27TH USENIX SECURITY SYMPOSIUM

Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors

Yazhou Tu, Zhiqiang Lin †, Insup Lee ‡, Xiali Hei

University of Louisiana at Lafayette

†The Ohio State University

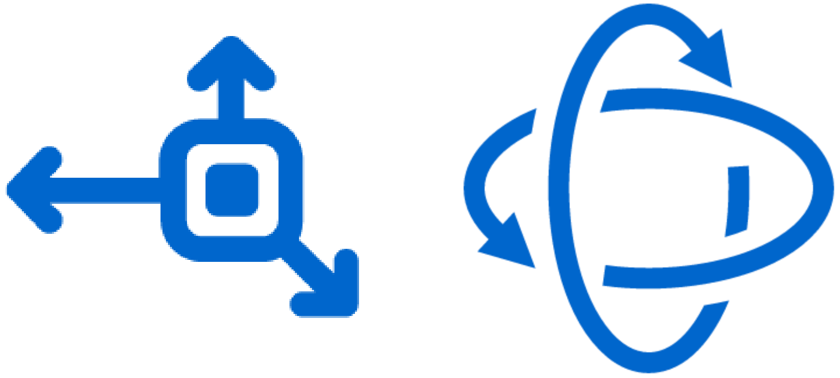
‡University of Pennsylvania

UNIVERSITY of LOUISIANA LAFAYETTE

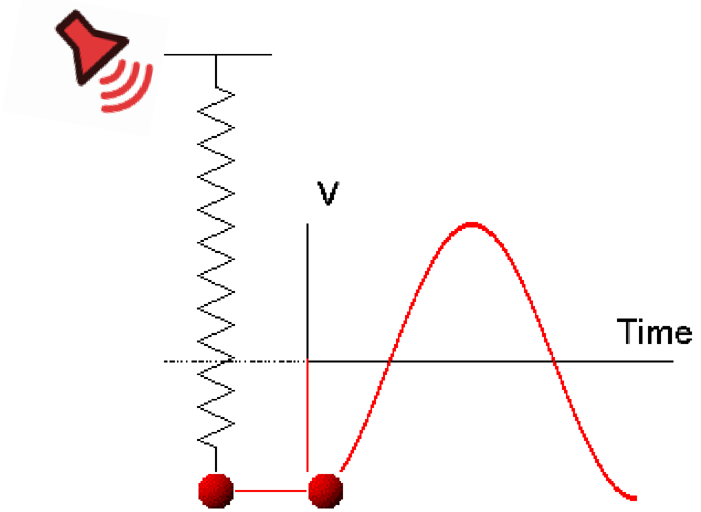
THE OHIO STATE UNIVERSITY

Penn UNIVERSITY of PENNSYLVANIA

MEMS Inertial Sensors



- Provide motion feedback
  - Accelerometer: Linear acceleration
  - Gyroscope: Angular velocity
- **Miniaturized** mechanical sensing structure
  - Similar to mass-spring
  - Transduce inertial stimuli to electrical signals
  - Vulnerable to ***acoustic resonance***

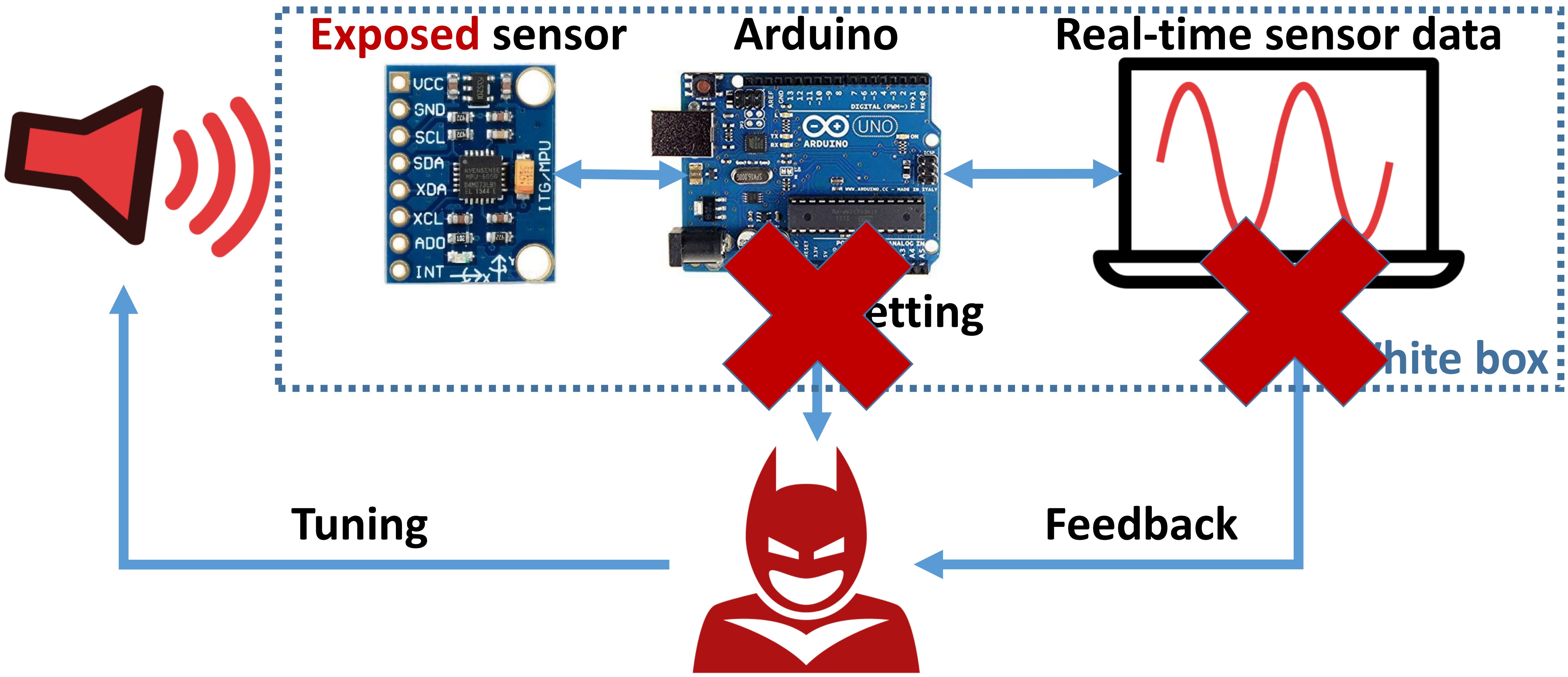


Acoustic Attacks on MEMS Inertial Sensors

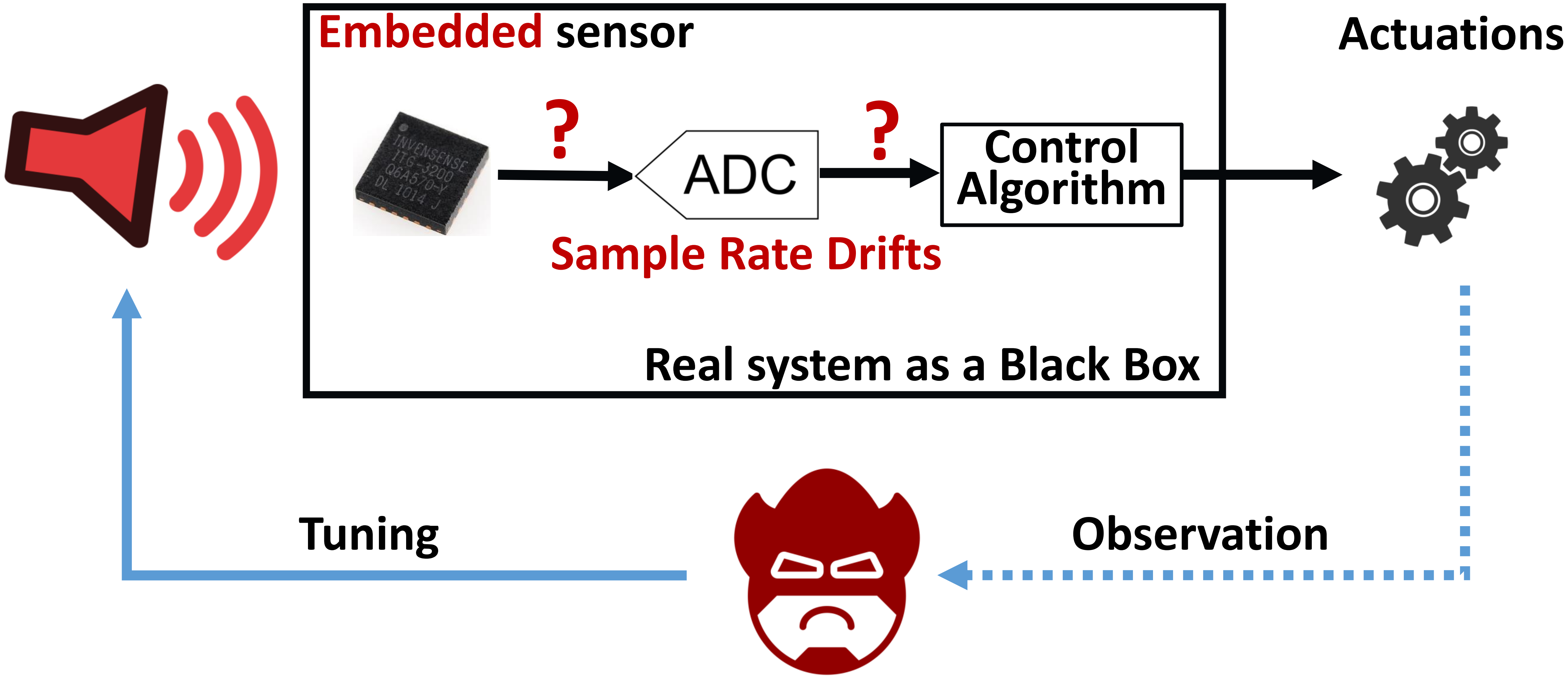
- Son et al. "**Rocking drones**" [USENIX Sec'15] [1]
  - **DoS** attack on gyroscopes

- Trippel et al. "**WALNUT**" [Euro S&P'17] [2]
  - Control **exposed** accelerometers connected to Arduino (**white box**)
  - Sample rate drifts
    - *"This limits an attacker's ability to achieve control over a sensor's output for more than 1–2 seconds*[2]*"*

White-box approach



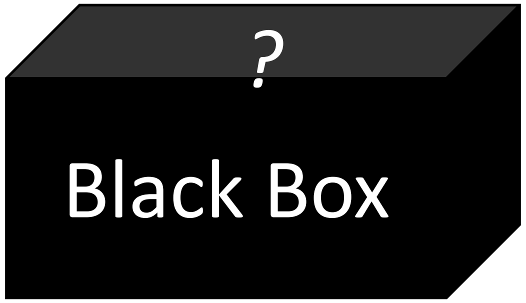
Motivation: A Real System is often a Black Box



Problem

How to ***non-invasively*** control output of ***embedded*** inertial sensors despite the sample rate drifts?

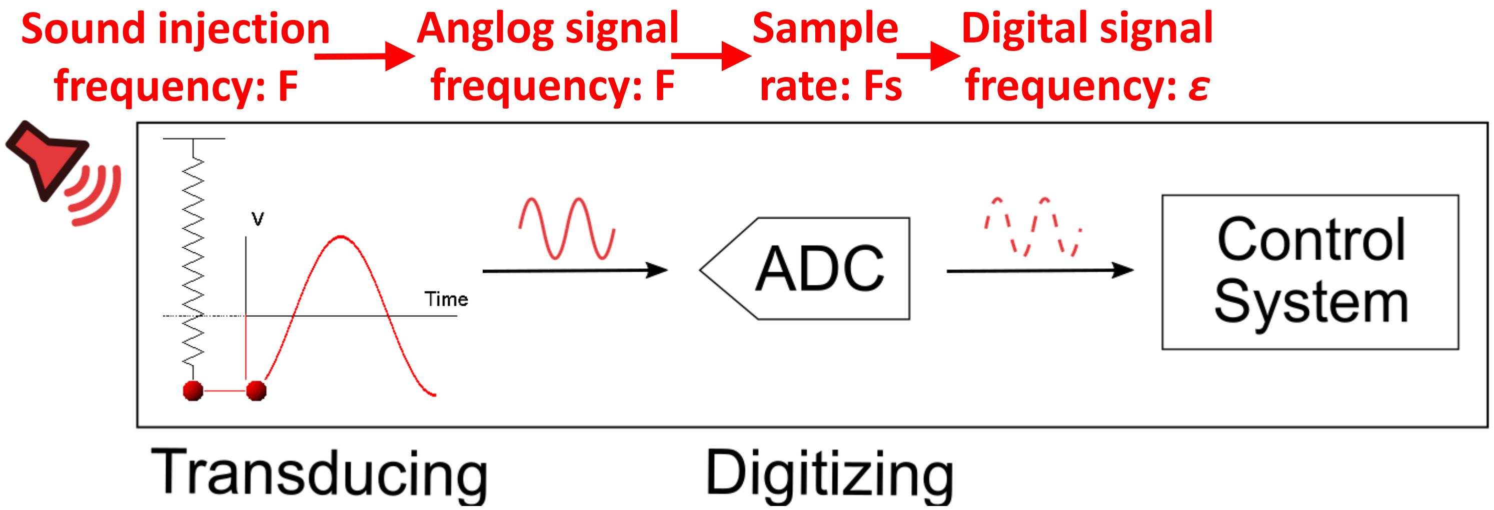
(***Black box*** approach)



Contributions

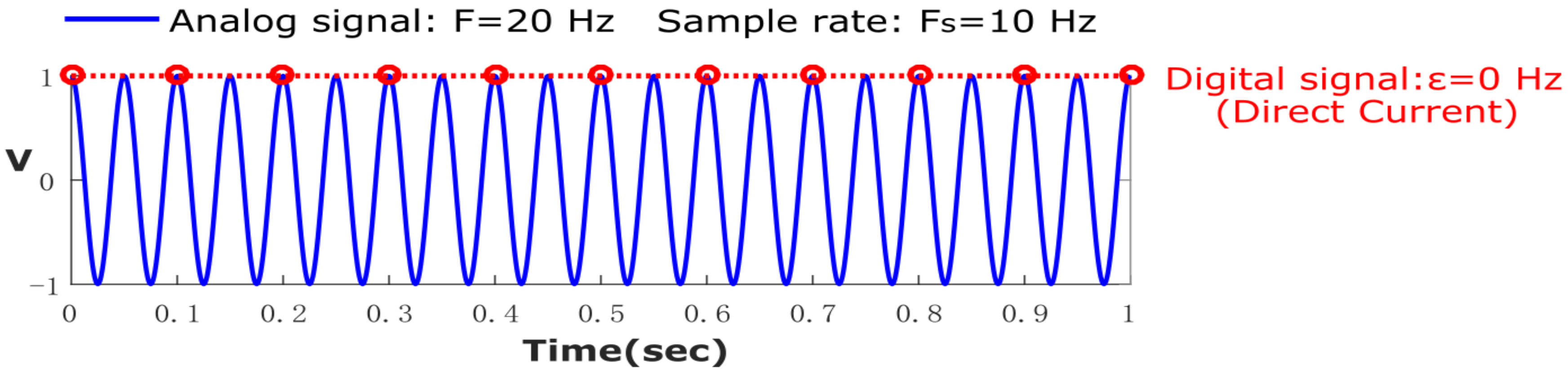
- **Theoretical results:**
  - Sample rate drifts amplification theorem
  - Two new methods: *Digital amplitude adjusting* and *Phase Pacing*
- ***Non-invasive*** attacks on sensors ***embedded in real systems***
  - *Side-Swing* and *Switching* attacks
  - Evaluated on 25 devices
  - Demonstrate implicit control over different kinds of systems
- ***Automatic*** attacks with feedback
- Attacks using ***non-resonant*** frequencies

Acoustic Injection

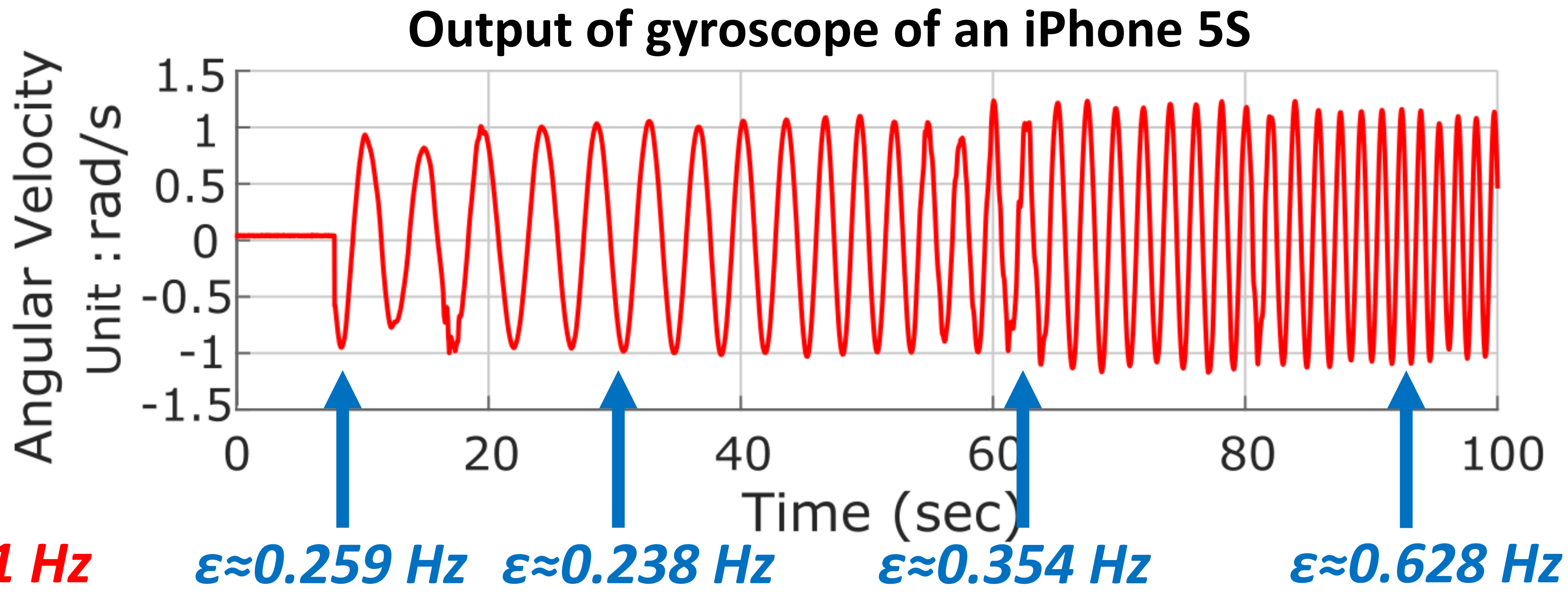


- ***Undersampling*** (*F > Fs/2*)
  - ***Aliasing***
  - When *F = nFs*, we have *ε = 0* (**Direct Current**, DC)

$$F = n \cdot F_S + \epsilon \quad \left(-\frac{1}{2}F_S < \epsilon \le \frac{1}{2}F_S, n \in \mathbb{Z}^+\right) \quad (3)$$



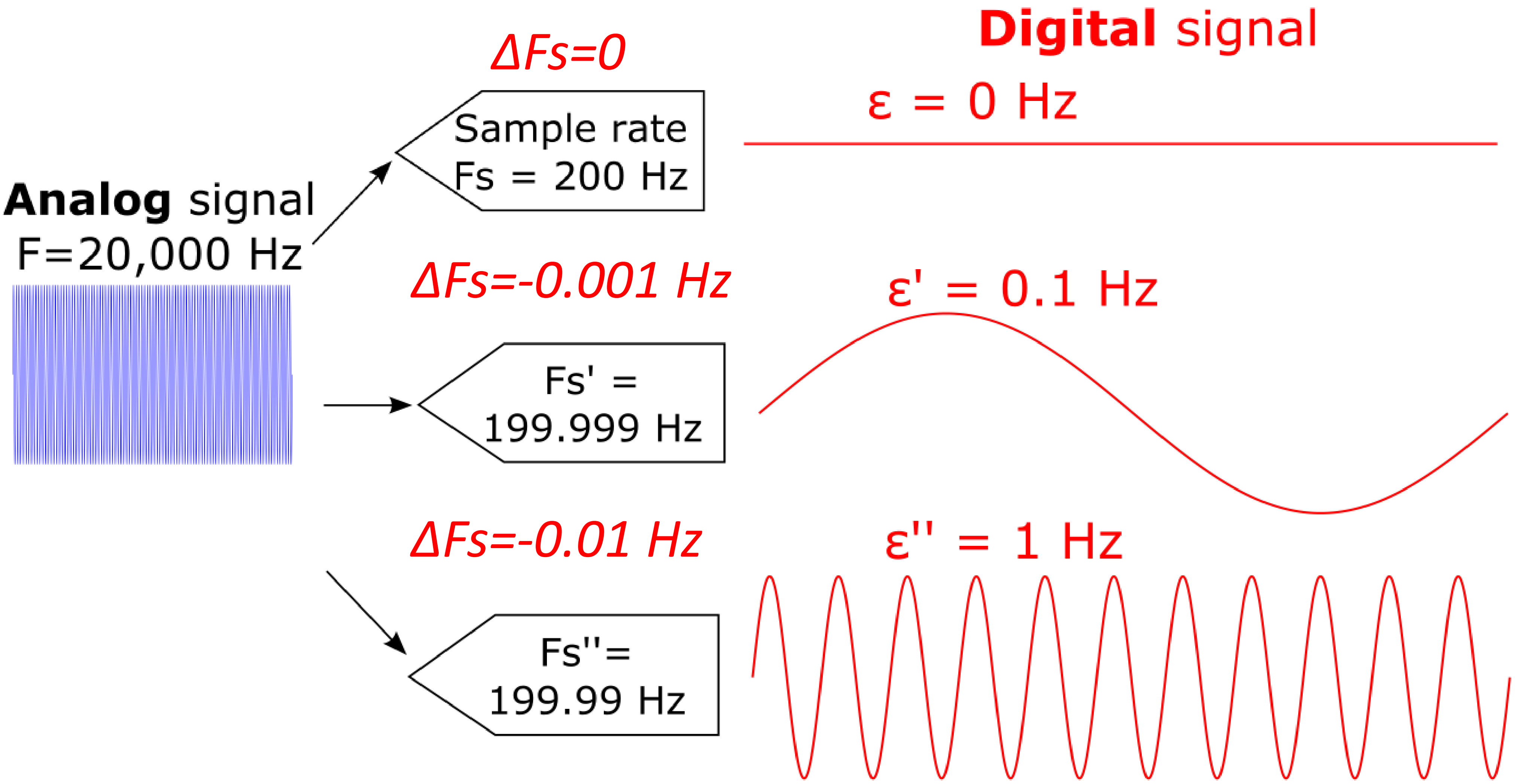
Amplification Effects of Sample Rate Drifts



$$F = n \cdot F_S + \varepsilon \quad \left(-\frac{1}{2}F_S < \varepsilon \leq \frac{1}{2}F_S, n \in \mathbb{Z}^+\right) \qquad (3)$$

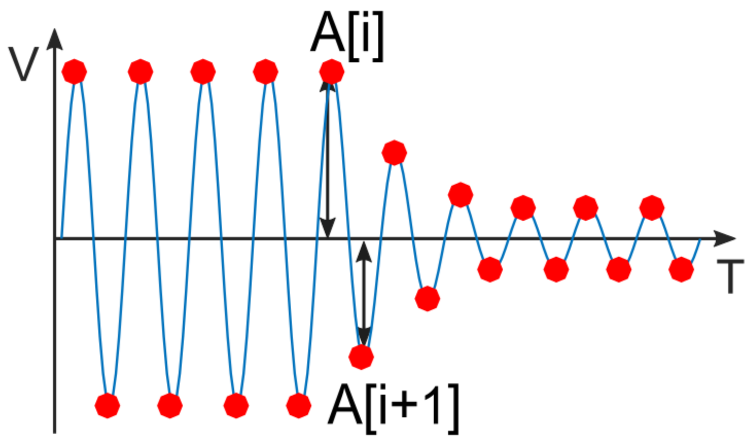
- F remains the same, but ε is deviating
- Cause: ***Fs is drifting***

Sample Rate Drifts Amplification Theorem



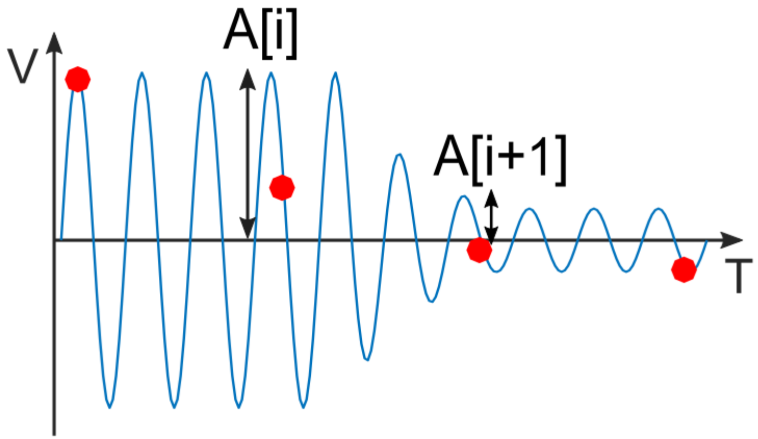
Digital Amplitude Adjusting

Sampled Correctly



A[i] and A[i+1] are correlated

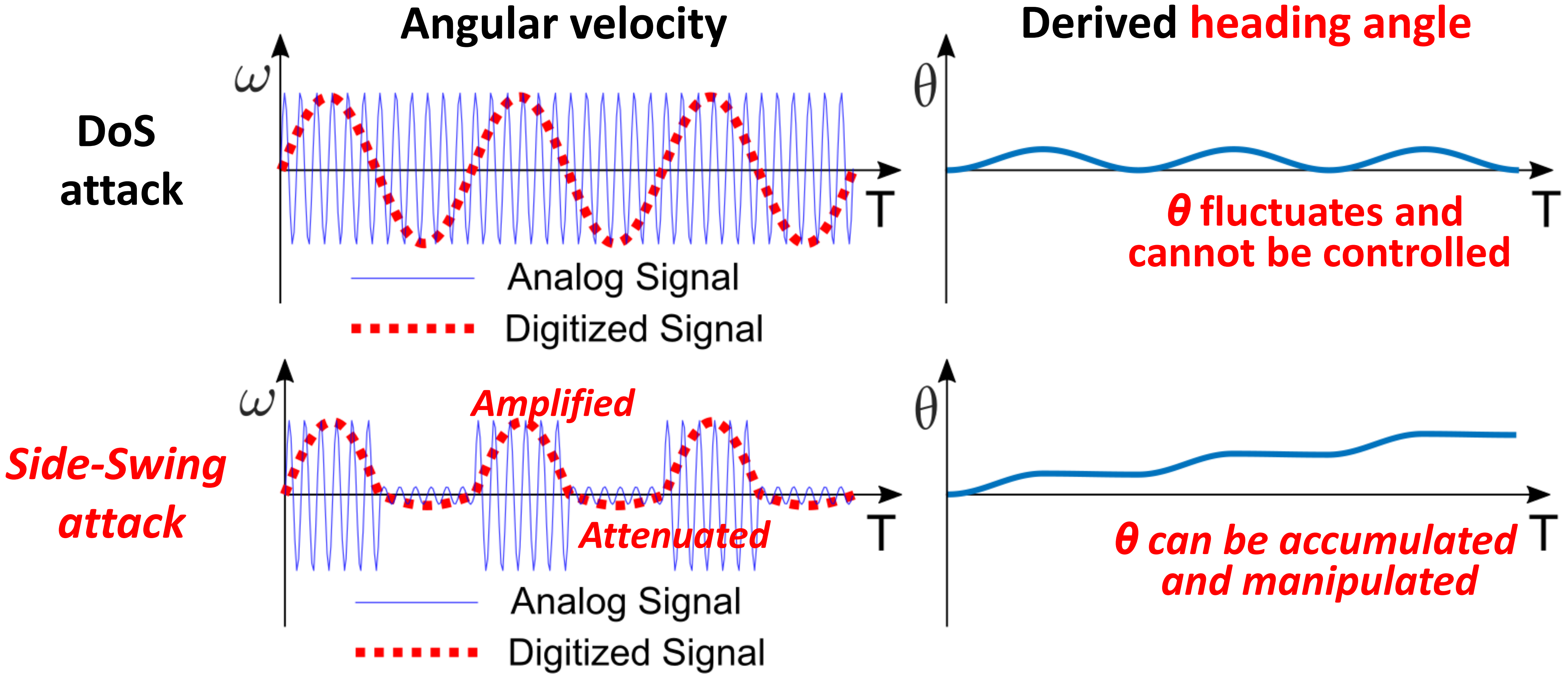
Undersampled



A[i] and A[i+1] are independent

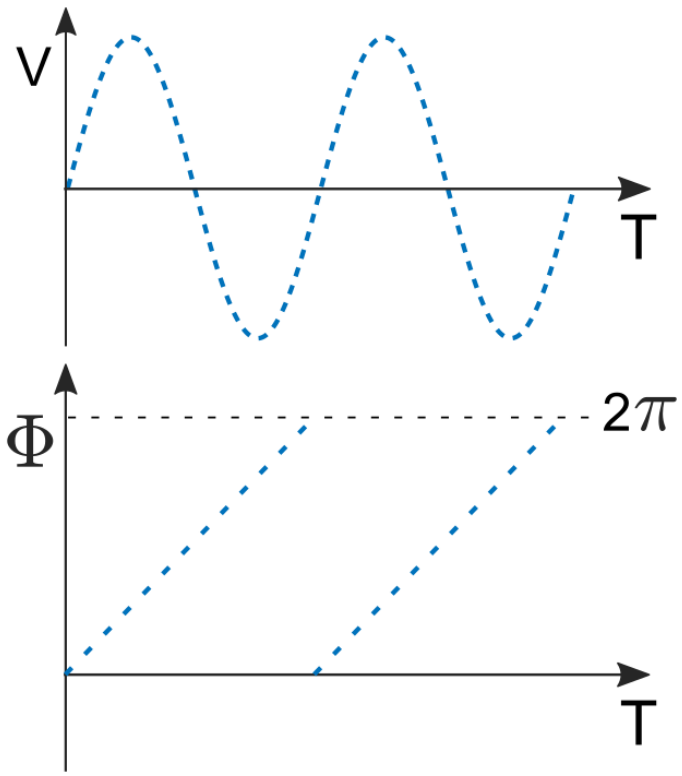
- **Undersampling** causes signal distortions
- Fabricate specific waveforms instead of oscillating sine wave

Side-Swing Attacks

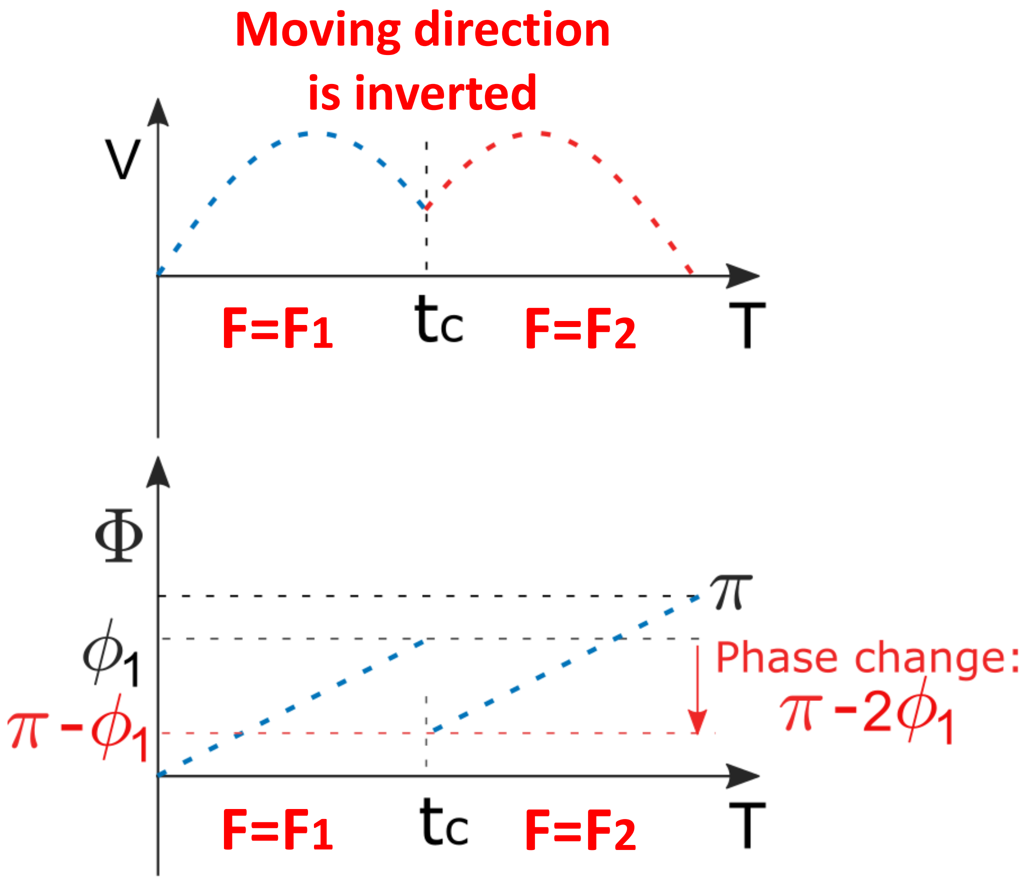


- Increase *A[i]* to amplify the induced output in the target direction
- Decrease *A[i]* to attenuate the output in the opposite direction

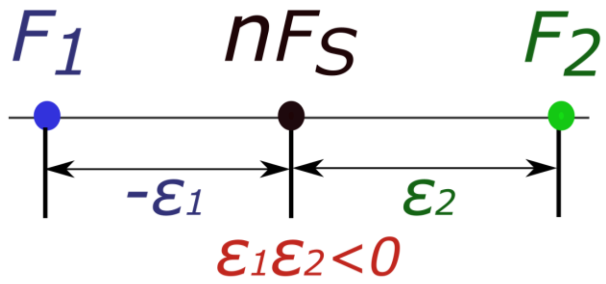
Phase Pacing



Without Phase Pacing



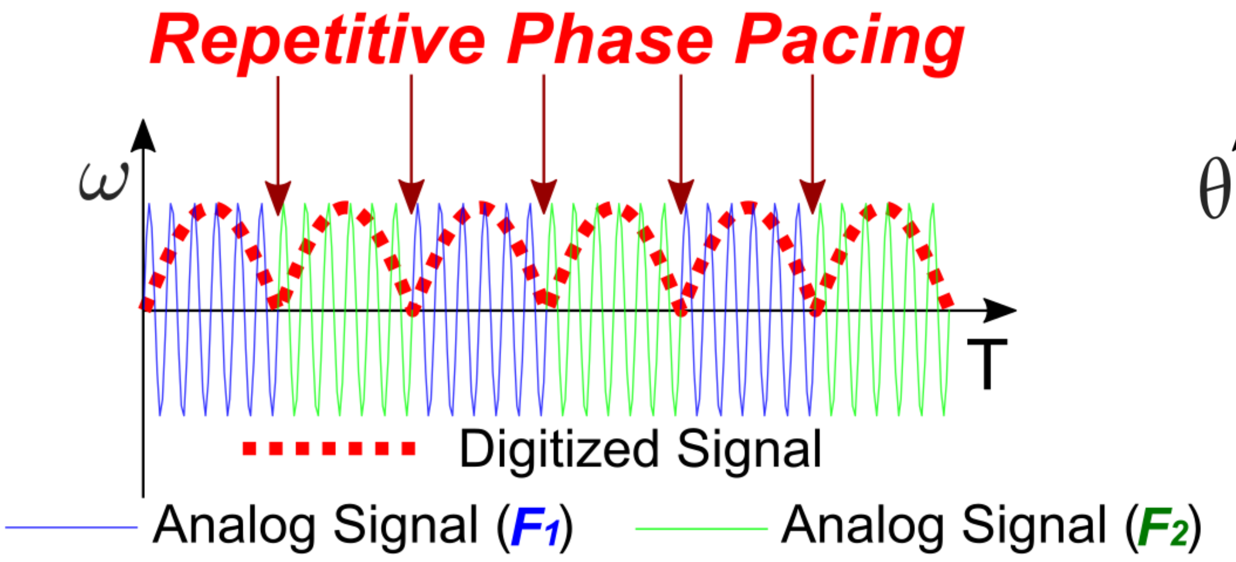
With Phase Pacing



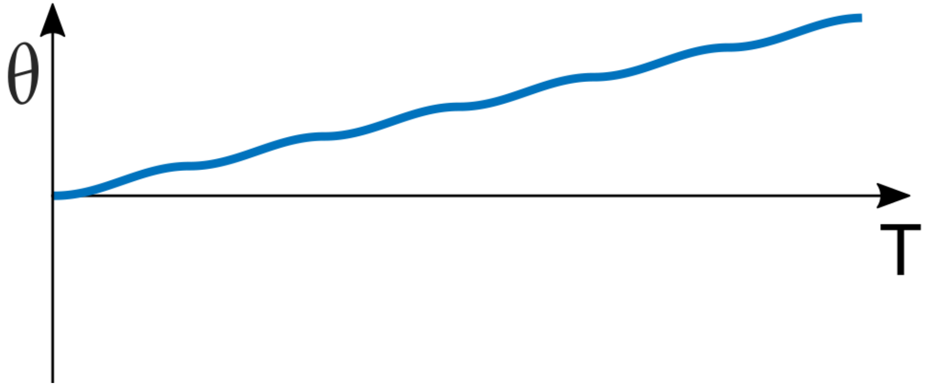
Condition of Phase Pacing

Ex: $nF_S = 20000, F_1 = 19999Hz, F_2 = 20001Hz$

Switching Attacks



Angular velocity



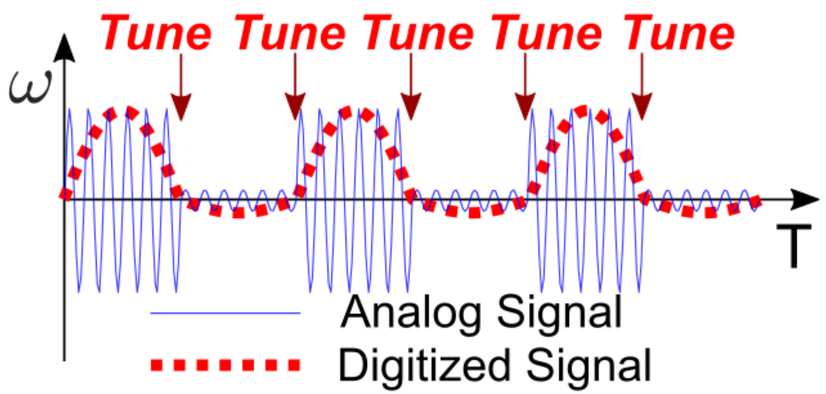
Derived heading angle

- **Repetitive *Phase Pacing***
  - Switch *F* between *F1* and *F2* back and forth

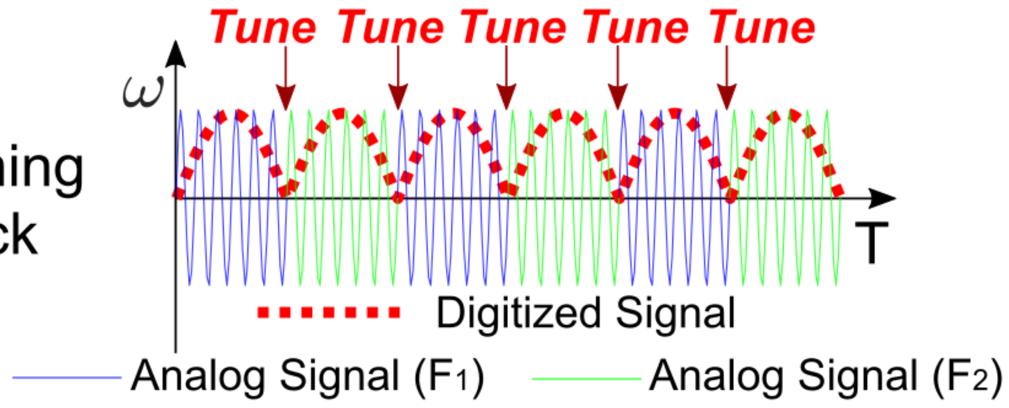
Challenges in the Black-box Approach

- Problem: Tuning time selection

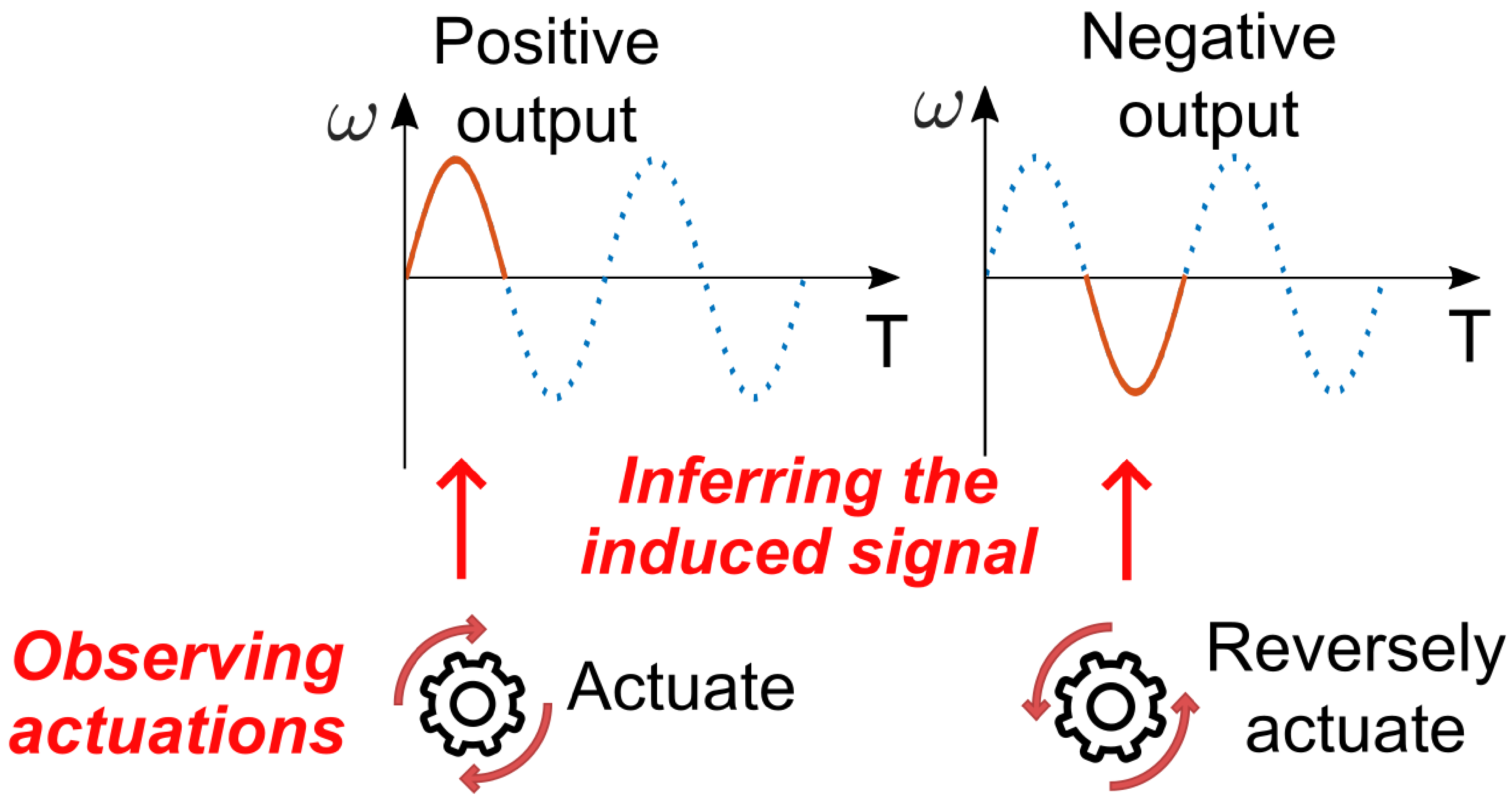
Side-Swing attack



Switching attack

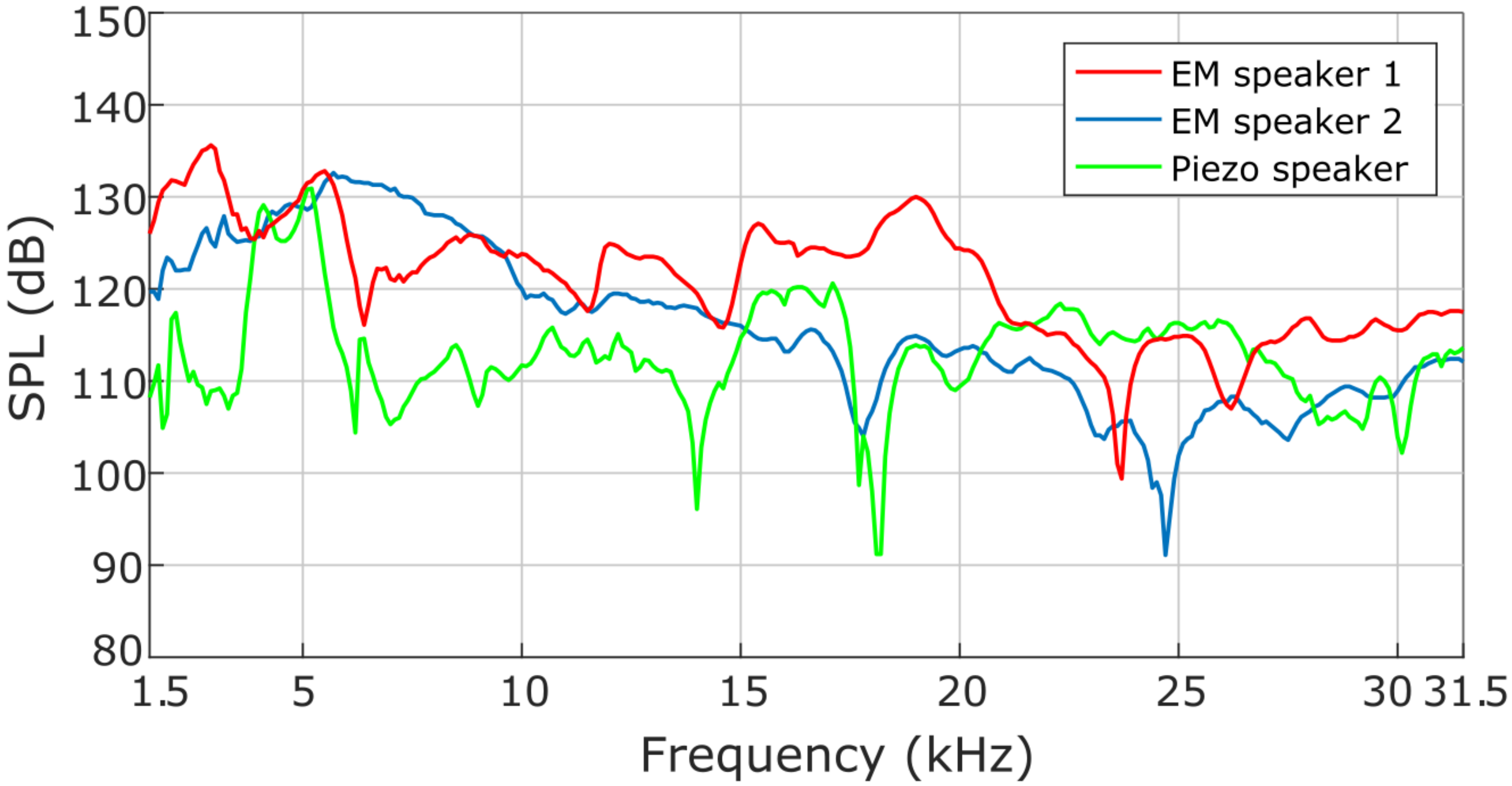


Reverse Signal Mapping



Experimental Setup

- **Sound source**
  - Sound Pressure Level
    - ***120 – 130 dB (<21 kHz)***
    - ***110 – 120 dB (>21 kHz)***
  - **50-Watt** audio amplifier
  - Function generator
  - Directivity horn



Closed-loop Control Systems

Table 1: Results of our attack experiments on closed-loop control systems

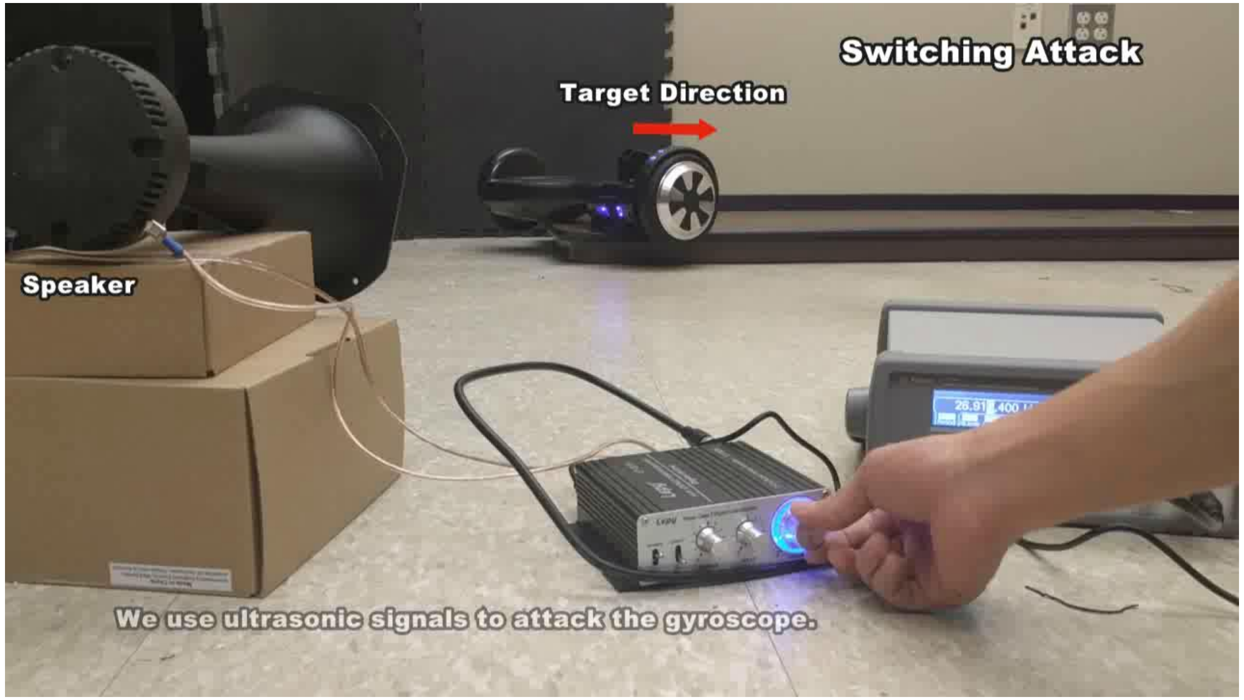
Device	Sensor		Resonant Freq. (kHz)	Affected/ Func. Axes	Max Dist. (m)	Control Level
	Type	Model†				
Megawheels scooter	Gyro	IS MPU-6050A	27.1~27.2	y/y	2.9	Implicit control
Veeko 102 scooter	Gyro	Unknown	26.0~27.2	x/x	2.5	Implicit control
Segway One S1	Gyro	Unknown	20.0~20.9	x/x	0.8	Implicit control
Segway Minilite	Gyro	Unknown	19.2~20.0	x/x	0.3	DoS
Mitu robot	Gyro	N/A SH731	19.0~20.7	x/x	7.8	Implicit Control
MiP robot	Acce	Unknown	5.2~5.4	x/x	1.2	DoS
DJI Osmo stabilizer	Gyro	IS MP65	20.0~20.3	x,y,z/x,y,z	1.2	Implicit control
WenPod SP1 stabilizer	Gyro	IS MPU-6050	26.0~26.9	z/y,z	1.8	Implicit control
Gyenno steady spoon	Gyro	Unknown	Not found	Unknown	N/A	Not affected
Liftware level handle	Acce	IS MPU-6050	5.1	x/x	0.1	DoS

† IS: InvenSense, N/A: Unknown manufacturer.

Closed-loop Control Systems

- **Self-balancing Transporter**
  - Side-Swing: https://youtu.be/Y1LLiyhCn9I
  - Switching: https://youtu.be/D-etuH04pms
- **Robot**
  - Side-Swing: https://youtu.be/oy3B1X41u5s
  - DoS: https://youtu.be/yDz8y_ht3Xg
- **Stabilizer**
  - Side-Swing: https://youtu.be/FDxaLUtgaCM
  - Switching: https://youtu.be/JcA_WXHrUEs
- **Anti-tremor device**
  - DoS: https://youtu.be/qNLzBMOKbnk

Switching attacks on a self-balancing transporter



Open-loop Control Systems

Table 2: Results of our attack experiments on open-loop control systems

Device	Sensor		Resonant Freq. (kHz)	Affected/ Func. Axes	Max Dist. (m)	Control Level
	Type	Model†				
IOGear 3D mouse	Gyro	IS M681	26.6~27.6	x,z/x,z	2.5	Implicit control
Ybee 3D mouse	Gyro	Unknown	27.1~27.3	x/x,z	1.1	Implicit control
ES120 screwdriver	Gyro	ST L3G4200D	19.8~20.0	y/y	2.6	Implicit control
B&D screwdriver	Gyro	IS ISZ650	30.3~30.6	z/z	0	Limited control
Dewalt screwdriver	Gyro	Unknown	Not found	none/y	N/A	Not affected
Oculus Rift	Gyro	BS BMI055	24.3~25.6	x/x,y,z	2.4	Implicit control
Oculus Touch	Gyro	IS MP651	27.1~27.4	x/x,y,z	1.6	Implicit control
Microsoft Hololens	Gyro	Unknown	27.0~27.4	x/x,y,z	0	Limited control
iPhone 5	Gyro	ST L3G4200D	19.9~20.1	x,y,z/x,y,z	5.8	Implicit control
iPhone 5S	Gyro	ST B329	19.4~19.6	x,y,z/x,y,z	5.6	Implicit control
iPhone 6S	Gyro	IS MP67B	27.2~27.6	x,y,z/x,y,z	0.8	Implicit control
iPhone 7	Gyro	IS 773C	27.1~27.6	x,y,z/x,y,z	2.0	Implicit control
Huawei Honor V8	Gyro	ST LSM6DS3	20.2~20.4	x,y,z/x,y,z	7.7	Implicit control
Google Pixel	Gyro	BS BMI160	23.1~23.3	x,y,z/x,y,z	0.4	Implicit control
Pro32 soldering iron	Acce	NX MMA8652FC	6.2~6.5	Unknown	1.1	DoS

† IS: InvenSense, ST:STMicroelectronics, BS: Bosch, NX: NXP Semiconductors.

Open-loop Control Systems

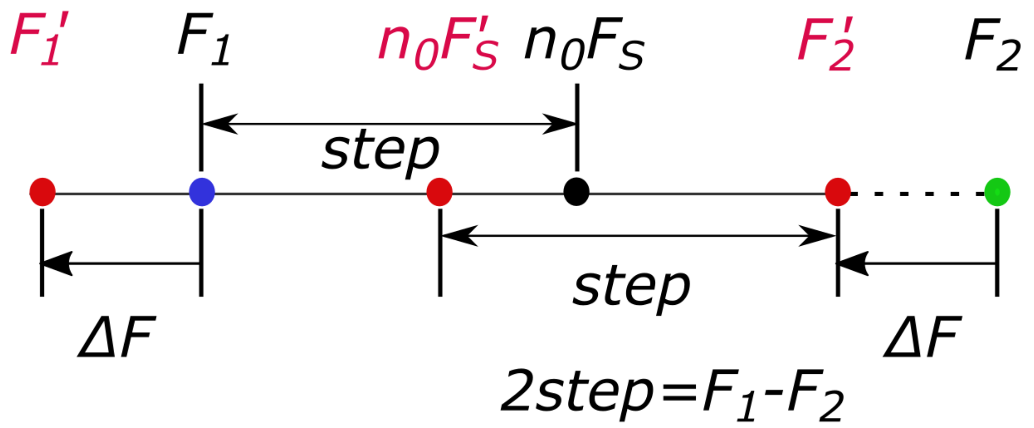
- **3D mouse**
  - Side-Swing: https://youtu.be/YoYpNeIJh5U
  - Switching: https://youtu.be/iWXTJ6We0UY
- **VR/AR device**
  - Side-Swing: https://youtu.be/KciiDeFdK9c
  - Switching: https://youtu.be/Jf9xHAW1PJY
  - Switching: https://youtu.be/MtXxcSzWcQA
- **Smartphone**
  - Side-Swing: https://youtu.be/t9rNJsDdGPg
  - Side-Swing: https://youtu.be/Wl6c_zBGlpU
  - Switching: https://youtu.be/psuOhyUvDQk
  - Switching: https://youtu.be/P4nLuTQZJ80
- **Motion-aware device (soldering iron)**
  - DoS: https://youtu.be/itgmOl21zoc

Conservative Side-Swing attacks on a screwdriver

- **Gyroscopic screwdriver**
  - Conservative Side-Swing: https://youtu.be/SCAYbyMIJAc

Automatic Switching Attack with Feedback

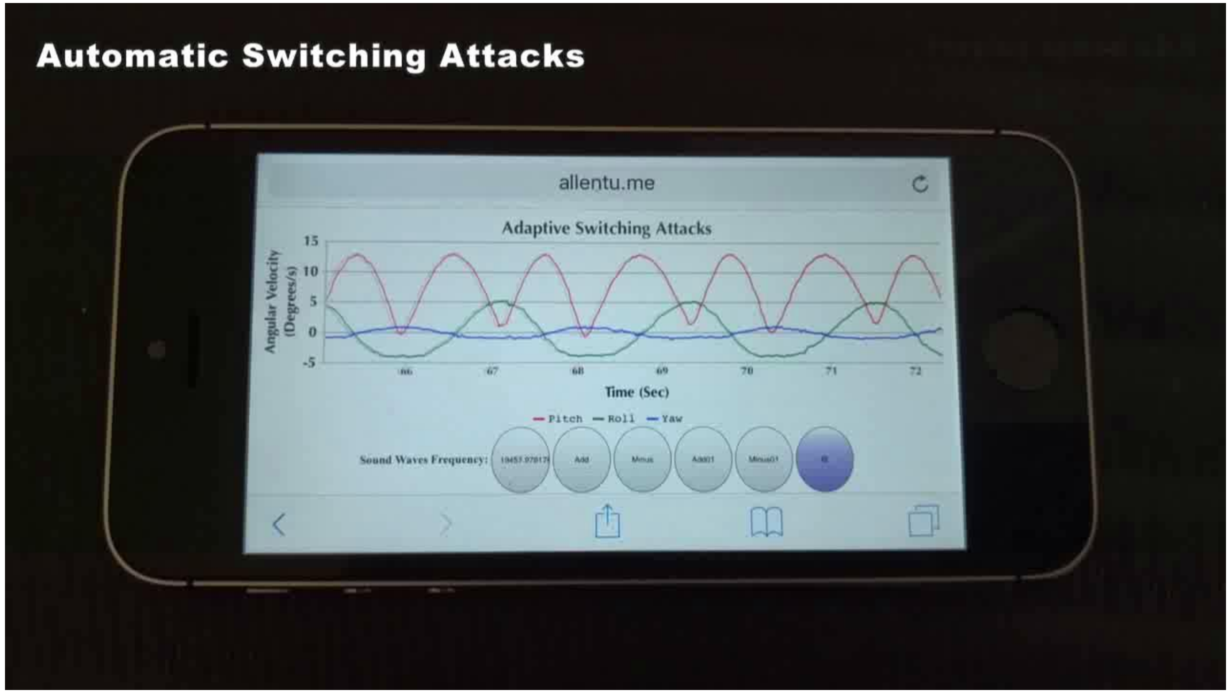
- Motivation:
  - Hand tuning is slow
  - Devices provide inertial sensor feedback
- Program modulates acoustic signals
  - More effective
  - Active adaptation



Adaptation Process

Implementations of Automatic Attacks

- Proof-of-concept implementations
  - **Android (Google Maps)**
    - https://youtu.be/dy6gm9ZLKuY
  - **IOS (VR game)**
    - https://youtu.be/kTQFi9CI8R8
  - **Web scripts (sample rate < 20 Hz)**
    - https://youtu.be/MkpW_j6gd8k
    - https://youtu.be/7yOSFTeF1so
    - **Resonant frequency scanner** https://youtu.be/vUDSvsfnJjg
  - **A moving phone**
    - https://youtu.be/1J1Q1jSzOD4
  - **Built-in speaker frequency < 24 kHz**

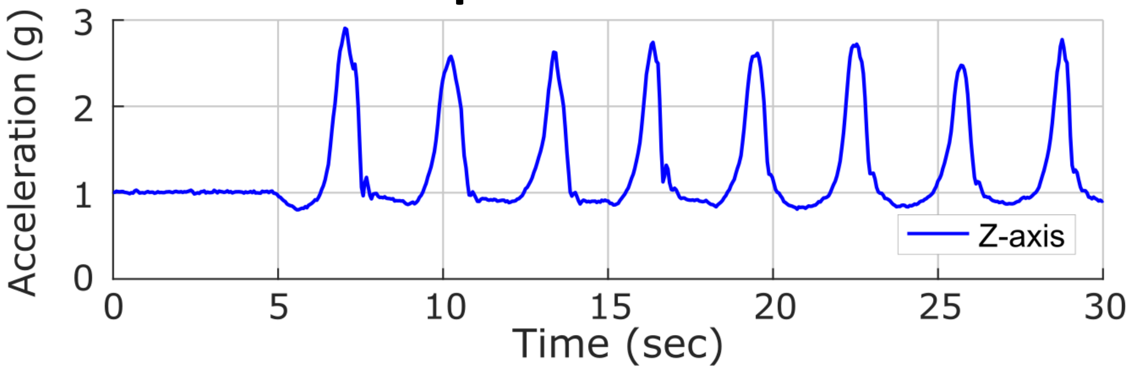


Rotating the orientation of Google Maps

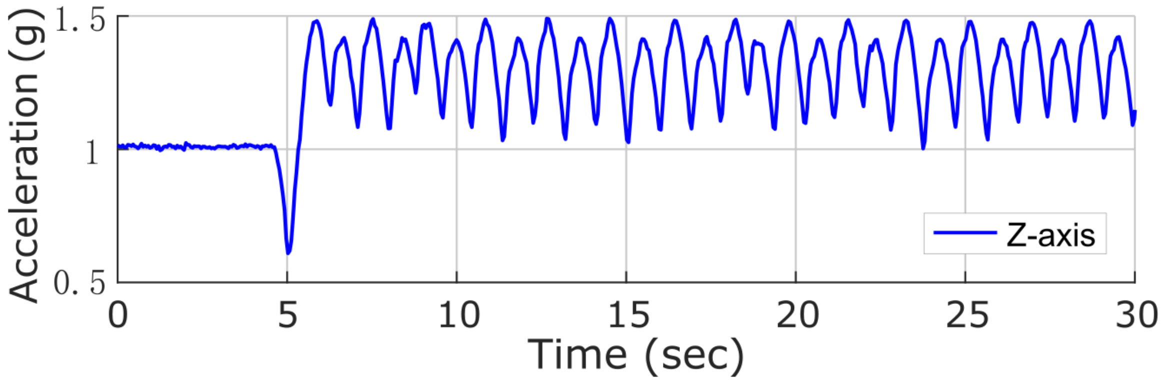
Shooting germs in VR games

Generalization: Using Non-resonant Frequencies

Accelerometer output:



Side-Swing attack (F=19.6 Hz)

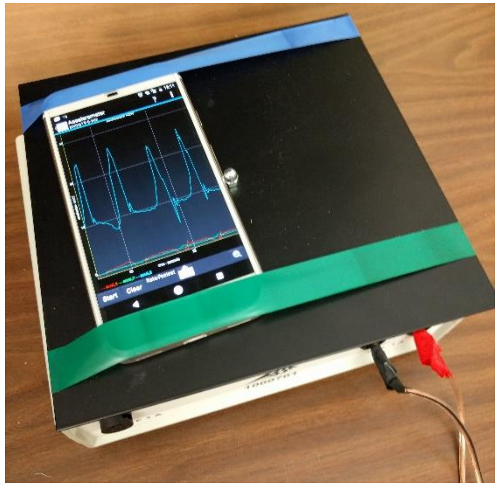


Switching attack (F1=19.4 Hz, F2=20.4 Hz)

- **Google Pixel smartphone on a vibration platform**
  - ***Vibration signals* with low frequency**
  - Sample rate of the ADC *Fs≈19.9*
- Accelerometer data shows:
  - **Launching to the sky**
  - **Accumulate a speed of over *70 m/s***

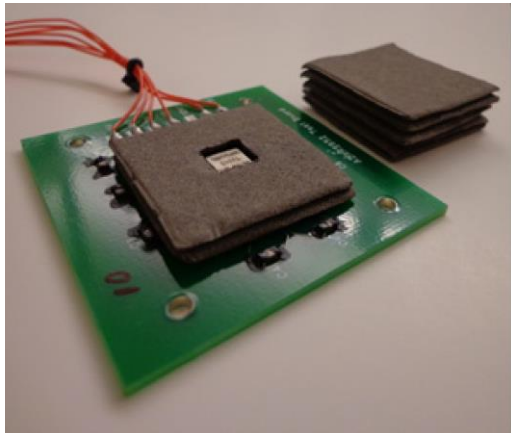
Sensor data shows

In reality

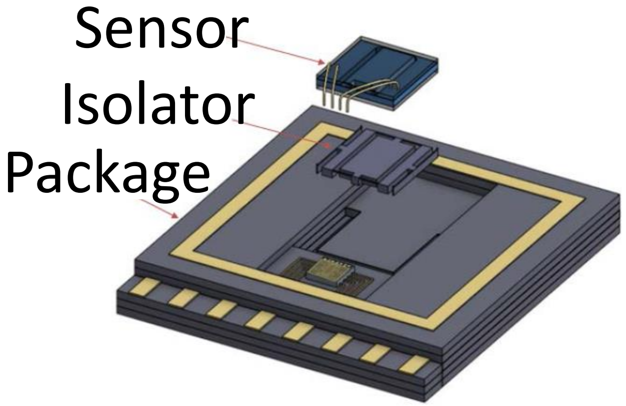


Possible Mitigation Methods

- Damping and isolation
  - Acoustic damping material
  - Isolating
  - Design suggestion
- Filtering and sampling
  - Low-pass filter [2]
  - Randomized and 180° out-of-phase sampling [2]
  - Dynamic sample rate *Fs*
- Redundancy-based approaches



Microfibrous cloth[3]



Micro-isolator[4]

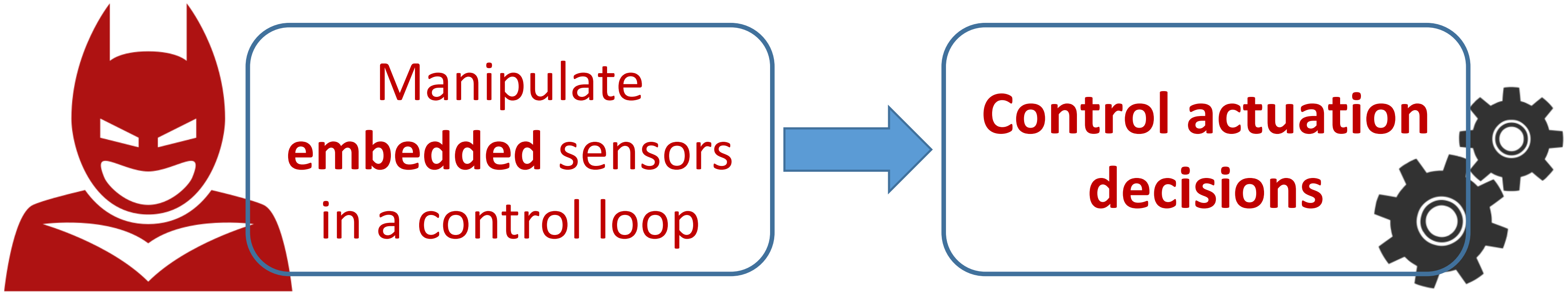
Discussion

- **Attack experiment with a drone**
- **Sound source**
  - Professional acoustic devices
  - Speaker/Transducer arrays
    - *N* coherent sound sources (Ex: *N=8*)
    - Possible sound level increase: *20log10(N) = 18 dB*

Trying to make the drone tilt to the left twice and then to the right twice (Side-Swing)

Conclusion

- We explored non-invasive attacks on embedded inertial sensors (***black-box*** approach)
- In attacks on real devices, realistic factors need be considered
  - In undersampling, sample rate drifts can be amplified
- Possible to implicitly control different kinds of systems by acoustic injections on inertial sensors



References

[1] Son et al. "Rocking drones with intentional sound noise on gyroscopic sensors." *In Proc. of USENIX Security symposium,* 2015.

[2] Trippel et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." In Proc. Of *IEEE European Symposium on Security and Privacy*, 2017.

[3] Soobramaney et al. "Mitigation of the Effects of High Levels of High-Frequency Noise on MEMS Gyroscopes Using Microfibrous Cloth." In *ASME 2015 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, 2015.

[4] Kranz et al. "Environmentally Isolating Packaging for MEMS Sensors." In *International Symposium on Microelectronics*, 2017. International Microelectronics Assembly and Packaging Society.

Questions & Comments

Thank You !

- Email: yazhou.tu1@louisiana.edu

- Attack demos are available in our YouTube Channel!

https://www.youtube.com/channel/UCGMX3ZbElV7BZYIX7RtF5tg

- Our earlier demos can be found at:

https://www.youtube.com/channel/UCeV47TrMGvnrcXgZesJYHtA