浙江大学
ZHEJIANG UNIVERSITY

ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters

Fengchen Yang, Zihao Dan, Kaikai Pan, Chen Yan, Xiaoyu Ji, Wenyuan Xu

Zhejiang University, ZJU QI-ANXIN IoT Security Joint Lab

智能系统安全实验室
UBIQUITOUS SYSTEM SECURITY LAB.

Power inverter

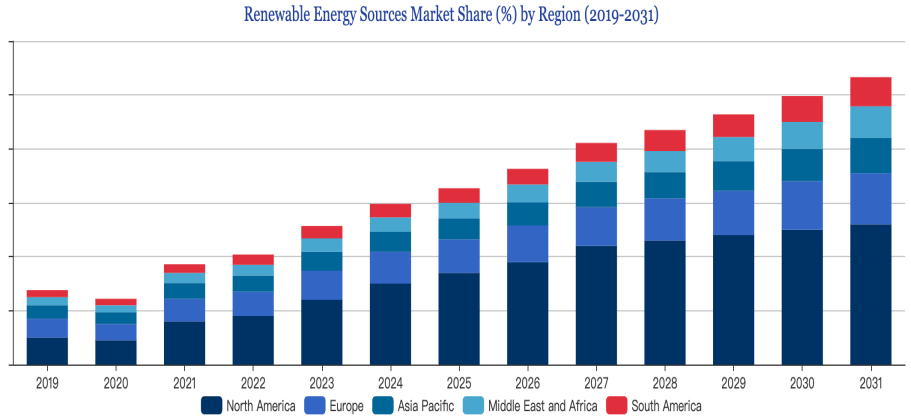
- Renewable energy has gradually replaced traditional energy and will expand at a compound annual growth rate (CAGR) of **17.20%**.[1]

Global climate challenge

Power inverter

- Renewable energy has gradually replaced traditional energy and will expand at a compound annual growth rate (CAGR) of **17.20%**.[1]

Global climate challenge

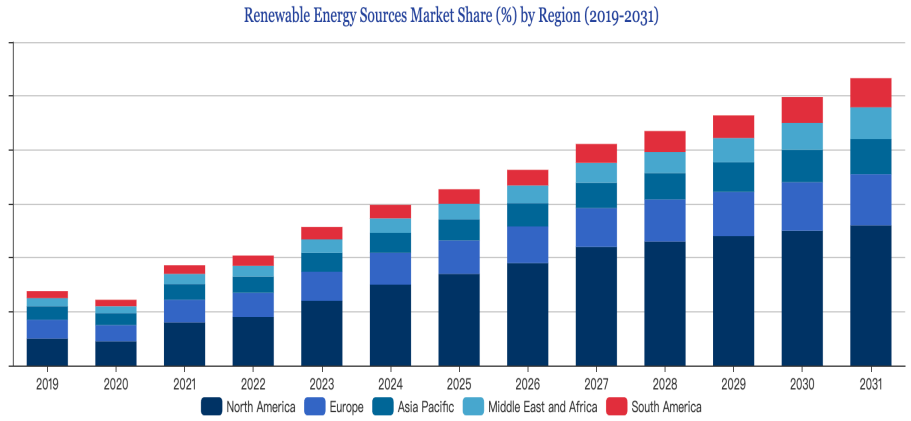


Renewable energy

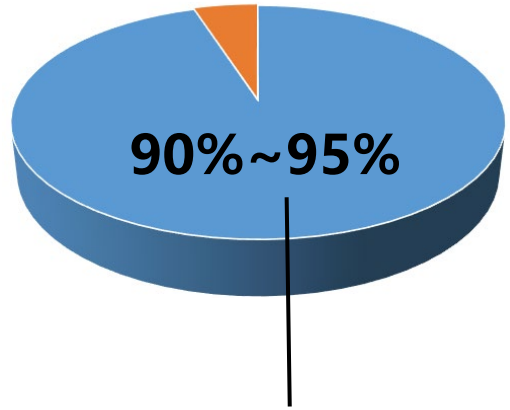
Power inverter

- Renewable energy has gradually replaced traditional energy and will expand at a compound annual growth rate (CAGR) of **17.20%**.[1]

Global climate challenge



Renewable energy



Cannot be fed into the grid

Most renewable energy (RES) **cannot** be directly fed into the grid

Power Inverter

- Transform the DC power from renewable energy to the AC power on the grid

Solar energy

Chemical energy

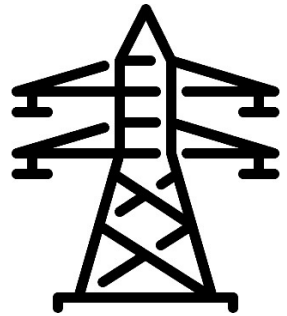
Bio-energy

Renewable energy

DC

Power inverter

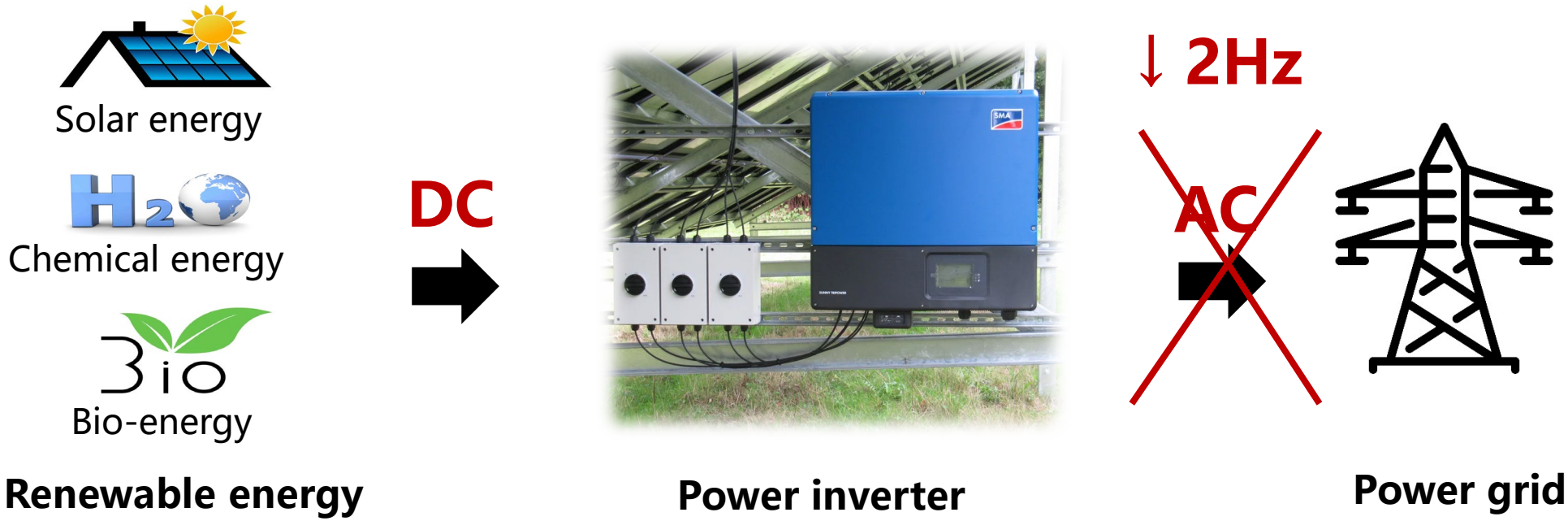
AC



Power grid

Power Inverter

- Transform the DC power from renewable energy to the AC power on the grid



Motivation and Threat model

- **Attack goal:** Shut down, power reduction, or even burnout

Motivation and Threat model

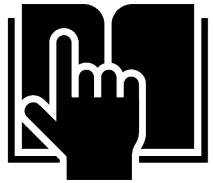
- **Attack goal:** Shut down, power reduction, or even burnout

- **Non-contact Access:** No touch or physical damage

Motivation and Threat model

- **Attack goal:** Shut down, power reduction, or even burnout

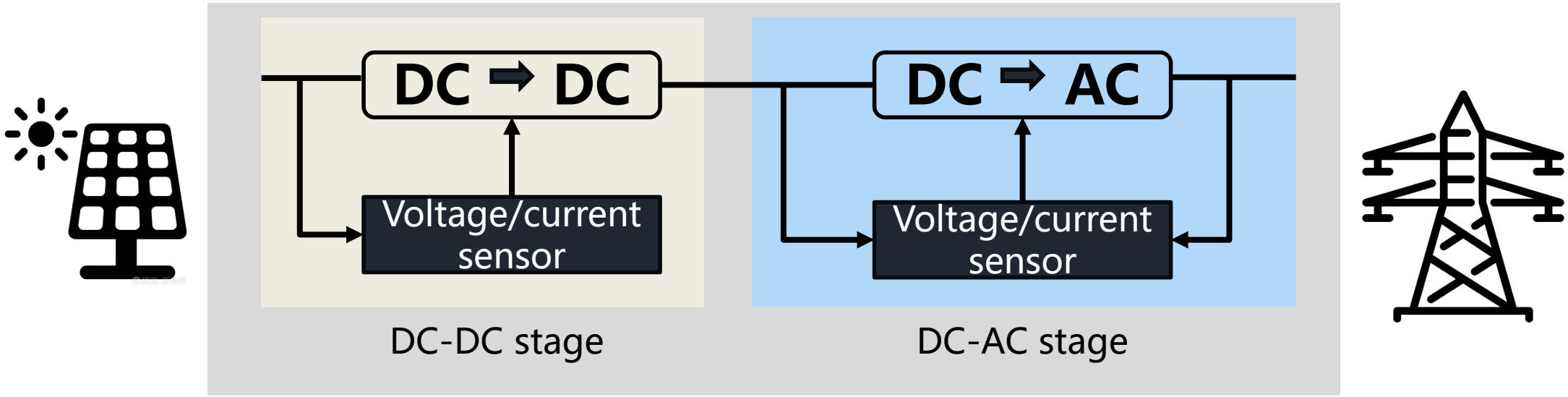
- **Non-contact Access:** No touch or physical damage



- **Prior Knowledge:** Prior knowledge of the target inverter

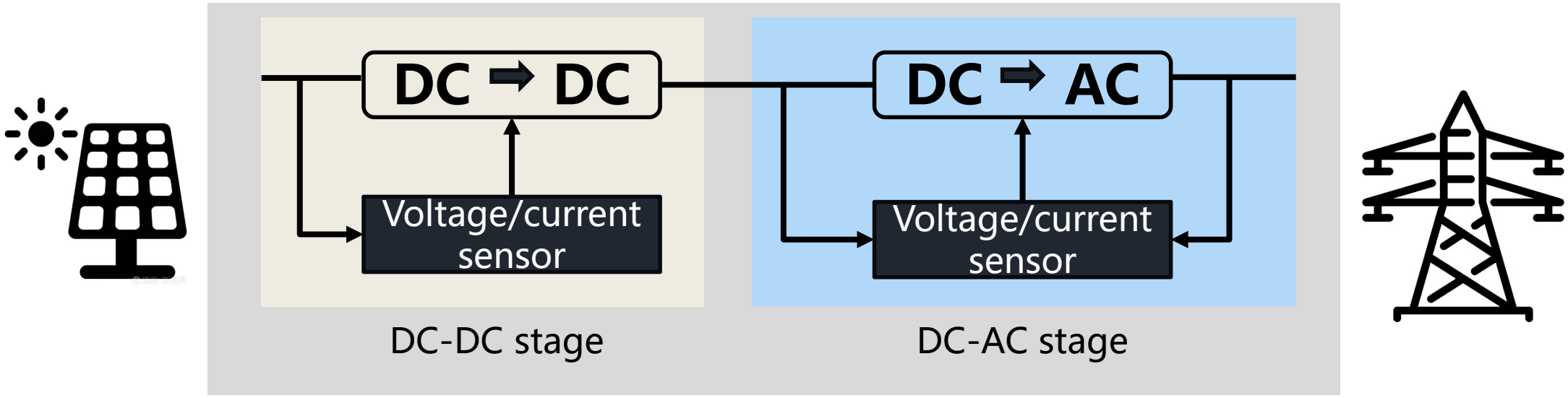
How does power inverter work?

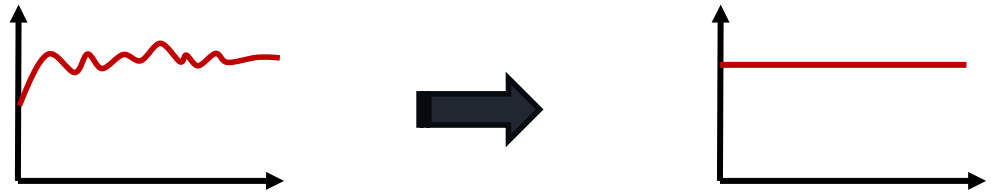
- Work principle



How does power inverter work?

- Work principle



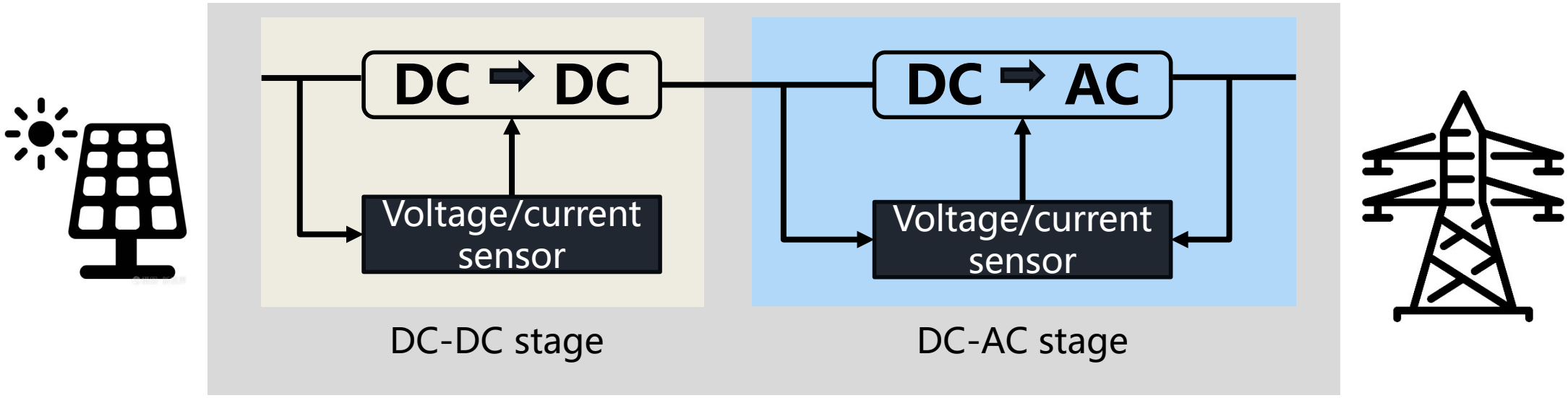


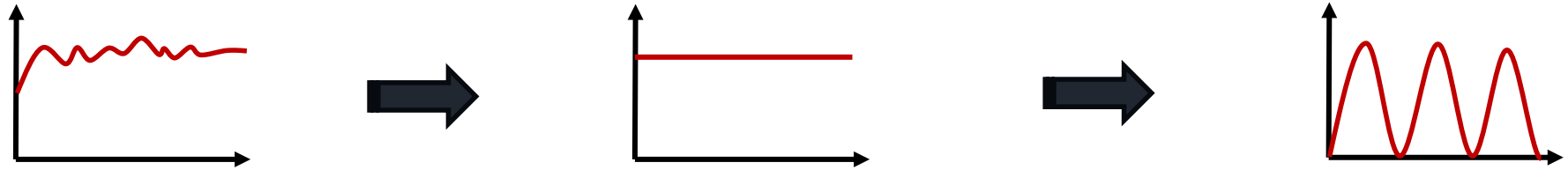
Input voltage (Substandard)

Bus voltage (**Standard** DC)

How does power inverter work?

- Work principle





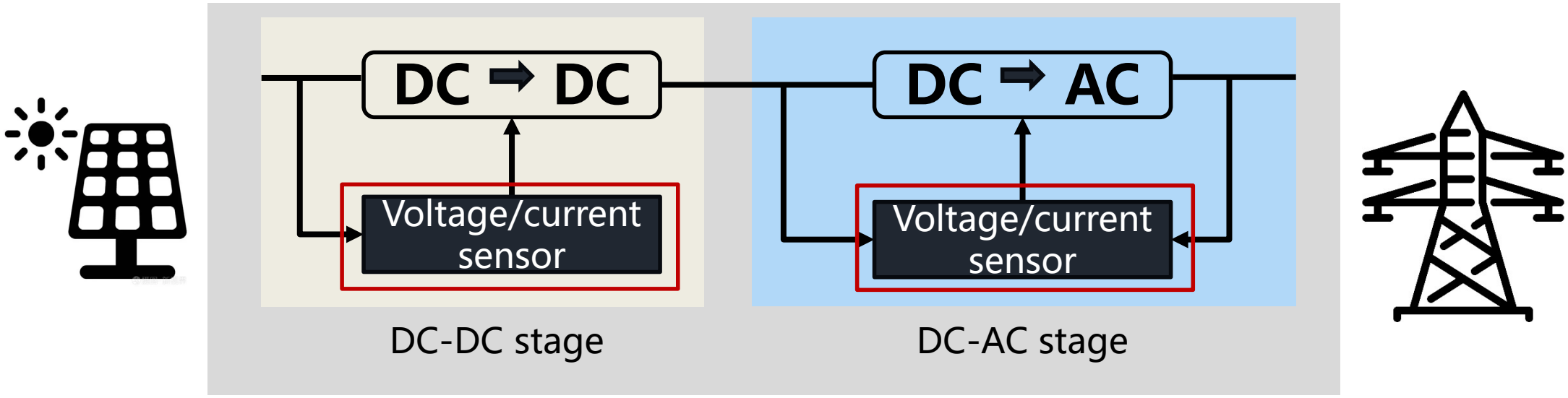
Input voltage (Substandard)

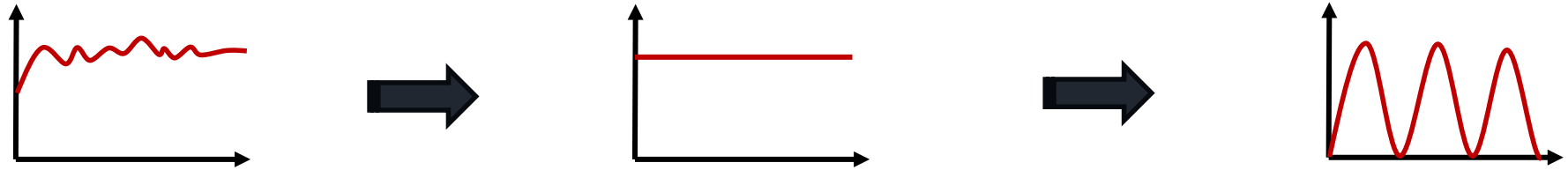
Bus voltage (**Standard** DC)

Output voltage (**Standard** AC)

How does power inverter work?

- Work principle





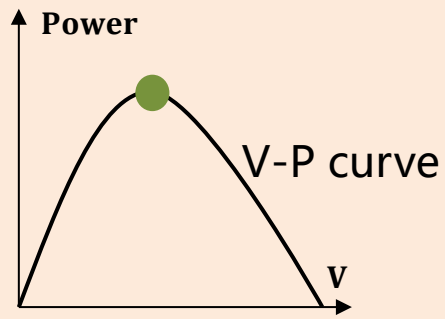
Input voltage (Substandard)

Bus voltage (**Standard** DC)

Output voltage (**Standard** AC)

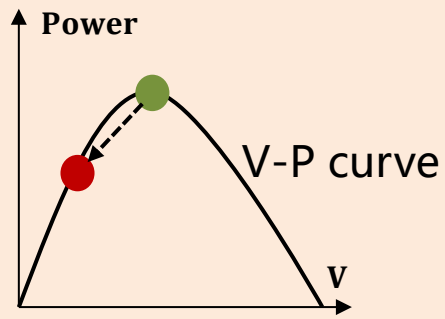
What if sensor goes wrong?

Input control



What if sensor goes wrong?

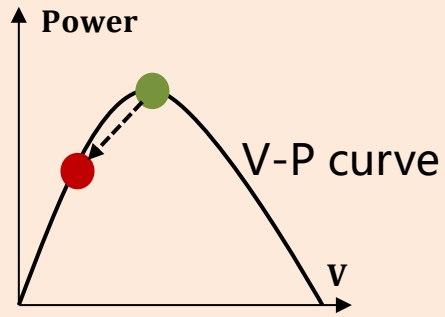
Input control



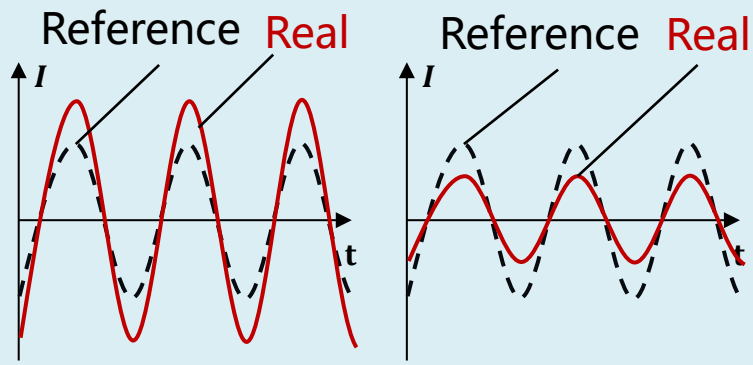
1. Damping

What if sensor goes wrong?

Input control



Output control

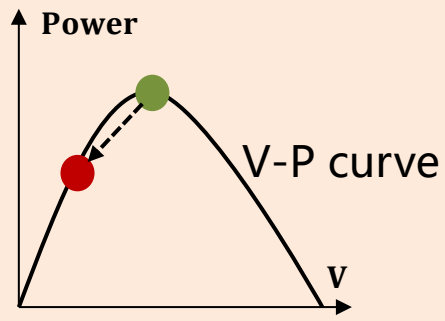


1. Damping

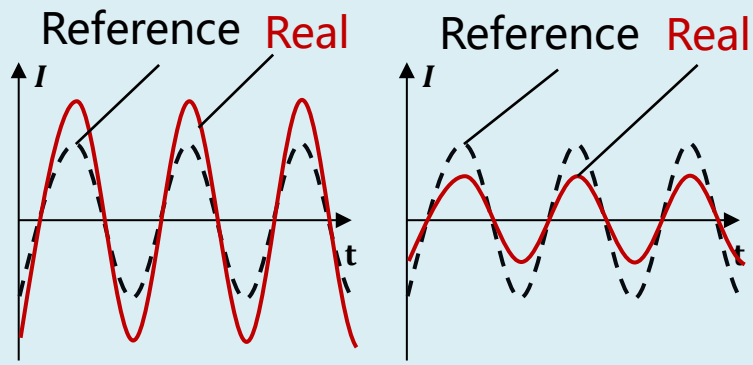
3. DoS

What if sensor goes wrong?

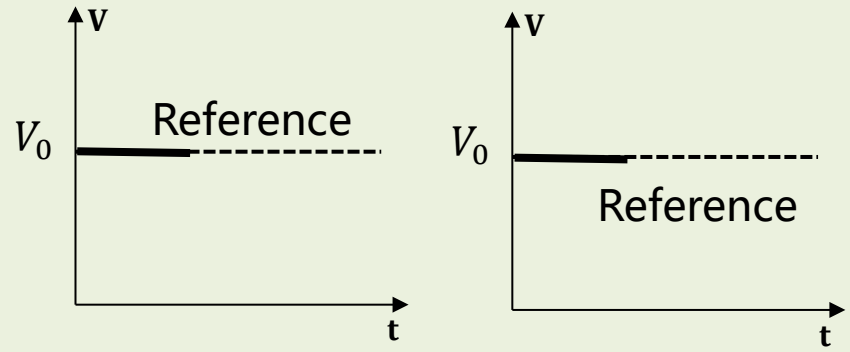
Input control



Output control



Bus voltage control

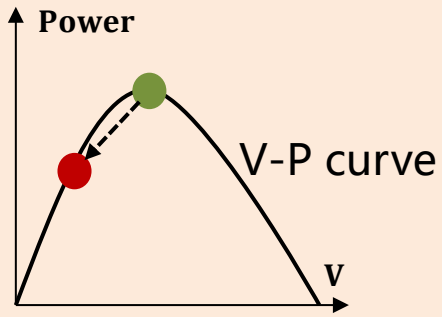


1. Damping

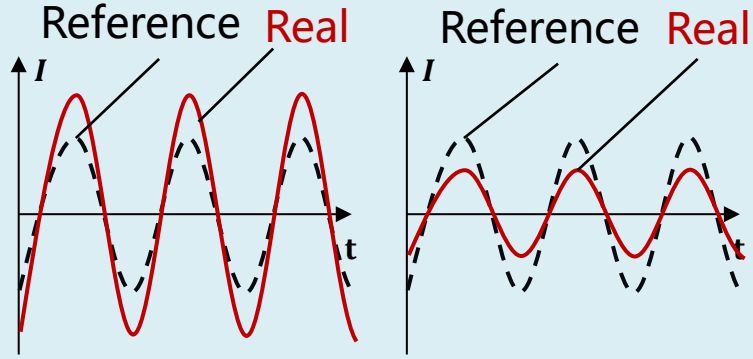
3. DoS

What if sensor goes wrong?

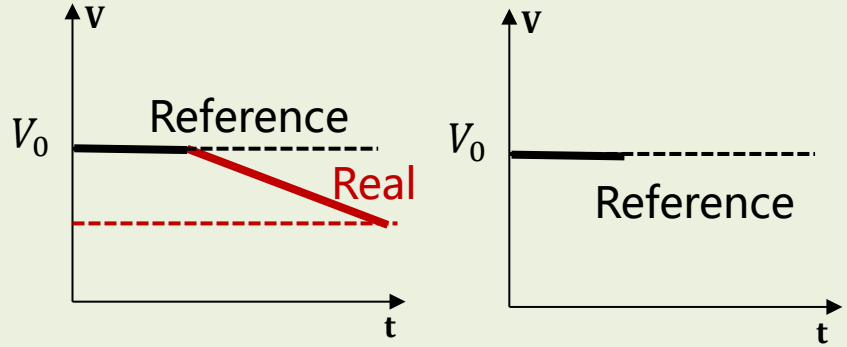
Input control



Output control



Bus voltage control

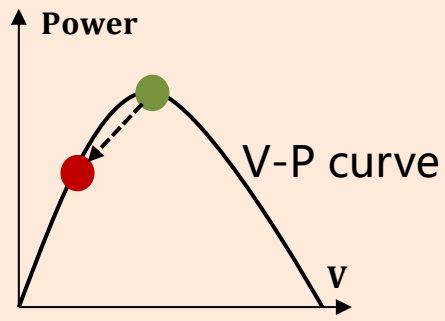


1. Damping

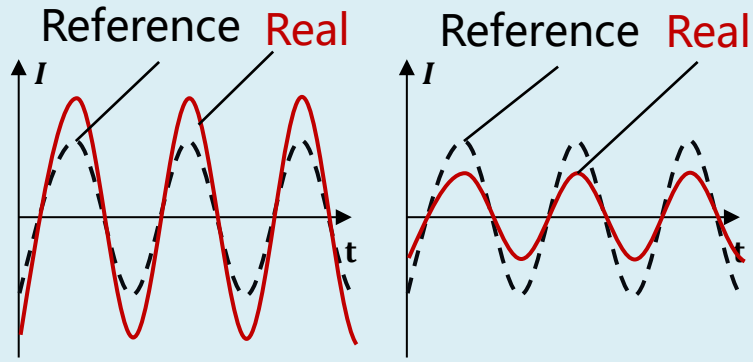
3. DoS

What if sensor goes wrong?

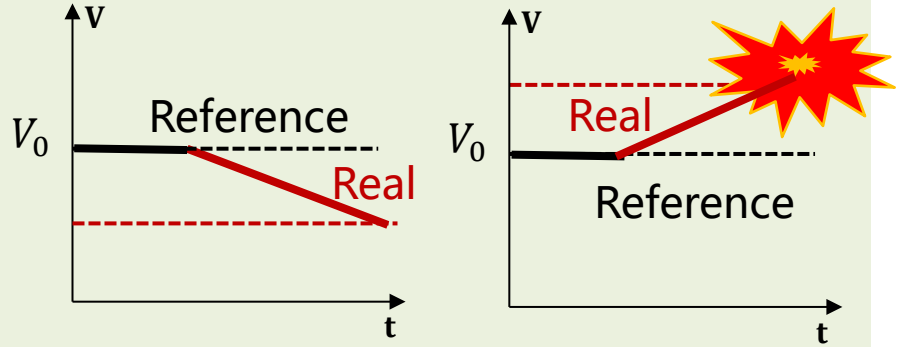
Input control



Output control



Bus voltage control



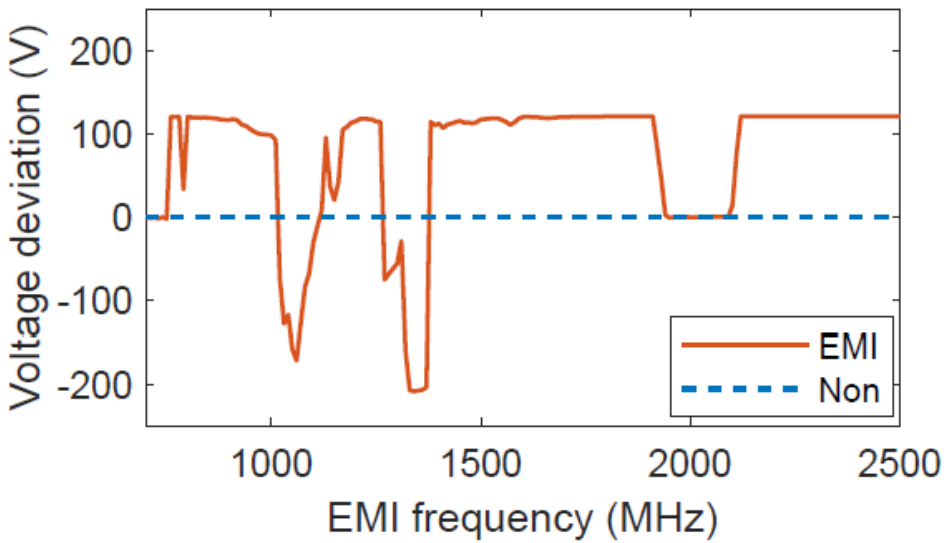
1. Damping

3. DoS

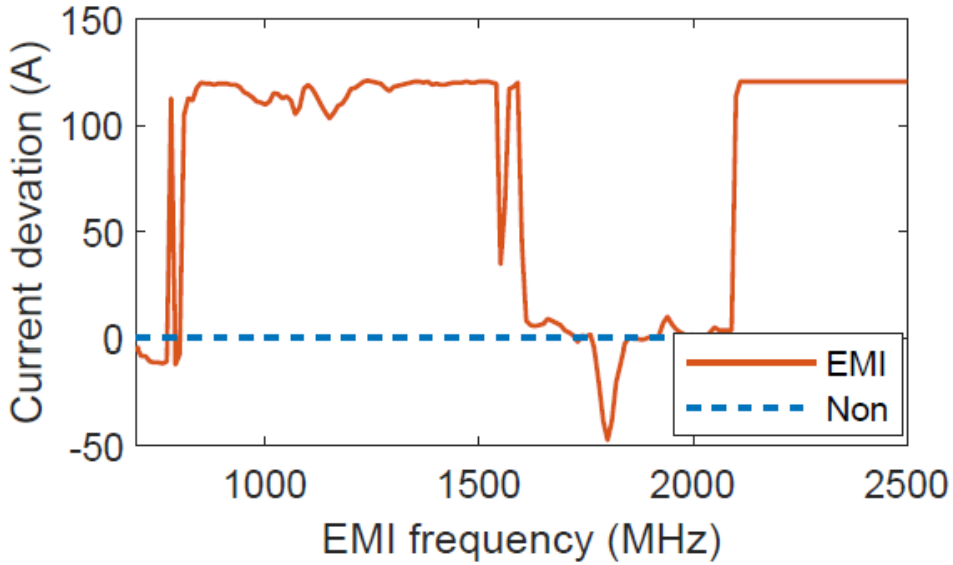
2. Damage

Whether EMI can impact sensors?

- Frequency sweep test



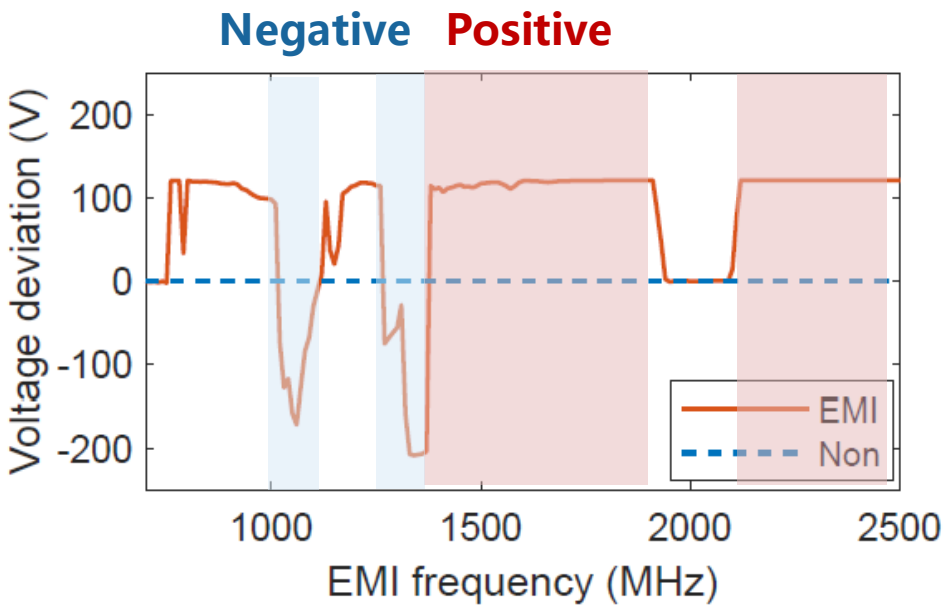
Voltage sensor



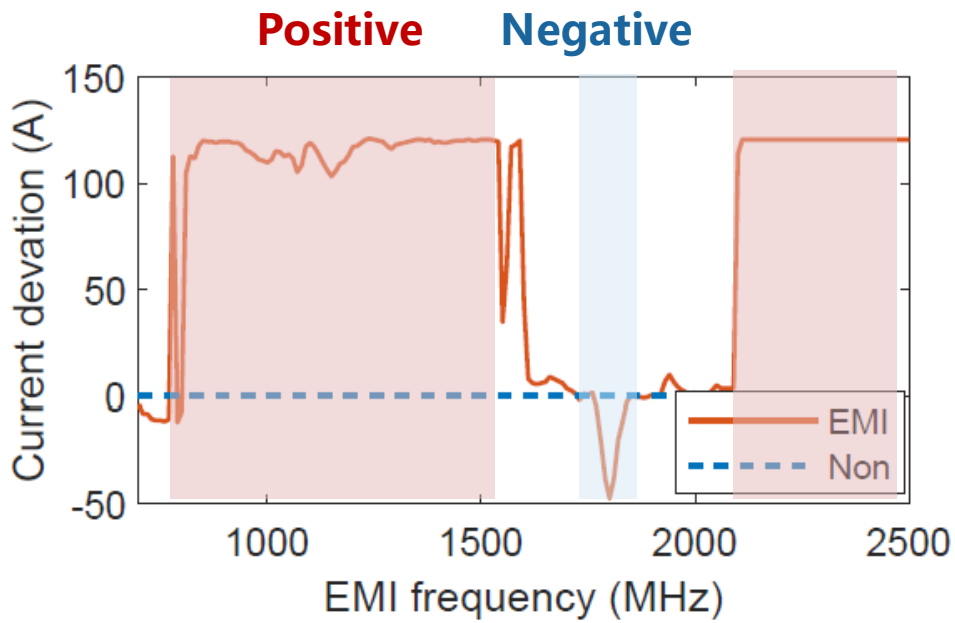
Current sensor

Whether EMI can impact sensors?

- Frequency sweep test



Voltage sensor



Current sensor

EMI can cause **positive** or **negative** offset on both **voltage and current** sensors

Questions

- Q1: Why does the injected **AC** noise induce a **DC** offset ?

Questions

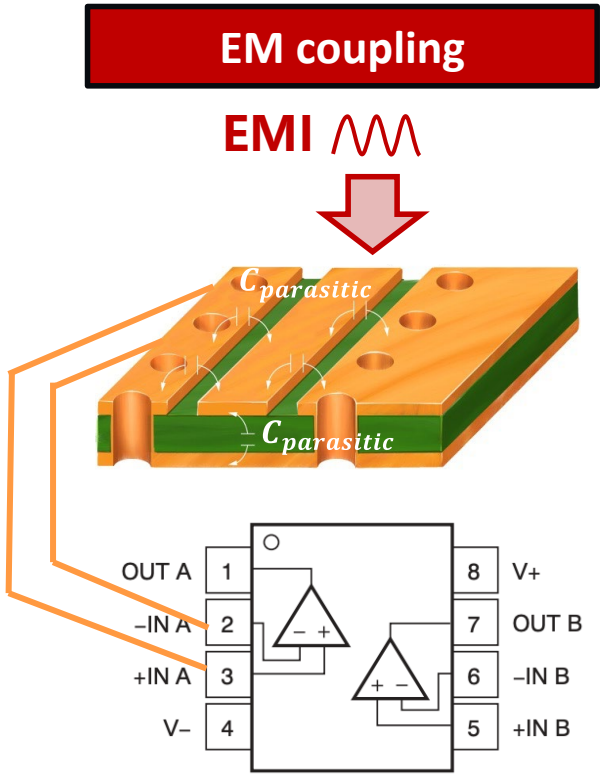
- Q1: Why does the injected **AC** noise induce a **DC** offset ?
- Q2: Why does the offset can be **positive** or **negative** ?

Questions

- Q1: Why does the injected **AC** noise induce a **DC** offset ?
- Q2: Why does the offset can be **positive** or **negative** ?
- Q3: How to achieve **controllable** manipulation ?

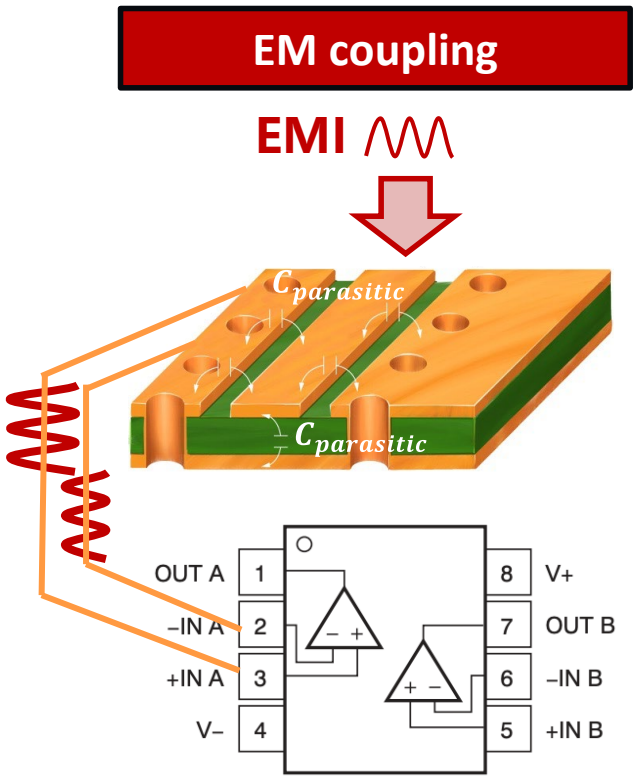
Q1: Why does the **AC** noise induce a **DC** offset?

- Voltage sensor



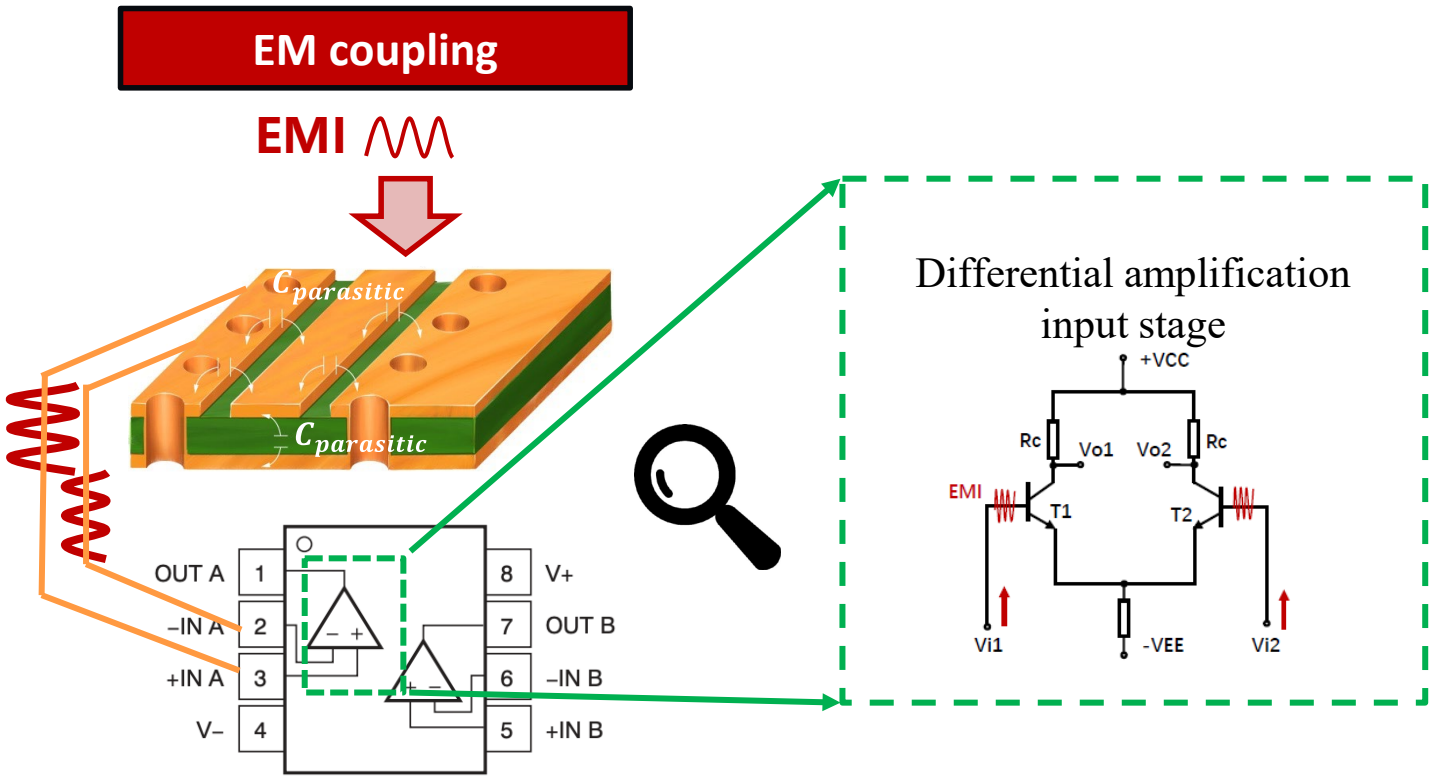
Q1: Why does the **AC** noise induce a **DC** offset?

- Voltage sensor



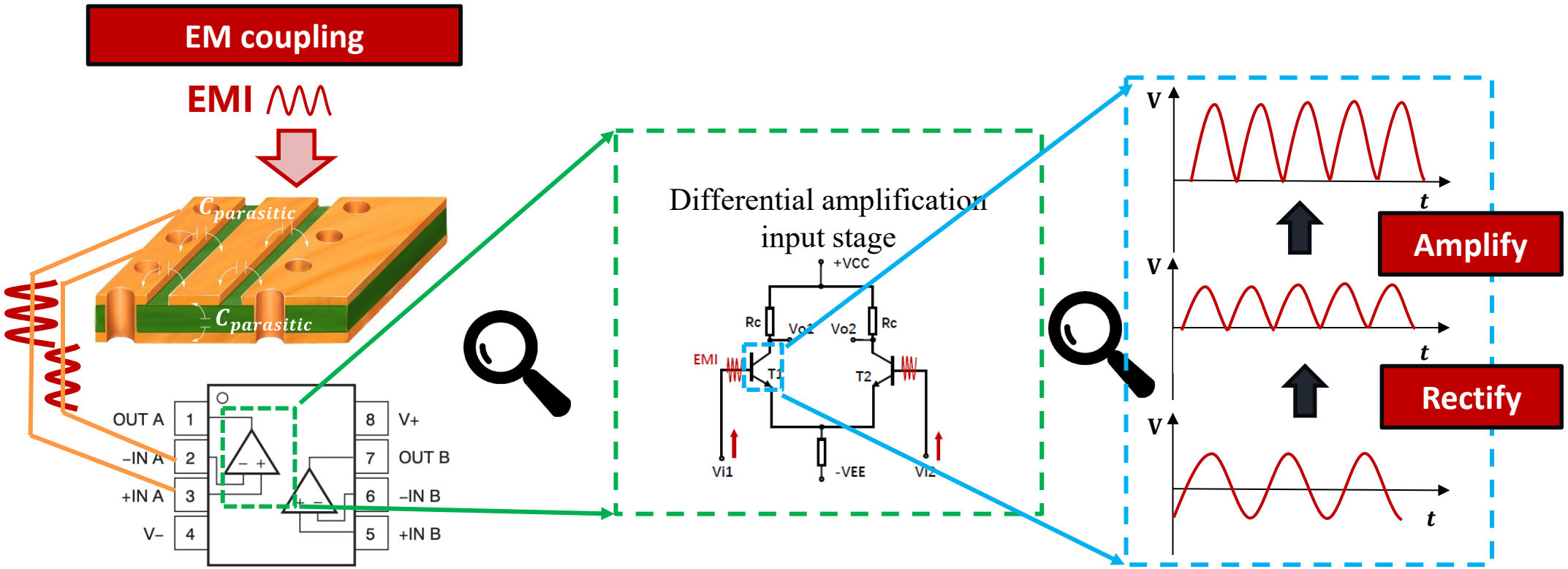
Q1: Why does the **AC** noise induce a **DC** offset?

- Voltage sensor



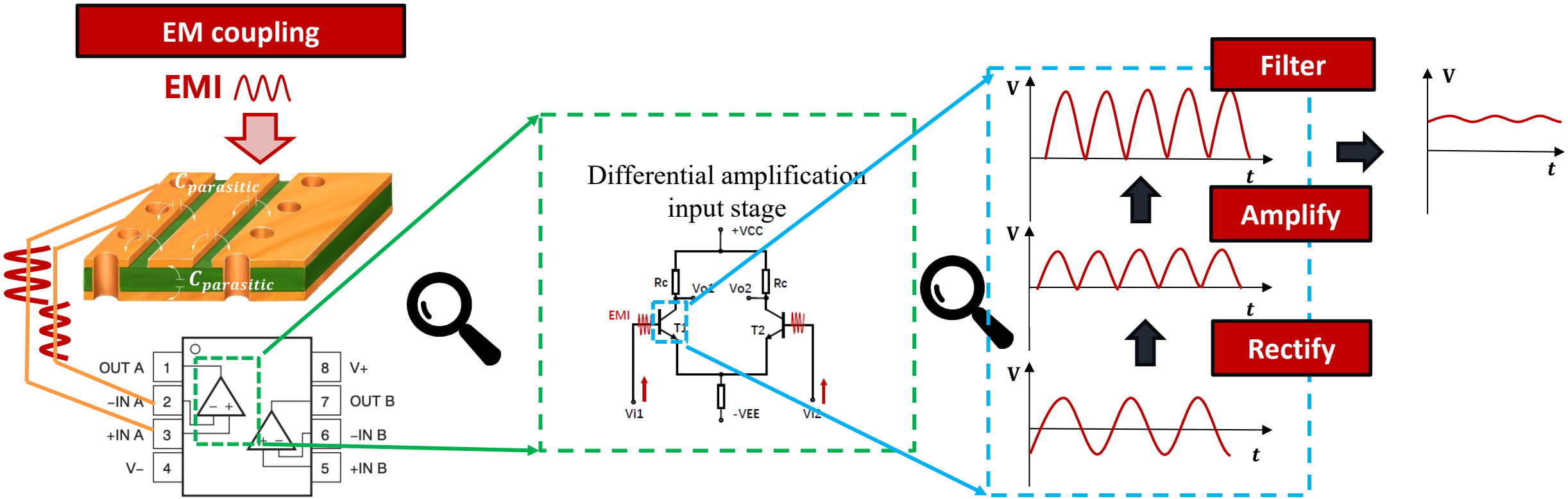
Q1: Why does the **AC** noise induce a **DC** offset?

- Voltage sensor



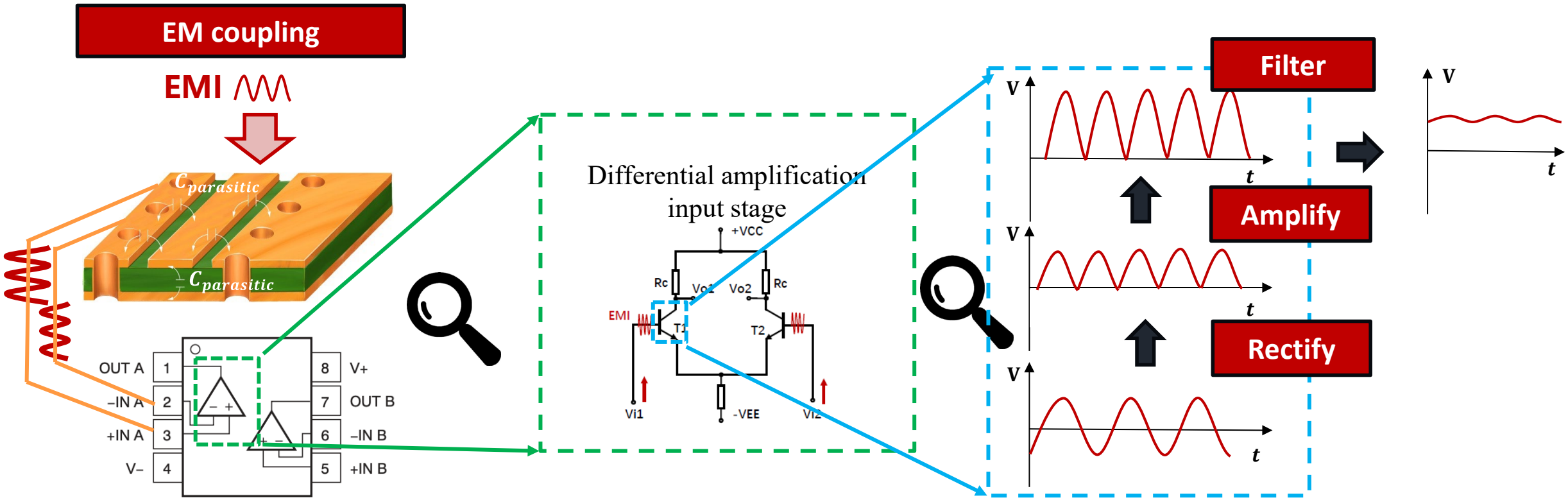
Q1: Why does the **AC** noise induce a **DC** offset?

- Voltage sensor



Q1: Why does the **AC** noise induce a **DC** offset?

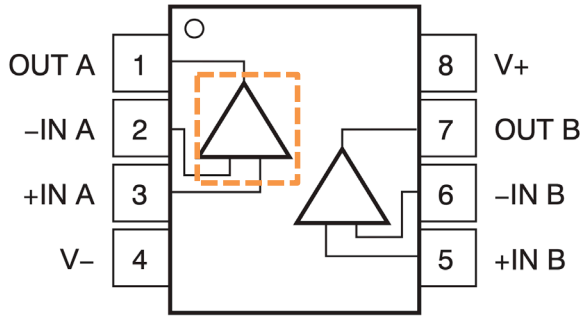
- Voltage sensor



The **operational amplifier** converts the **AC** noise into **DC** offset !

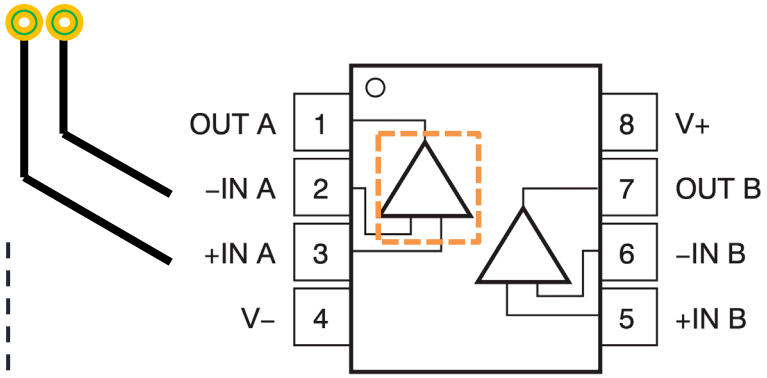
Q2: Why does the offset can be **positive** or **negative**?

- Operational amplifier



Q2: Why does the offset can be **positive** or **negative**?

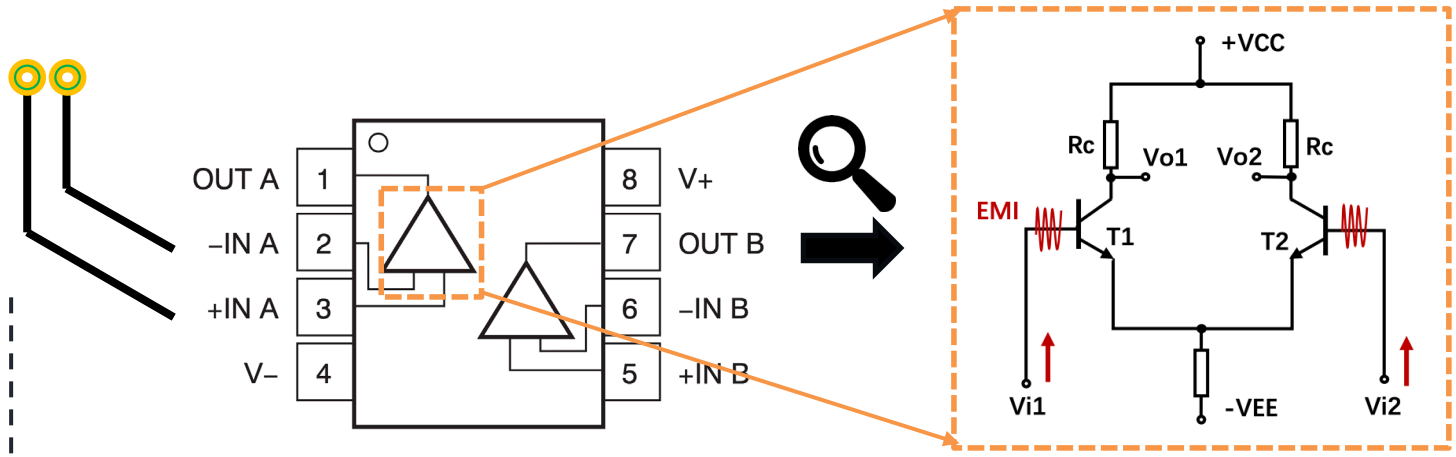
- Operational amplifier



Different **length** ⇒ **Different** **frequencies**

Q2: Why does the offset can be **positive** or **negative**?

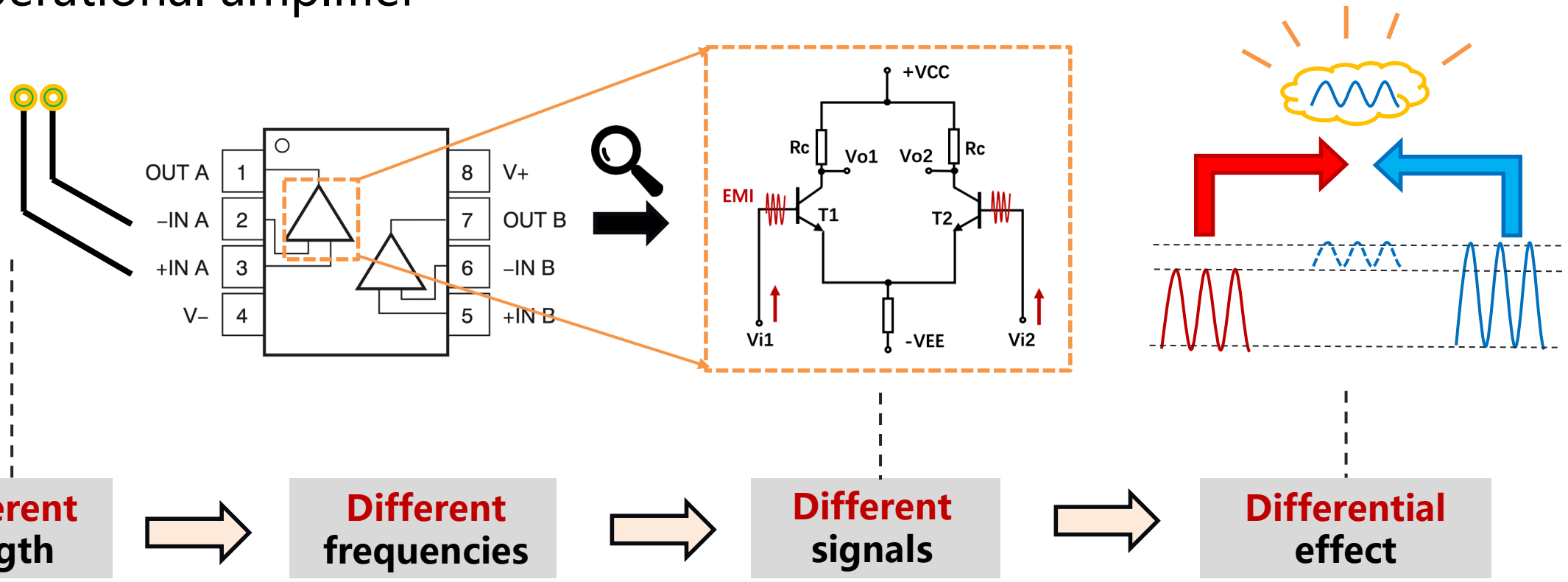
- Operational amplifier



Different length → **Different frequencies** → **Different signals**

Q2: Why does the offset can be **positive** or **negative**?

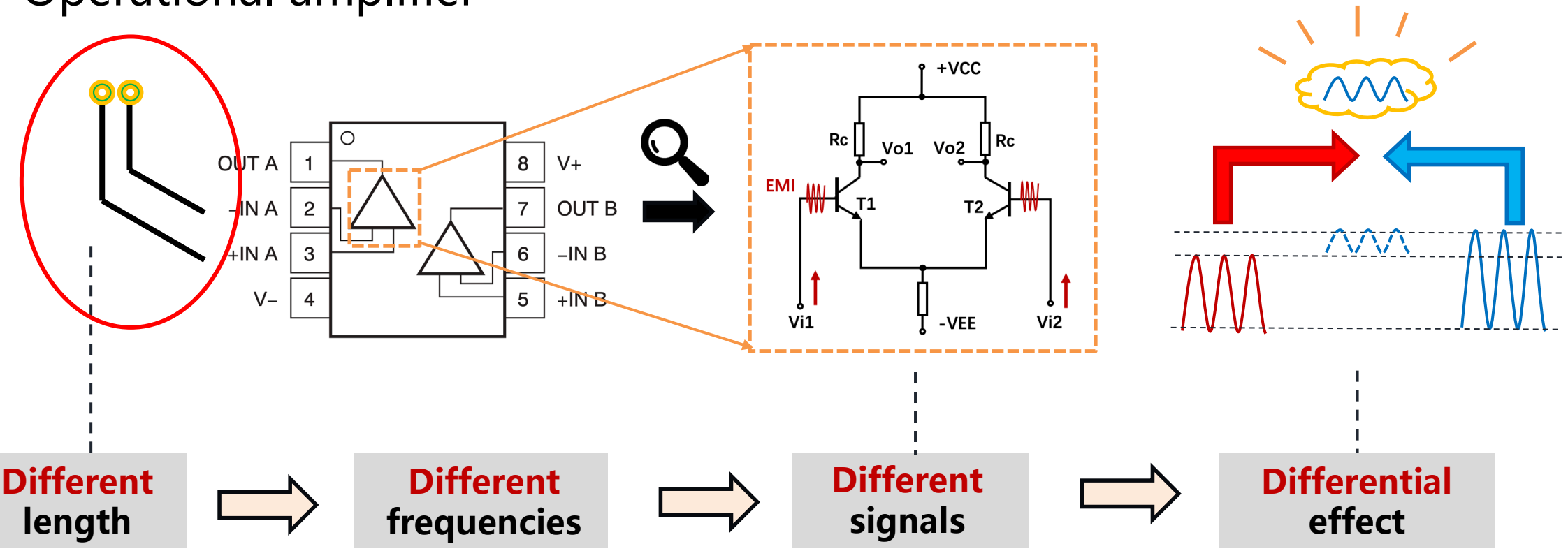
- Operational amplifier



Different length → **Different frequencies** → **Different signals** → **Differential effect**

Q2: Why does the offset can be **positive** or **negative**?

- Operational amplifier



Different length → **Different frequencies** → **Different signals** → **Differential effect**

The **asymmetric layout** enables the offset to be positive or negative!

Q3: How to control sensors?

- Amplitude modulation

$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t$$

Amplitude — Modulated signal — Carrier frequency

Q3: How to control sensors?

- Amplitude modulation

$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t$$

Amplitude — Modulated signal — Carrier frequency

Sensor manipulation experiment

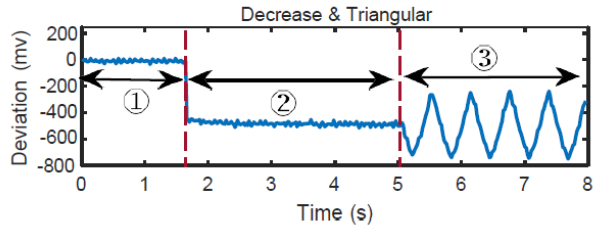
Q3: How to control sensors?

- Amplitude modulation

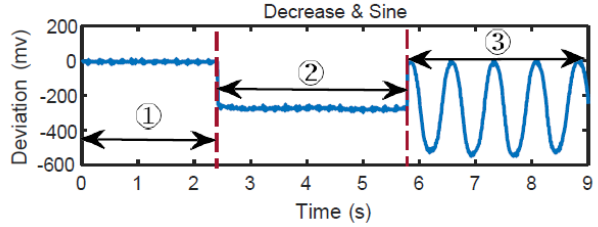
$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t$$

Amplitude — Modulated signal — Carrier frequency

Decrease → Triangular



Decrease → Sine



Sensor manipulation experiment

Q3: How to control sensors?

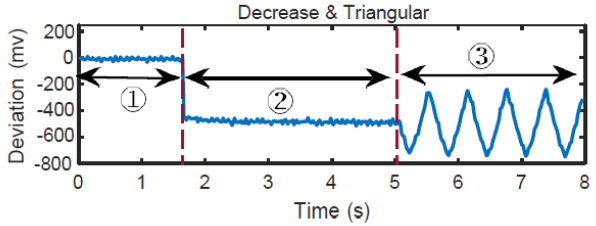
- Amplitude modulation

$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t$$

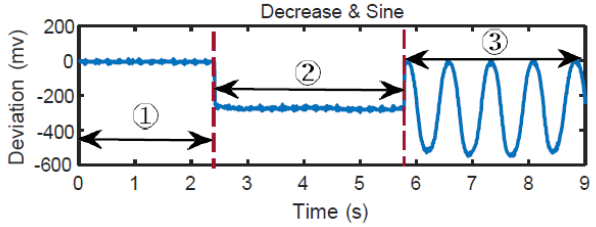
Amplitude — Modulated signal — Carrier frequency

Sensor manipulation experiment

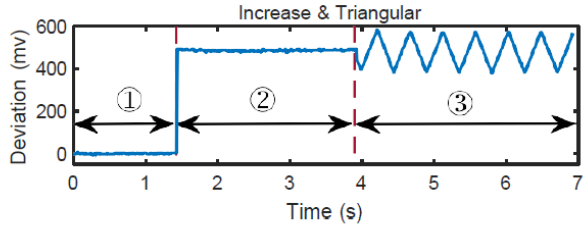
Decrease → Triangular



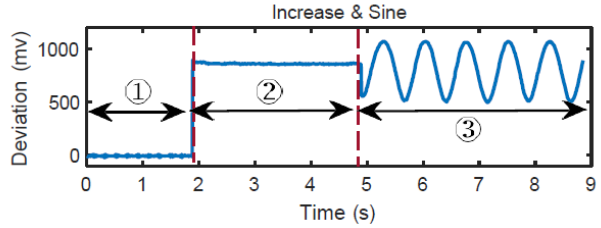
Decrease → Sine



Increase → Triangular



Increase → Sine



Q3: How to control sensors?

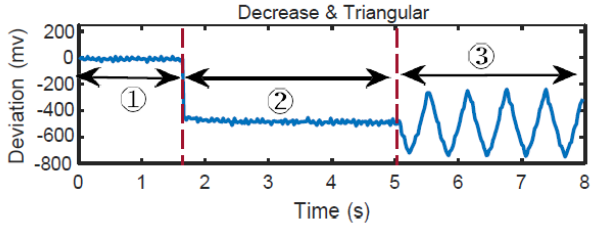
- Amplitude modulation

$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t$$

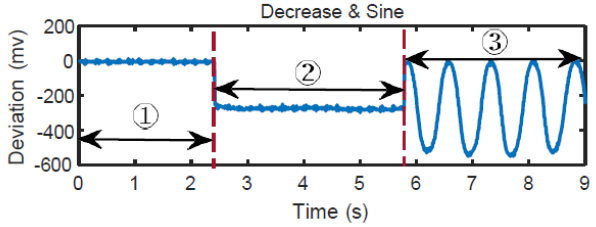
Amplitude — Modulated signal — Carrier frequency

Sensor manipulation experiment

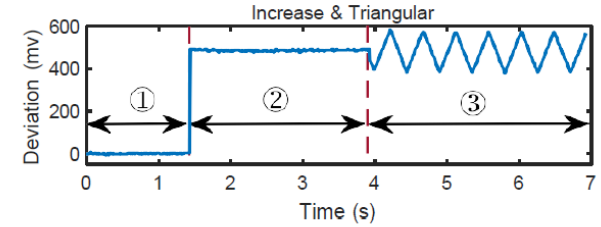
Decrease ↓ Triangular



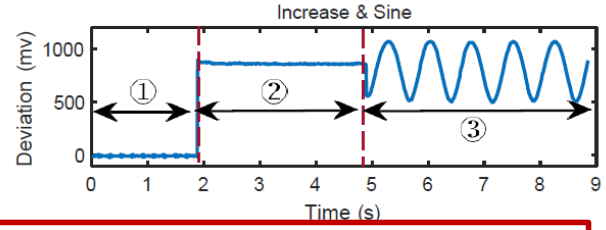
Decrease ↓ Sine



Increase ↓ Triangular



Increase ↓ Sine



The **AM** can achieve controllable manipulation on sensors!

Attack design

- **Design of DoS Attack**
- Design of Damage Attack
- Design of Damping Attack

Attack design

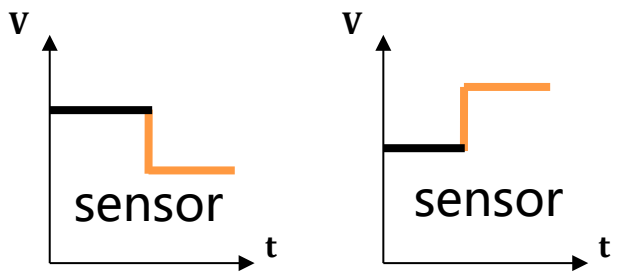
- Design of **DoS Attack**

DC side

Attack design

- Design of **DoS Attack**

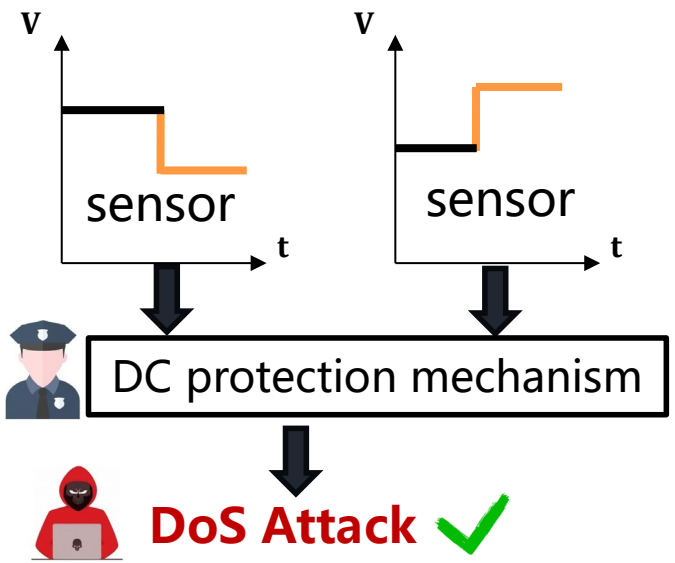
DC side



Attack design

- Design of **DoS Attack**

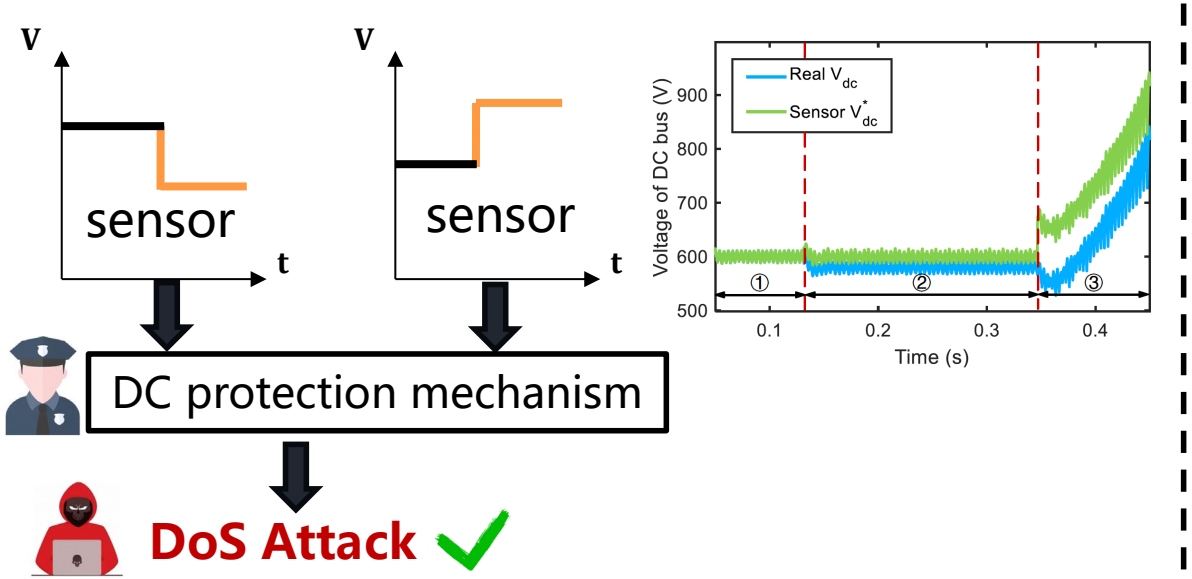
DC side



Attack design

- Design of **DoS Attack**

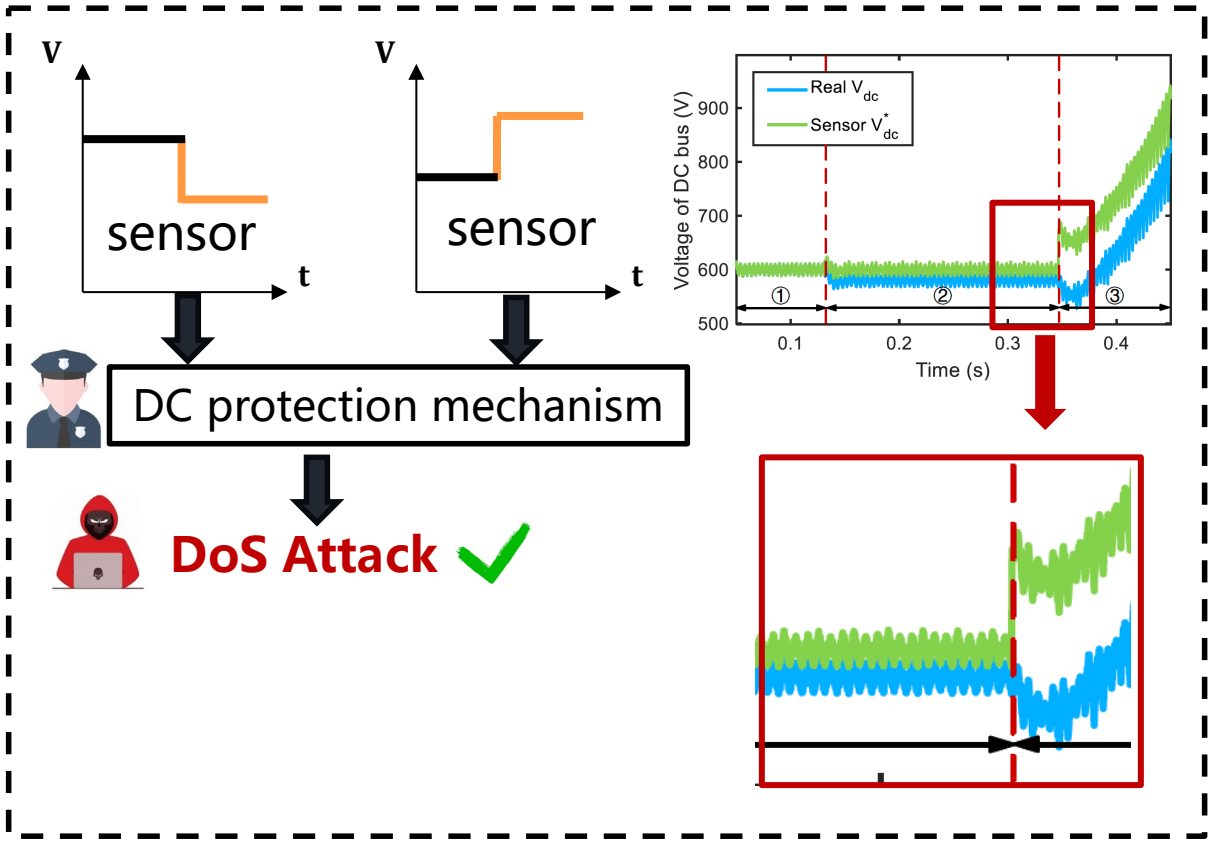
DC side



Attack design

- Design of **DoS Attack**

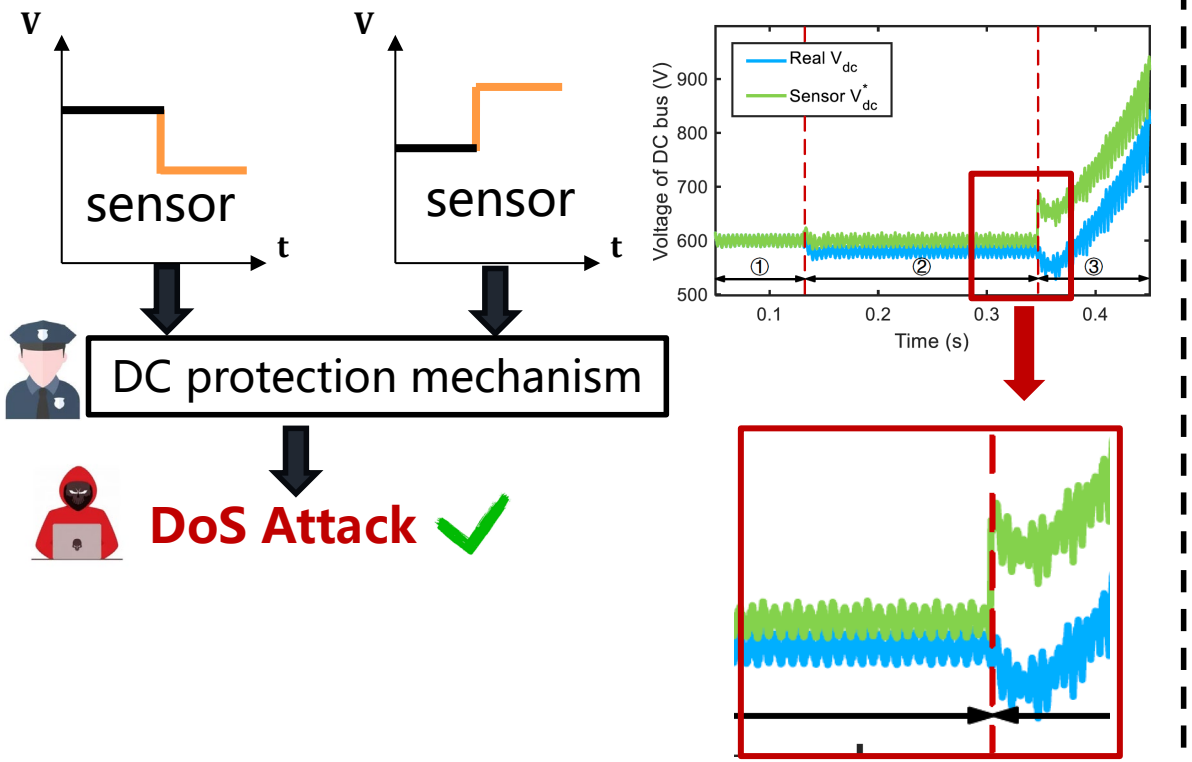
DC side



Attack design

- Design of **DoS Attack**

DC side

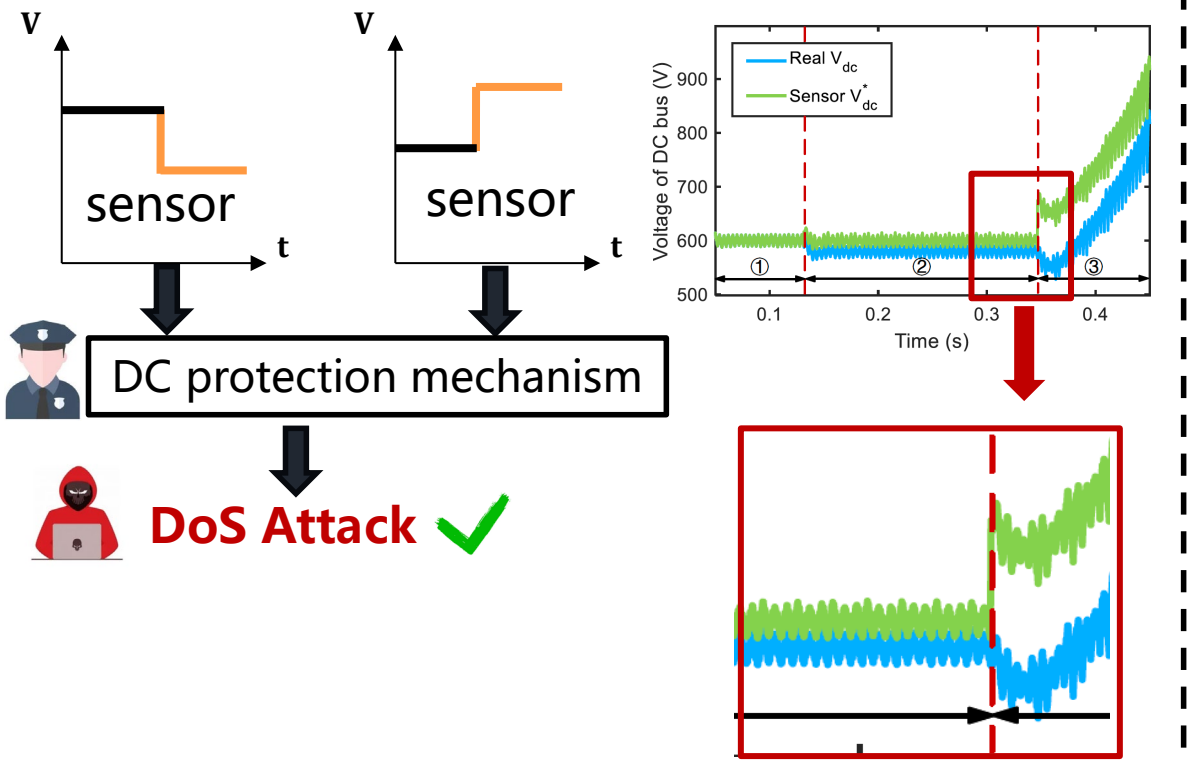


AC side

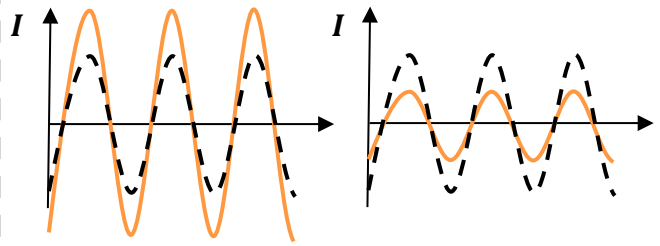
Attack design

- Design of **DoS Attack**

DC side



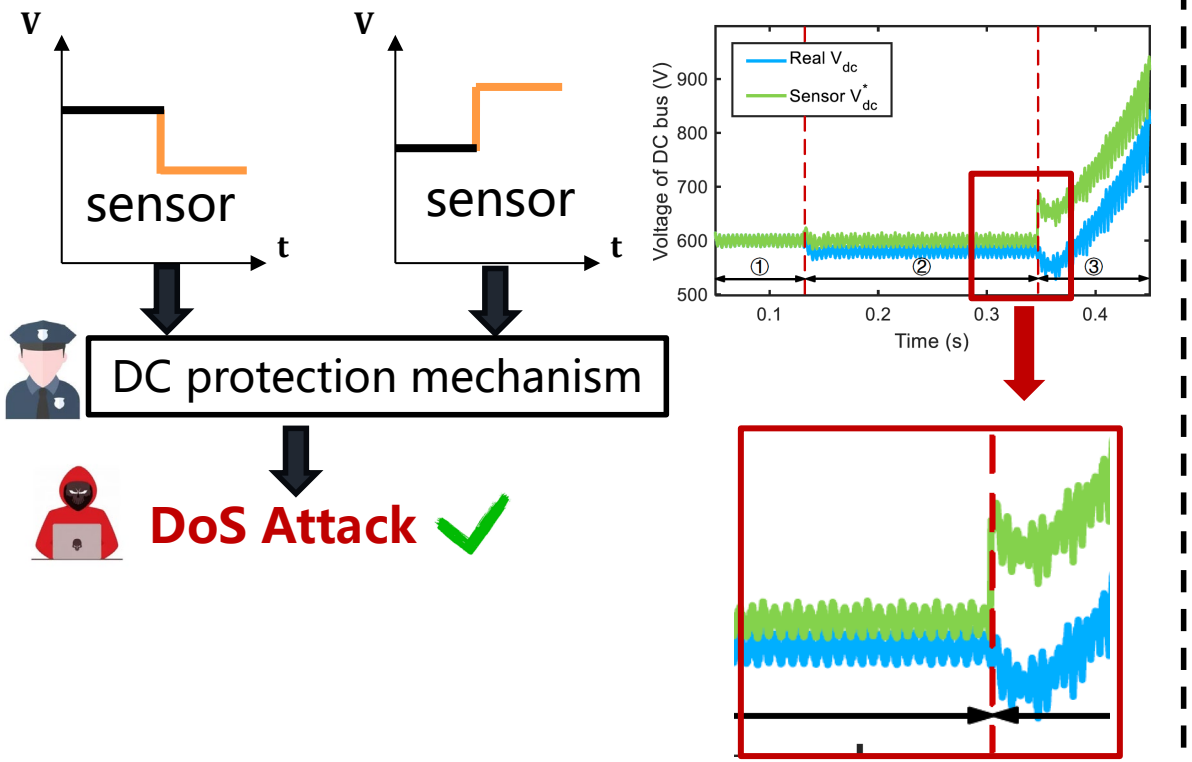
AC side



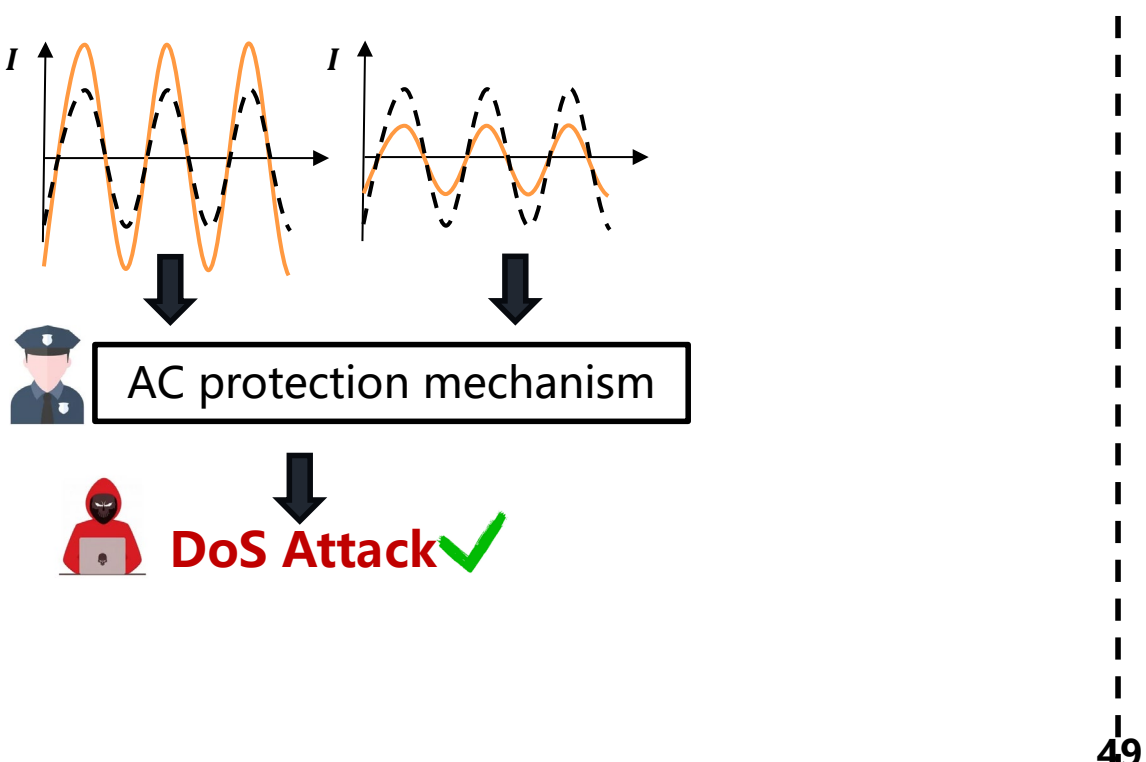
Attack design

- Design of **DoS Attack**

DC side



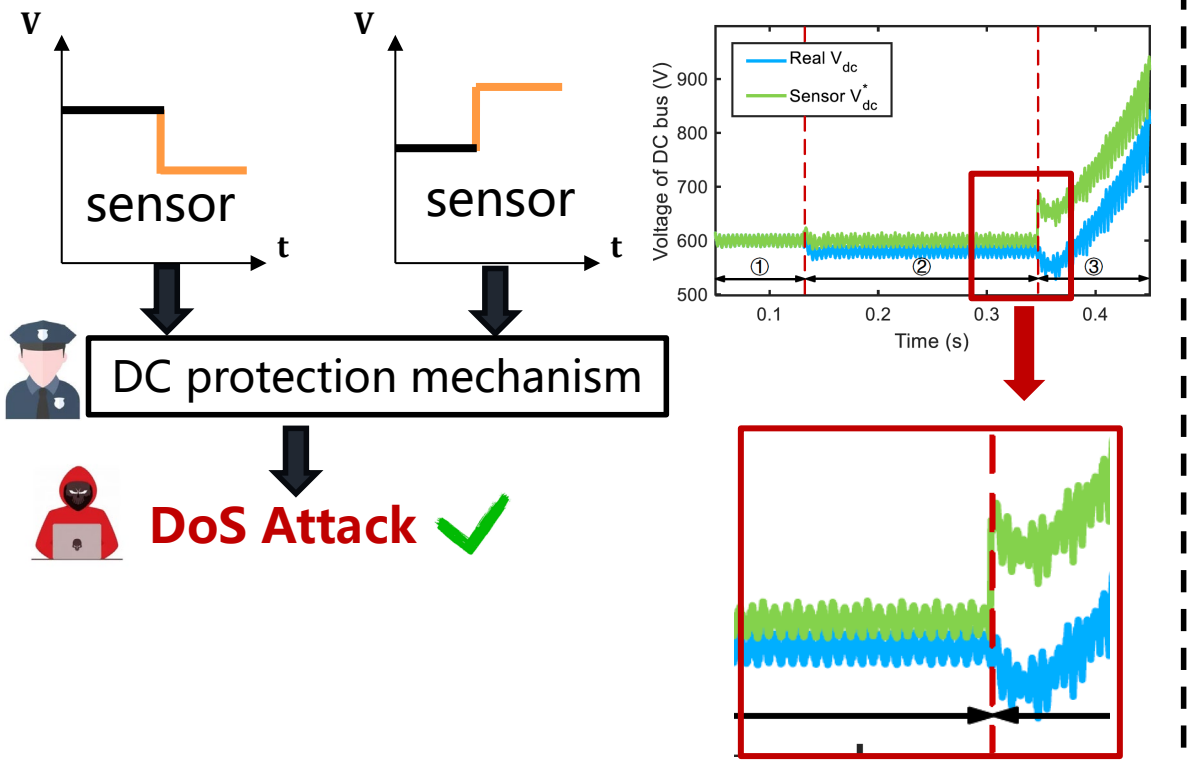
AC side



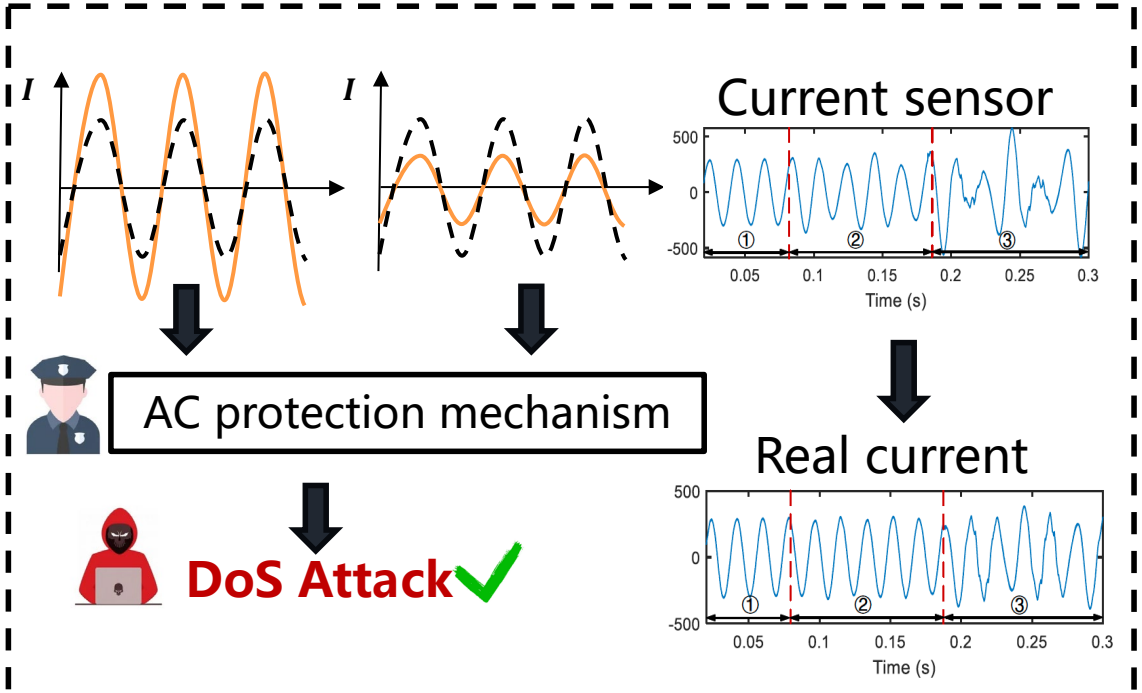
Attack design

- Design of **DoS Attack**

DC side



AC side



Attack design

- Design of DoS Attack
- **Design of Damage Attack**
- Design of Damping Attack

Attack design

- Design of **Damage Attack**

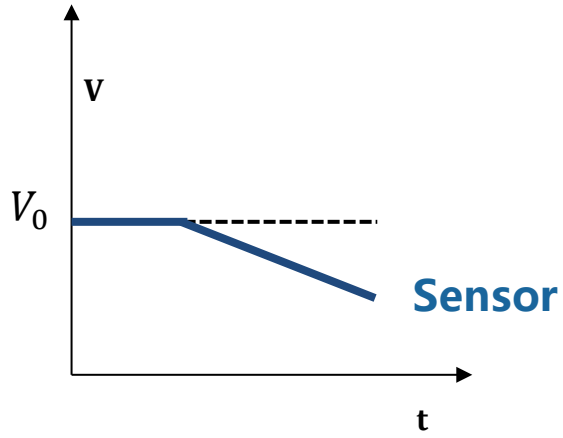
The key is to avoid triggering the protection mechanisms.

Attack design

- Design of **Damage Attack**

The key is to avoid triggering the protection mechanisms.

Analysis



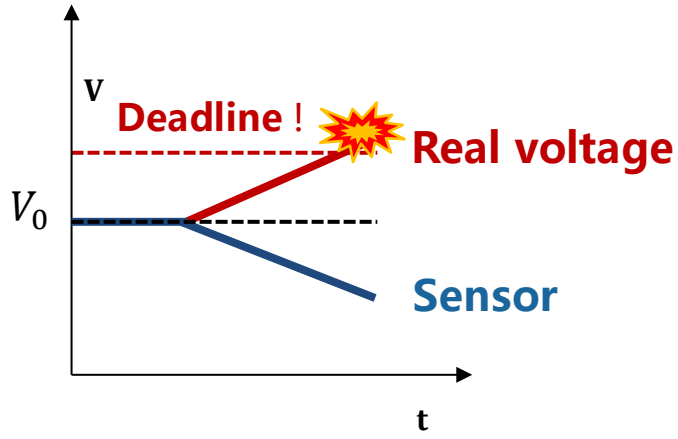
Damage attack

Attack design

- Design of **Damage Attack**

The key is to avoid triggering the protection mechanisms.

Analysis



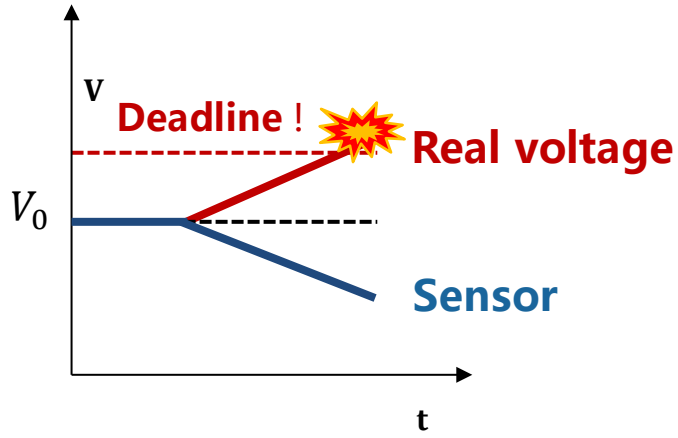
Damage attack

Attack design

- Design of **Damage Attack**

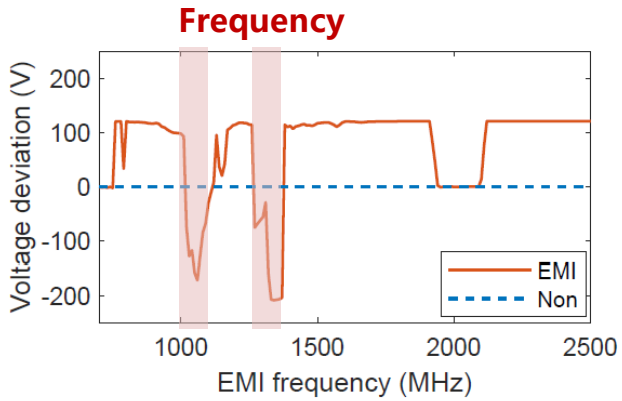
The key is to avoid triggering the protection mechanisms.

Analysis



Damage attack

Signal Design



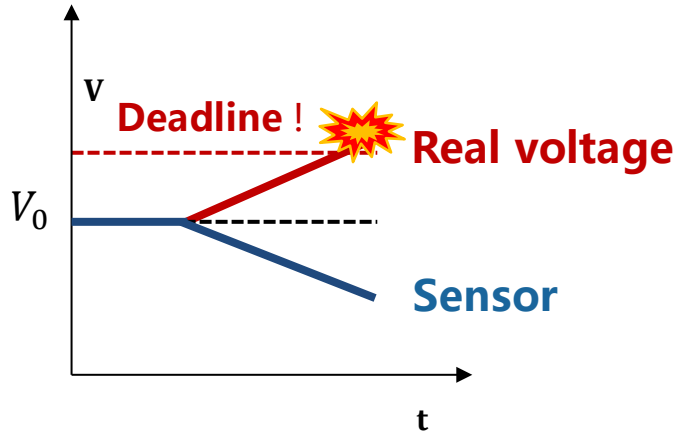
Step 1

Attack design

- Design of **Damage Attack**

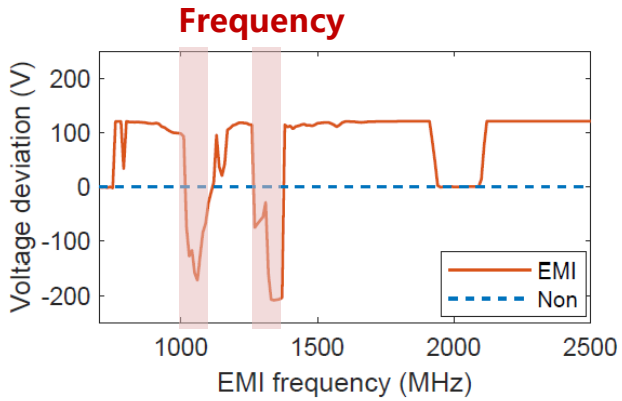
The key is to avoid triggering the protection mechanisms.

Analysis

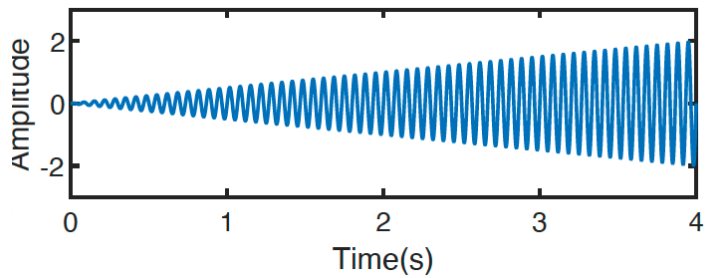


Damage attack

Signal Design



Step 1



Step 2

Attack design

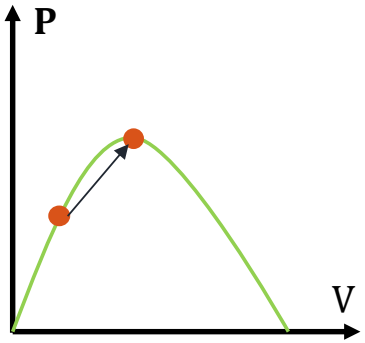
- Design of DoS Attack
- Design of Damage Attack
- **Design of Damping Attack**

Attack design

- Design of **Damping Attack**

Analysis

Without Attack

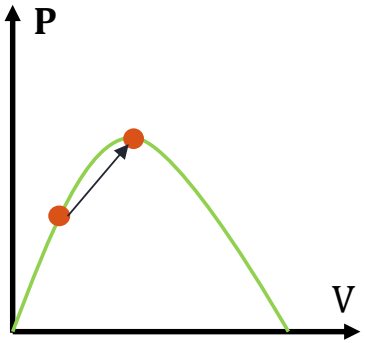


Attack design

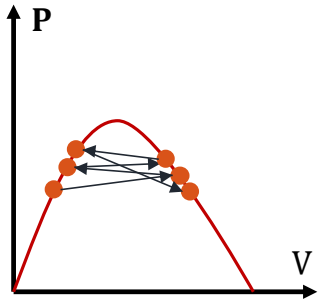
- Design of **Damping Attack**

Analysis

Without Attack



With Attack

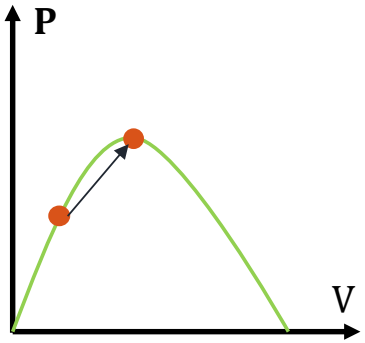


Attack design

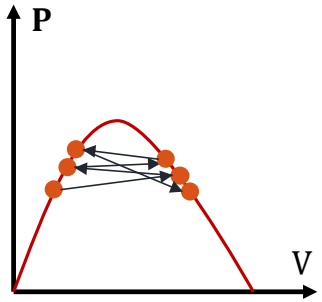
- Design of **Damping Attack**

Analysis

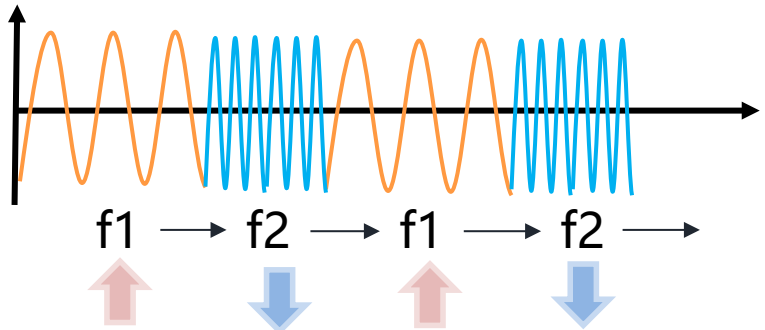
Without Attack



With Attack



Signal Design

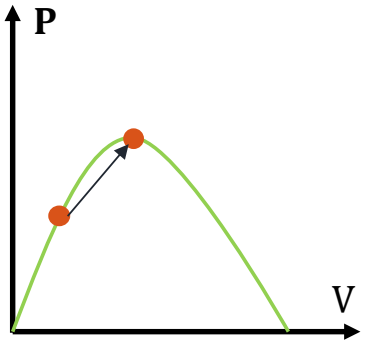


Attack design

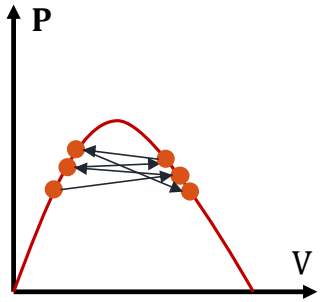
- Design of **Damping Attack**

Analysis

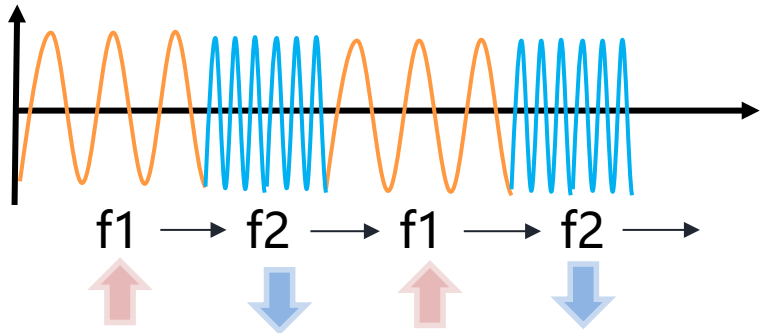
Without Attack

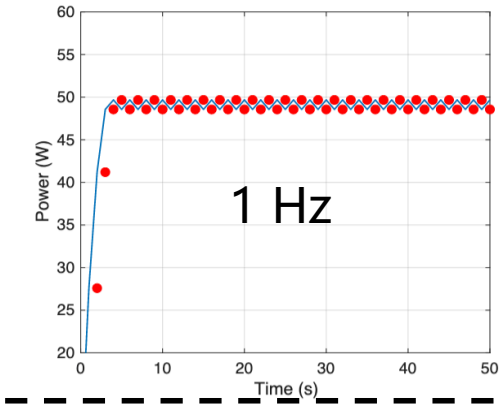


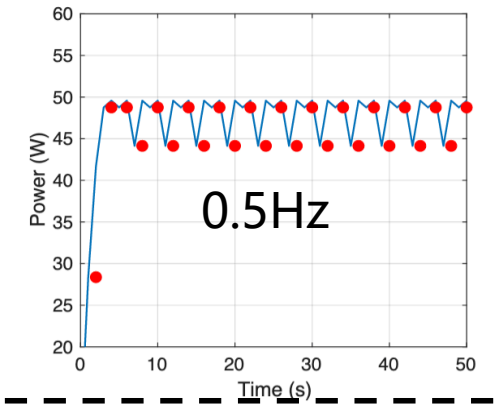
With Attack



Signal Design







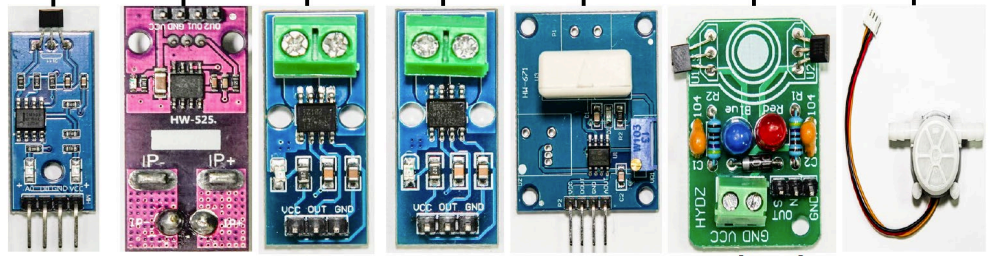
Evaluation

1. Evaluation on sensors

Evaluation

1. Evaluation on sensors

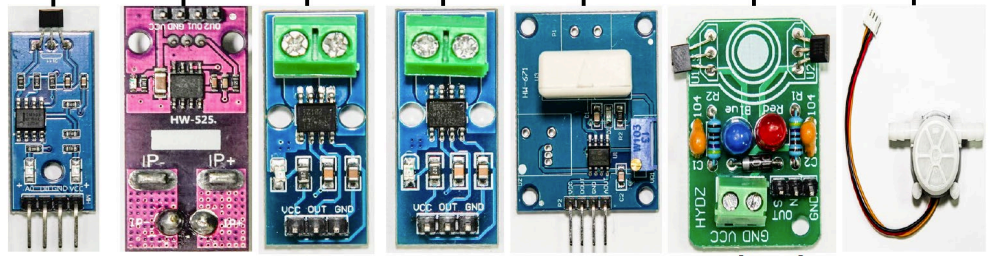
Hall sensors



Evaluation

1. Evaluation on sensors

Hall sensors

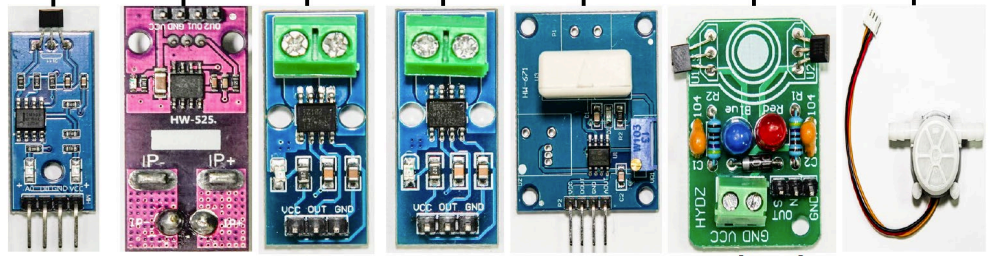


Sensor type	Sensor model	Output type	Measure-ment span	Test parameters		Output				
				Freq.(MHz)[3] (Pos. /Neg.)[3]	Pow.(W)[3]	Original value	Pos. dev.[1,3]	Pos. dev. rate	Neg. dev.[1,3]	Neg. dev. rate
Current	WCS1800 (Wire)	Analog	0∼30A	685/1030	10	5 A	15.7 A	+214.00%	-6.1 A	-222.00%
Current	WCS1800 (Wireless)	Analog	0∼35 A	1000/876	10	5 A	31.5 A	+530.00%	-7.6 A	-252.00%
Current	ACS712 (20 A)	Analog	0∼20 A	779/1223	10	5 A	13.2 A	+164.00%	-13.2 A	-364.00%
Current	ACS712 (5 A)	Analog	0∼5 A	627/1212	10	2.5 A	5.1 A	+104.00%	-7.75 A	-410.00%
Speed	3144	Digital	0/1	677	10	0/1	bit-flap[2]	+100.00%	bit-flap	-100.00%
North pole	3144	Digital	0/1	724	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%
Water flow	YF-S401	Digital	0/1	1322	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%

Evaluation

1. Evaluation on sensors

Hall sensors

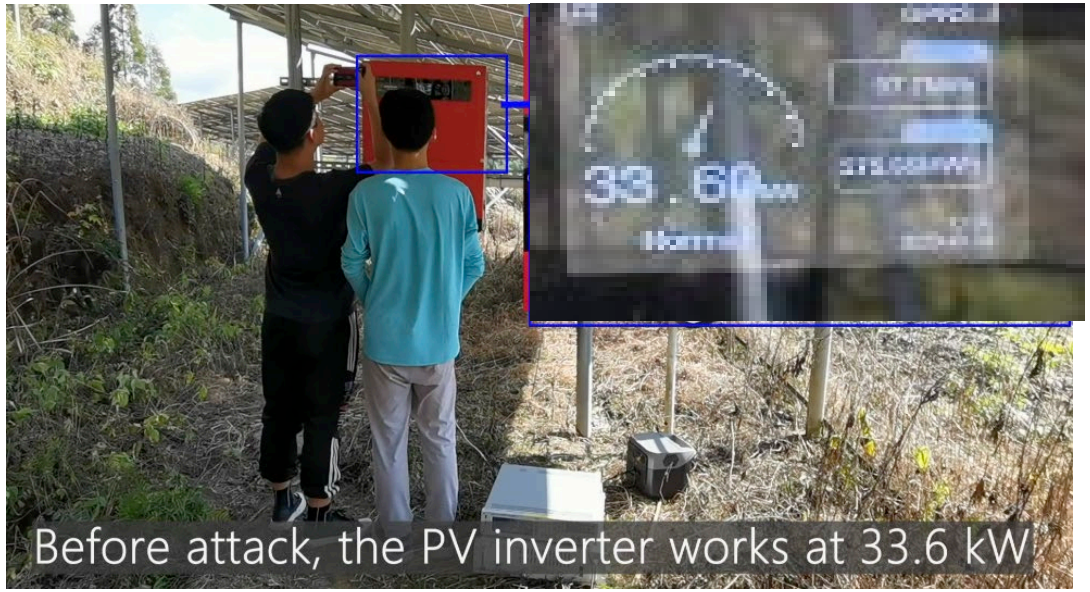


Sensor type	Sensor model	Output type	Measure-ment span	Test parameters		Output				
				Freq.(MHz)[3] (Pos. /Neg.)[3]	Pow.(W)[3]	Original value	Pos. dev.[1,3]	Pos. dev. rate	Neg. dev.[1,3]	Neg. dev. rate
Current	WCS1800 (Wire)	Analog	0∼30A	685/1030	10	5 A	15.7 A	+214.00%	-6.1 A	-222.00%
Current	WCS1800 (Wireless)	Analog	0∼35 A	1000/876	10	5 A	31.5 A	+530.00%	-7.6 A	-252.00%
Current	ACS712 (20 A)	Analog	0∼20 A	779/1223	10	5 A	13.2 A	+164.00%	-13.2 A	-364.00%
Current	ACS712 (5 A)	Analog	0∼5 A	627/1212	10	2.5 A	5.1 A	+104.00%	-7.75 A	-410.00%
Speed	3144	Digital	0/1	677	10	0/1	bit-flap[2]	+100.00%	bit-flap	-100.00%
North pole	3144	Digital	0/1	724	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%
Water flow	YF-S401	Digital	0/1	1322	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%

Both **analog and digital** Hall sensors can be attacked by EMI

Evaluation

2. Evaluation on inverters --- DoS

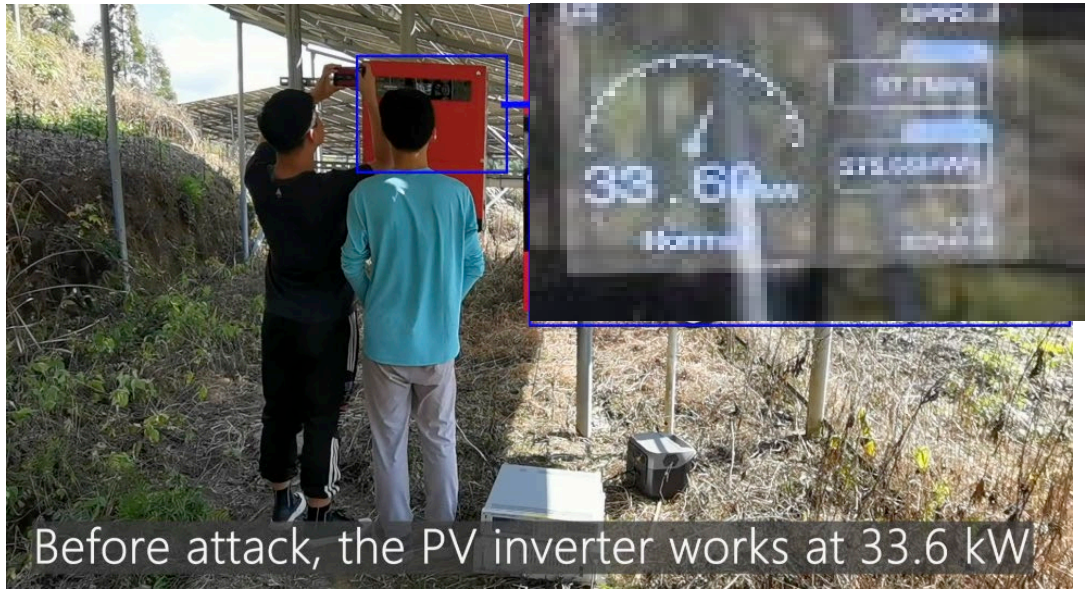


Before Attack

See demo video at https://tinyurl.com/ReThinkDemoVideos

Evaluation

2. Evaluation on inverters --- DoS



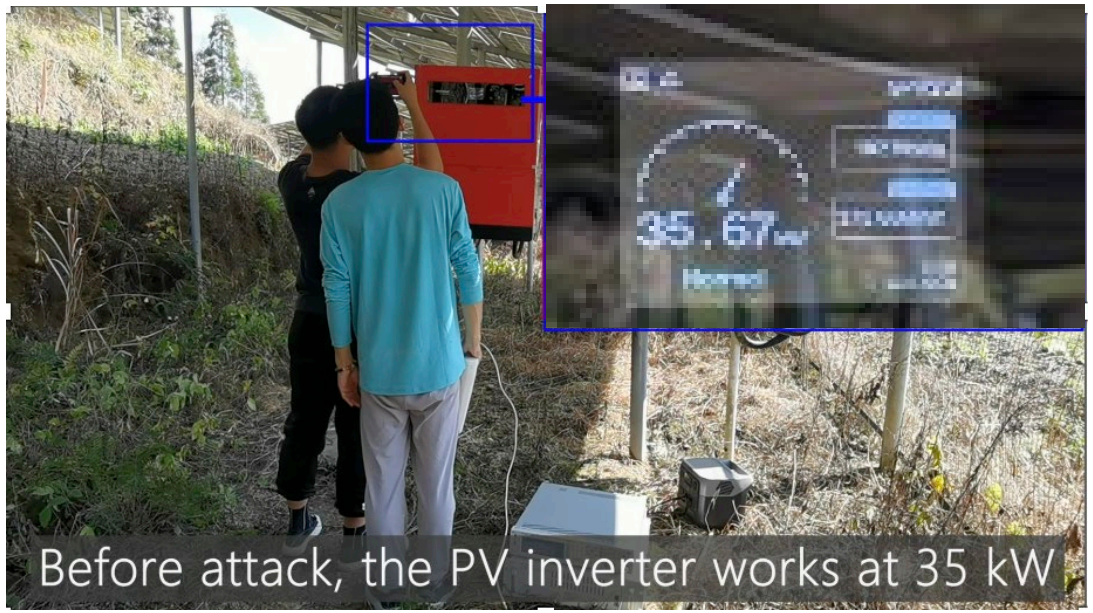
Before Attack

After Attack

See demo video at https://tinyurl.com/ReThinkDemoVideos

Evaluation

2. Evaluation on inverters --- Damping

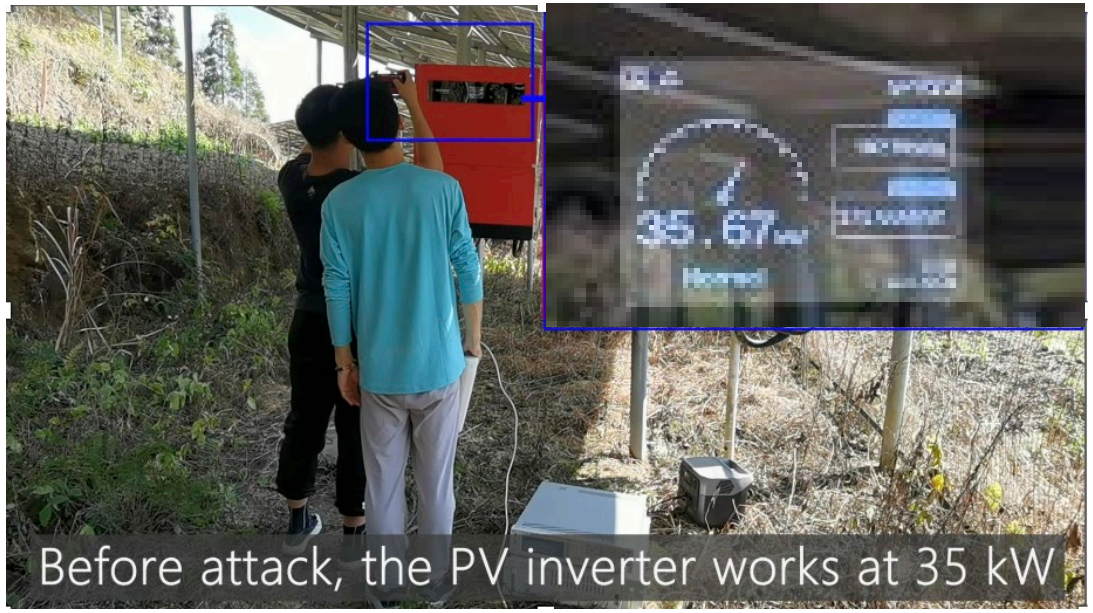


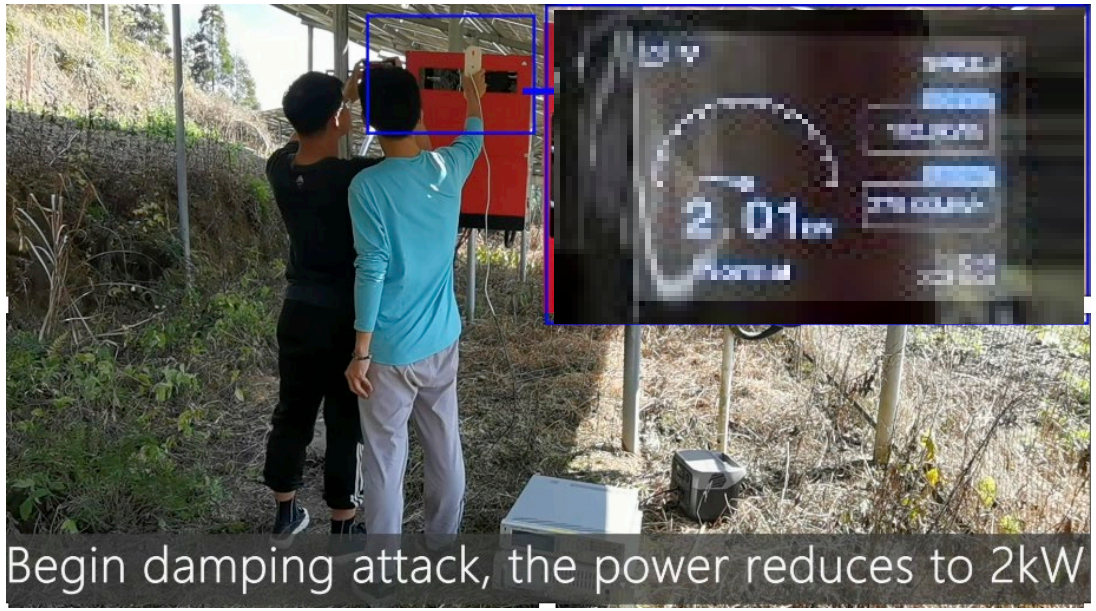
Before Attack (35 kW)

See demo video at https://tinyurl.com/ReThinkDemoVideos

Evaluation

2. Evaluation on inverters --- Damping





Before Attack (35 kW)

After Attack (2 kW)

See demo video at https://tinyurl.com/ReThinkDemoVideos

Evaluation

2. Evaluation on inverters --- Damage

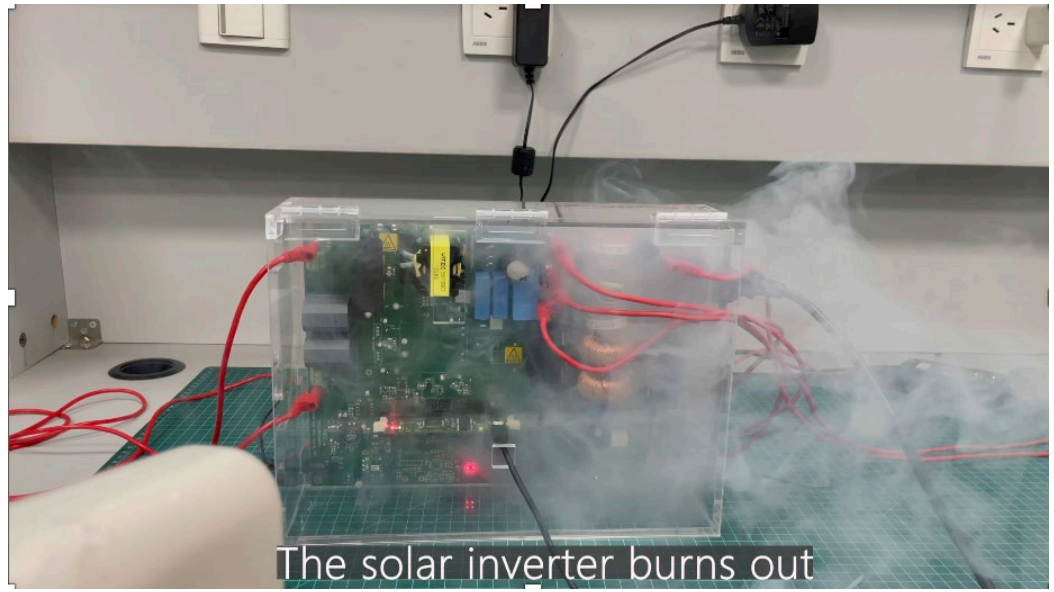
Before Attack

See demo video at https://tinyurl.com/ReThinkDemoVideos

Evaluation

2. Evaluation on inverters --- Damage

Before Attack

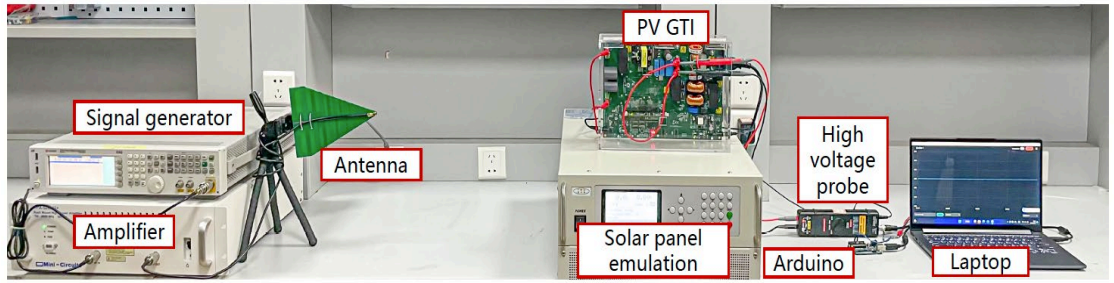


After Attack

See demo video at https://tinyurl.com/ReThinkDemoVideos

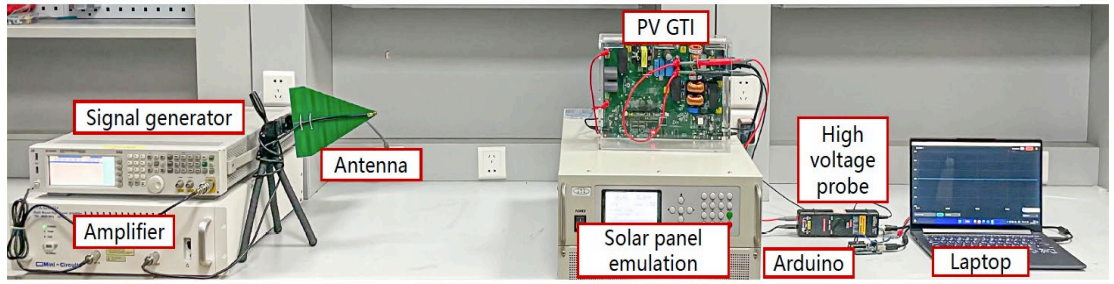
Evaluation

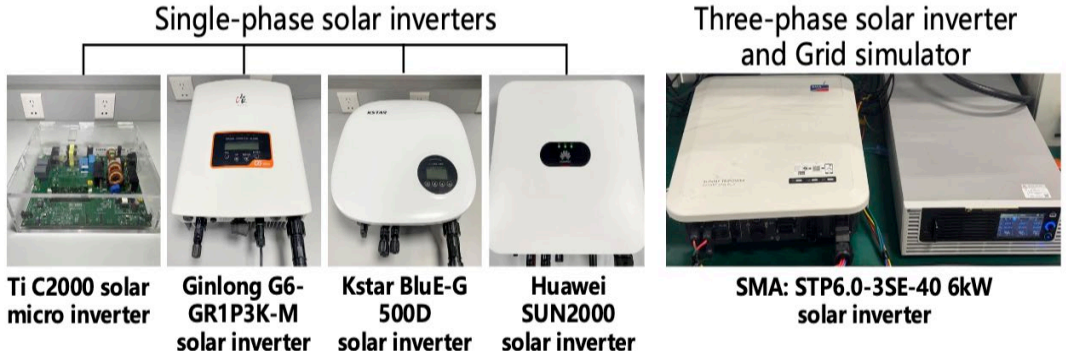
2. Evaluation on inverters



Evaluation

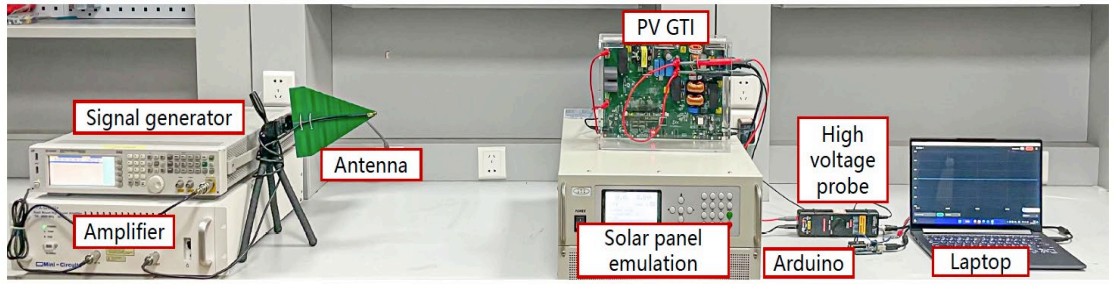
2. Evaluation on inverters





Evaluation

2. Evaluation on inverters



Single-phase solar inverters

Ti C2000 solar micro inverter | Ginlong G6-GR1P3K-M solar inverter | Kstar BluE-G 500D solar inverter | Huawei SUN2000 solar inverter

Three-phase solar inverter and Grid simulator

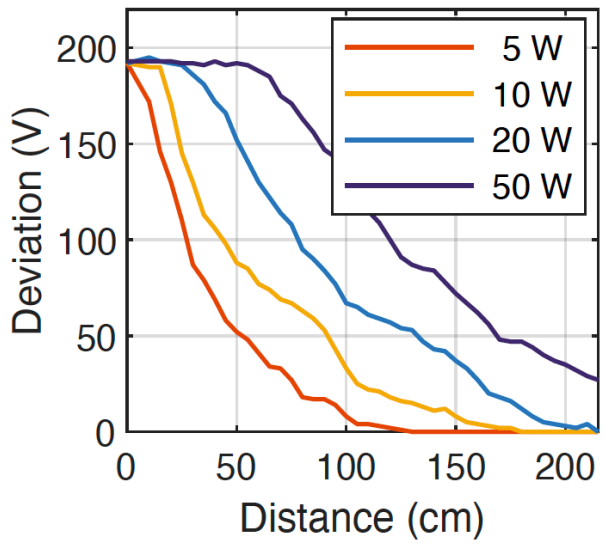
SMA: STP6.0-3SE-40 6kW solar inverter

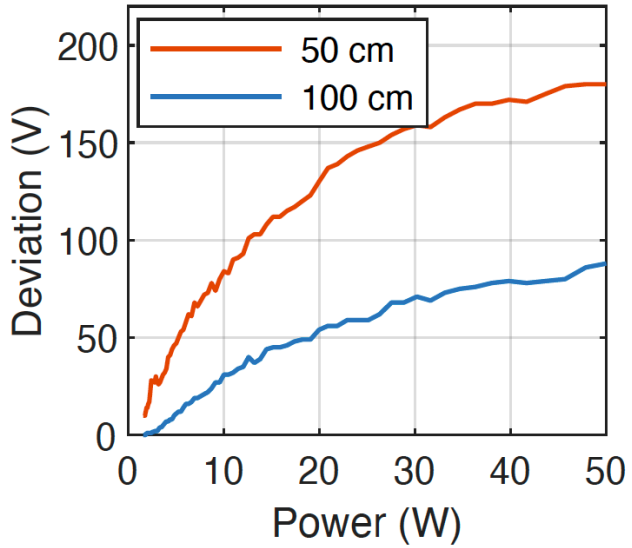
Inverter	DoS						Damage			Damping			
	On DC side			On AC side			Pow. (W)	Freq. (MHz)	Result	Freq. (MHz)	Pow.(W) before Damping	Pow.(W) after Damping [2]	Pow. dev. rate
	Pow. (W)	Freq. (MHz)	Success rate[1]	Pow. (W)	Freq.(MHz) Pos./Neg.[4]	Success rate[1]							
Ti C2000	5	735	100%	5	1036/1490	100%	10	1000	100%	760	80	25	68.75%
Ginlong	10	916	100%	10	625/1210	80%	-[3]	-	-	1192	1980	1390	29.8%
Kstar	10	749	100%	10	990/810	90%	-	-	-	998	1995	1560	21.8%
Huawei[5]	10	1150	100%	10	980/1020	80%	-	-	-	1330	1960	1420	27.6%
SMA	10	675	100%	10	1125	100%	-	-	-	753	2950	2660	9.8%
GW(LCD,50kW)	20	920	100%	-	-	-	-	-	-	960	35.6k	2k	94.3%
GW(LED,60kW)[6]	20	945	100%	-	-	-	-	-	-	-	-	-	-

All tested PV inverters can be attacked

Evaluation

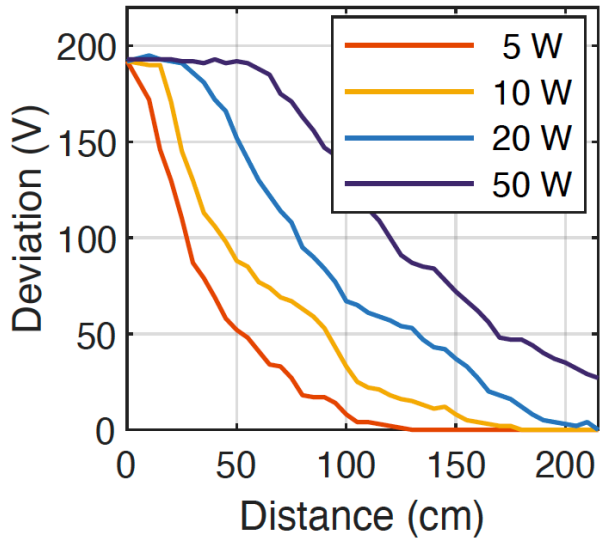
3. Distance and power

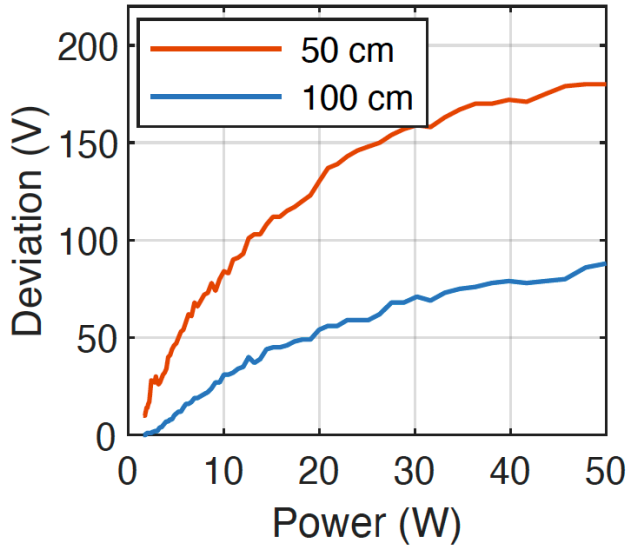


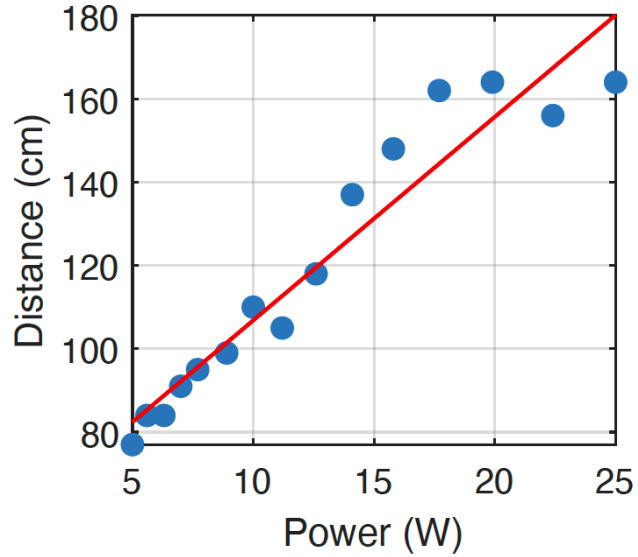


Evaluation

3. Distance and power



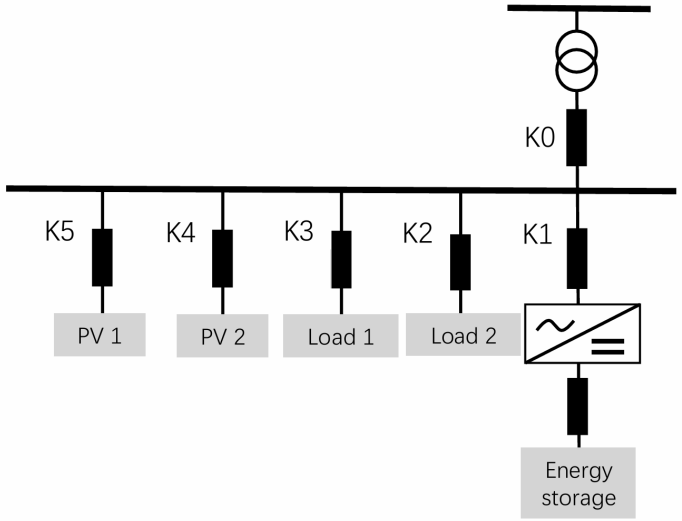


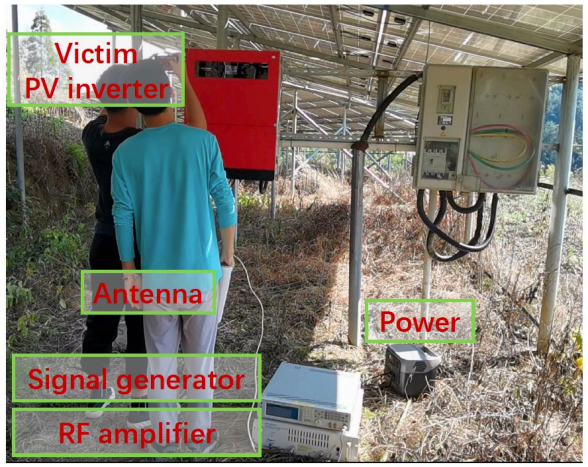


The attack ability can be further improved with **larger attack power**

Evaluation

4. Real-world grid

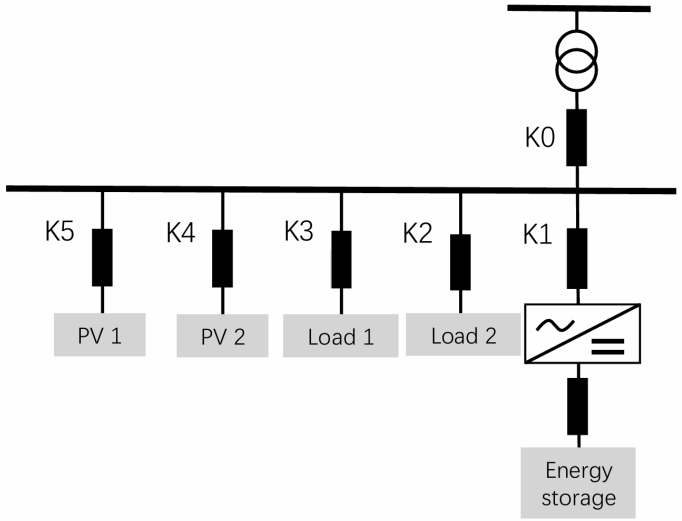


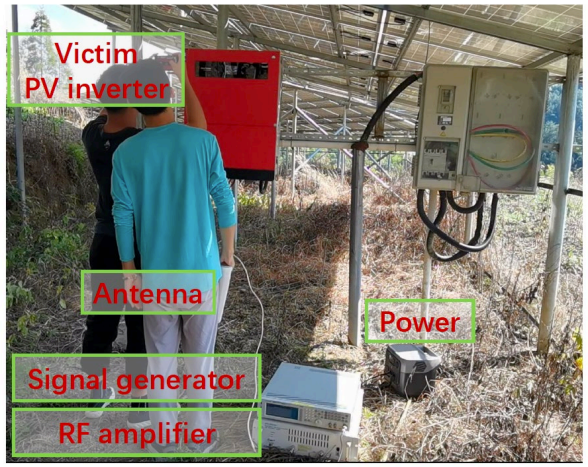


Attack on a 400 kVA microgrid in real world

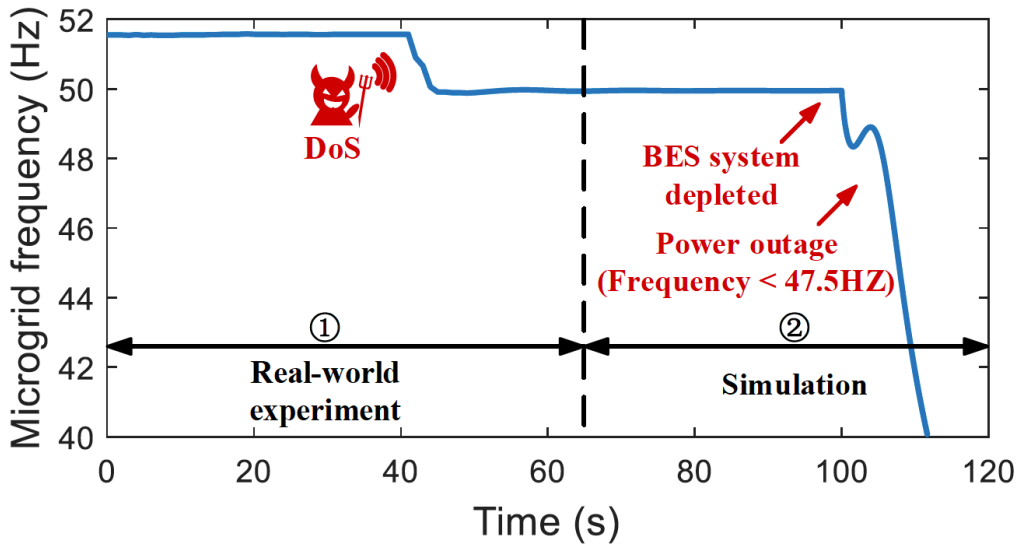
Evaluation

4. Real-world grid





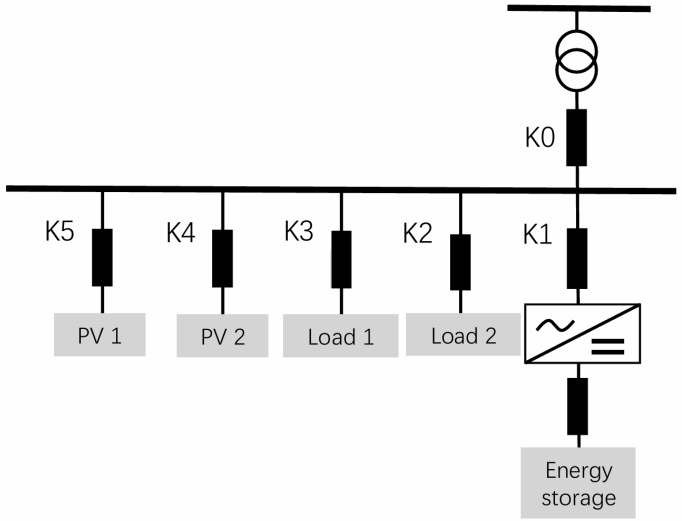
Attack on a 400 kVA microgrid in real world

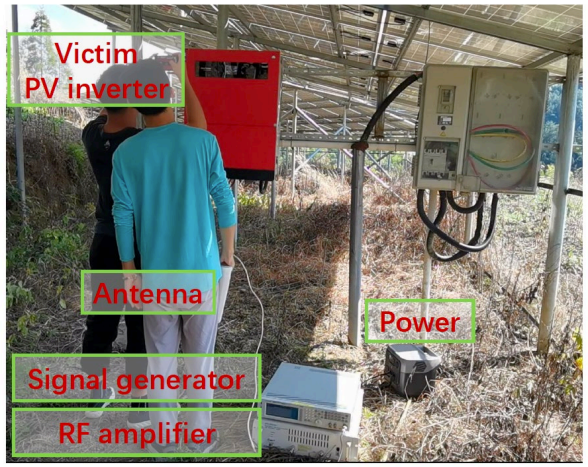


Experiment and simulation result

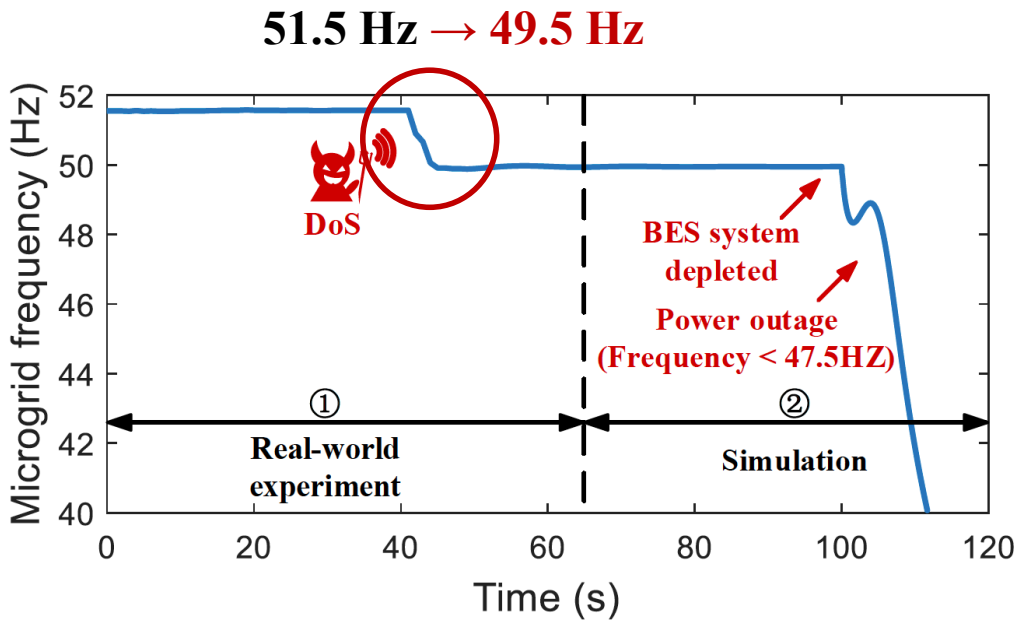
Evaluation

4. Real-world grid





Attack on a 400 kVA microgrid in real world



Experiment and simulation result

Discussion

Countermeasures

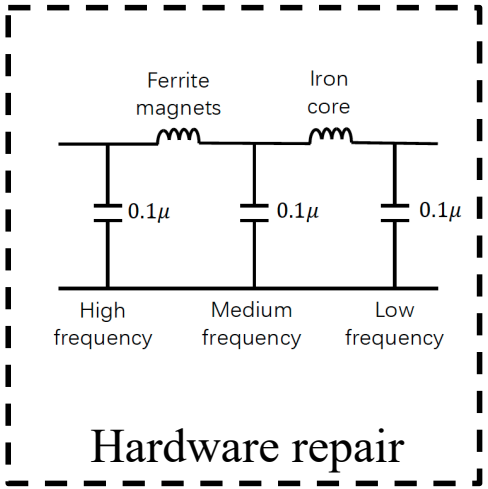
Discussion

Countermeasures

(1) Filtering Leakage and Multi-stage filter

(2) Shielding

(3) Detection



Hardware repair

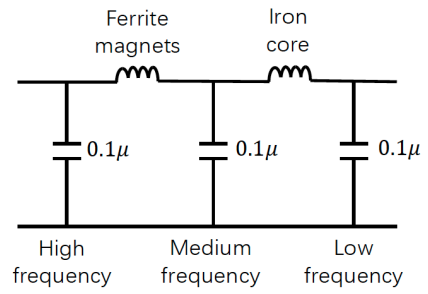
Discussion

Countermeasures

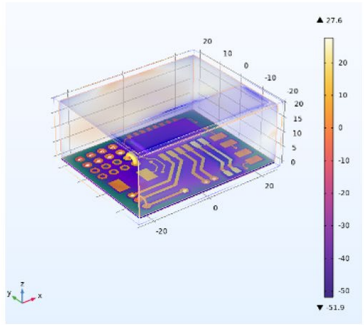
(1) Filtering Leakage and Multi-stage filter

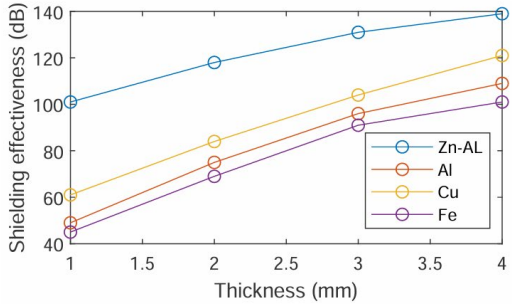
(2) Shielding

(3) Detection



Hardware repair





Shielding repair

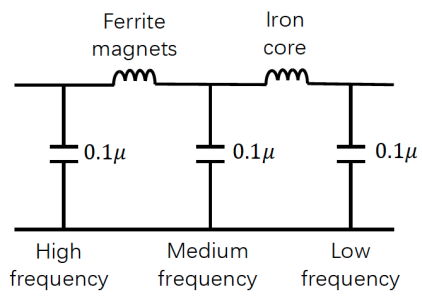
Discussion

Countermeasures

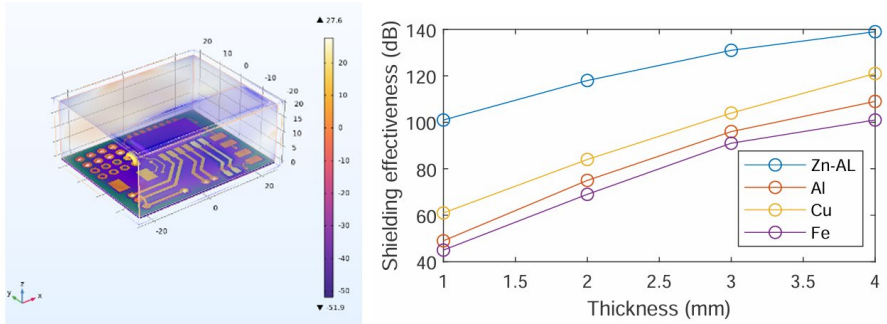
(1) Filtering Leakage and Multi-stage filter

(2) Shielding

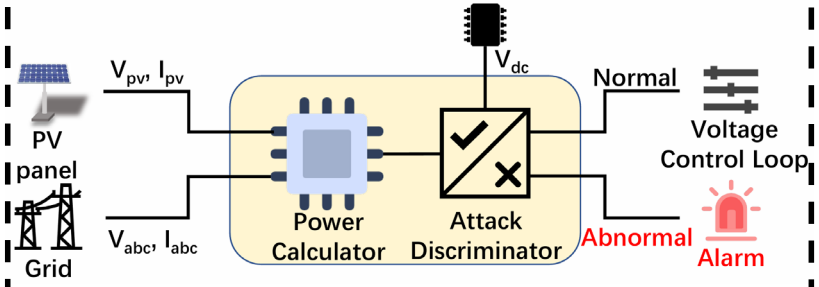
(3) Detection



Hardware repair



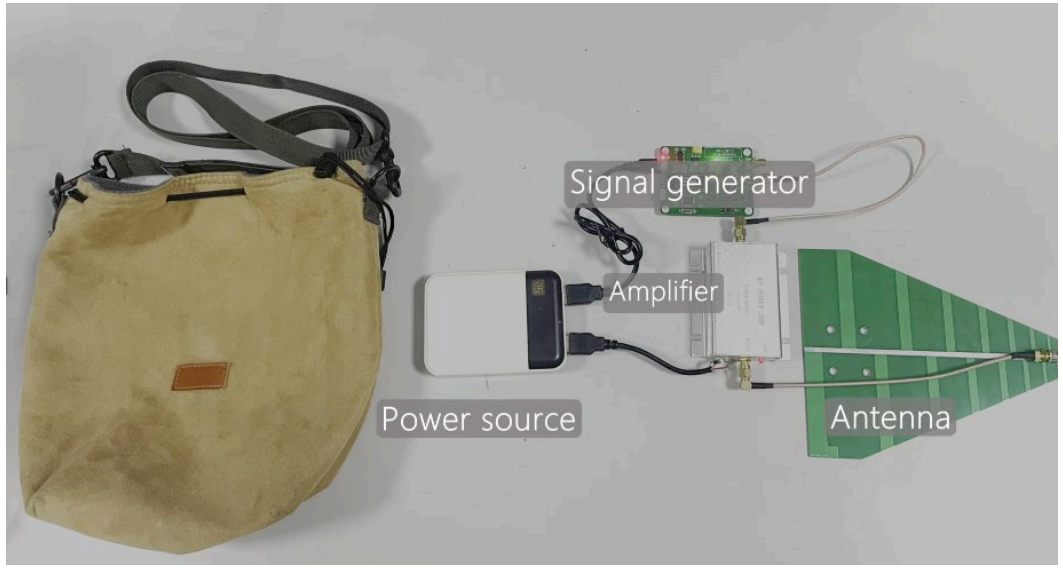
Shielding repair



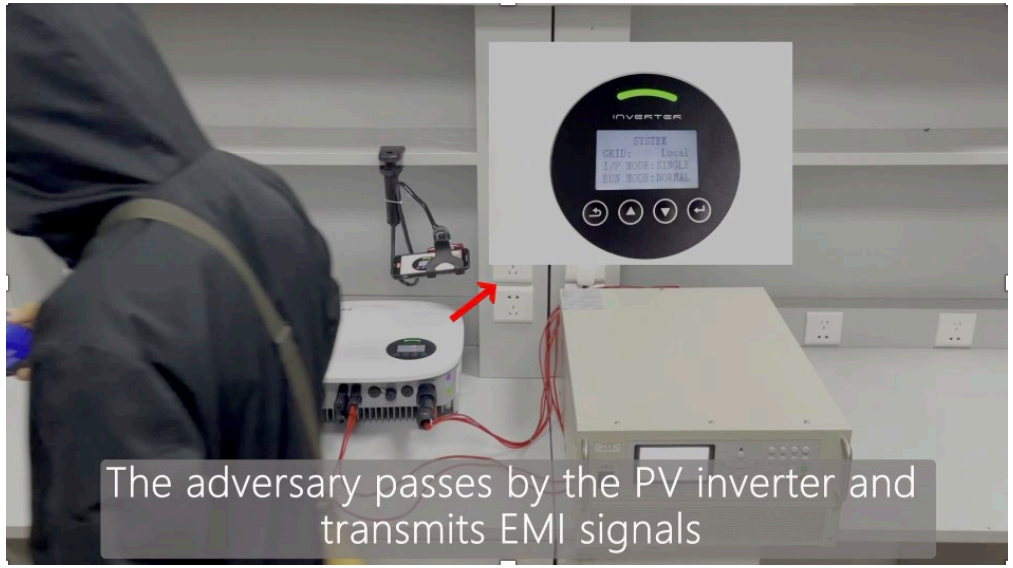
Algorithm repair

Discussion

- Portable attack device



Portable attack device



Experiment

See demo video at https://tinyurl.com/ReThinkDemoVideos

Summary

- We systematically analyze the security of power inverters.
- We propose 3 impacts that can cause the victim PV inverter to shut down, physically burn out, and reduce output power, respectively.
- We successfully evaluate on an inverter development kit, 5 off-the-shelf PV inverters and a real-world microgrid.

Questions & Answer

Authors

USSLAB Website: www.usslab.org

Demo website:

https://tinyurl.com/ReThinkDemoVideos

浙江大学
ZHEJIANG UNIVERSITY

Thanks
Q&A

智能系统安全实验室
UBIQUITOUS SYSTEM SECURITY LAB.