

PowerRadio: Manipulate Sensor Measurement via Power GND Radiation

Yan Jiang¹, Xiaoyu Ji ^{*}¹, Yancheng Jiang¹, Kai Wang¹, Chenren Xu², Wenyan Xu¹



¹Ubiquitous System Security Lab, Zhejiang University

²Software-hardware Orchestrated ARchitecture Lab (SOAR), Peking University

Network and Distributed System Security (NDSS) 2025



浙江大学
ZHEJIANG UNIVERSITY



**PEKING
UNIVERSITY**

Sensors are everywhere!



False sensor values induce security events



False sensor values induce security events

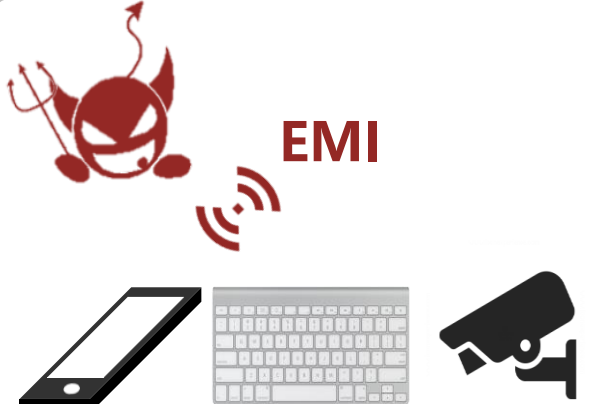


Reliable sensor measurement is essential for users' security and safety !

Sensors can be manipulated by attackers

- Various studies have demonstrated that sensors can be manipulated by physical signals.

(1) Radiated EMI-based




The diagram illustrates an EMI-based attack. At the top, a red devil icon with horns and a pitchfork is shown emitting red radio waves labeled 'EMI'. Below this, three icons represent the targets: a smartphone, a keyboard, and a security camera. The labels [1] TP, [2] Keyboard, and [3] Camera are placed under their respective icons.

[1] TP [2] Keyboard [3] Camera

[1] GhostTouch, Wang et al.
[2] GhostType, Jiang et al.
[3] GlitchHiker, Jiang et al.

(2) Invisible Laser-based



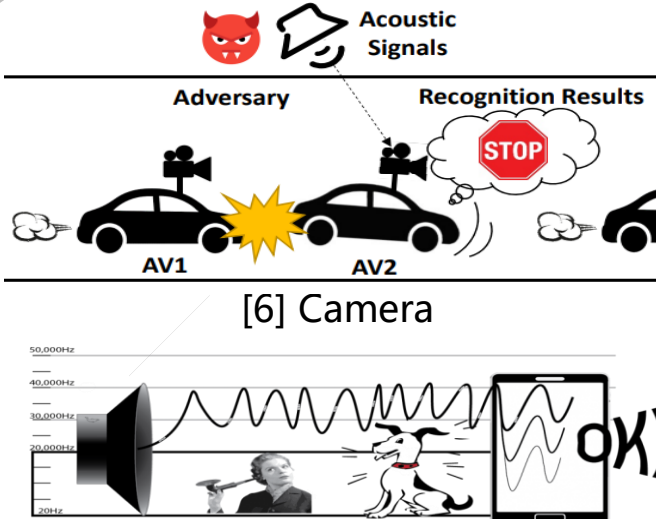
This section contains two diagrams. The top diagram, labeled [4] Camera, shows a street scene with a 'Target vehicle' and a 'Traffic light'. An 'Attack equipment' is positioned to emit a red laser beam at the vehicle. The bottom diagram, labeled [5] Microphone, shows a 'Light spot covering the entire target' and a 'Microphone holes' on a device. A 'Target' is shown at a distance of '50 m'. A circular icon with musical notes and a red arrow points towards the microphone.

[4] Camera

[5] Microphone

[4] Rolling Shutter, Yan et al.
[5] LightCommand, Jiang et al.

(3) Sound/Ultrasound-based



This section contains two diagrams. The top diagram, labeled [6] Camera, shows an 'Adversary' (a red devil icon) sending 'Acoustic Signals' to a car labeled 'AV1'. The car is shown with a 'Recognition Results' cloud containing a red 'STOP' sign. The bottom diagram, labeled [7] Microphone, shows a speaker emitting sound waves towards a person and a dog. A smartphone screen displays a waveform and the text 'OK!'.

[6] Camera

[7] Microphone

[6] Poltergeist, Ji et al.
[7] DolphinAttack, Zhang et al.

Sensors can be manipulated by attackers

- Various studies have demonstrated that sensors can be manipulated by physical signals.

(1) **Radiated EMI**-based

(2) **Invisible Laser**-based

(3) **Sound/Ultrasound**-based

Are there other potential threats to sensor readings?

[1] TP [2] Keyboard [3] Camera

- [1] GhostTouch, Wang et al.
- [2] GhostType, Jiang et al.
- [3] GlitchHiker, Jiang et al.



[5] Microphone

- [4] Rolling Shutter, Yan et al.
- [5] LightCommand, Jiang et al.

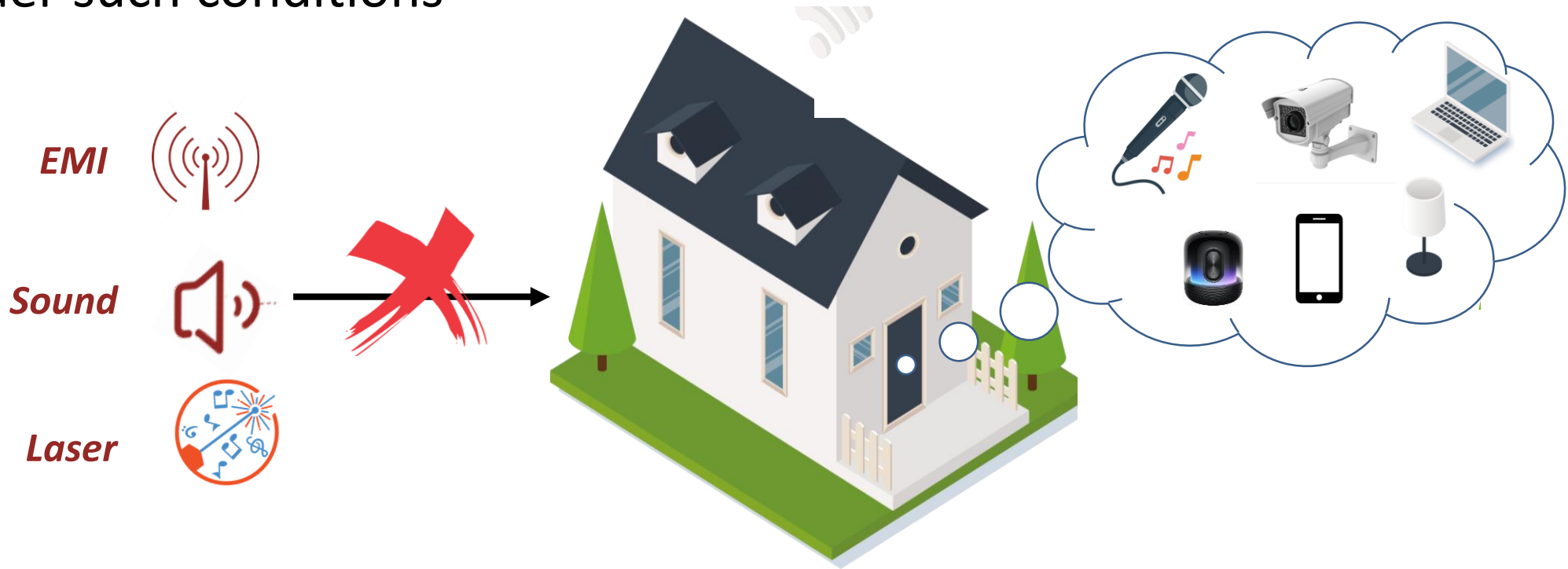


[7] Microphone

- [6] Poltergeist, Ji et al.
- [7] DolphinAttack, Zhang et al.

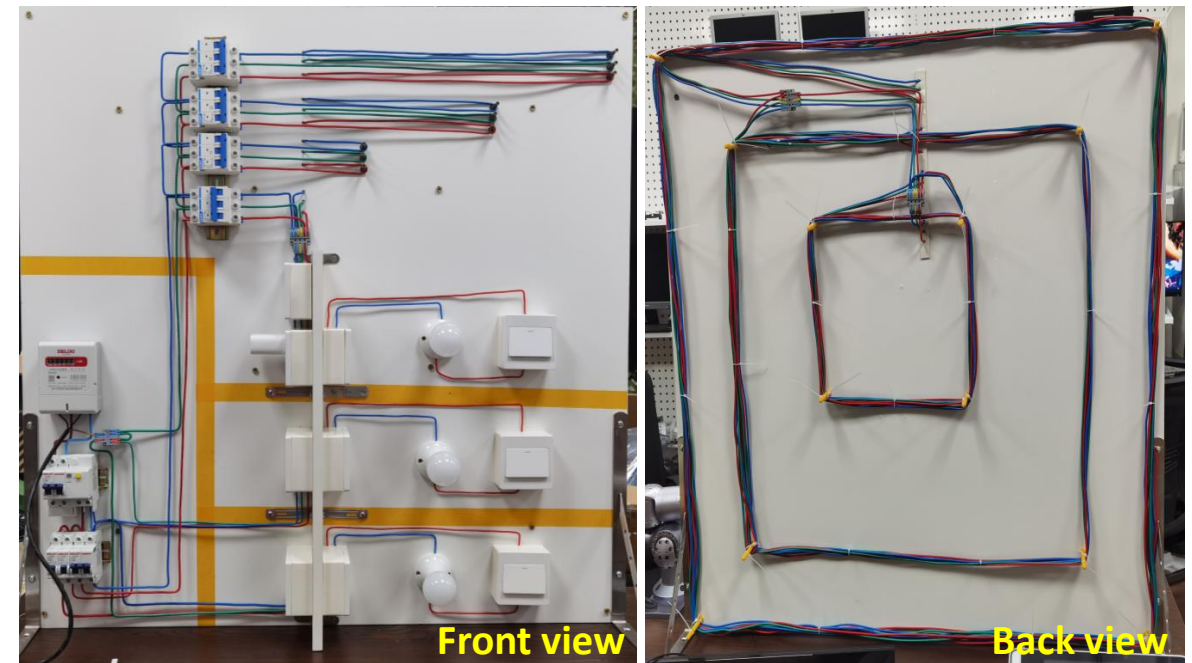
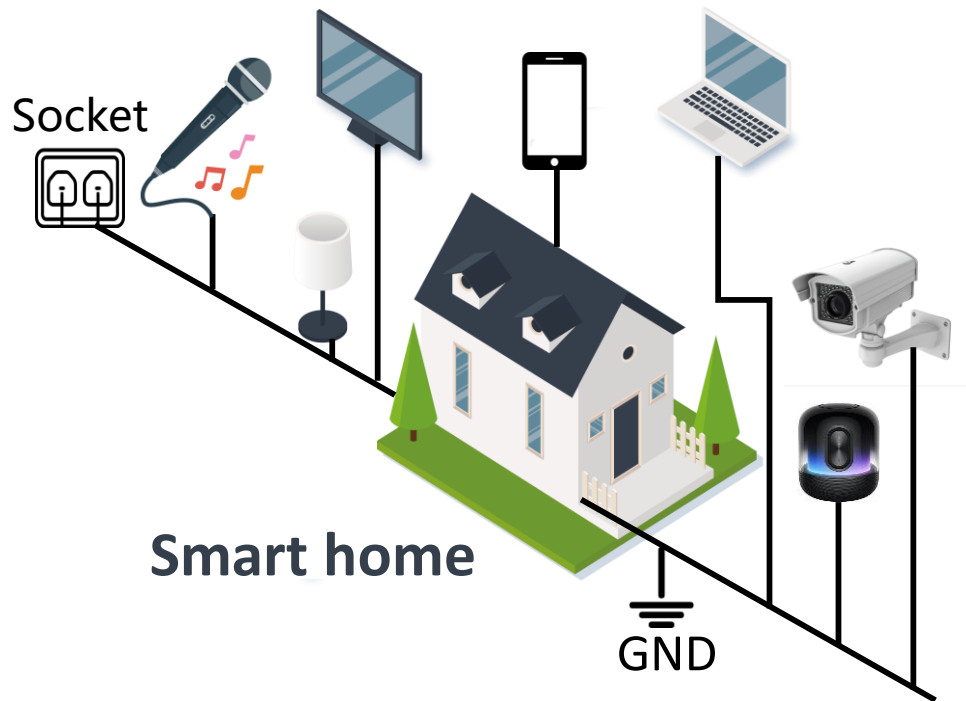
Sensors are well-packaged

- *Sensors are often well-protected* within enclosed spaces and it is hard for wireless signals to penetrate.
- Can we identify new threat vectors that *target diverse sensor types* under such conditions



Almost every sensor needs to be powered

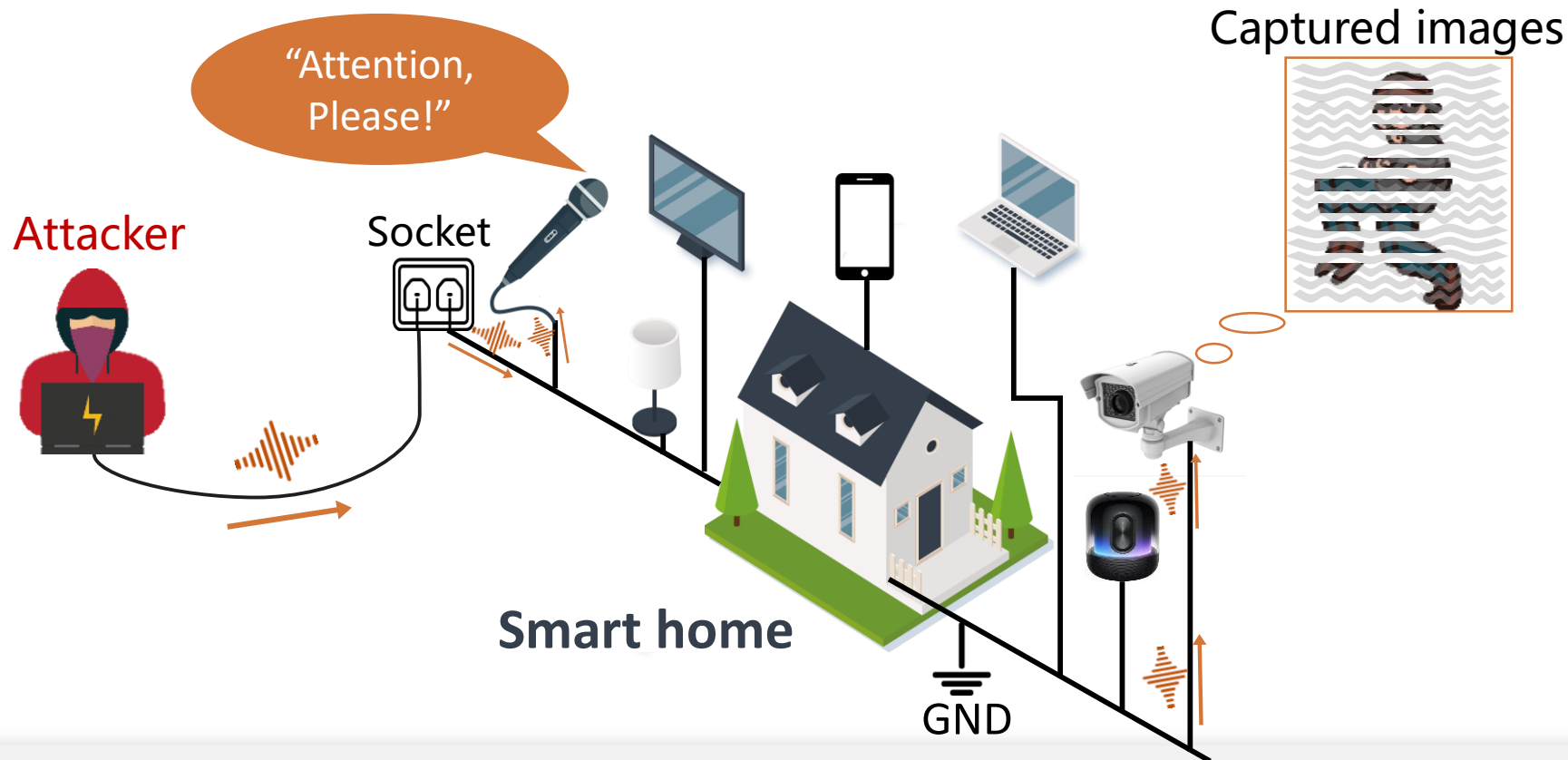
- Every sensor *needs to be powered* and their *GND cable are interconnected* in a local power grid, such as the home wiring system.



Local home wiring system

We present *PowerRadio*

- *PowerRadio*: A power-cable based sensor manipulation attack, which can *remotely interfere* with sensor measurements *without the needs of line-of-sight* and *specific properties*.



Our goal

- ❑ To understand the **new threat vector** of sensor manipulation via a power cable.
- ❑ To **mitigate** the new threat and improve the security of sensor systems.



Sensor system (by ChatGPT)

Threat model

➤ *Attack goal*

Aims to **induce false measurements** for sensors.

Threat model

➤ *Attack goal*

Aims to **induce false measurements** for sensors.

➤ *Capability and knowledge*

- Cannot **access** the sensor except its **GND cable**.
- Knows victim **sensor model** and conducts assessment beforehand.

Threat model

➤ *Attack goal*

Aims to **induce false measurements** for sensors.

➤ *Capability and knowledge*

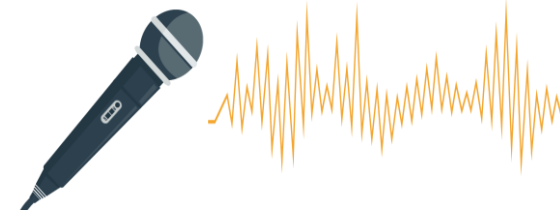
- Cannot **access** the sensor except its **GND cable**.
- Knows victim **sensor model** and conducts assessment beforehand.

➤ *Attack device*

- Install PowerRadio behind a wall as a power plug.
- Package the attack device as a power station or a charging device, e.g., a charging PC.

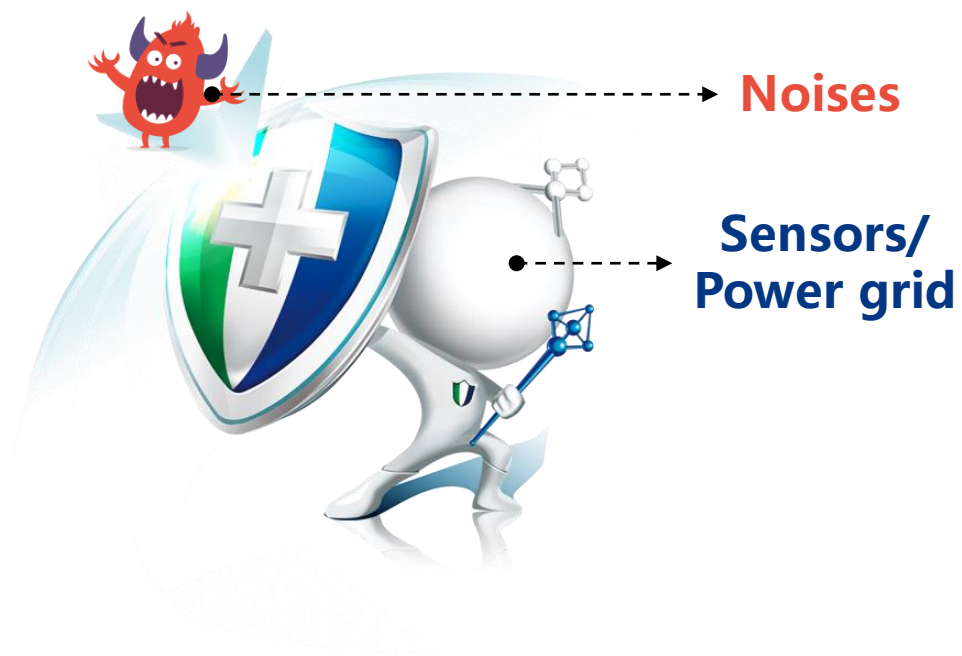
Challenges

Challenges



Challenge 1: How to **Interfere** with Sensor Measurements

- **Stable power grids:** strong noise filtering and isolation mechanism
- **Resilient sensors:** voltage regulators and noise filtering



Challenges



Challenge 1: How to **Interfere** with Sensor Measurements

- Stable power grids: strong noise filtering and isolation mechanism
- Resilient sensors: adaptive regulators and noise filtering



➤ Where to inject?

➤ What signal?

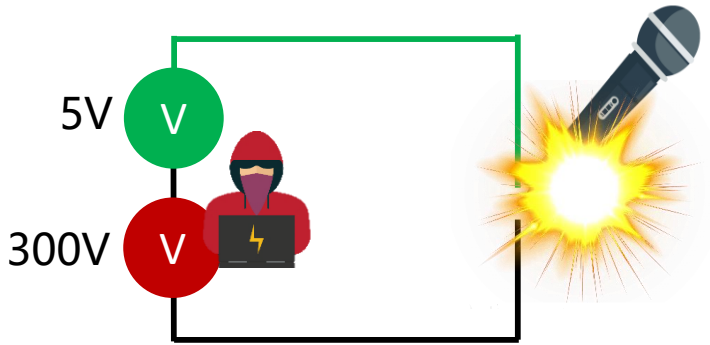
? Where to inject?

- Prevent being filtered and damaging devices
- Spread attack signals



? Where to inject?

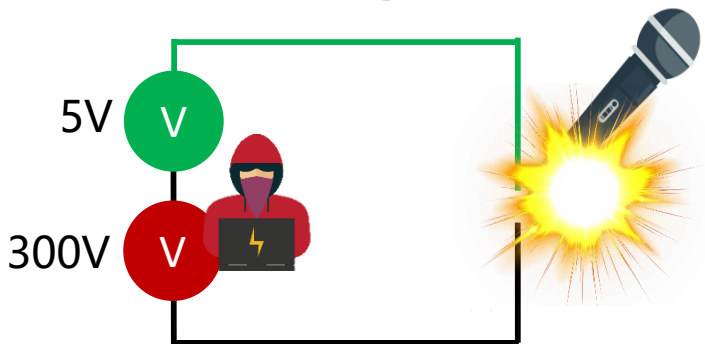
- Prevent being filtered and damaging devices
- Spread attack signals



“Microphone will be broken down by high voltage”

? Where to inject?

- Prevent being filtered and damaging devices
- Spread attack signals



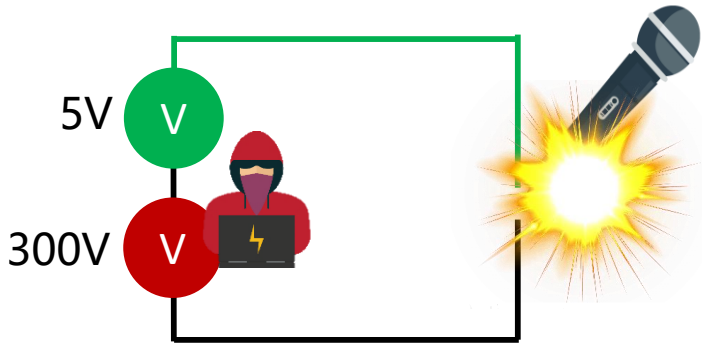
“Microphone will be broken down by high voltage”



*Use one of wires of the power cable
to inject attack signal*

? Where to inject?

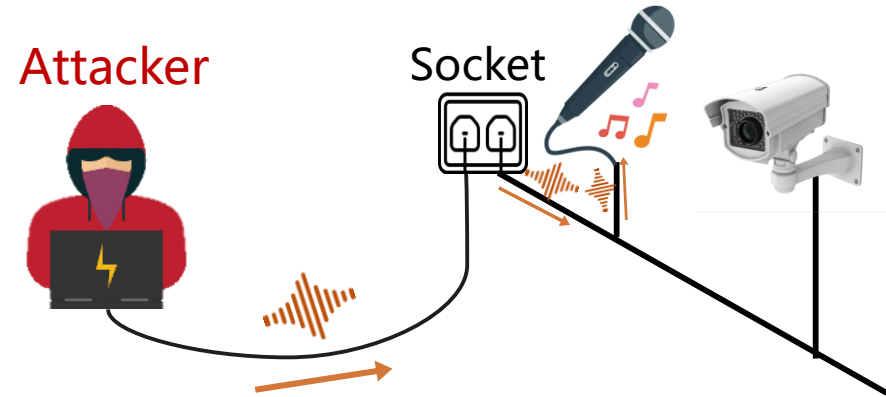
- Prevent being filtered and damaging devices
- Spread attack signals



“Microphone will be broken down by high voltage”



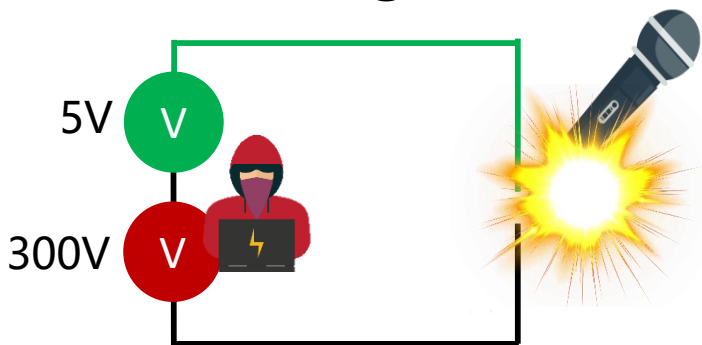
*Use one of wires of the power cable
to inject attack signal*



“The GND cable can connect all devices”

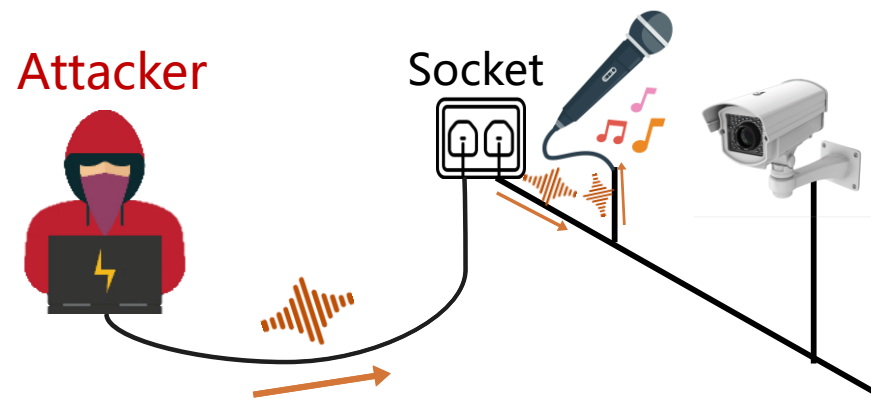
? Where to inject?

- Prevent being filtered and damaging devices
- Spread attack signals



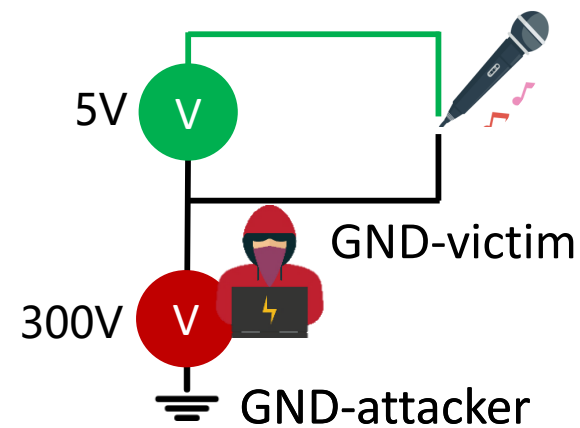
"Microphone will be broken down by high voltage"

Use one of wires of the power cable
to inject attack signal



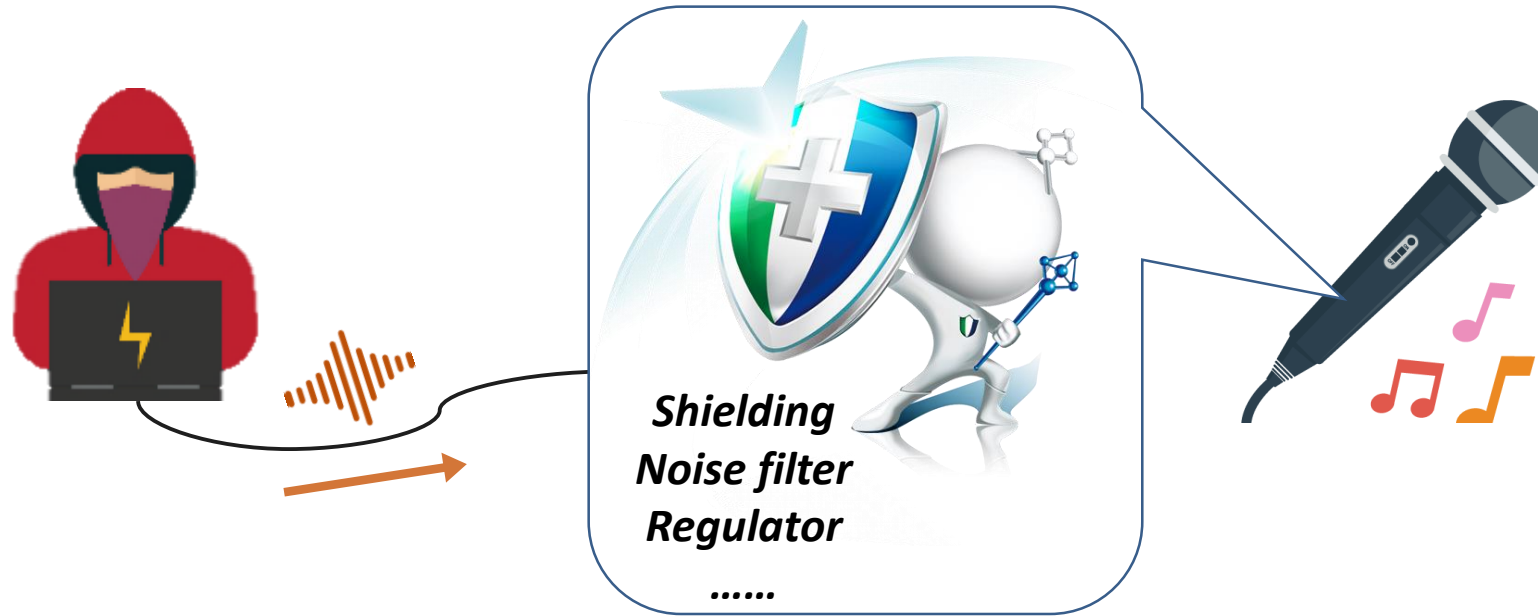
"The GND cable connectect all devices"

Choose the
GND cable
as the
injection port



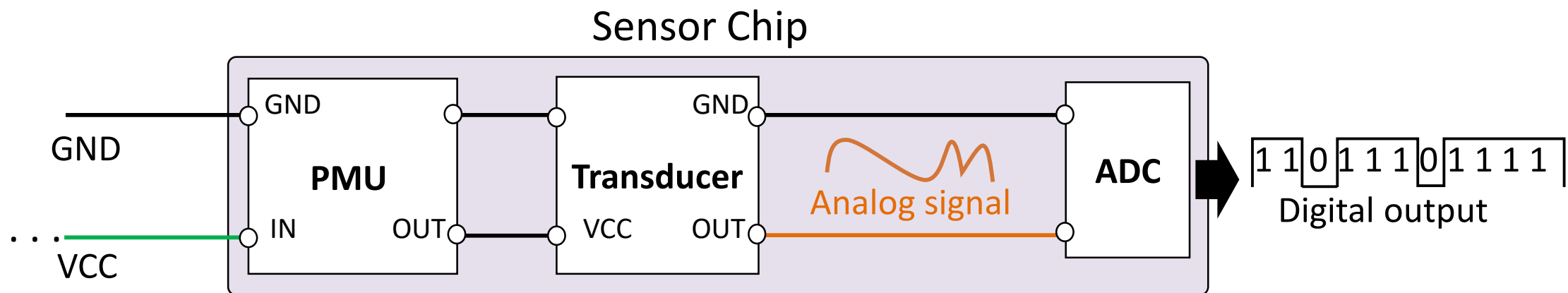
? What signal is effective?

- How can attack signal **survives from noise filters and regulators** to interfere with the analog measurements of sensors?



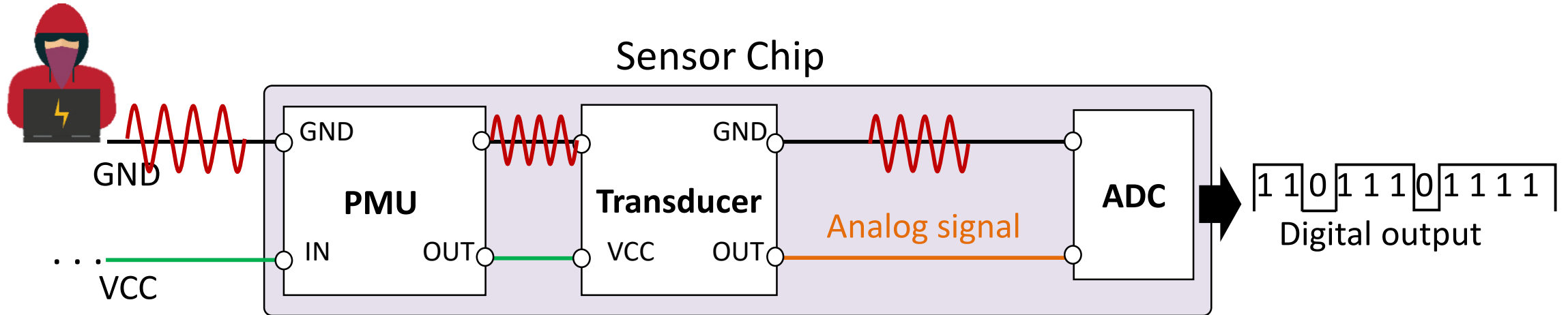
? What signal is effective?

- The *transducer* is powered by a *power management unit* (PMU) and converts the physical stimulus into an analog signal, which further being digitized by the *ADC*.



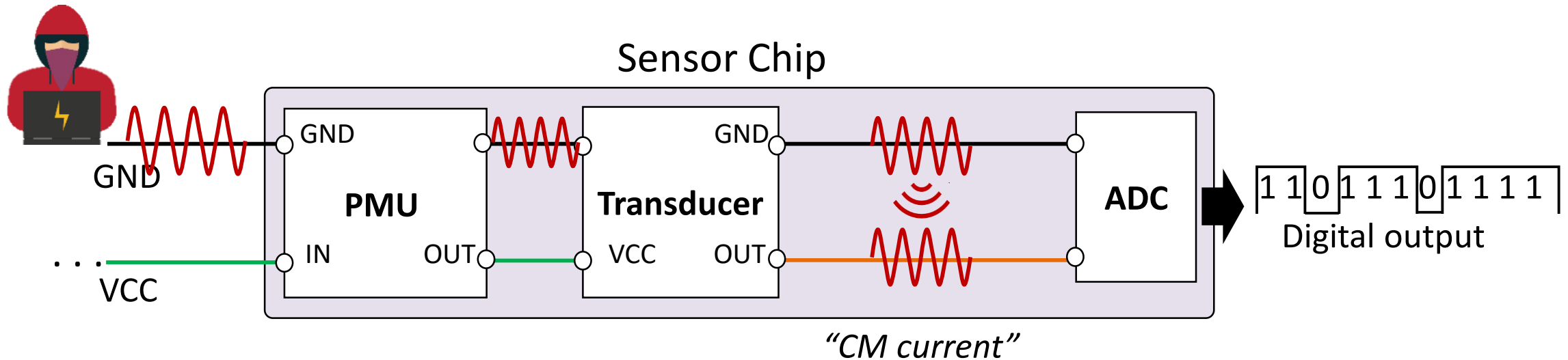
? What signal is effective?

- The attack signal will flow through internal GND cable



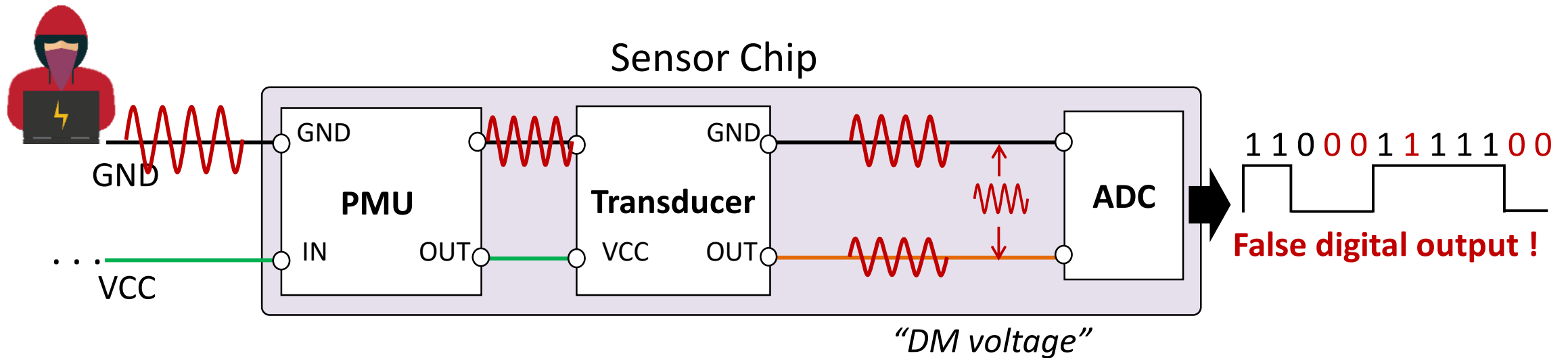
? What signal is effective?

- The attack signal will flow through internal GND cable
- The GND cable will radiate the attack signal into the nearby analog signal cable and induce common-mode (CM) current



? What signal is effective?

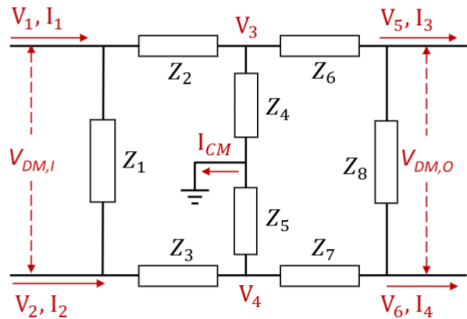
- The attack signal will flow through internal GND cable
- The GND cable will radiate the attack signal into the nearby analog signal cable and induce common-mode (CM) current
- The CM current will be converted into differential-mode (DM) voltage due to asymmetrical circuits and components





What signal is effective?

- By establishing signal transmission model and conducting simulation experiments, we find the *signal frequency* and *magnitude* play critical roles in *energy conversion*.



$$I_1 - \frac{V_1 - V_3}{Z_2} - \frac{V_1 - V_2}{Z_1} = 0$$

$$\frac{V_6 - V_4}{Z_7} - \frac{V_4 - V_2}{Z_3} - \frac{V_4}{Z_5} = 0$$

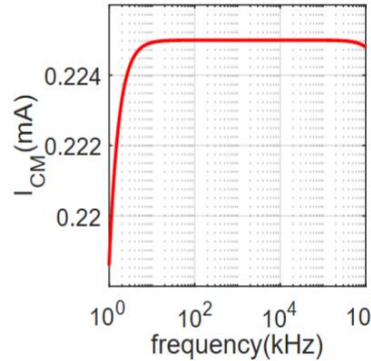
$$I_2 + \frac{V_1 - V_2}{Z_1} + \frac{V_4 - V_2}{Z_3} = 0$$

$$\frac{V_3 - V_5}{Z_6} - \frac{V_5 - V_6}{Z_8} = I_3$$

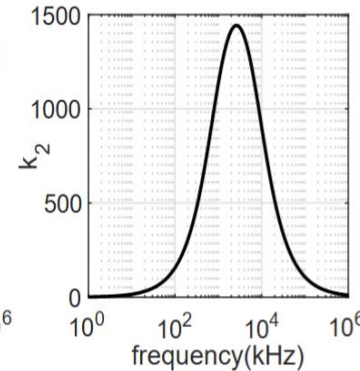
$$\frac{V_1 - V_3}{Z_2} - \frac{V_3 - V_5}{Z_6} - \frac{V_3}{Z_4} = 0$$

$$\frac{V_5 - V_6}{Z_8} - \frac{V_6 - V_4}{Z_7} = I_4$$

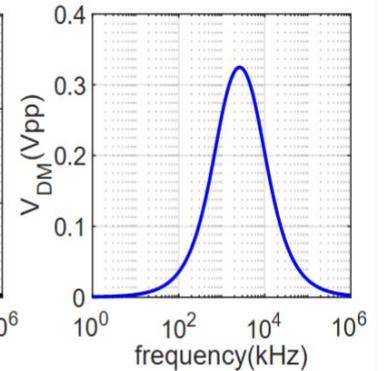
Signal Transmission model



(a) FRC of I_{CM} .



(b) FRC of k_2 .



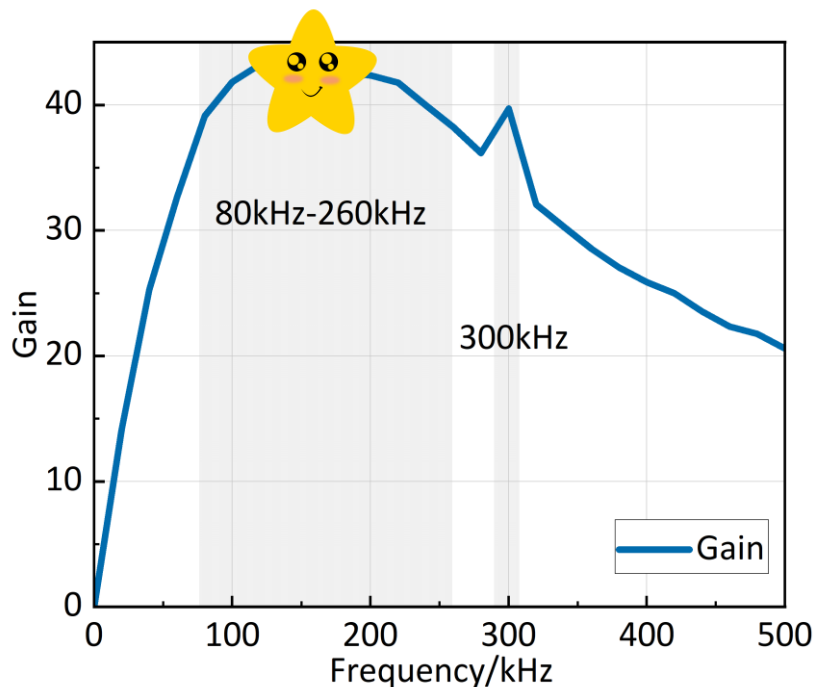
(c) FRC of V_{DM} .

Simulation Results

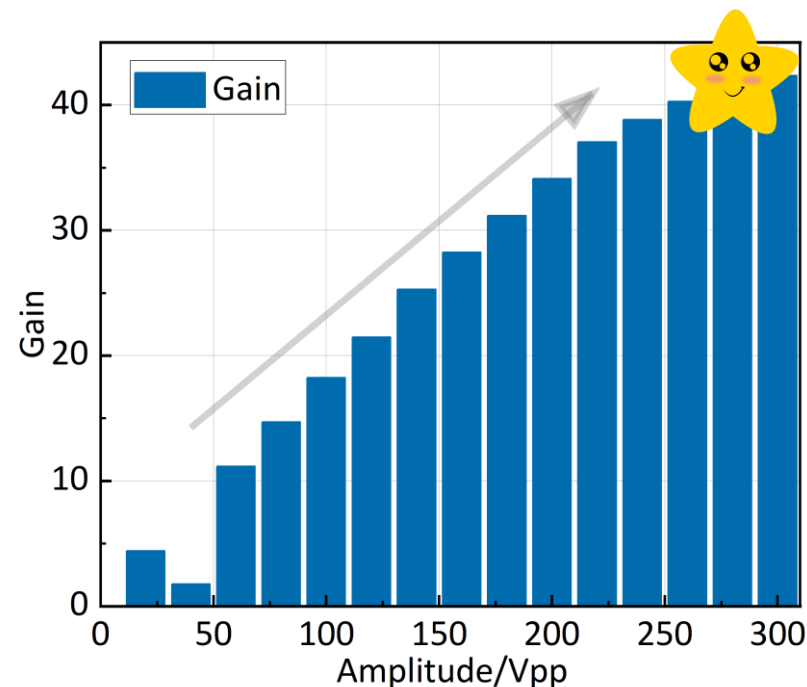


What signal is effective?

- By conducting physical experiments, we select effective attack signal parameters, i.e., frequency and magnitude, where the **sensor derivation can reach the maximum value**.



Optimize Signal Frequency



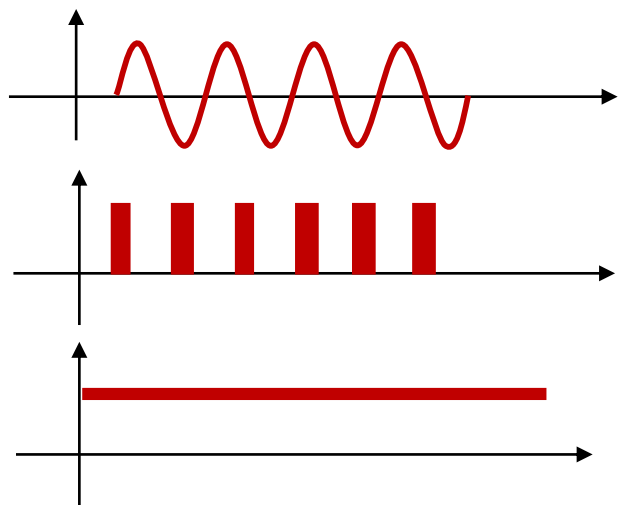
Optimize Signal Amplitude

Challenges



Challenge 2: How to Create **Desired Outputs**?

- **Limited access:** data cable are hidden and well protected.
- **Diverse outputs:** various output types, e.g., AC, pulse, DC.



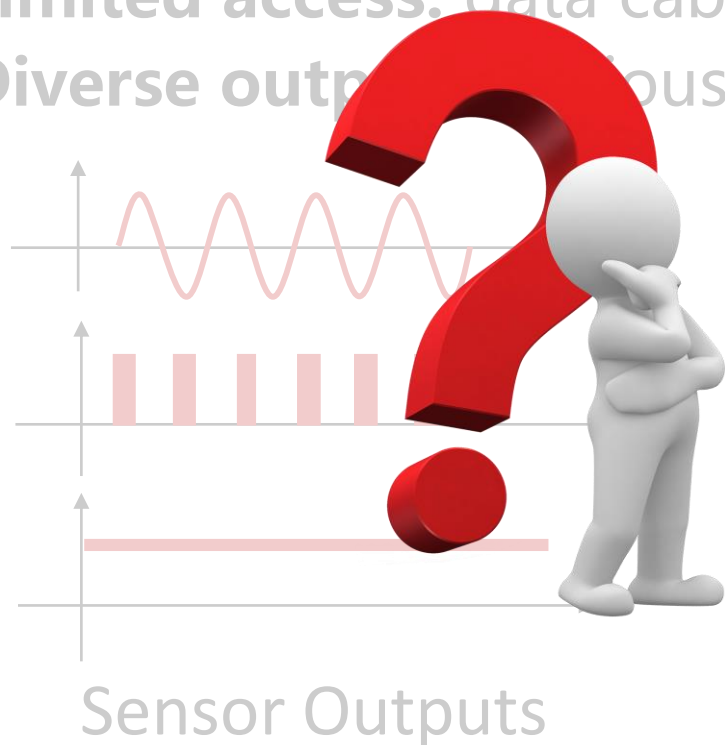
Sensor Outputs

Challenges



Challenge 2: How to Create **Desired Outputs**?

- **Limited access:** data cable are hidden and well protected.
- **Diverse output:** various output types, e.g., AC, pulse, DC.

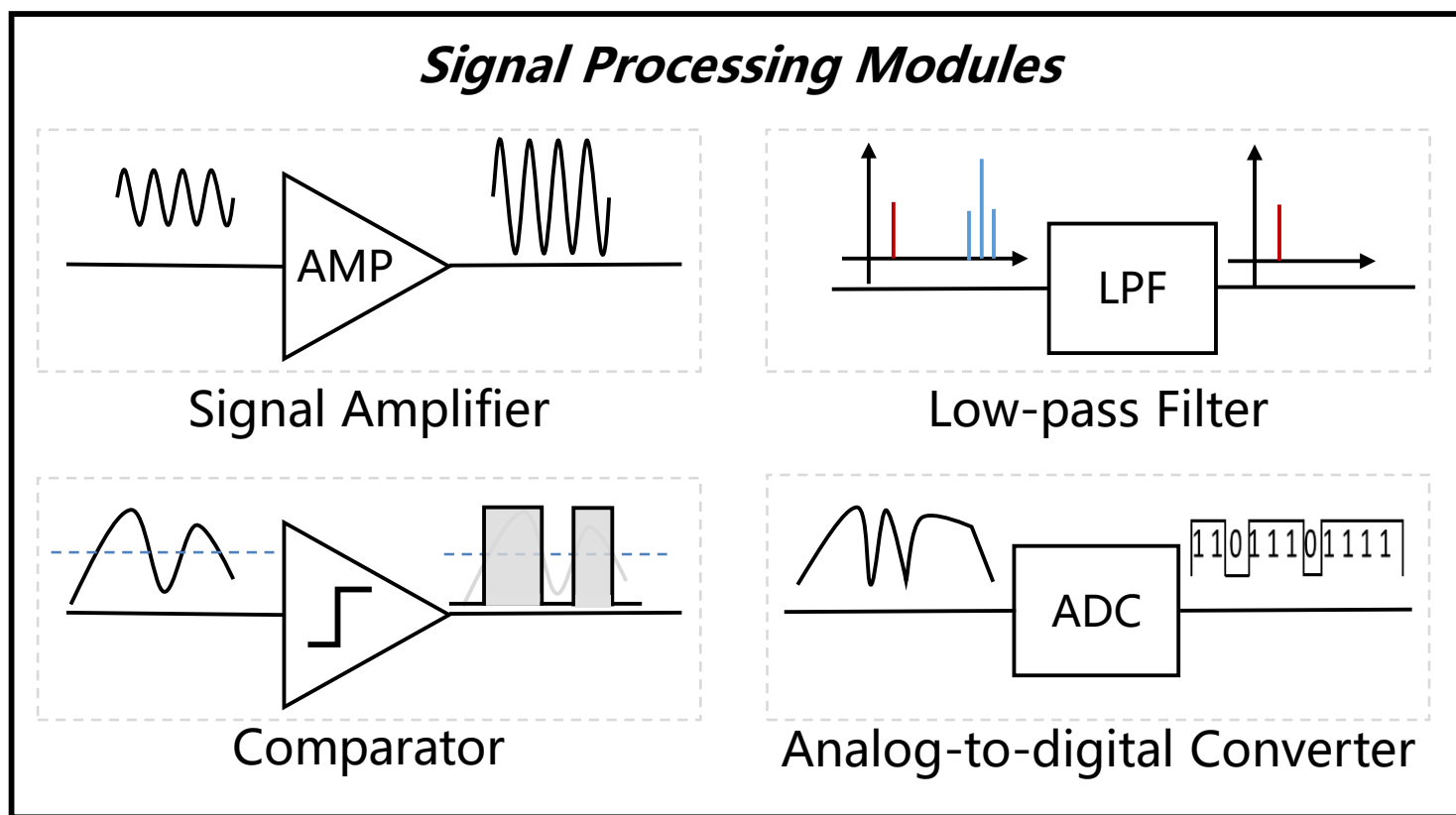


➤ How to shape signal?



How to shape signal?

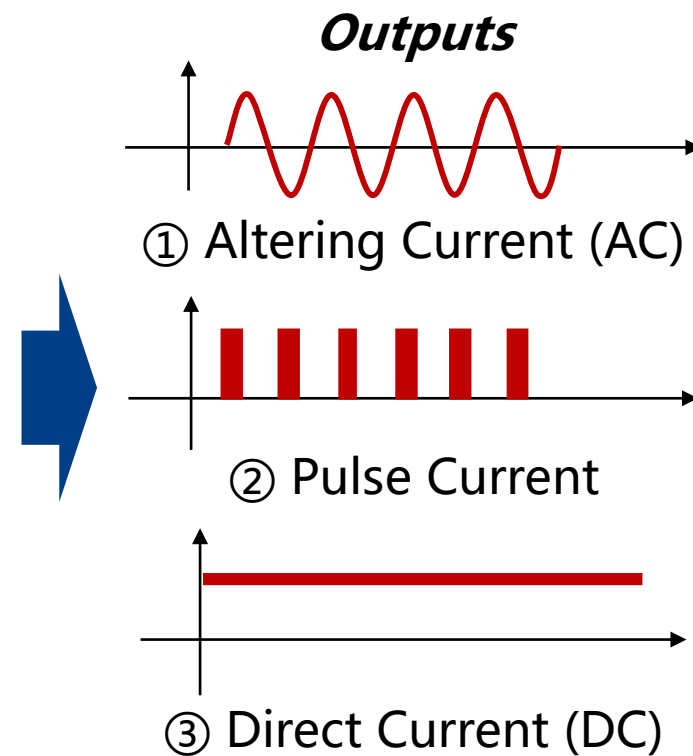
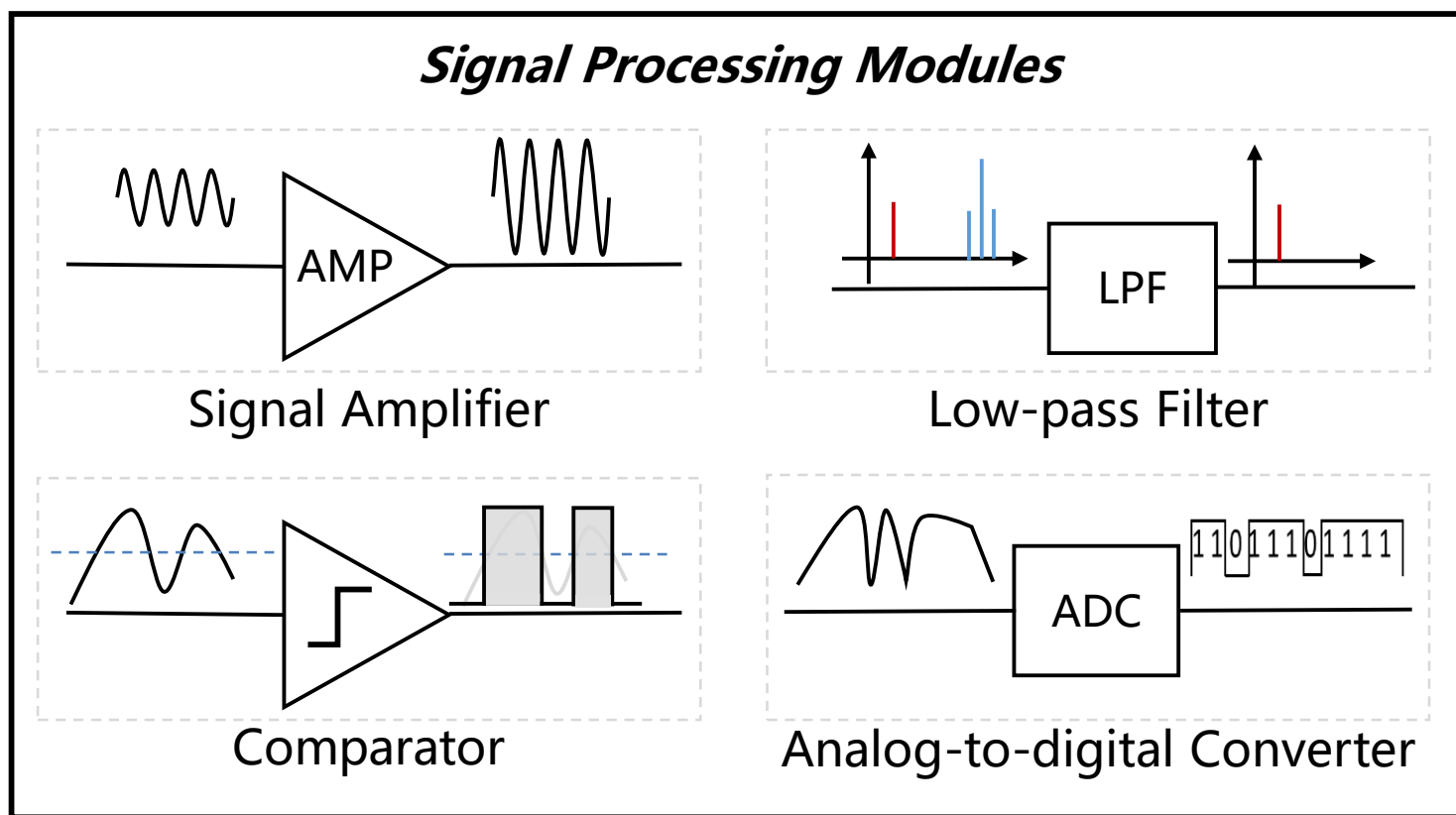
- Sensors shape signals via various signal processing modules





How to shape signal?

- Sensors shape signals via various signal processing modules
- They output AC, pulse, DC or random signals

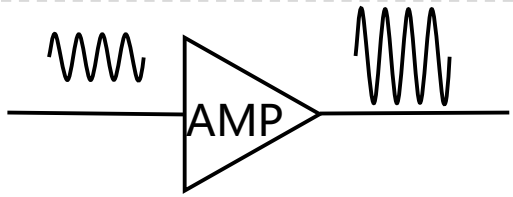




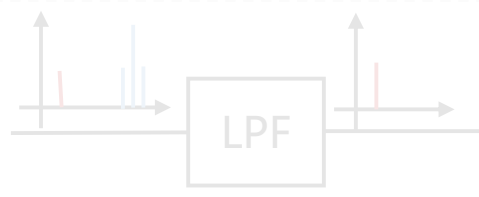
How to shape signal?

- However, signal processing modules are *not perfect*, which may induce *unexpected behaviors*.

Unexpected Behaviors of Signal Processing Modules



Signal Amplifier



Low-pass Filter

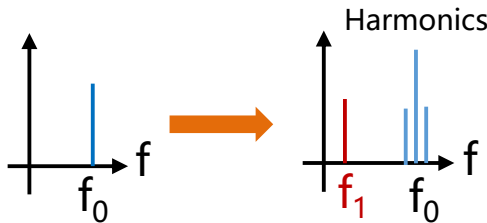


Comparator



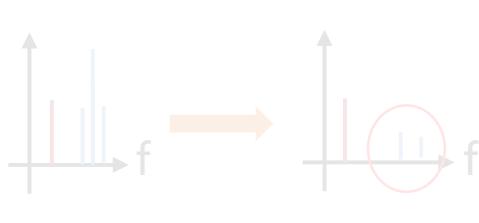
ADC

Non-linear behavior



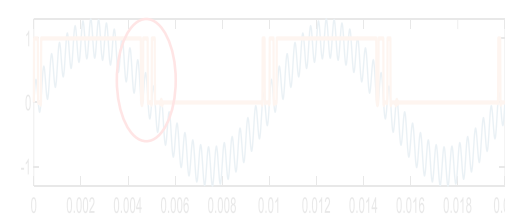
- Induce new frequency

Incomplete Filtering



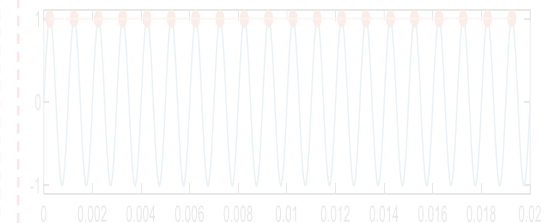
- Remain high frequency

Limited Hysteresis



- Induce unexpected pulses

Aliasing Effect



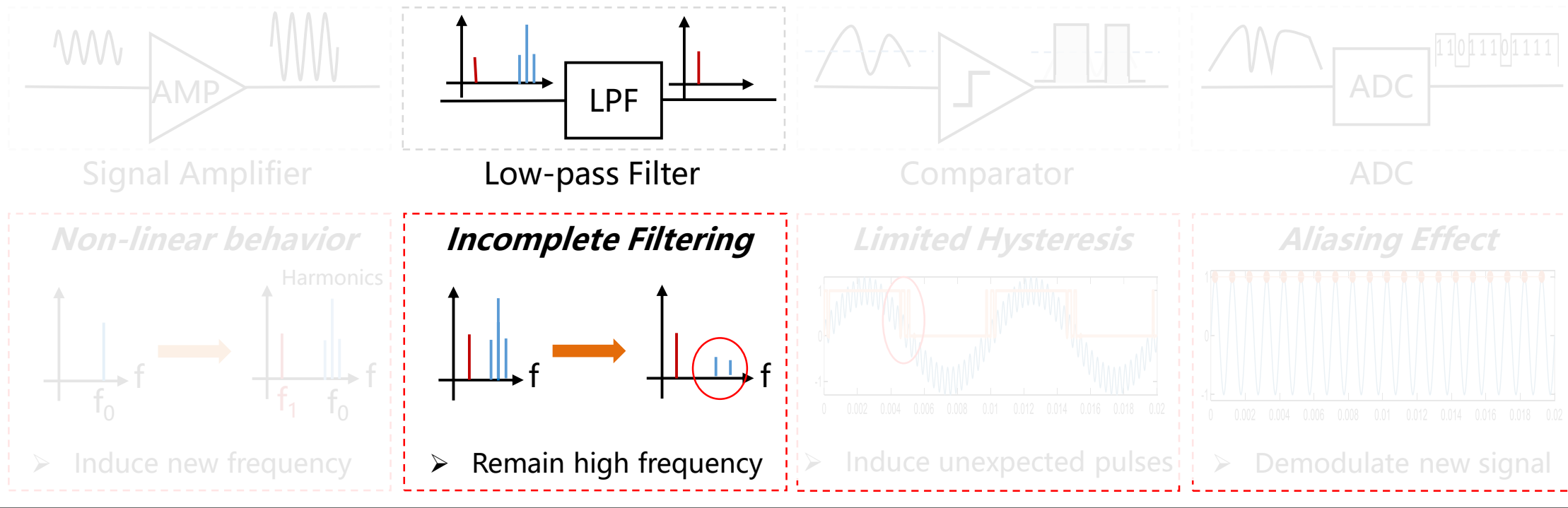
- Demodulate new signal



How to shape signal?

- However, signal processing modules are *not perfect*, which may induce *unexpected behaviors*.

Unexpected Behaviors of Signal Processing Modules

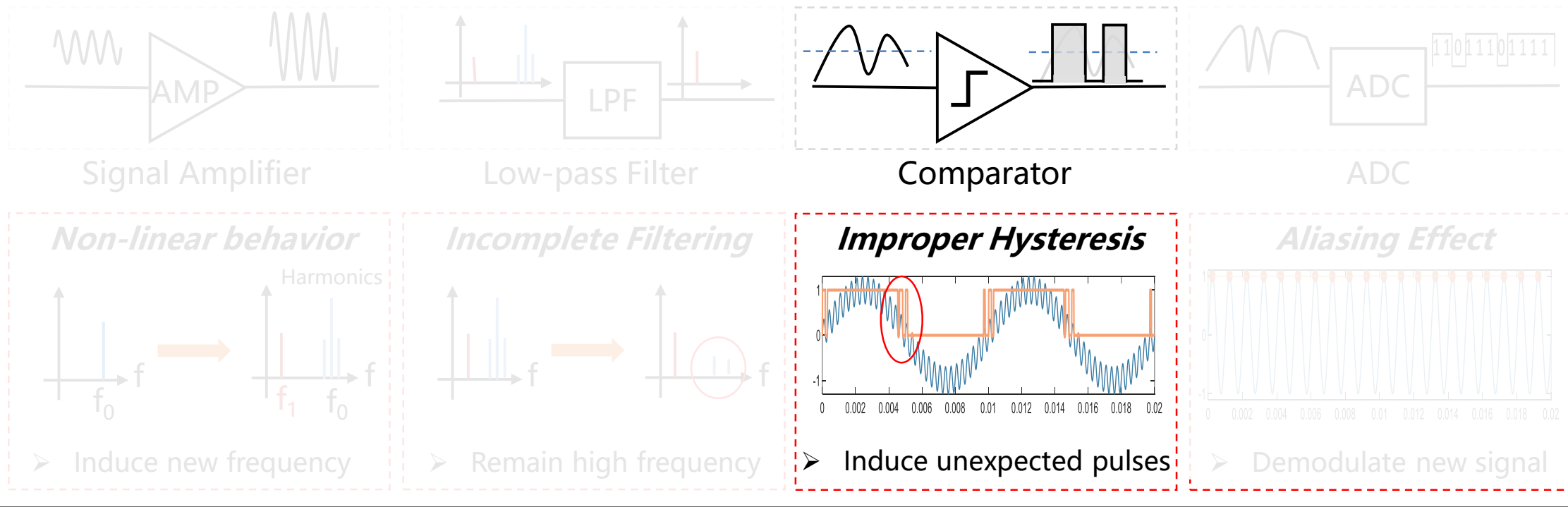




How to shape signal?

- However, signal processing modules are *not perfect*, which may induce *unexpected behaviors*.

Unexpected Behaviors of Signal Processing Modules

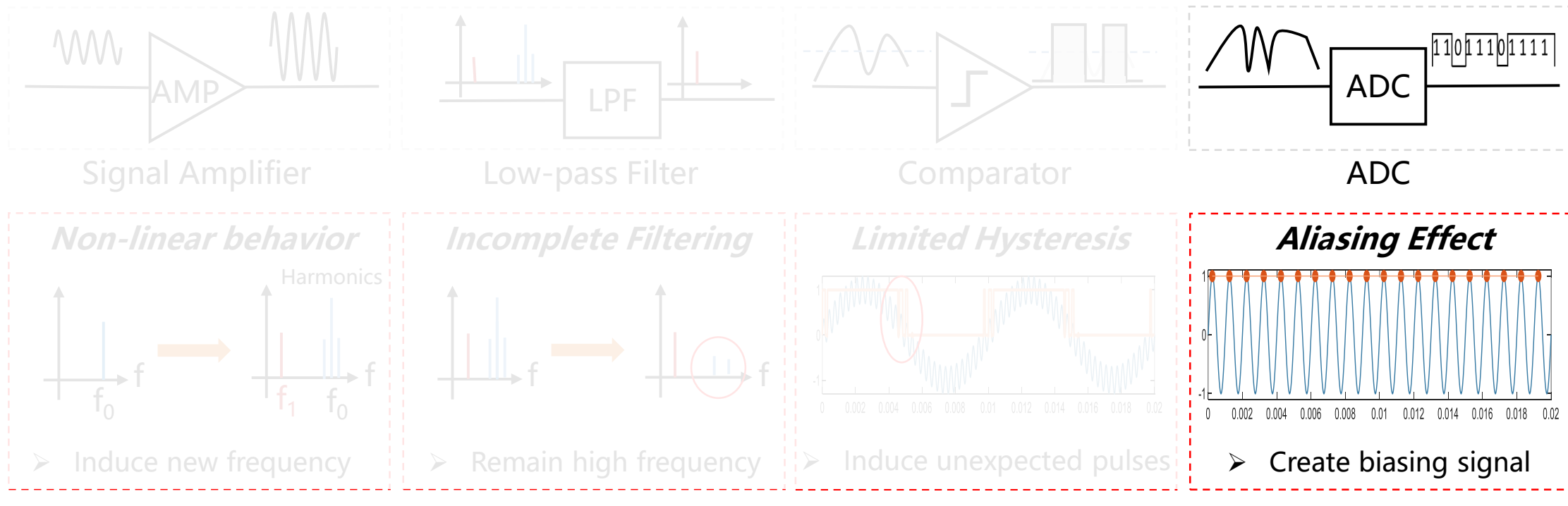




How to shape signal?

- However, signal processing modules are *not perfect*, which may induce *unexpected behaviors*.

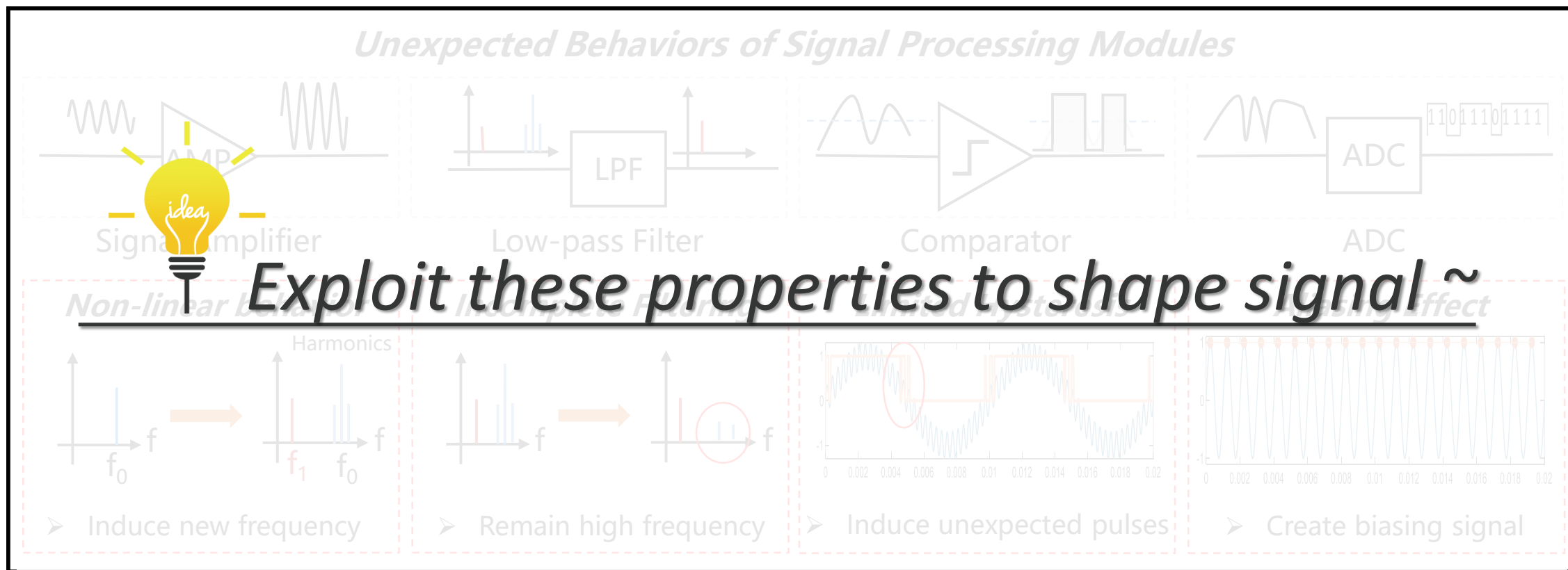
Unexpected Behaviors of Signal Processing Modules





How to shape signal?

- *PowerRadio* exploits vulnerabilities of signal processing modules to shape attack signals.

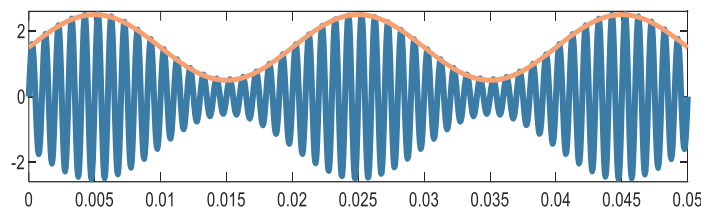
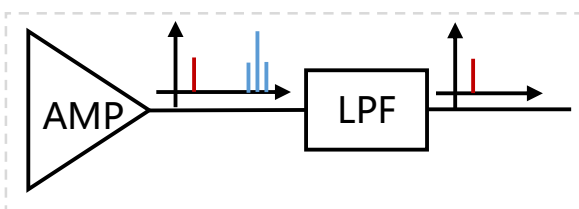




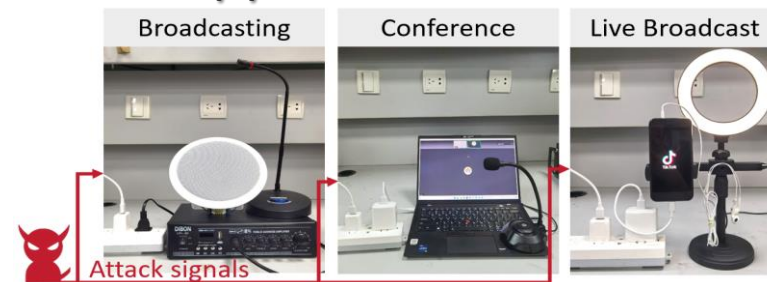
How to shape signal?

- Exploiting shaping properties of modules to design attack signal.

(1) Nonlinearity-based **AC** Injection Method



Applicable Scenes

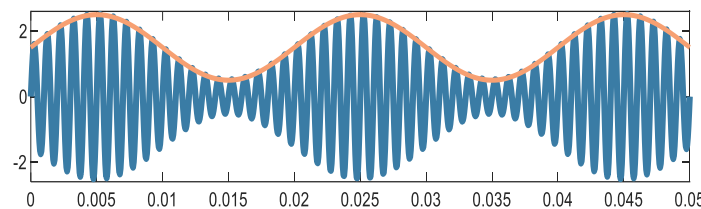
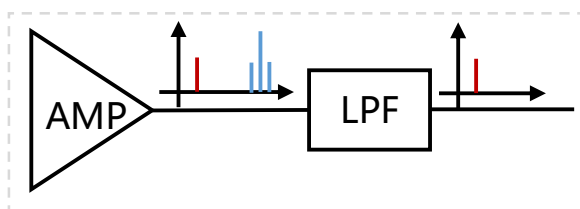




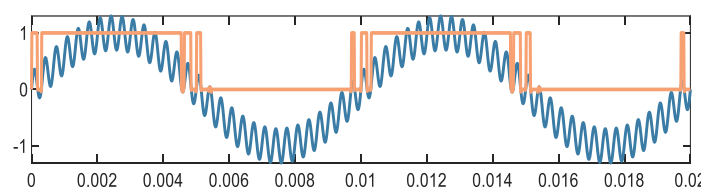
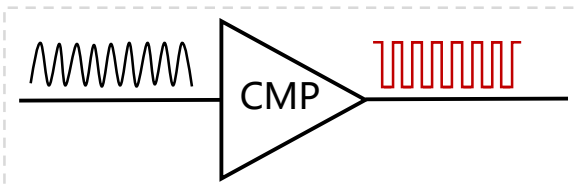
How to shape signal?

- Exploiting shaping properties of modules to design attack signal.

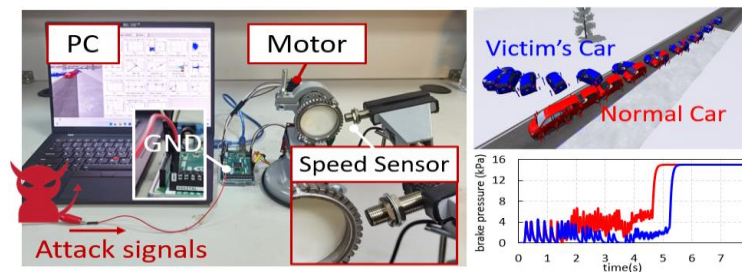
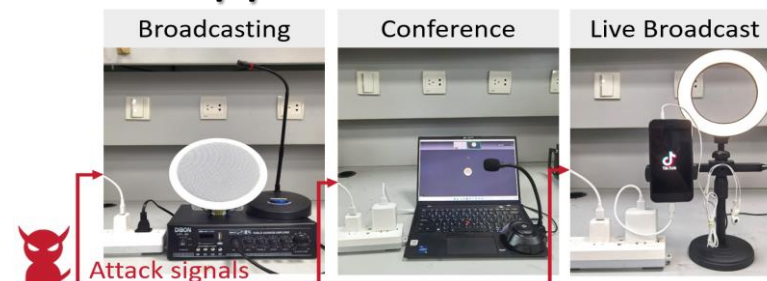
(1) Nonlinearity-based **AC** Injection Method



(2) Jitter-based **Pulse** Injection Method



Applicable Scenes

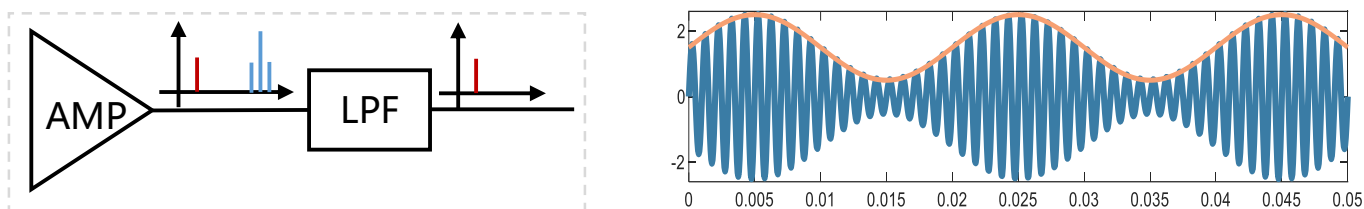




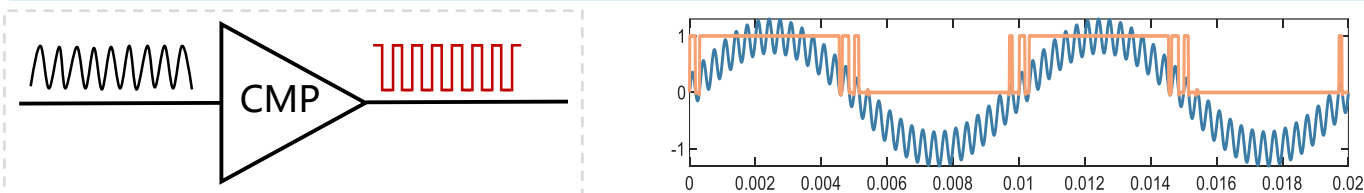
How to shape signal?

- Exploiting shaping properties of modules to design attack signal.

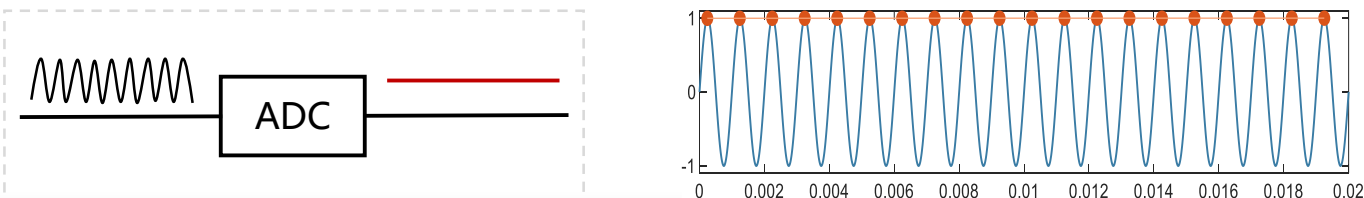
(1) Nonlinearity-based **AC** Injection Method



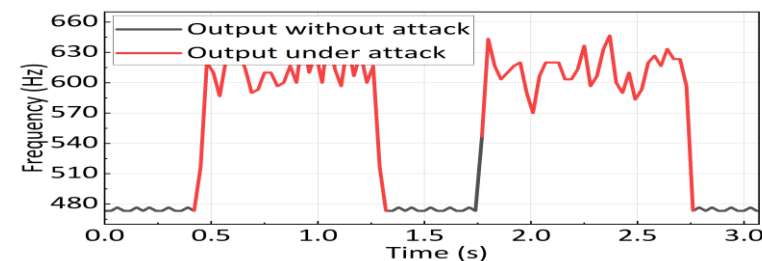
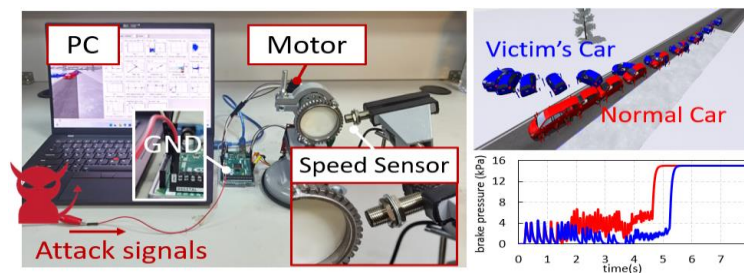
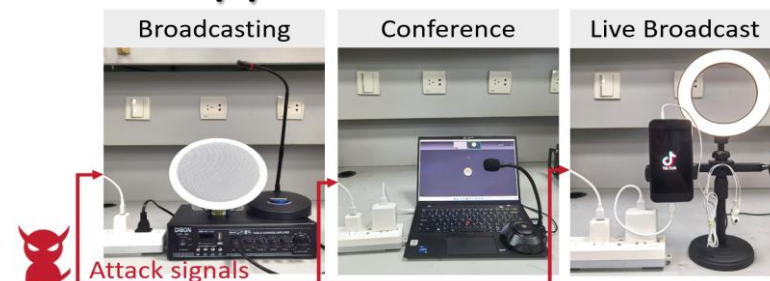
(2) Jitter-based **Pulse** Injection Method



(3) Biasing-based **DC** Injection Method

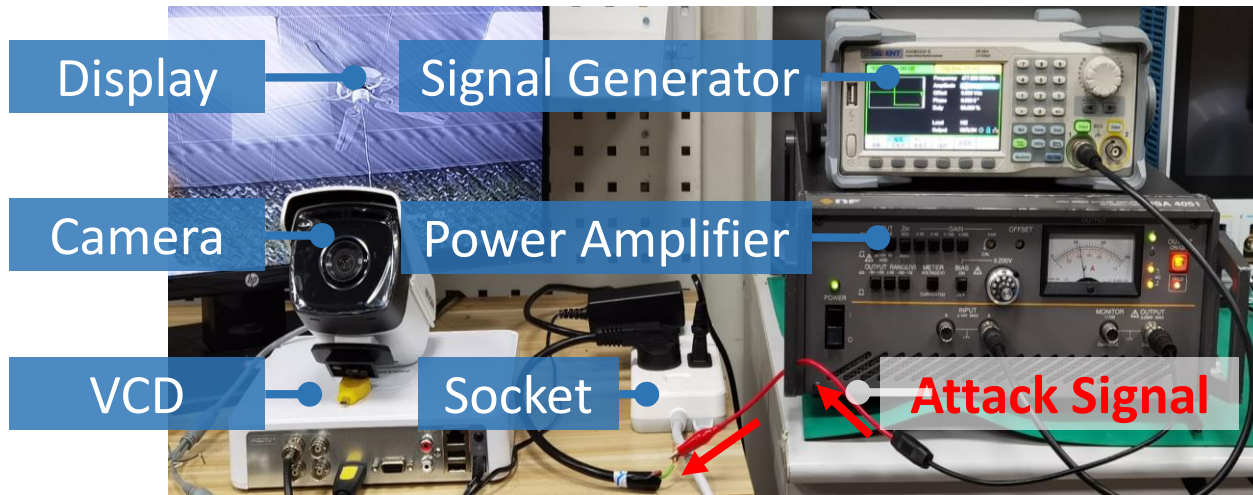


Applicable Scenes



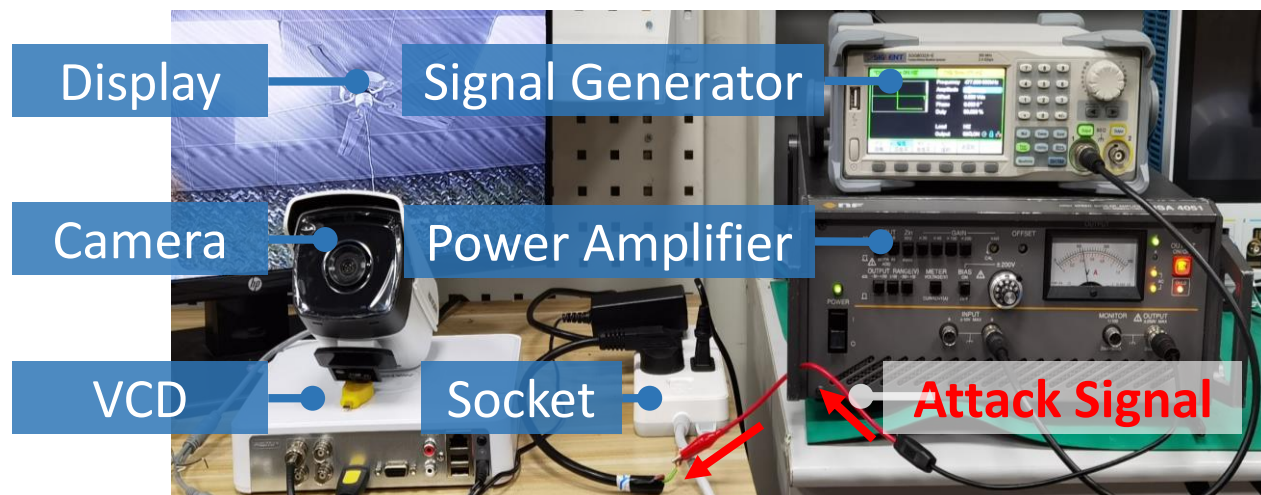
Evaluation — Surveillance Camera

- Attack against **surveillance system** to bypass detection.



Evaluation — Surveillance Camera

- Attack against **surveillance system** to bypass detection.



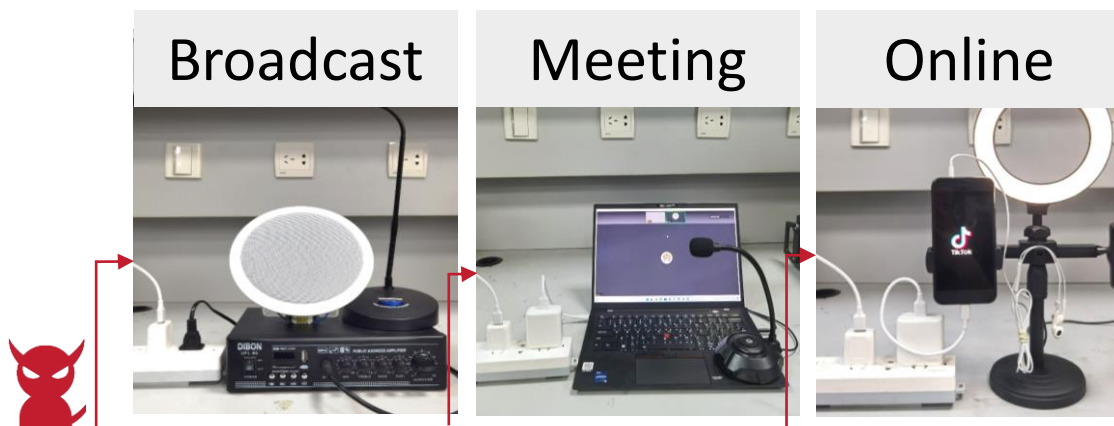
Experimental Setup



**Fail to
detect
the
intruder**

Evaluation — Broadcast Microphone

- Attack against **broadcast system** to inject malicious audios.



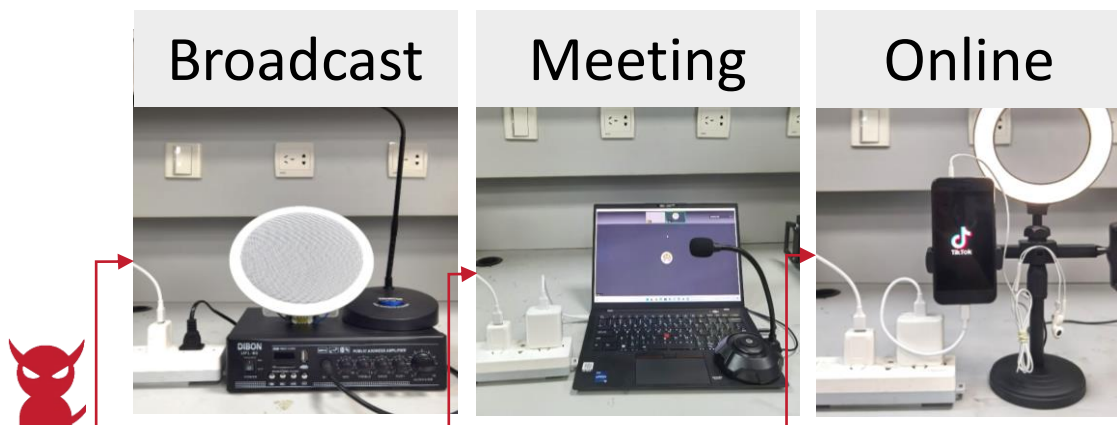
Attack Signal



Experimental Setup

Evaluation — Broadcast Microphone

- Attack against **broadcast system** to inject malicious audios.



Attack Signal



Experimental Setup



In-room attack

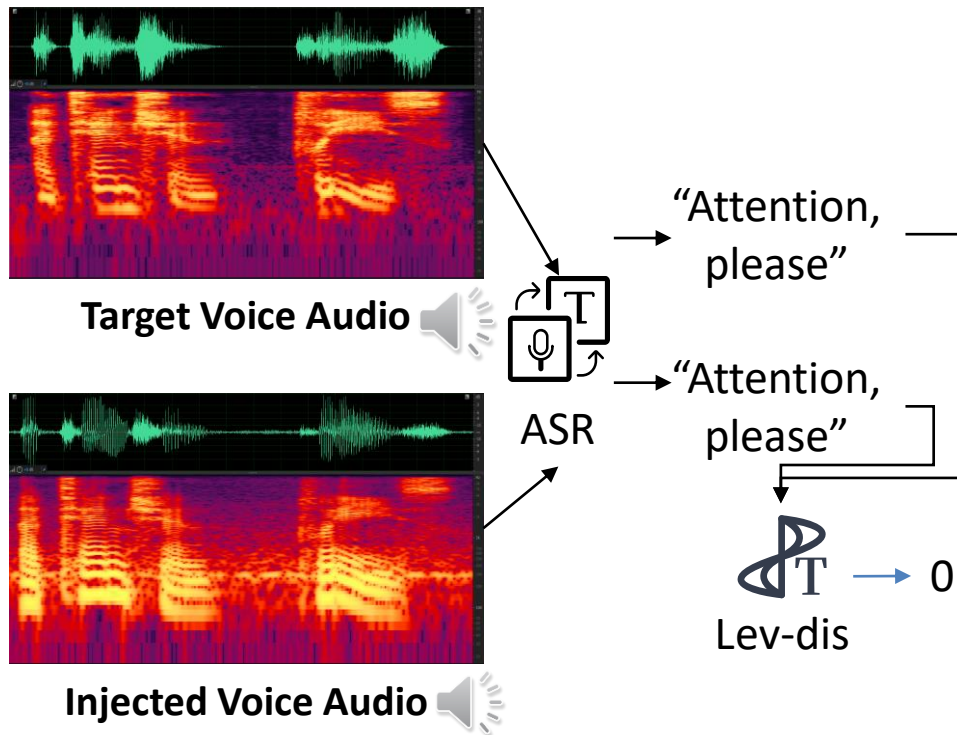


Across-room attack

Evaluation — Broadcast Microphone



- Audio complexity evaluation



#	Voice Commands	Scenarios	BL	W2V	L-dis
1	“Keep your phone switched off”	Airport	0.73	0.63	0
2	“Flight will arrive at platform”	Airport	0.84	0.60	13
3	“Attention, please”	Fire alarm	0.79	0.69	0
4	“Fire alarm activated”	Fire alarm	0.82	0.54	7
5	“Please evacuate the building”	Market	0.83	0.65	0
6	“Deadline is approaching”	Office	0.82	0.62	0
7	“Stay indoors”	Weather	0.85	0.63	0
8	“Tomorrow will have showers”	Weather	0.50	0.58	2

Examples:



#1



#3



#5



#6

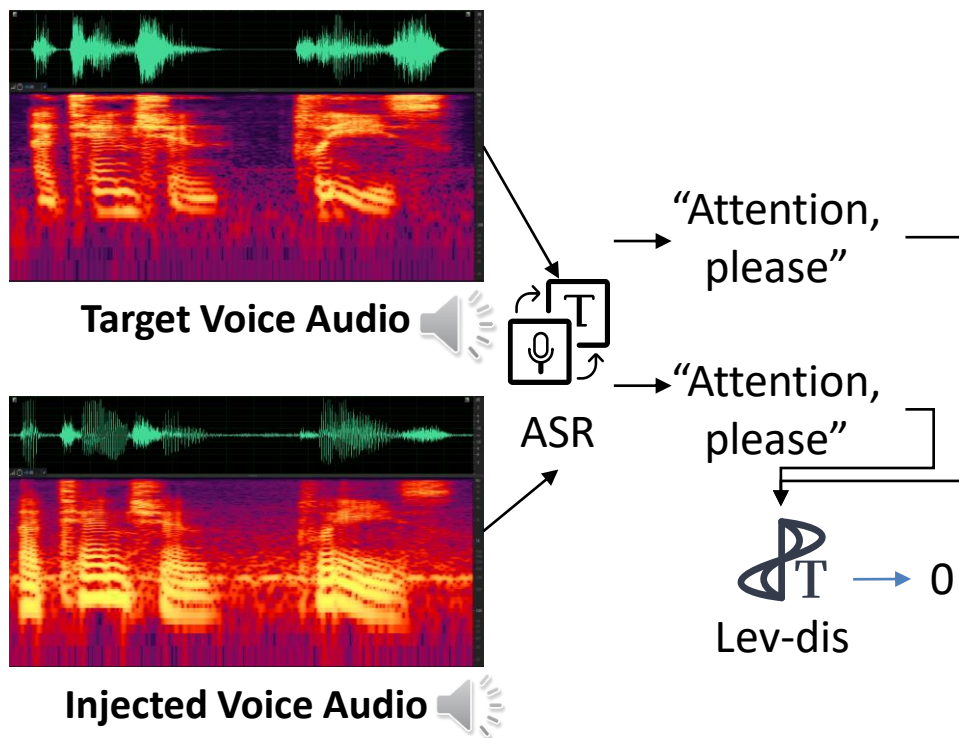


#7

Evaluation — Broadcast Microphone



- Audio complexity evaluation



#	Voice Commands	Scenarios	BL	W2V	L-dis
1	“Keep your phone switched off”	Airport	0.73	0.63	0
2	“Flight will arrive at platform”	Airport	0.84	0.60	13
3	“Attention, please”	Fire alarm	0.79	0.69	0
4	“Fire alarm activated”	Fire alarm	0.82	0.54	7
5	“Please evacuate the building”	Market	0.83	0.65	0
6	“Deadline is approaching”	Office	0.82	0.62	0
7	“Stay indoors”	Weather	0.85	0.63	0
8	“Tomorrow will have showers”	Weather	0.50	0.58	2

Examples:

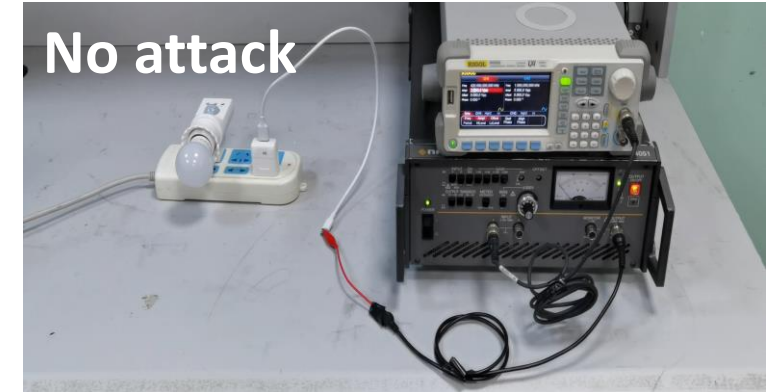


➡ *PowerRadio* can successfully inject voice audio with **accurate semantics** into the microphones and spoof the broadcast system with **varying phrases**.

Evaluation — Other Sensors

- Successfully attack against **17** common sensors.

Sensor	Models	Attack Signal		Output Signals		
		Fre.(kHz)	Amp.(Vpp)	Normal	Attack	Dev.(%)
Light	CGMCU101	120	180	929	1024	10.2
Mic.	LM386	100	300	0.371	1.37	269.3
	MAX4466	0.15	300	0.17	0.59	247.1
	MK519	500	300	0.01	0.78	7700.0
	TDA1308	150	280	53	58	9.4
	EG8542	370	300	13	155	1092.3
	CJMCU622	170	300	500	690	38.0
	MAX9814	220	230	235	280	19.1
Encoder	E6B2	380	300	2066	15000	626.04
	GMR	350	210	129	660	411.63
	ABS	250	300	10	320	3100.00
Shock	SW18010P	27	300	0	1	100.00
Distance	HCSR04	306	300	153	0	100.00
	HCSR05	90	300	0	1	100.00
Water	LM393	410	300	1.87	2.12	13.37
Acc.	ADXL345	49.93	280	0g	2g	100.00
Hall	Hall	160	300	2°	40°	1900.00



Motion detection sensor attack

Evaluation — Other Factors

- Electric factors in a household system

Local Household Wiring System (*front&back view*)



Electric Factors		L-distance
Breakers		0
Type of wiring	1.5m2	0
	2.5m2	0
	4m2	0
Electrical noise	1 bulb	0
	3 bulbs	0
	charging phone	0
	voice assistant	0
	fan	0
	desktop	0
Layout of electrical system	in-room	0
	cross-wall	0
	cross-room	0
Distances	5m	0
	10m	0
	15m	0

Evaluation — Other Factors

- Device Models

Different Microphone Models

Microphone Model	Connector	Auxiliary Device	Parameters		Inject Audio	L-dis
			fre.	amp.		
HUAWEI AM115	3.5mm	Phone	320	220	✓	0
HP DHP-1100I	3.5mm	Phone	30	300	✓	1
Lenovo Lecoo MC01	3.5mm	Phone	315	290	✓	0
UGREEN CM564	USB	Phone	31	280	✓	13
SM88	XLR	UFL-60	320	300	✓	0
TAKSTAR MS-118	XLR	UFL-60	320	260	✓	0
HIKVISION DS-KAU30HG-M	XLR	UFL-60	320	250	✓	0

Different Camera Models

Camera Model	Parameters		Inject Stripe	Success	
	fre.	amp.		Facenet	Yolov8
HIKVISION DS-2CE56C3T-IT3	478	140	✓	99.0%	100.0%
HIKVISION DS-2CE16G0T-IT3	477.9	170	✓	98.5%	100.0%
DH-HAC-HFW1200M-I2	450.2	150	✓	89.1%	100.0%
Panasonic WV-CW314LCH	485.3	270	✓	59.7%	75.5%
SAMSUNG SCO-2080RP	411.2	310	✓	88.2%	100.0%
SONY CCD673-1200	468.6	200	✓	89.7%	93.1%
SONY CCD-1200	453	200	✓	98.6%	100.0%
SONY IMX323	506.2	120	✓	97.4%	100.0%



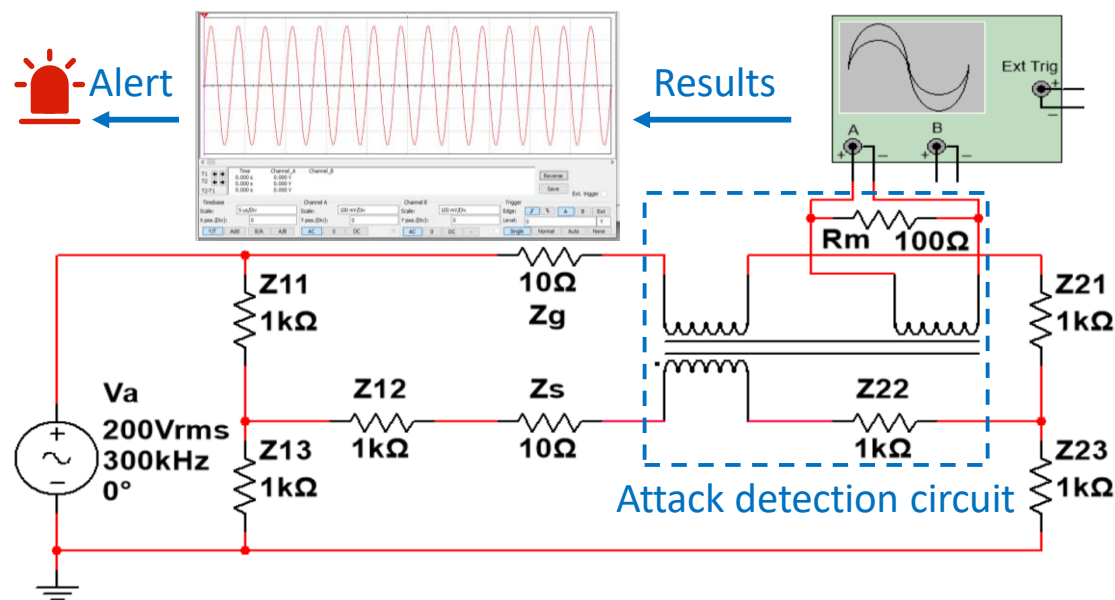
PowerRadio can successfully manipulate sensors with **various models**.

Countermeasures

□ Detection Methods

Detect the attack signal by using an auxiliary circuit and alert the users.

- Use a **3-phase common-mode choke** (3P CMC) to deattenuate and detect the CM noise.

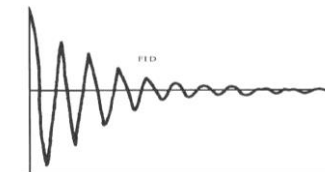


□ Prevention Methods

Prevent attackers to conduct attacks by **increasing** the attack **overhead and difficulty**.

• Signal Attenuation

- Filter
- Shielding



• Predictability Reduction

- Random time delay
- Random sampling



• Structure Optimization

- Symmetric circuits
- Balanced impedance



Conclusion

- Proposed *PowerRadio*, a new **sensor manipulation attack** by injecting attack signals via a GND cable, without line-of-sight and distance limitation.

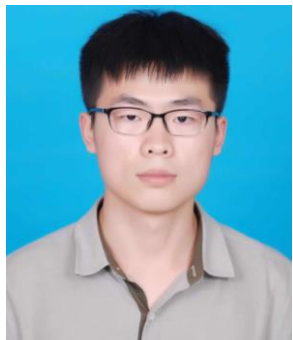
Conclusion

- Proposed *PowerRadio*, a new **sensor manipulation attack** by injecting attack signals via a GND cable, without line-of-sight and distance limitation.
- Analyzed the **underlying principle** of **energy conversion** and successful sensor measurement manipulation theoretically and experimentally.

Conclusion

- Proposed *PowerRadio*, a new **sensor manipulation attack** by injecting attack signals via a GND cable, without line-of-sight and distance limitation.
- Analyzed the **underlying principle** of **energy conversion** and successful sensor measurement manipulation theoretically and experimentally.
- Validated the **feasibility** of *PowerRadio* on **33** common sensors and **2** types of commercial sensor systems, and proposed **countermeasures** to mitigate the threat.

Thank You !



Corresponding authors: xji@zju.edu.cn



USSLAB Website: www.usslab.org



浙江大學
ZHEJIANG UNIVERSITY



PEKING
UNIVERSITY