浙江大學
ZHEJIANG UNIVERSITY

THE HONG KONG
POLYTECHNIC UNIVERSITY
香港理工大學

西安交通大學
XI'AN JIAOTONG UNIVERSITY

ACM SenSys 2022

KITE: Exploring the Practical Threat from Acoustic Transduction Attacks on Inertial Sensors

[1]Ming Gao, [1]**Lingfeng Zhang**, [2]Leming Shen, [1,3]Xiang Zou,

[1]Jinsong Han, [1]Feng Lin, [1]Kui Ren

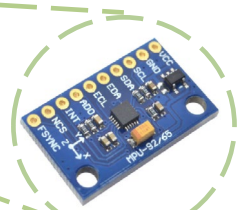
[1]Zhejiang University, Hangzhou, China

[2]The Hong Kong Polytechnic University, Hong Kong, China

[3]Xi'an Jiaotong University, Xi'an, China

Inertial Sensor

Inertial Sensor



accelerator
(reflect changes in speed)

gyroscope
(reflect changes in direction)

5m/s

3m/s

1m/s

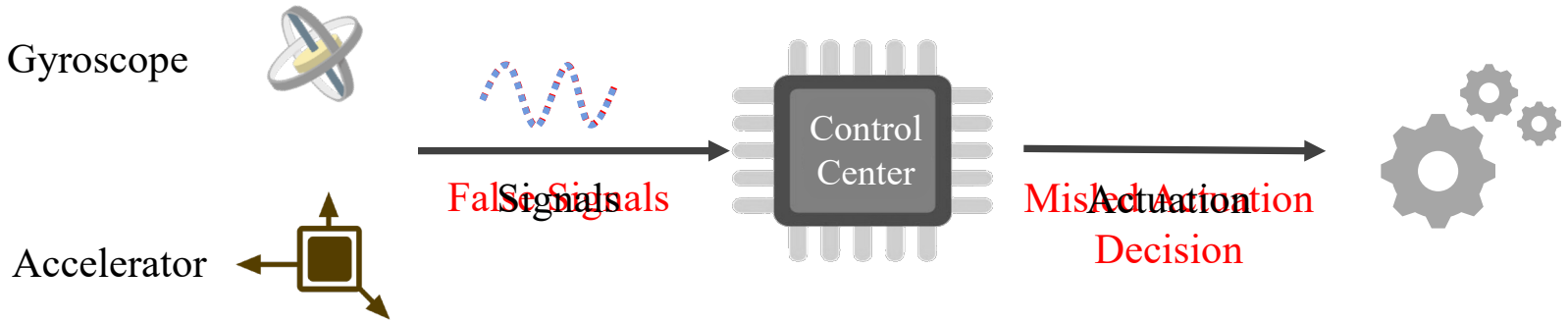
turn right

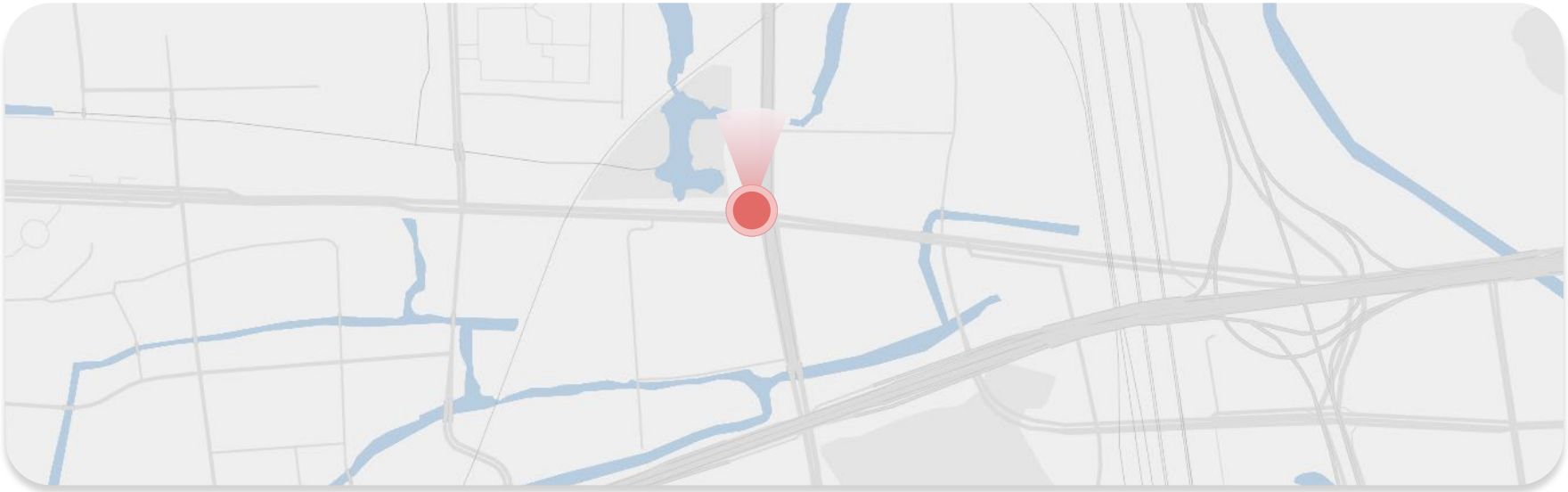
Acoustic Interference

Zhejiang University

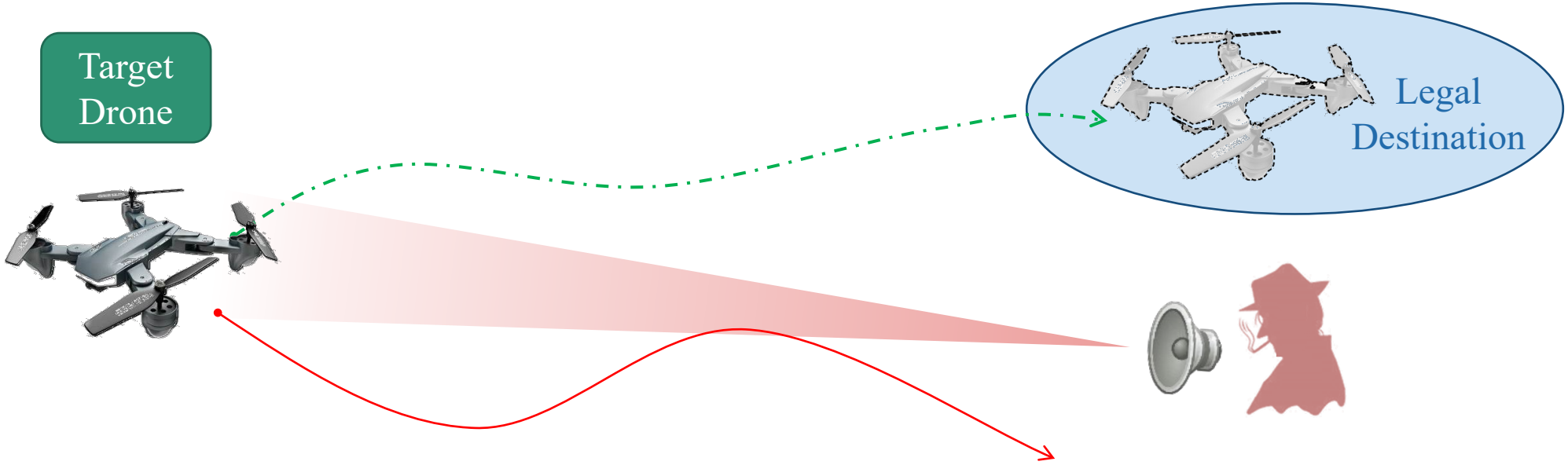
Inertial Sensors ≠ Reliable !

Acoustic Transduction Attack





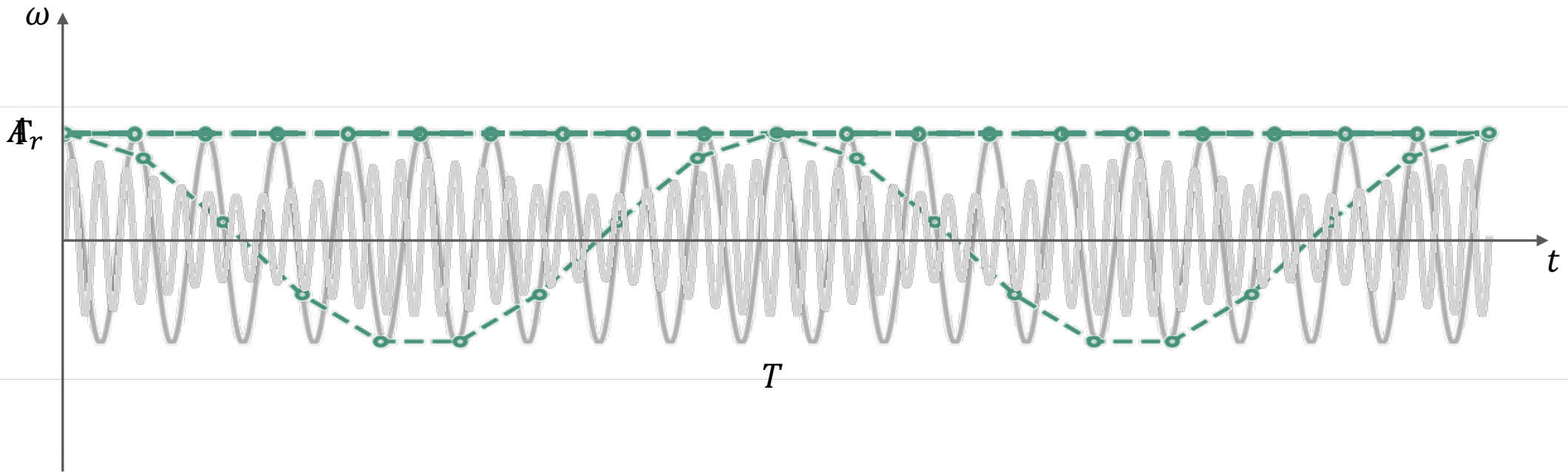
Our Vision



- Manipulate a multiple-degree-of-freedom system to follow the maliciously assigned trajectory even the target is moving

1.How to inject stable and controllable signals?

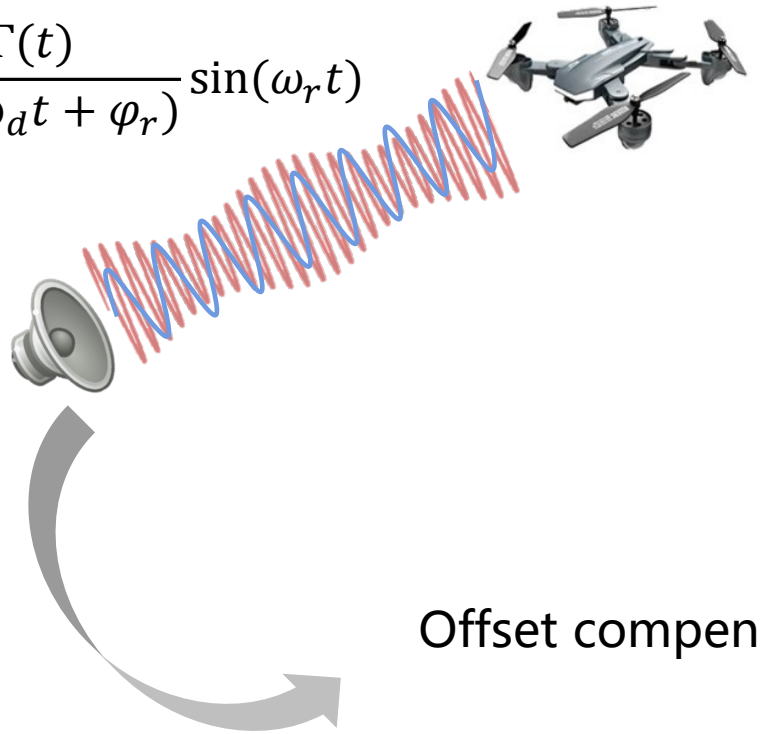
- Existing Approach



$$F(t) = \frac{\Gamma(t)}{\cos(\omega_d t + \varphi_r)} \sin(\omega_r t).$$

Solution: Offset Compensation and Phase Estimation

$$F(t) = \frac{\Gamma(t)}{\cos(\omega_d t + \varphi_r)} \sin(\omega_r t)$$



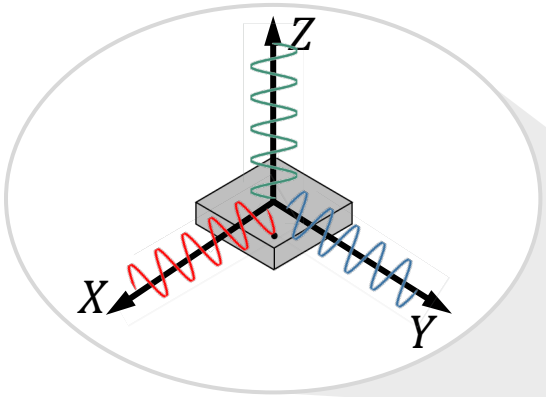
Offset compensation: $\omega_{r_2} = \omega_{r_1} - n_p \Delta F s$

Phase estimation: $\varphi_{r_2} = \varphi_{r_1} + \frac{1}{\xi}(\omega_{d_2} - \omega_{d_1})$

2.How to control the direction of injection

- SDOF system
  - one direction motion
  - easy to be controlled

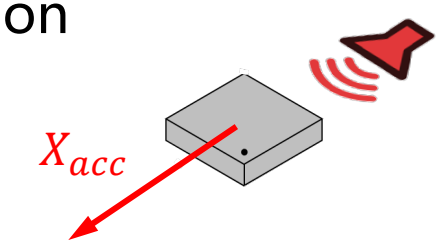
- MDOF system
  - move free in space
  - multi-axis simultaneous resonance

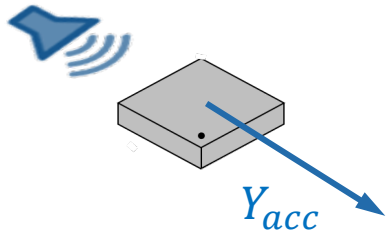


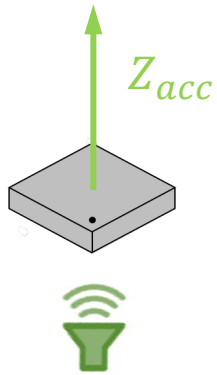
Solution: multiple acoustic sources

- Our observation

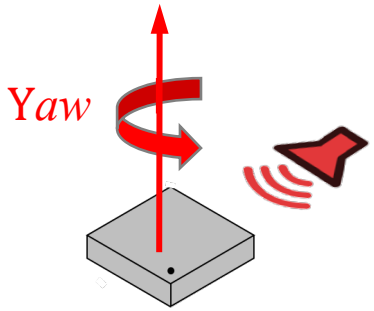
Accelerator

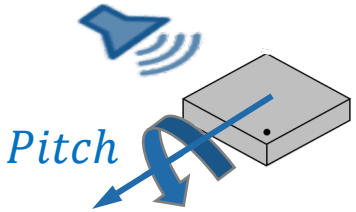


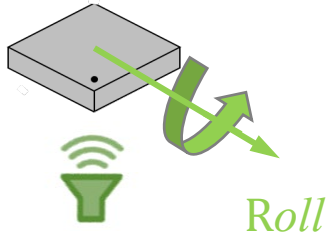




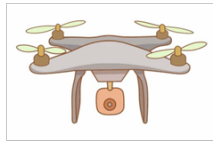
Gyroscope

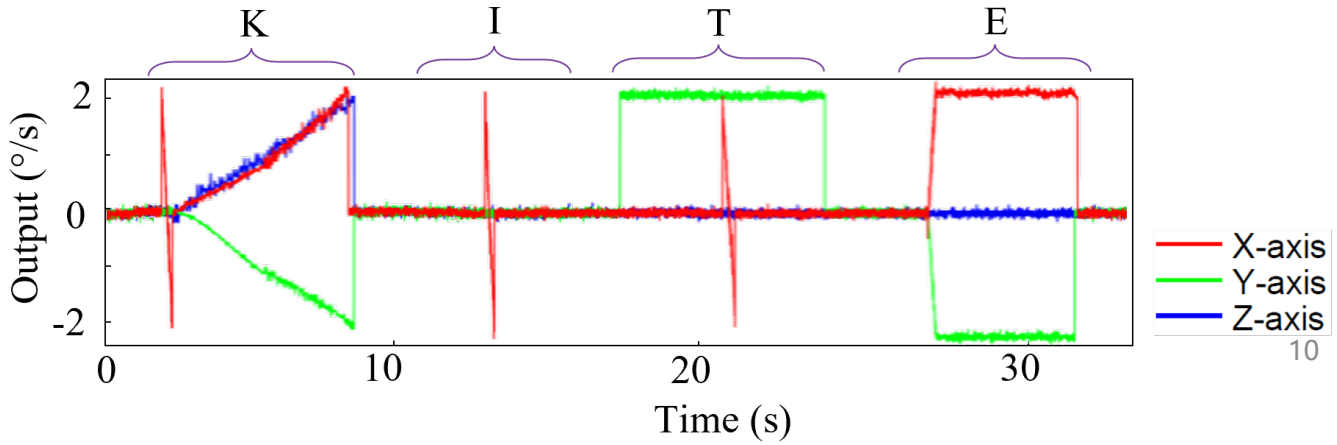






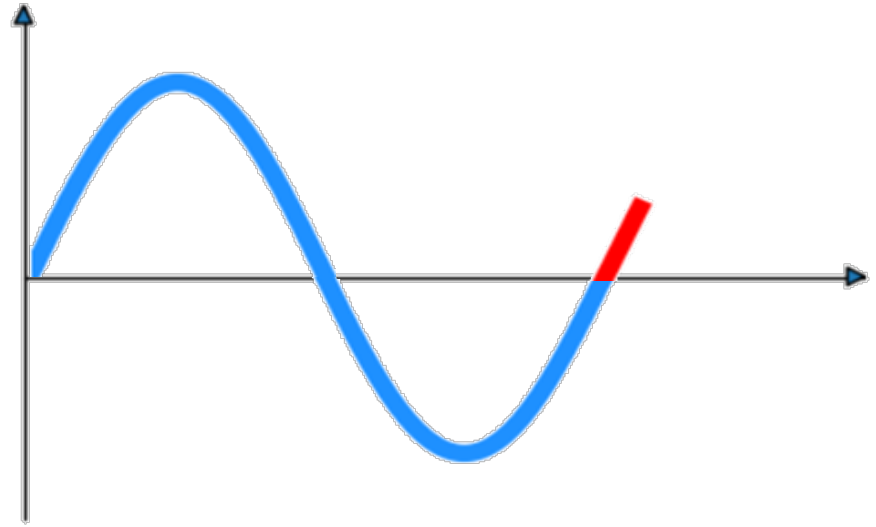
- Orientation control





3. How to eliminate the motion influence

- Phase fluctuation



original phase: 0 ➡ new phase: $\frac{\pi}{8}$

3. How to eliminate the motion influence

➢Coupling effect

$$x(t) = \frac{2mA_d\Omega}{\omega_n c^2}\cos(\omega_n t) - a_r F_x \cos(\omega_r t + \varphi_r) + 2ma_r^2 F_y \Omega \omega_r \cos(\omega_n t + \varphi_r)$$

Ture Motion

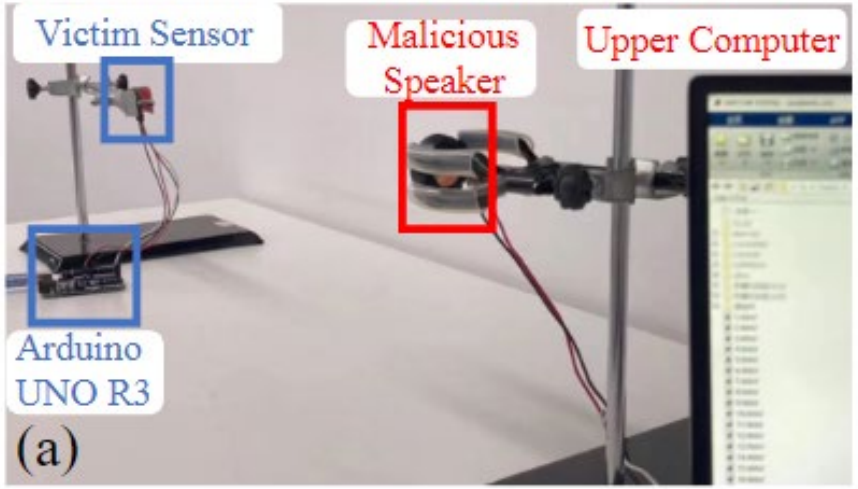
False Injection

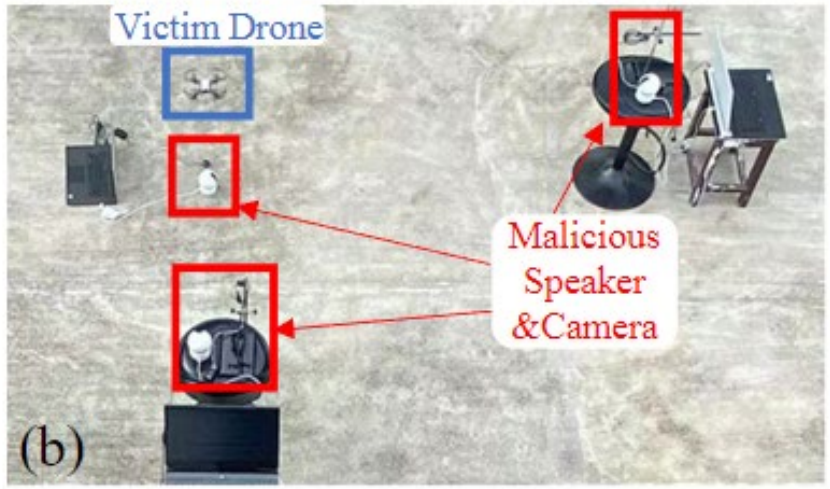
Noises caused by
The coupling effect

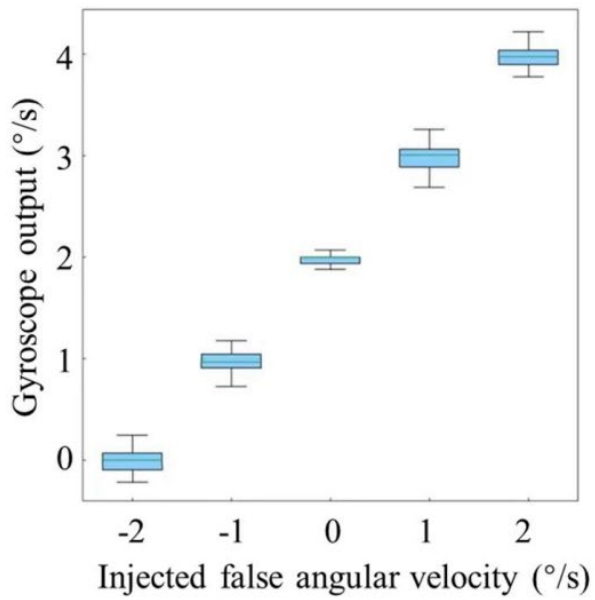
PZT

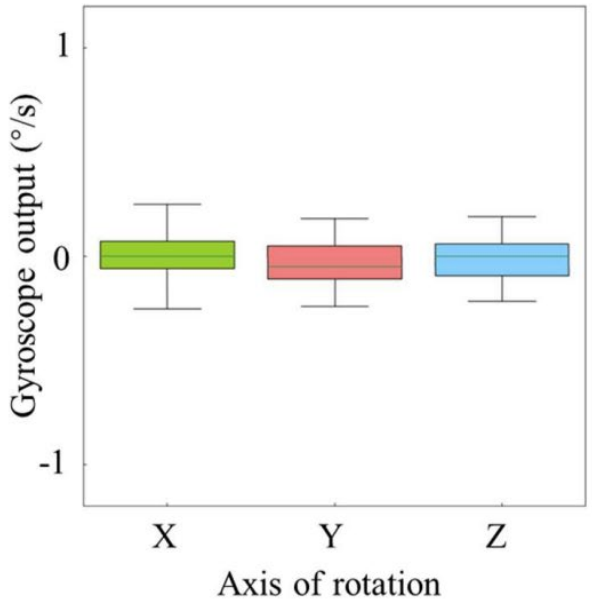
Drone

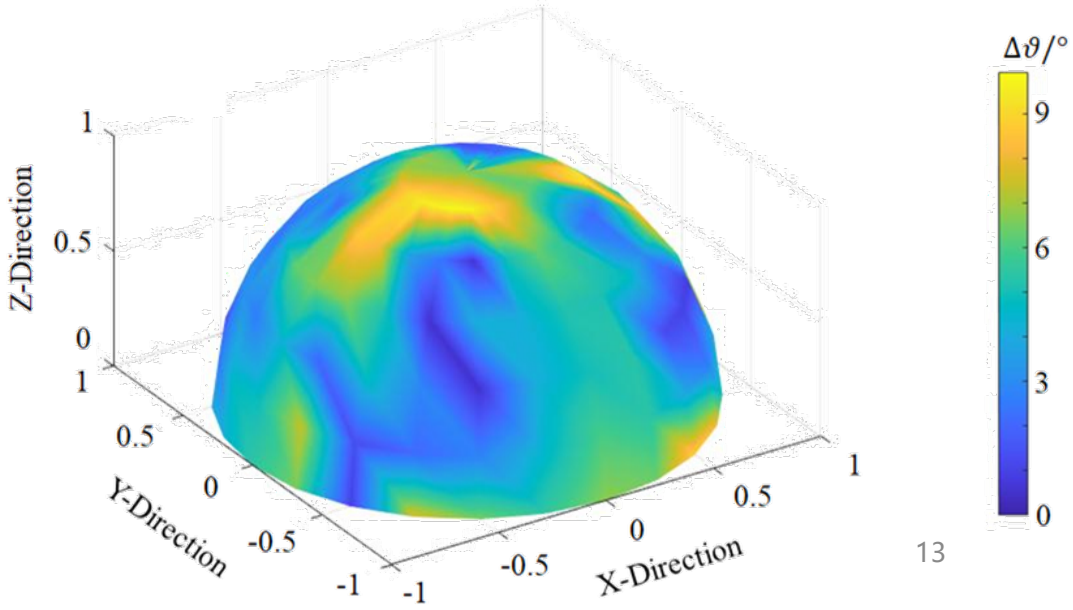
Evaluation


Victim Sensor
Malicious Speaker
Upper Computer
Arduino UNO R3
(a)


Victim Drone
Malicious Speaker &Camera
(b)

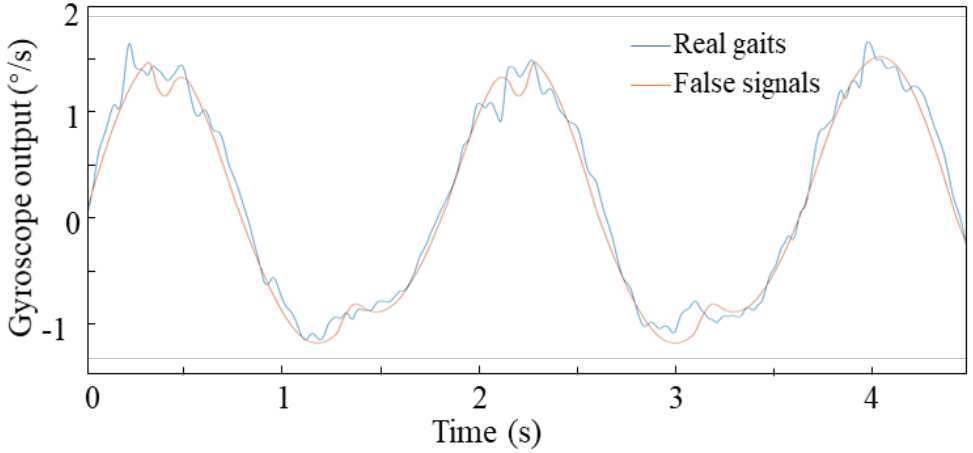

Gyroscope output (°/s)
Injected false angular velocity (°/s)


Gyroscope output (°/s)
X
Y
Z
Axis of rotation

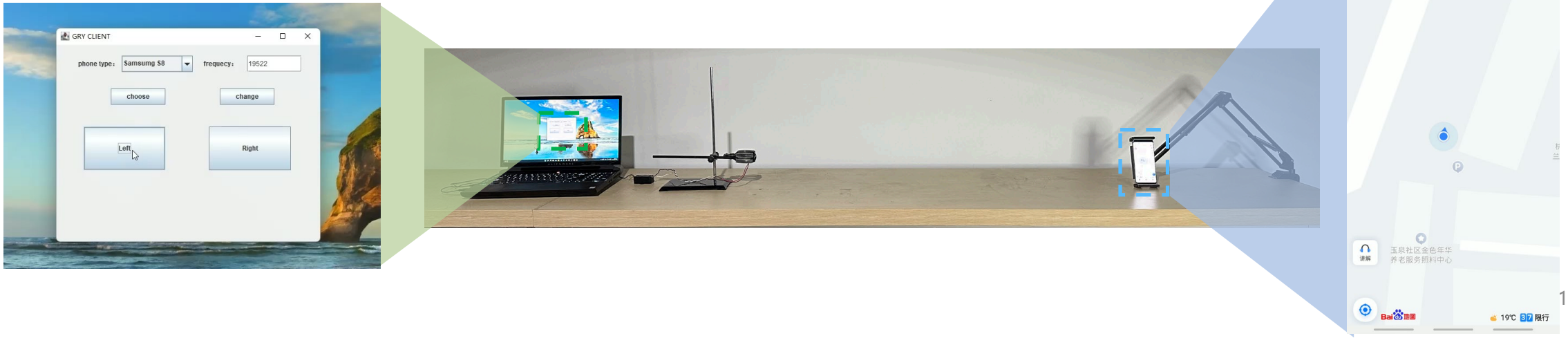

Z-Direction
Y-Direction
X-Direction
Δϑ/°

End-to-end Attack Cases: on smartphones

- Step count (pedometer)



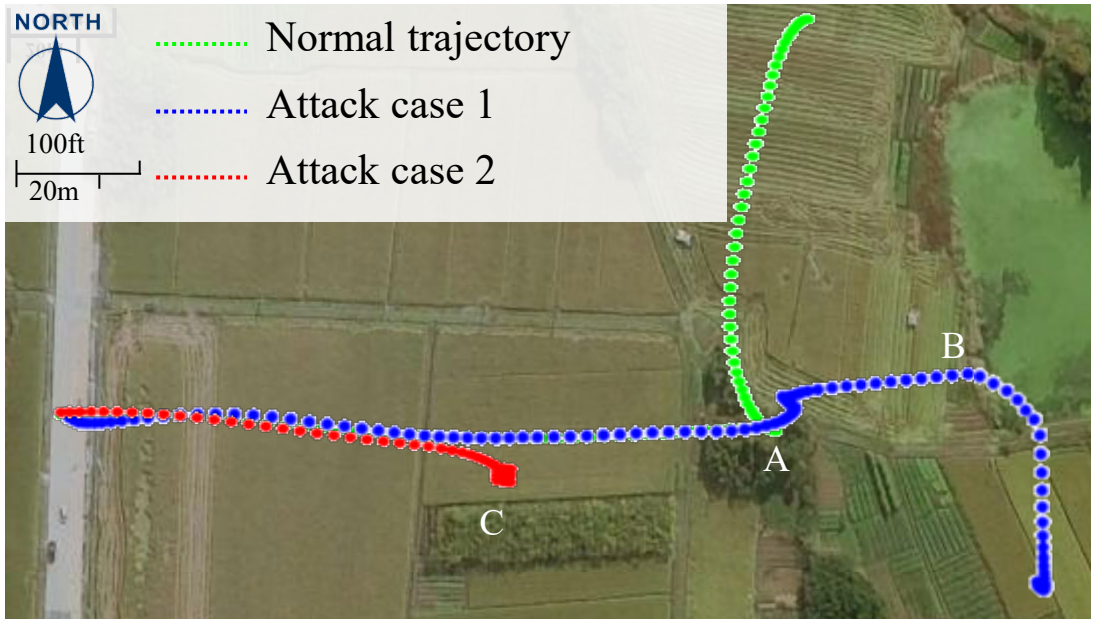
- Navigation service



End-to-end Attack Cases: on drone

➢ Target device

➢ Attack effect



Countermeasure

- Existing Approaches
  - Dampening and Isolation
  - Filtering
  - Common-mode difference 
  - Redundancy
- Our suggestion
  - We design a method that alters sampling rate and reduces its side effect of the accuracy loss.

$$SNR = -20log_{10}\left(\omega \times rms(t_a)\right)$$
$$t_a[i] = \alpha_m,\ (m = i\ mod\ C,\ i \in N)$$

Conclusion

- We propose a new acoustic modulation-based attacking method to exploit the practical potential threat of a realistic attacker covering most of possible attack scenarios.
- We expand the attack surface into MDOF systems and suppress the motion influence.
- We accomplish control over COTS in an automatic manner using the designed PCB proto-type.

Thanks for your listening!

Q&A