EECS 598-13

WALNUT: Waging Doubt on Integrity of MEMS Accelerometers with Acoustic Injection Attacks

By Timothy Trippel, Ofir Weisse, Wenyuan Xu*, Peter Honeyman, Kevin Fu

Summary Presentation By: Devesha Tewari, Leonard Blado, Saylee Chandavarkar

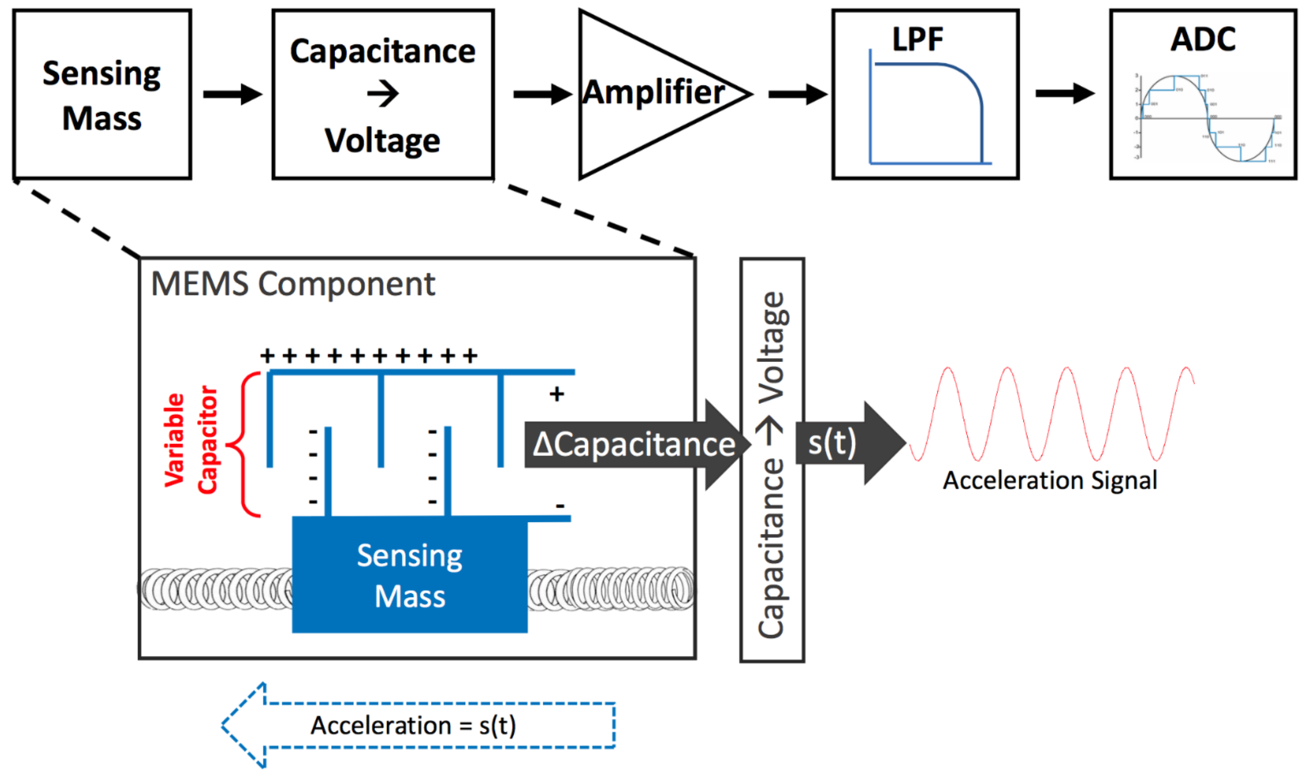
UNIVERSITY OF MICHIGAN

Agenda

1. Modelling the malicious interference on MEMS accelerometers
2. Acoustic injection attacks on MEMS accelerometers - Output biasing, Output control
3. Applications using MEMS accelerometers - Fitbit, RC car
4. Defenses
5. Related Work

Modelling the malicious interference on MEMS accelerometers

Capacitive MEMS Accelerometer



Newton's Second Law of Motion:
$F = ma$

Hooke’s Law
$F = -k_s d$

→ Acceleration voltage signal:
$a = -k_s d/m$

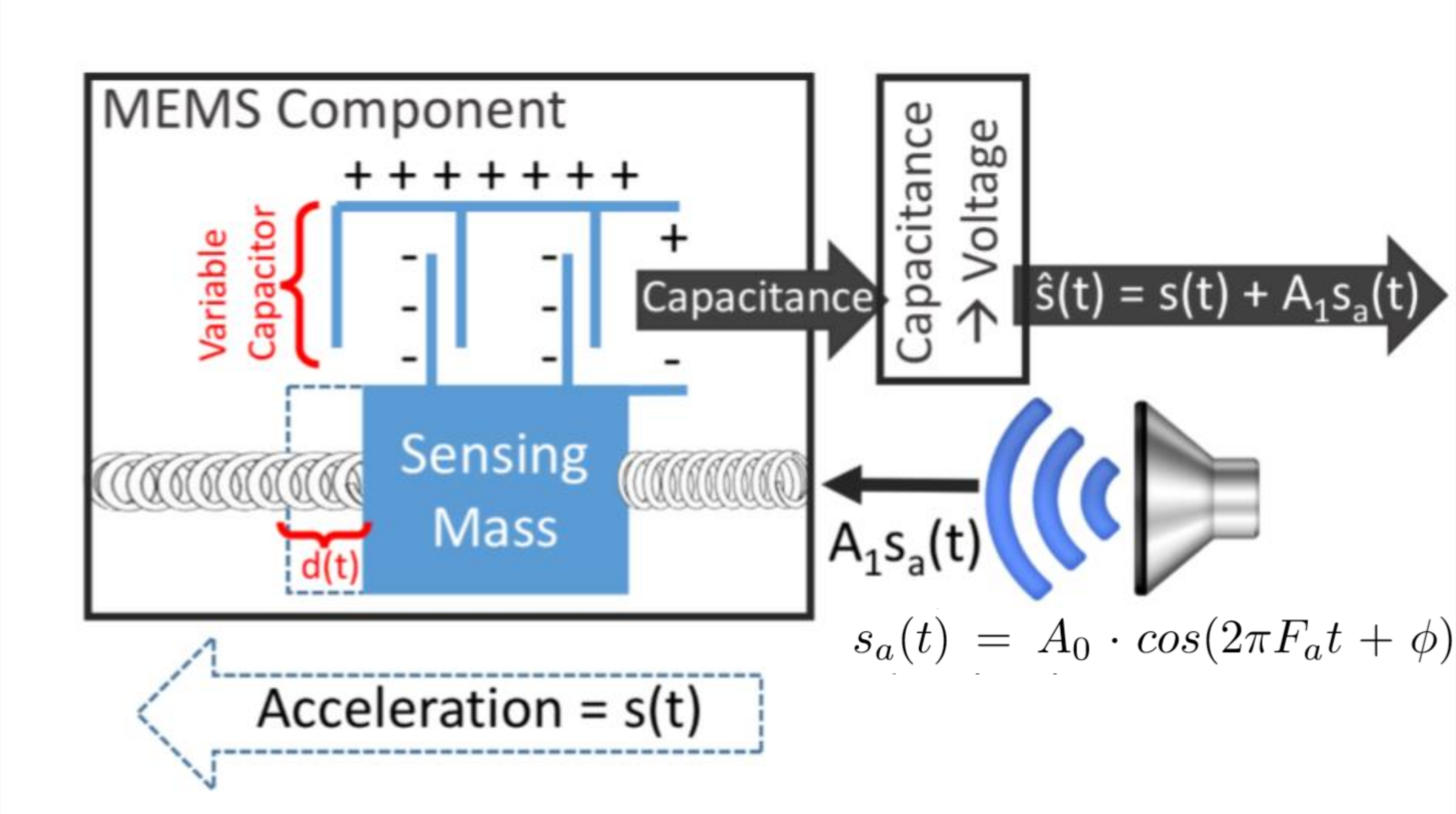
Threat Model

Attack Scope - emitting nearby acoustics to affect integrity of sensor data

Sensor Access - gain access to substantially identical device to study acoustic attack capabilities. Needed to extract exact model of MEMS accelerometer and profile its behavior under different acoustic frequencies and amplitudes

Speaker access - able to induce sound in any shape in the vicinity of the victim device, at frequencies in the human audible to ultrasonic range (2 - 30kHz).

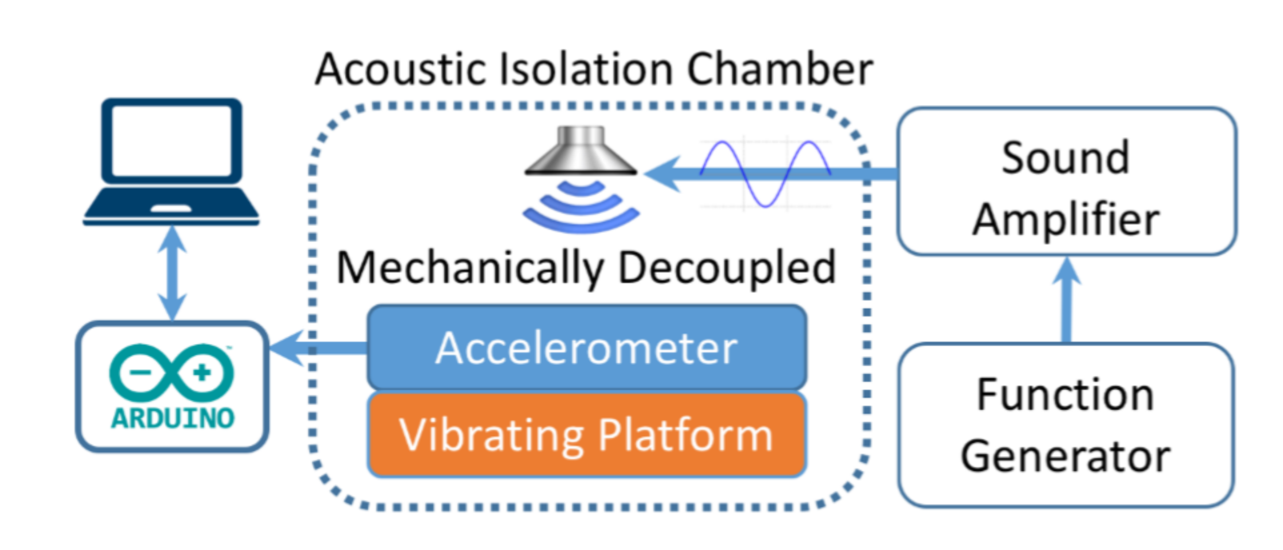
Attack Modeling



$$s_a(t) = A_0 \cdot cos(2\pi F_a t + \phi)$$

$$\hat{s}(t) = s(t) + A_1 A_0 \cdot cos(2\pi F_a t + \phi)$$

Experiment: Evaluating Model



Vibrating platform - vibrating at 70Hz to simulate true acceleration

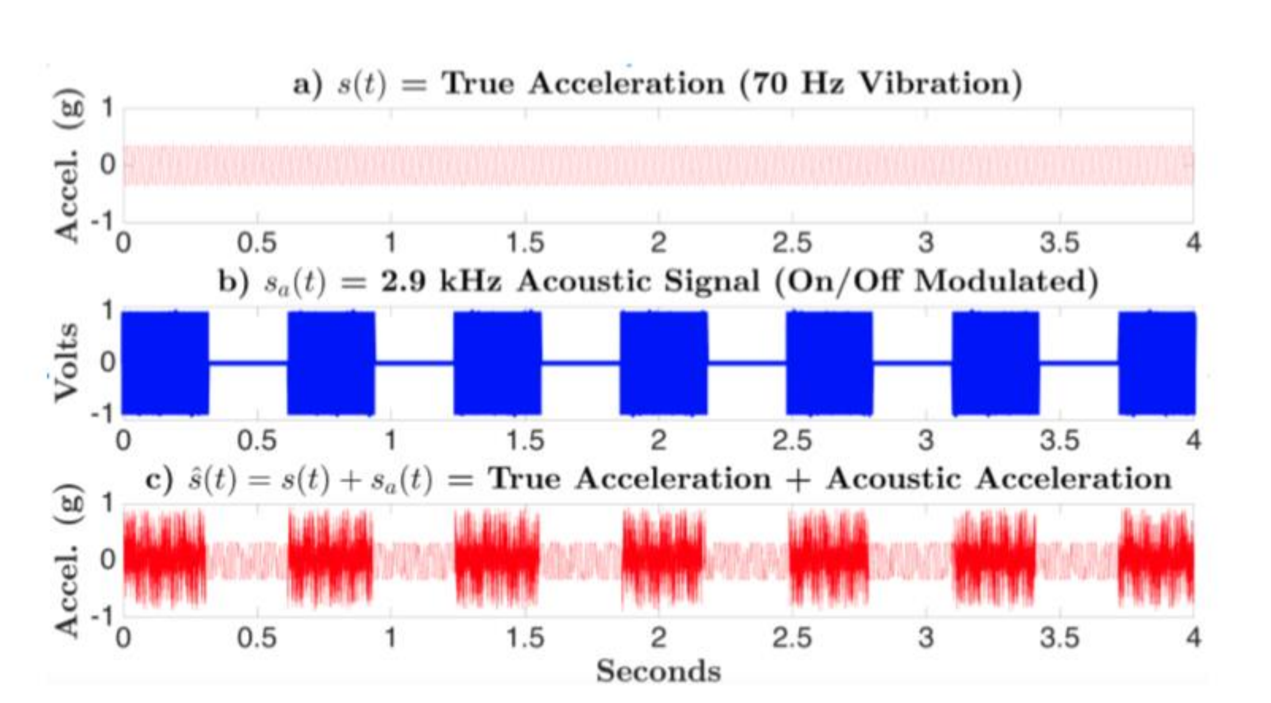
Sampled by ADC at 7kHz

Placed in an acoustic isolation chamber to avoid external noise

Sound amplifier amplified a 2.9kHz acoustic signal supplied to speaker

Acoustic signal was on/off modulated at 0.5Hz

Results



Measured acceleration is a linear combination of the true acceleration and the artificial acoustic acceleration, proposed by the model.

Maximizing the Acoustic Disturbance - Resonance

Recall that the measured acceleration signal is:

$$\hat{s}(t) = s(t) + A_1 \cdot s_a(t)$$

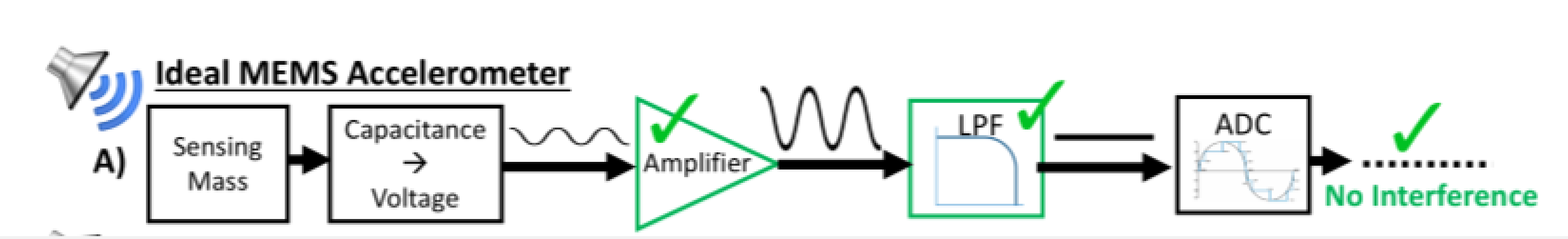
To maximize the acoustic disturbance, based on the mode, the attenuation coefficient A_1 should be maximized.

A_1 is maximized when the system is vibrated at its resonant frequencies. I.e. achieving maximum displacement of mass. (A_1 = 1).

Thus, the acoustic frequency must match the mechanical resonant frequency of the sensor to generate acoustic acceleration.

Attacks on Signal Conditioning Hardware - Ideal

Ideal Case: Any injected acoustic acceleration is removed by the signal conditioning hardware.



However, this does not always occur due to limitations in the signal conditioning hardware, which includes the:

- Low pass filter
- Amplifier

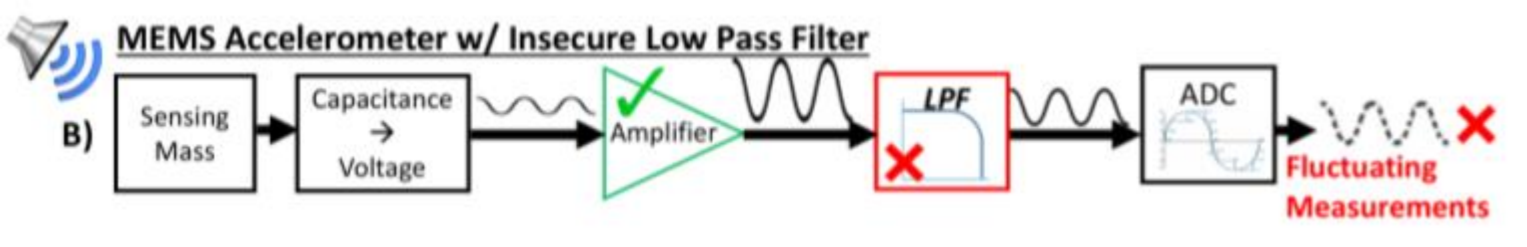
Attacks on Signal Conditioning Hardware - LPF

Low Pass Filter functions to prevent high frequency noise from contaminating the ADC samples.

Nyquist Requirement: The sampling frequency should be at least twice the highest frequency contained in the signal.

Design: $F_{\text{cutoff}} = \frac{1}{2} F_s$

Limitation: there can be a range of frequencies around Fcutoff which are attenuated but not removed completely.

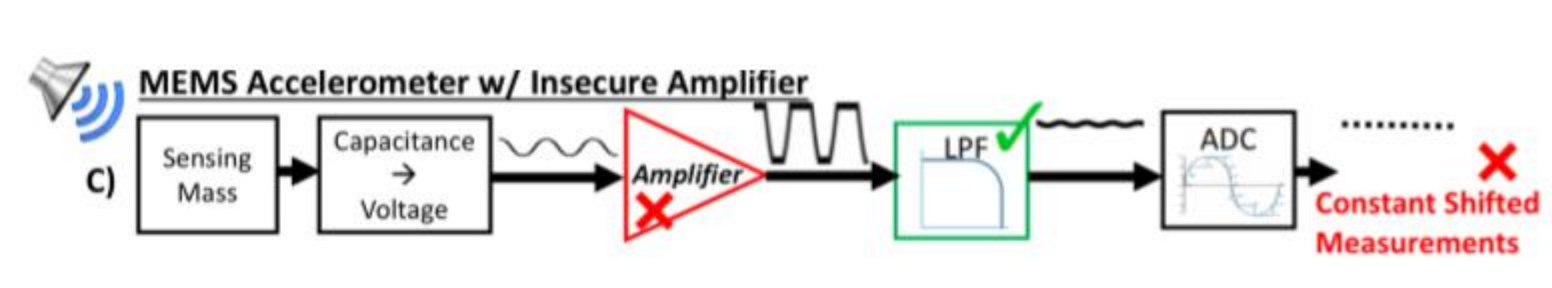


Result: Sinusoidally fluctuating acceleration measurements

Attacks on Signal Conditioning Hardware - Amplifier

Amplifier should have a dynamic range large enough to handle the maximum specified acceleration.

Limitation: This range can be exceeded if resonant acoustic interference causes a higher amplitude acceleration signal. This causes signal clipping and introduction of a non zero DC component into the signal.


MEMS Accelerometer w/ Insecure Amplifier
C)
Sensing Mass
Capacitance → Voltage
Amplifier
LPF
ADC
Constant Shifted Measurements

Result: Constant shifted acceleration measurements

Experiment: Finding Resonant Frequencies

At resonant frequency, the output measurement deviate from normal.i.e. fluctuating (std. dev.) or constantly shifted (mean).

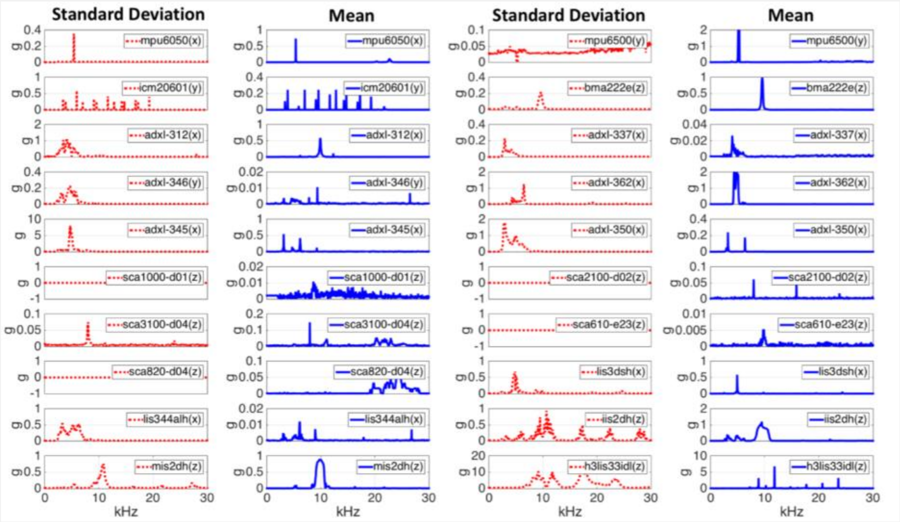
Method: Acquire several acceleration measurements within a frequency range.

Results:
Peaks indicate the acoustic interference at resonant frequency

Resonant frequencies can fall in a range

Several sensors have multiple resonant frequencies

Sensors not affected are physically larger



Acoustic injection attacks on MEMS accelerometers

Controlling Accelerometer Output

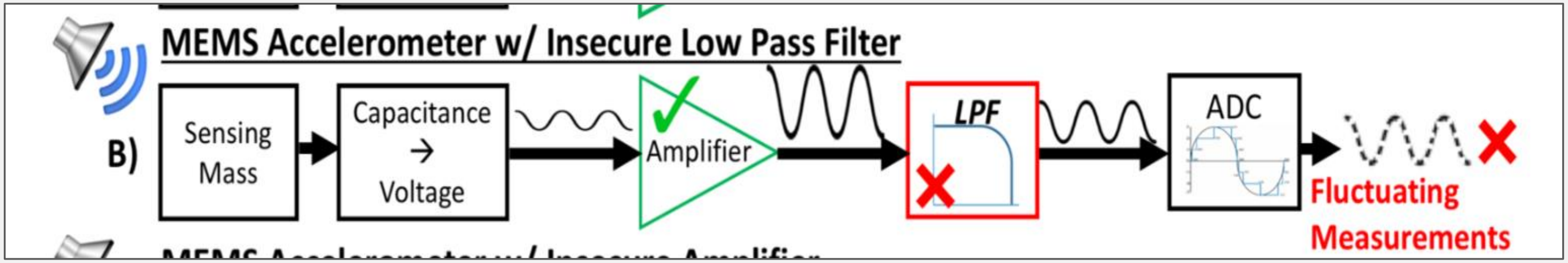
Goal - To control time series output of sensor

Two Acoustic Injection attacks :

- Output Biasing
- Output Control

Output Biasing Attacks:

- Gives control over accelerometers output over several seconds
- Accelerometers experience fluctuating false measurements at resonant frequencies due to insecure LPF



Output Biasing attack is achieved by

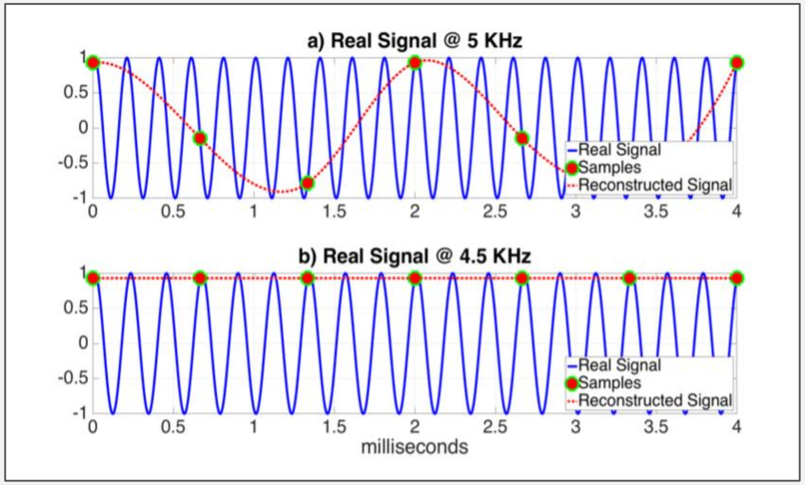
- Stabilise fluctuating false measurements into constant measurements
- Reshape the desired output signal by modulating it on top of the acoustic resonant frequency

1) **Stabilising** - Achieved by signal aliasing
2) **Reshaping** - Achieved by signal modulation

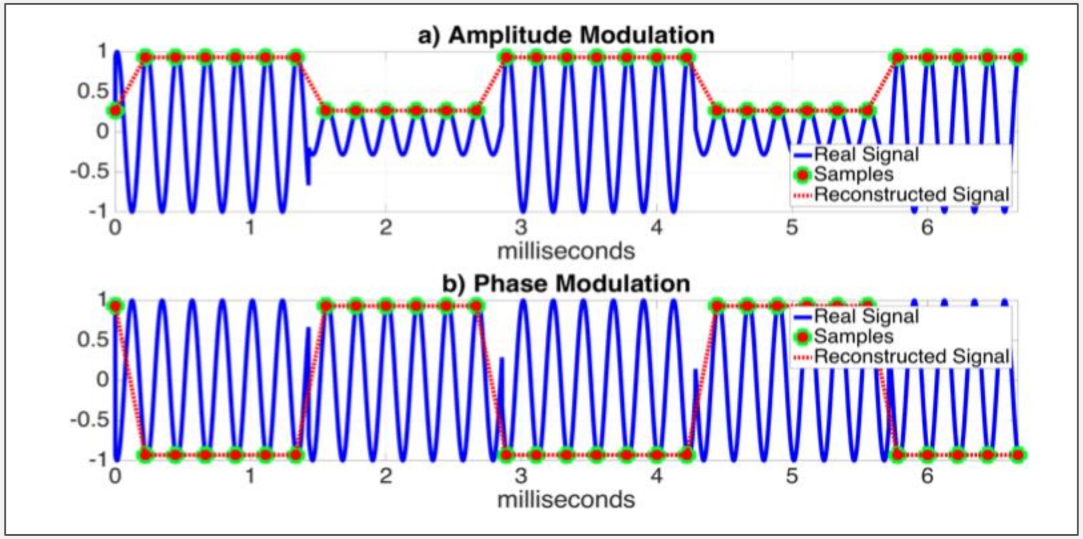
SIGNAL ALIASING:

Indistinguishable signals due to an inadequate sampling rate

Signal with max frequency component $\mathbf{F_{max}}$ should be sampled at $\mathbf{2.\ F_{max}}$ to **avoid aliasing**



SIGNAL MODULATION



Transmit information signals over carrier signal.

1) Amplitude Modulation - Vary the amplitude of F_C according to the Amplitude of the information signal

$$S_{AM} = A(t) \cdot sin(2\pi t f + \phi)$$

2) Phase Modulation - Vary the phase of F_C according to the Amplitude of the information signal

$$S_{PM}(t) = A \cdot sin(2\pi t f + \phi(t))$$

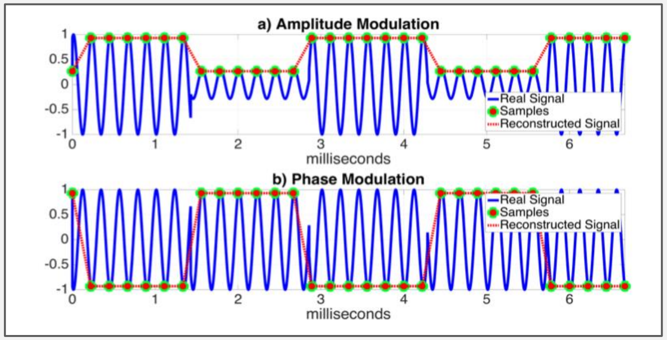
OUTPUT BIASING:

1) STEP 1 - Stabilising

Sampling rate of the Accelerometer is fixed - $\mathbf{F_{samp}}$

Sampling times at discrete intervals K is denoted by $\mathbf{t_k = k.1/F_{samp}}$

Resonant frequencies of MEMS accelerometers are **over a range.** Hence, attacker can use an acoustic frequency **within the resonant frequency range** and **integer multiple of sampling rate** to produce a **DC alias**



$$\begin{aligned}\hat{s}(t_k) &= s(t_k) + A_1 \cdot s_a(t_k) \\ &= s(t_k) + A_1 A_0 \cdot cos(2\pi F_a t_k + \phi) \\ &= s(t_k) + A_1 A_0 \cdot cos(2\pi N k + \phi) \\ &= s(t_k) + A_1 A_0 \cdot cos(\phi)\end{aligned}$$

2) STEP 2 - Reshaping

Phase Modulation allows an attacker to use full Amplitude of the carrier

Amplitude Modulation utilizes the upper or lower half of carrier signal

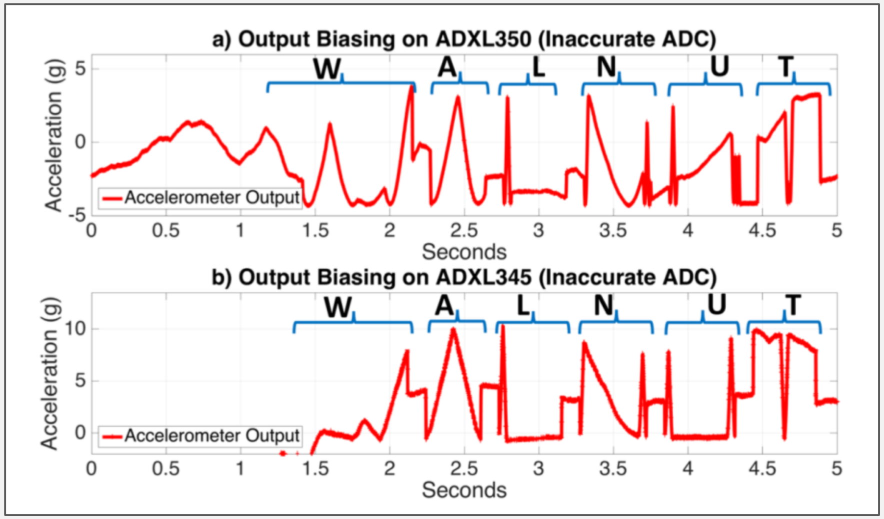
LIMITATIONS

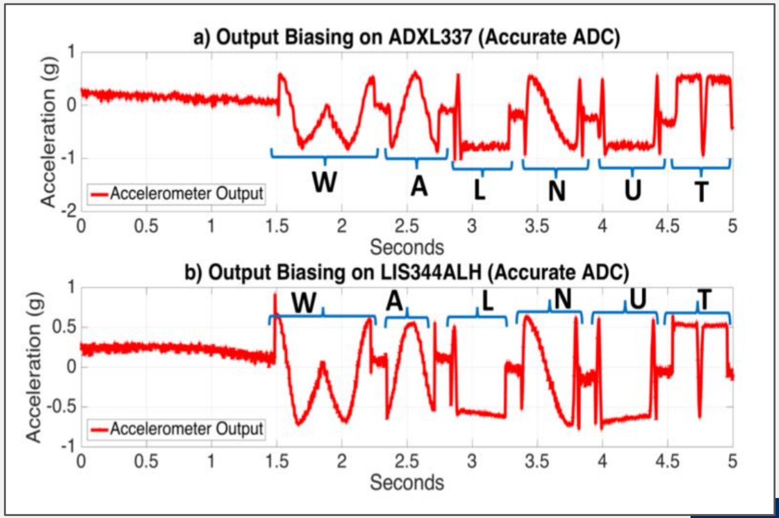
PM allows only relative control. Needs feedback from the accelerometer to tune Φ with Φ_{samp}

EVALUATION

Fluctuating output measurements for f around the resonant frequency of accelerometer

RESULTS



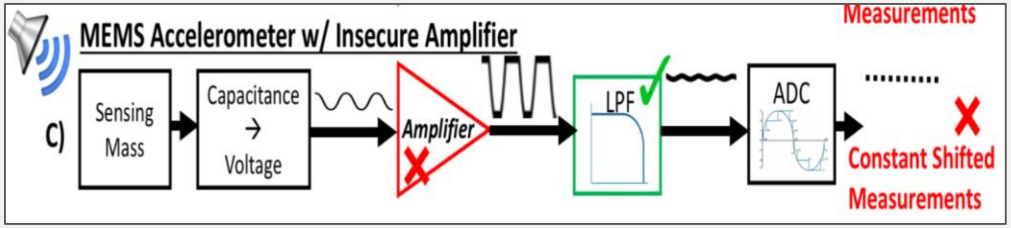


Distortion due to inaccurate ADC

Distortion is less

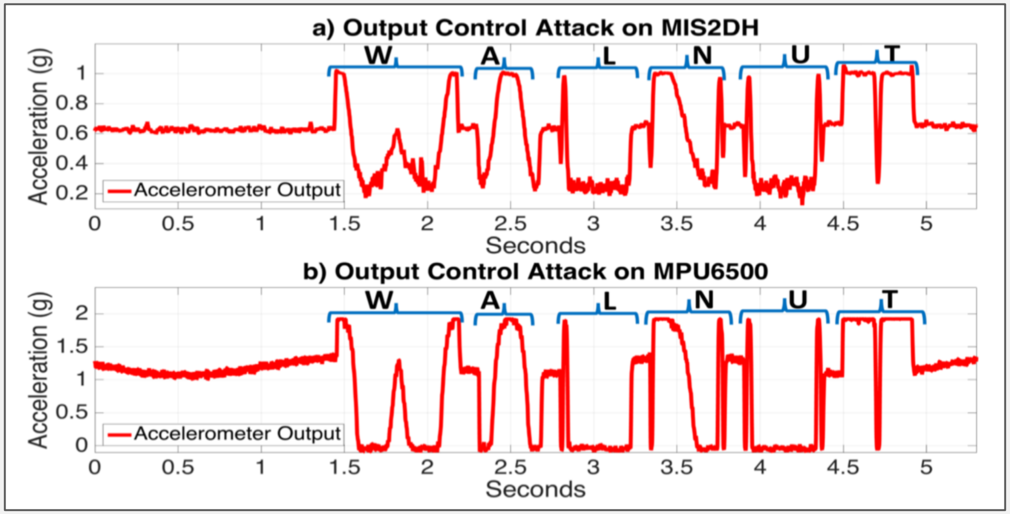
OUTPUT CONTROL ATTACK

- Gives full control of accelerometers output
- Applicable to accelerometers that exhibit constant shifted false measurements at resonant frequencies due to **insecure amplifiers**
- No signal aliasing required
- **AM** yields more effective attack


Measurements
MEMS Accelerometer w/ Insecure Amplifier
C)
Sensing Mass
Capacitance → Voltage
Amplifier
LPF
ADC
Constant Shifted Measurements

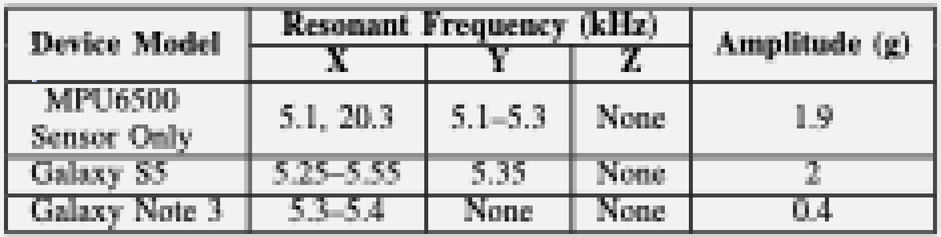
RESULTS

This attack leverages the security flaw in the amplifier



Applications using MEMS accelerometers - Fitbit, RC car

Attack #1: RC Car via Galaxy Smartphone



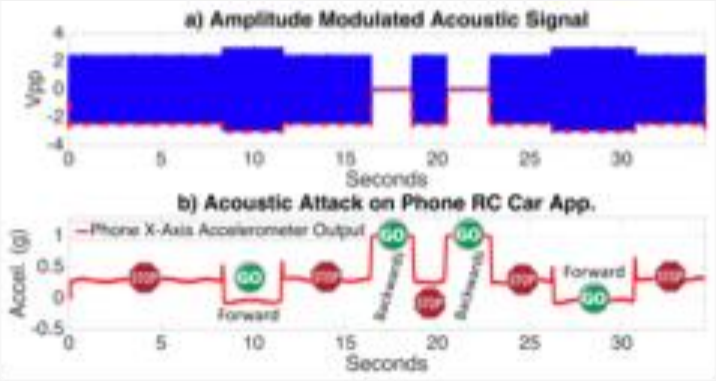
Device Model	Resonant Frequency (kHz)			Amplitude (g)
	X	Y	Z	
MPU6500 Sensor Only	5.1, 20.3	5.1–5.3	None	1.9
Galaxy S5	5.25–5.55	5.35	None	2
Galaxy Note 3	5.3–5.4	None	None	0.4

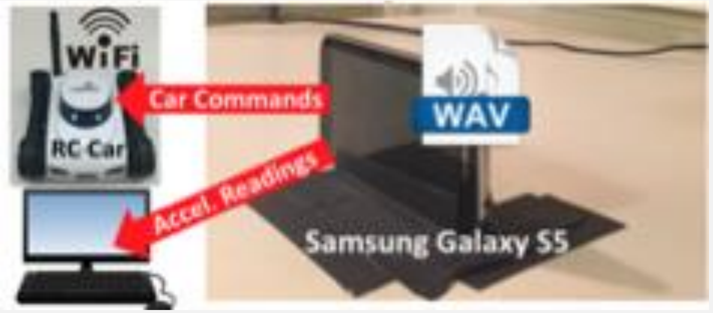
Sensor and Raw Accelerometer vary

- Resonant Frequency remains similar
- Amplitude can be capped.

Galaxy Smartphones (S5/Note 3)

- Lateral movement controls RC car
- Internal speaker spoofs accelerometers





Attack #2: Fitbit

- Tethered Fitbit One to online account
- Used acoustic interference to create false footsteps
- No signal aliasing or modulation required.

Defenses

Defense: Low Pass Filter/Amplifier

Absence of Low-Pass Filter provides no protection

- Add a Low-Pass Filter

Amplifier clips to rails easily, introducing DC component

- Make amplifier more tolerant
- Filter out resonant frequencies prior to amplification

Resonant Frequency within transmission band

- Cutoff frequency should be less than half sampling frequency
- Lower the cutoff frequency
- Narrow the transition band
- Change physical design so mass-spring exhibits a higher resonant frequency
- All of these reduce responsiveness of sensor

Defense: Other Methods

Acoustic Dampening Materials

- Creates a physical filter by dampening vibration but requires additional space

Randomized Sampling

- Prevents tuning to a resonant frequency to create a DC alias
- Does not affect amplifier clipping
- Adds inaccuracy that needs to be accommodated
- Tested with ADXL337/LIS334ALH and Arduino

180° Out-of-Phase Sampling

- Creates a simple band-stop filter around resonant frequency by summing signal with time-shifted version of signal
- Does not affect amplifier clipping
- Tested with ADXL337/LIS334ALH and Arduino

Conclusion

A host of work has been done in spoofing analog sensors, the impact of interference and information leakage. This work is the first to realize the use of acoustic interference to control output.

Additional Thoughts:

- Using additional sensors (multiple accelerators per axis, onboard microphone, adaptive filters with auxiliary sensors) subtract acoustic interference.
- Dynamically adjusting attack based on observed system behavior.

Thank you