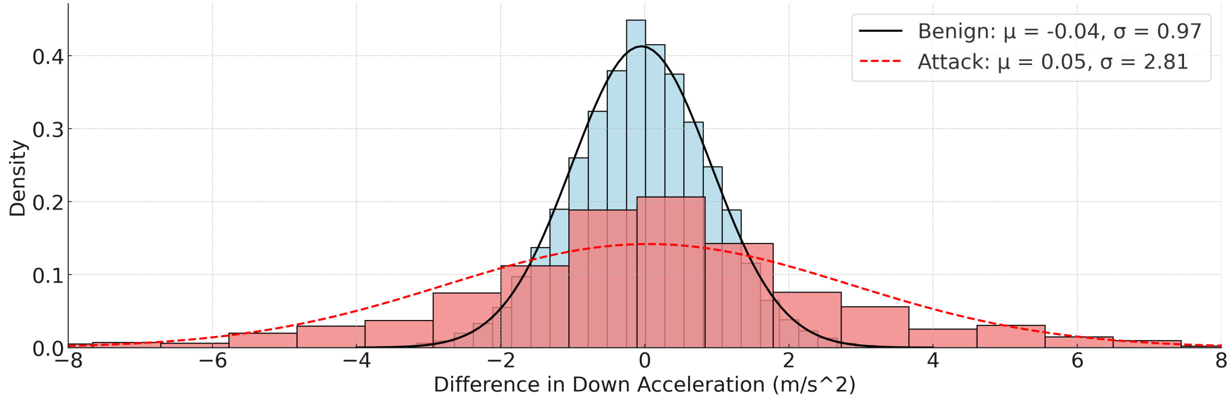
# Post-Hoc Two-Layer RCA

- Stage 1: IMU Attack Detection (statistical anomaly detection)
- Stage 2: GPS Attack Detection (Kalman filter-based sensor fusion)
- Workflow:
  - Acoustic signature prediction
  - Residual analysis against IMU measurements
  - IMU integrity decision
  - GPS spoofing detection based on velocity discrepancies



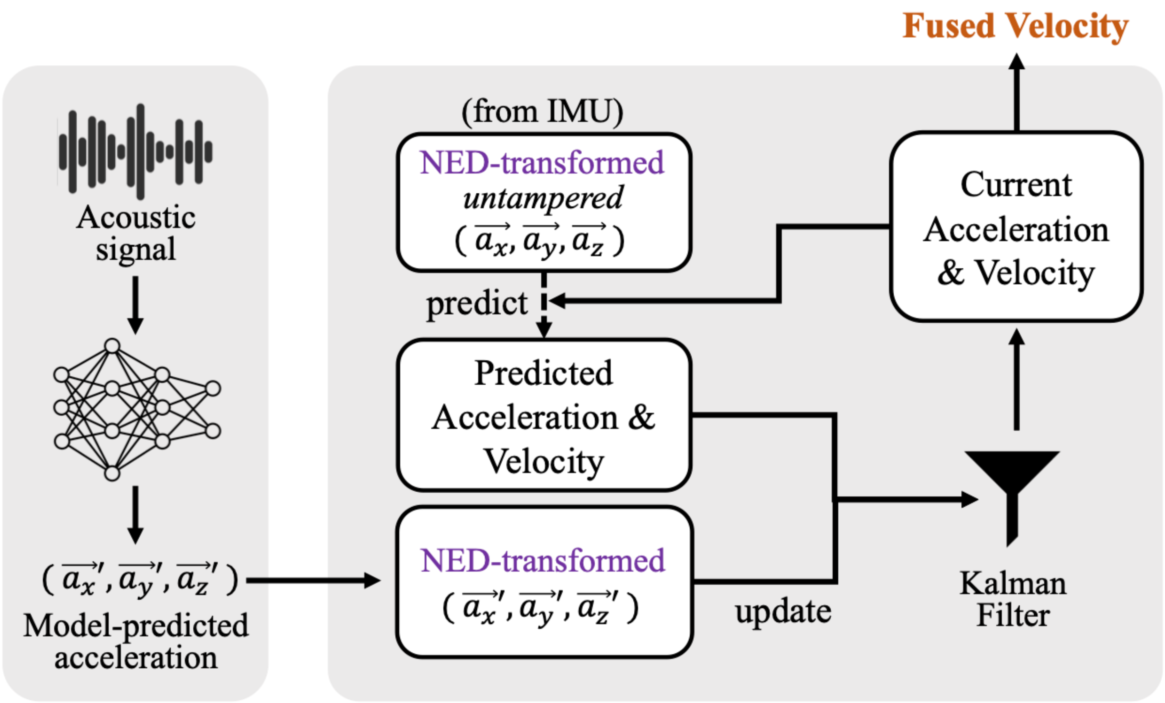
# IMU Attack Detection

- Residual distribution analysis
- Statistical detection using Kolmogorov-Smirnov test



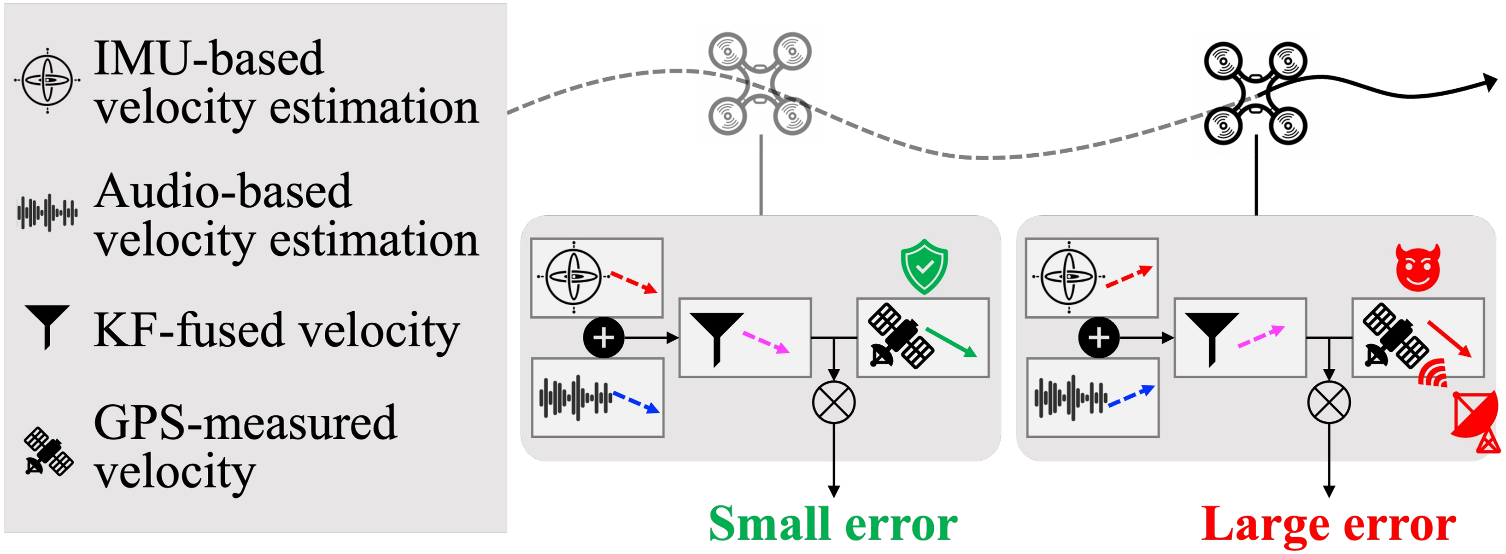
# GPS Attack Detection

- Kalman filter-based sensor fusion with two versions:
  - Audio Only KF: Used when IMU is compromised; relies solely on acoustic-based acceleration predictions for velocity estimation.
  - Audio + IMU KF: Used when IMU is trustworthy; combines IMU measurements with acoustic predictions for weighted sensor fusion.



# GPS Attack Detection

- Detection achieved through velocity discrepancy analysis between GPS-reported and KF predicted velocities



# Implementation

- Hardware:
  - Holybro X500 Quadcopter with PX4 autopilot
  - Raspberry Pi
  - ReSpeaker microphone array strategically positioned *off-center* on the UAV's frame
- Data collection:
  - Outdoor UAV flights under varying environmental conditions
  - Designed flight missions with diverse maneuvers for model generalization

# Attack Setup

- IMU biasing attacks:
  - Synthetic accelerometer DoS attack
  - Synthetic gyroscope Side-Swing attack
- GPS spoofing attacks:
  - Physical GPS spoofing attack
  - SDR device called HackRF One
  - An open-source signal generation tool called GPS-SDR-SIM

# Evaluation: IMU Attack Detection

- Attack detection
  - True positive rate: 100%
  - False positive rates: 10%
- Insights: High accuracy demonstrates robustness and reliability of acoustic-based statistical anomaly detection on IMU attacks

# Evaluation: GPS Spoofing Attack Detection

| | SoundBoost | | Baselines | | | | |
|---|---|---|---|---|---|---|---|
| System Inputs | audio only | audio & IMU | Failsafe [33] IMU only | LTI [10] yaw | LTI [10] vx | LTI [10] vy | DNN [15] (LSTM) |
| # Benign Flights | 30 | 30 | 30 | 30 | 30 | 30 | 30 |
| # Alerted | 7 | 2 | 5 | 3 | 0 | 1 | 22 |
| # Attack Flights | 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| # Alerted | 15 | 17 | 11 | 5 | 1 | 1 | 13 |
| TPR | **0.79** | **0.89** | 0.58 | 0.26 | 0.05 | 0.05 | 0.68 |
| FPR | 0.23 | **0.10** | 0.17 | 0.10 | 0 | 0.03 | 0.73 |

- Accuracy:
  - 89% (Audio + IMU), 79% (Audio Only)
- False positive rates:
  - 10% (Audio + IMU), 23% (Audio Only)
- Baseline comparison:
  - Outperforms traditional GPS spoofing detection methods significantly
- Insights:
  - Both version surpass the SOTA performance
  - Inclusion of trusted IMU data improves detection accuracy, highlighting the importance of multi-modal sensor fusion

# Adversarial Robustness

| Attacks | Amplitude | 1 TPR | 1 FPR | 2 TPR | 2 FPR | 3 TPR | 3 FPR | 4 TPR | 4 FPR |
|---|---|---|---|---|---|---|---|---|---|
| Canceling | 0% | 0.74 | 0.41 | 0.74 | 0.47 | 0.76 | 0.56 | 0.70 | 0.57 |
| | 25% | 0.79 | 0.40 | 0.76 | 0.46 | 0.76 | 0.48 | 0.76 | 0.57 |
| | 50% | 0.84 | 0.38 | 0.81 | 0.40 | 0.78 | 0.47 | 0.79 | 0.43 |
| | 75% | 0.84 | 0.28 | 0.84 | 0.38 | 0.84 | 0.38 | 0.79 | 0.40 |
| Amplifying | 125% | 0.79 | 0.13 | 0.64 | 0.06 | 0.59 | 0.06 | 0.53 | 0.07 |
| | 150% | 0.62 | 0.08 | 0.52 | 0.04 | 0.45 | 0.06 | 0.42 | 0.07 |
| | 175% | 0.59 | 0.06 | 0.47 | 0.04 | 0.39 | 0.07 | 0.37 | 0.07 |
| | 200% | 0.55 | 0.04 | 0.42 | 0.04 | 0.38 | 0.07 | 0.37 | 0.07 |

(Channels: 1, 2, 3, 4)

*The baseline TPR and FPR are 0.89 and 0.1.

- Real-world record-and-replay attacks
  - Fail to cause measurable effects on acceleration predictions
  - Insight: Real-world spoofing sounds fail to phase-synchronize with UAV acoustic signals
- Simulated phase synchronization attacks
  - Canceling (0%): reduces the TPR to 0.7 on 4 channels and 0.74 on 1 channel
  - Amplifying (200%): reduces the TPR to 0.37 on 4 channels and 0.55 on 1 channel
  - Insights: Amplification makes downstream detection more susceptible, while cancellation make detection overly sensitive but not easily bypassed
- Attacker's Limitations
  - Precise synchronization requirement difficult to achieve practically
  - Acoustic power and range significantly limit attacker effectiveness

# Conclusion

- Acoustic side-channel as reliable source for UAV root cause analysis
- Effective detection of both GPS and IMU spoofing attacks
- Demonstrated adversarial robustness in both real-world and simulated attacks

# Q&A