WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens

Yan Jiang[1], Xiaoyu Ji*[1], Kai Wang[1], Chen Yan[1], Richard Mitev[2], Ahmad-Reza Sadeghi[2], Wenyuan Xu*[1]

[1]Ubiquitous System Security Lab, Zhejiang University

[2]System Security Lab, Technical University of Darmstadt

IEEE Security & Privacy 2022

浙江大學 ZHEJIANG UNIVERSITY

TECHNISCHE UNIVERSITÄT DARMSTADT

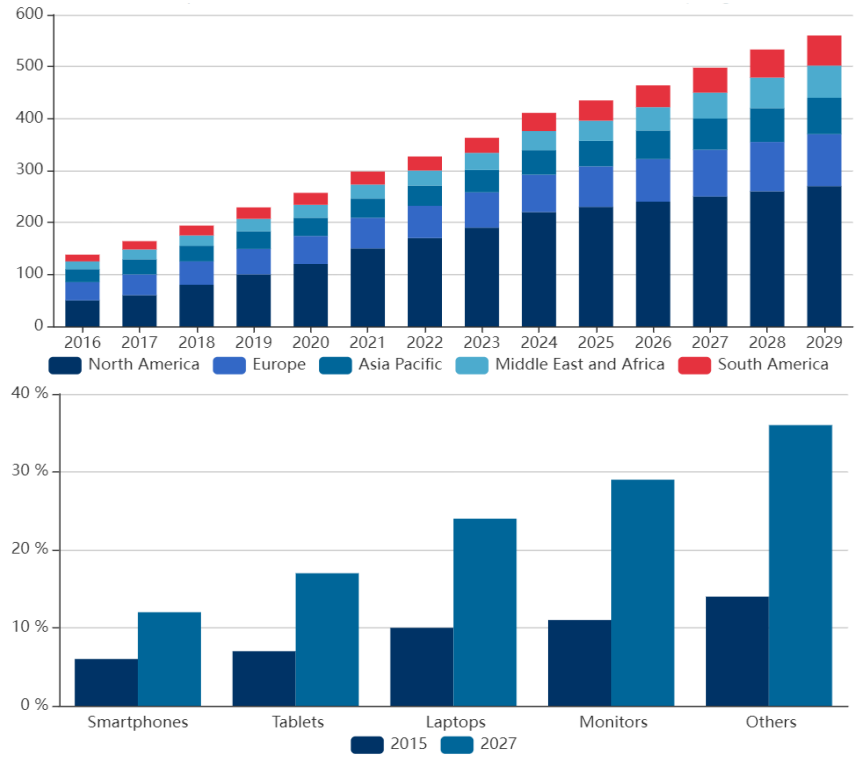
Capacitive touchscreens

Smartphones

Tablets

Laptops

Vehicles

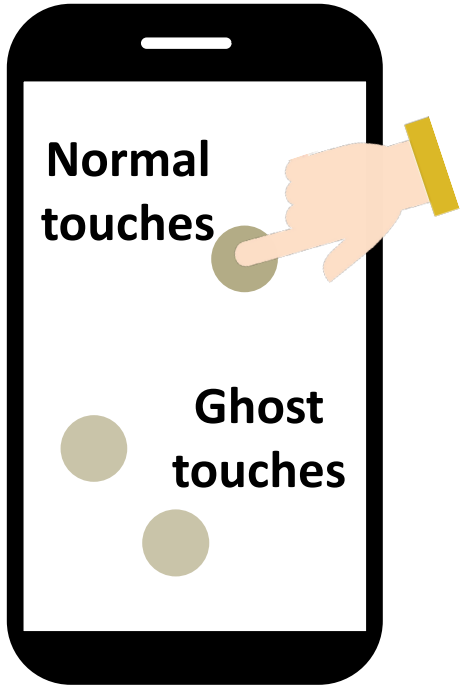


Revenue trends of capacitive touchscreens

Capacitive touchscreens are essential human-computer interfaces and are widely-used in smart devices!

Ghost Touches

Ghost touches: Touchscreen outputs **fake touches** and **controls the device by itself.**



News of ghost touches

Glitchy Touchscreen Caused by Charger

Asked 8 years, 8 months ago Modified 8 years, 8 months ago Viewed 13k time

J Iphone X Ghost Touch

Why does my touch screen go crazy while charging?

Touchscreen problems while charging

slane35 · Jul 20, 2012 · question

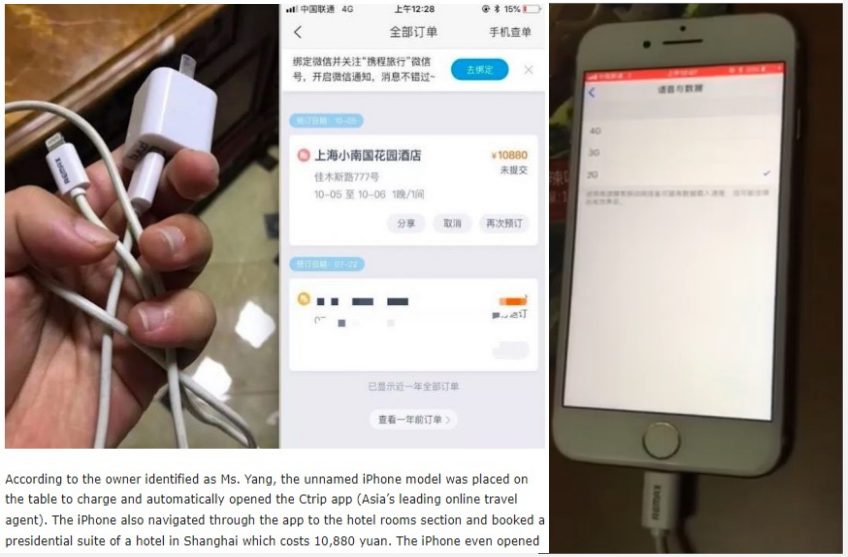
How to fix ghost touch issues on Android phones

adminguides November 18, 2020 0

...

Bizzare! iPhone user reports her charger controls the phone and even booked a presidential suite

By **Jed John Ikoba** - Oct 9, 2018

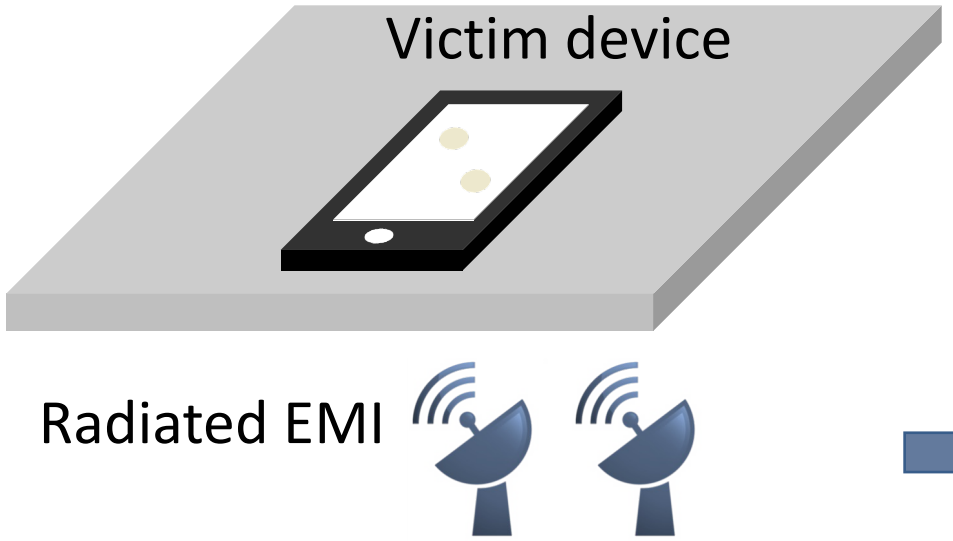


According to the owner identified as Ms. Yang, the unnamed iPhone model was placed on the table to charge and automatically opened the Ctrip app (Asia's leading online travel agent). The iPhone also navigated through the app to the hotel rooms section and booked a presidential suite of a hotel in Shanghai which costs 10,880 yuan. The iPhone even opened

Reliable touch is critical and we aim to analyze the feasibility of injecting ghost touches at chosen locations.

https://www.gizmochina.com/2018/10/09/bizzare-iphone-user-reports-her-charger-controls-the-phone-and-even-booked-a-presidential-suite/

Related work



[1] Maruyama et al., S&P 2017

[2] Wang et al., USENIX 2022

Close-range attacks

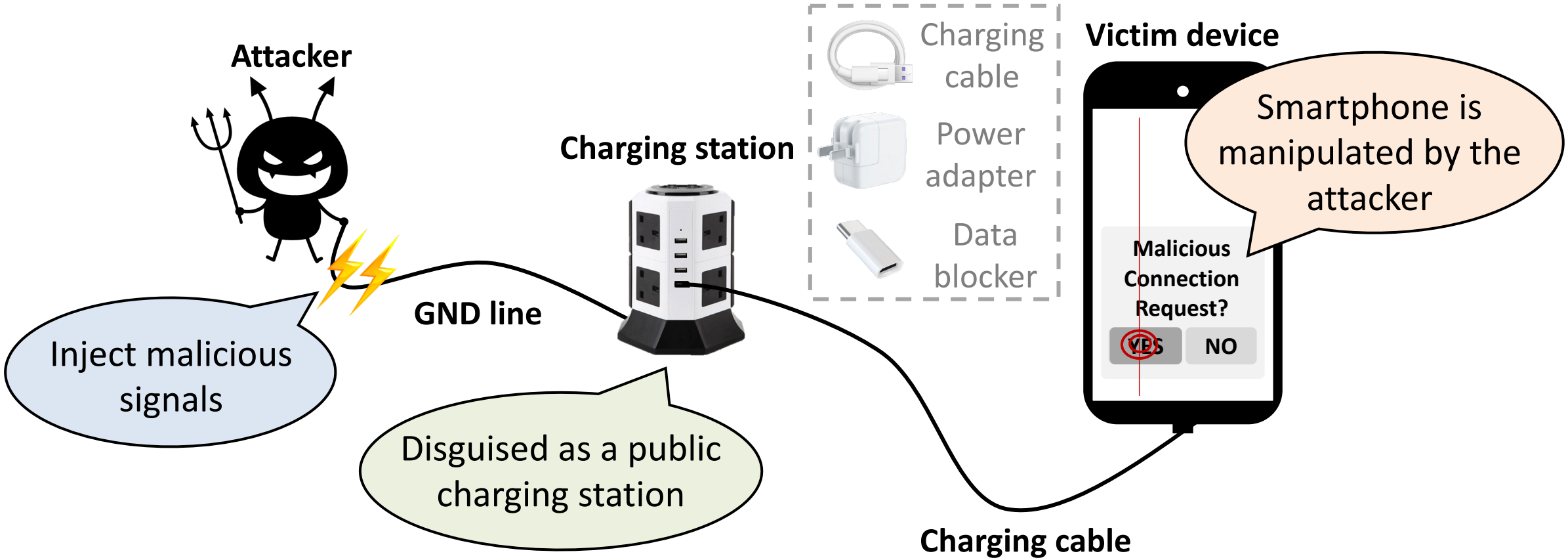
We aim to investigate whether the attacker can intentionally create ghost touches via a charging cable.

Our goals

- To understand the **new threat vector** against capacitive touchscreens via a charging cable

- To **mitigate** the new threat and improve the security of smart devices.

WIred GHost Touch attacks

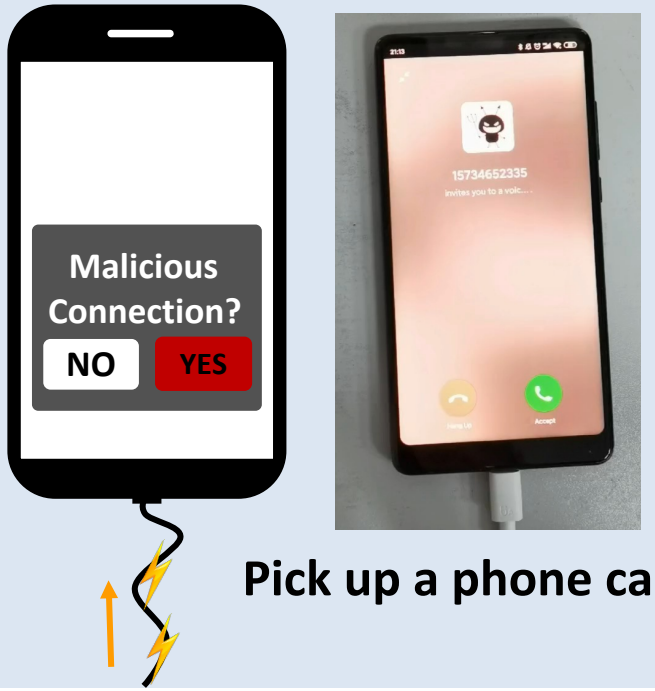


Attacker injects attack signals via a charging cable and manipulate the victim device even across a power adapter or data blocker.

WIGHT Attacks

■ Injection attack

Create fake touches to **operate the device** without user's awareness.



Pick up a phone call

■ Alteration attack

Create ghost touches to **alter the user's chosen touch**.

"Decline" →"Accept"

■ DoS attack

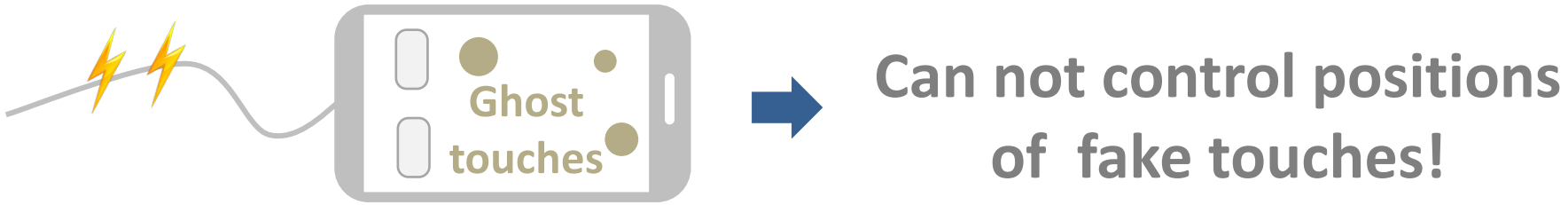
Disable the touch service of the smartphone.

Can not operate the phone

Challenges

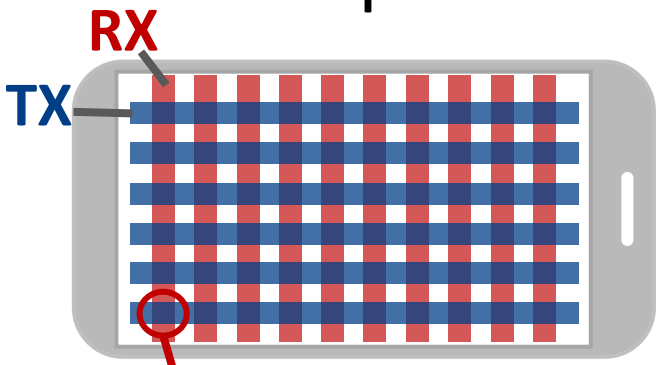
C1 **Injection:** What type of signal can be injected to create fake touches?

C2 **Position-control:** How to control the positions of ghost touches?

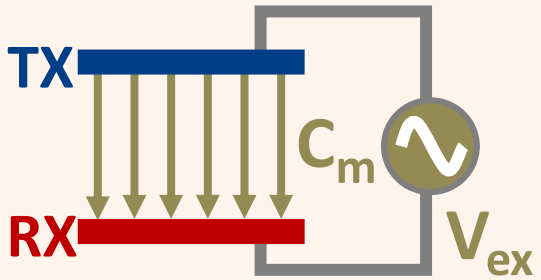


Injection attack

- How capacitive touchscreens work?

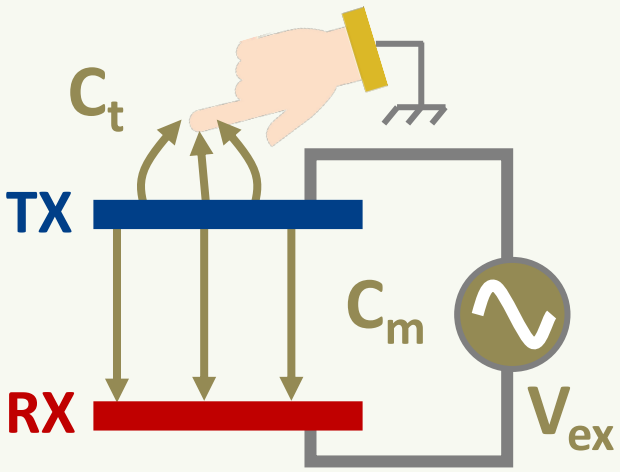


No touch:



$$V_{out} = V_{ref} - \frac{2\,C_m\,V_{ex}}{C_{fb}}$$

Finger touch:



$$V_{out} = V_{ref} - \frac{2(C_m - C_t)\,V_{ex}}{C_{fb}}$$

Injection attack:

Change V_{ex}

$$V_{out} = V_{ref} - \frac{2\,C_m\,V_{ex}}{C_{fb}}$$

Increase V_{out}

Fake touch

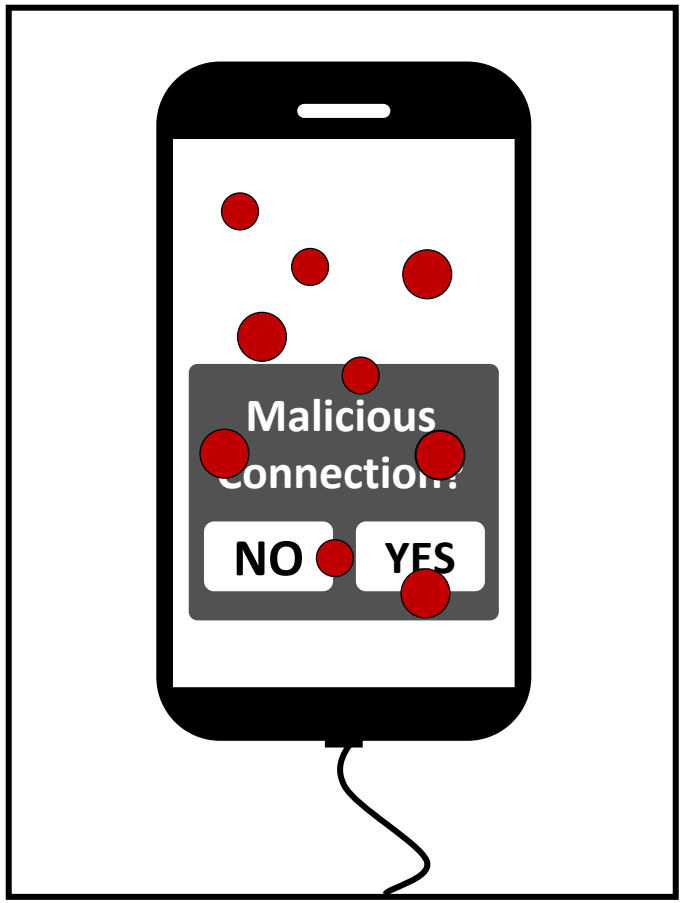
Attack design

➢ **Step1: Generate ghost touches.**

- Where to inject attack signal?
- How to select an attack signal?

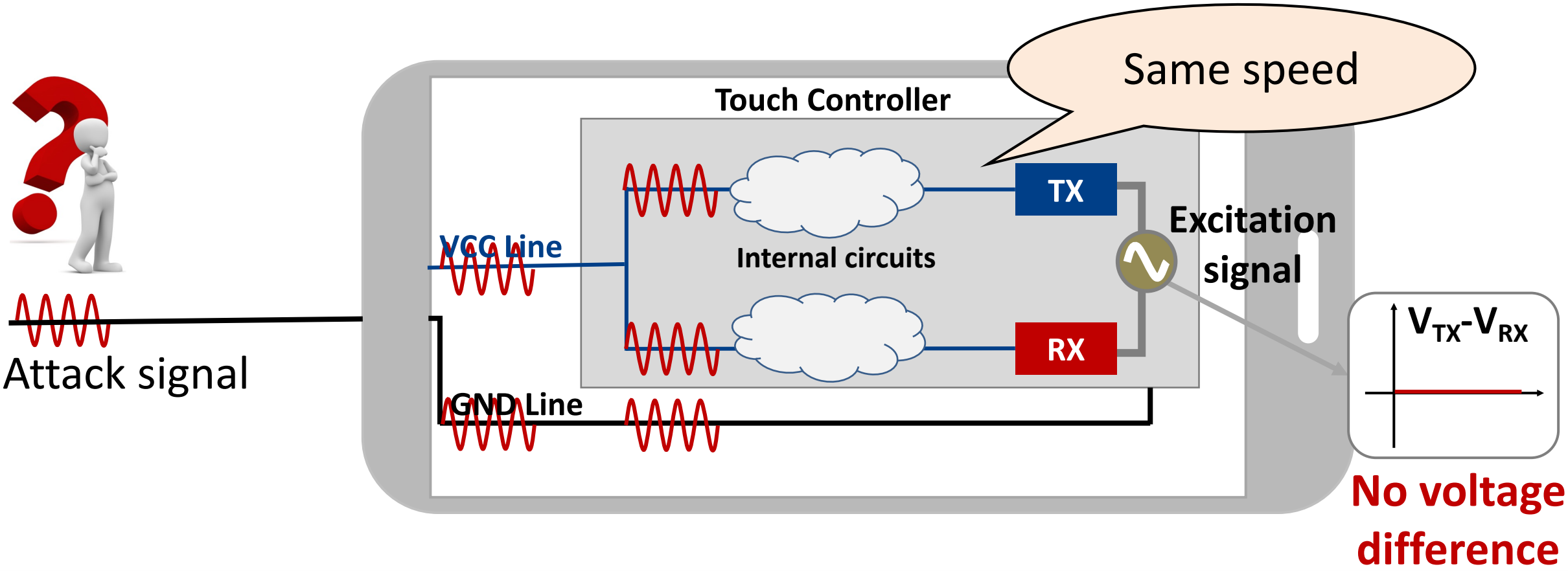
➢ **Step2: Control ghost touches.**

- Where are targeted positions?
- When to inject attack signals?



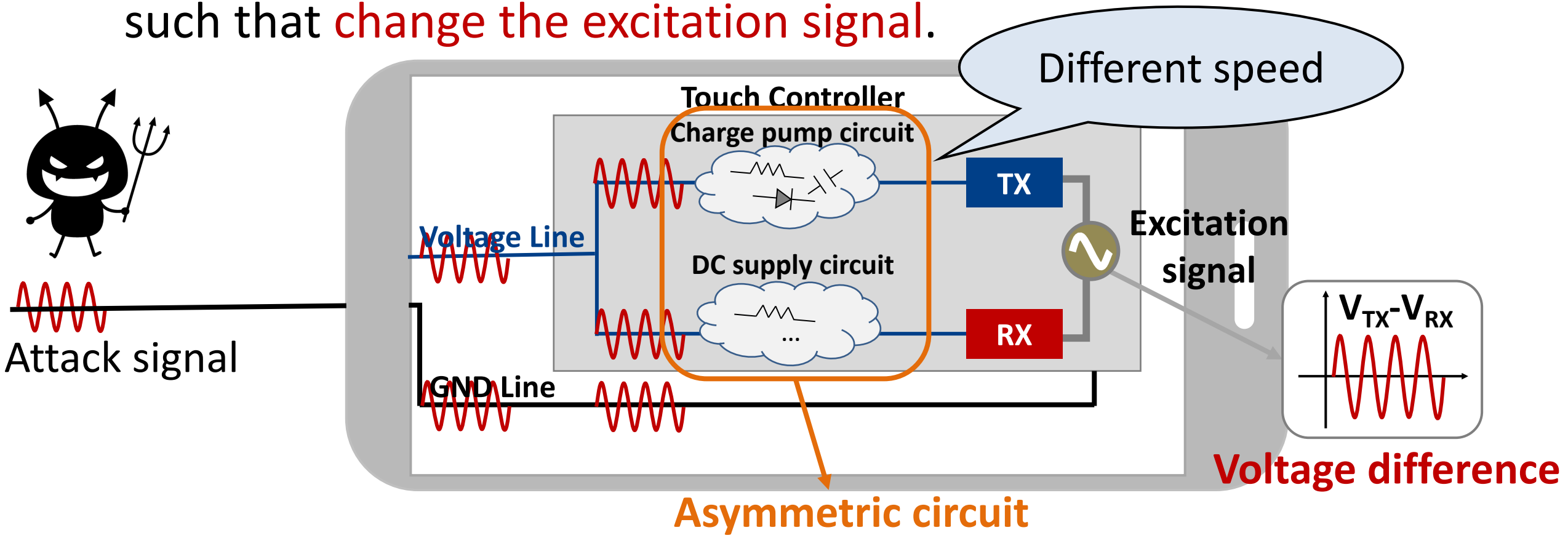
Where to inject attack signal?

- Usually, an attack signal injected via the GND line should have the **same impact on** the internal circuits.



Where to inject attack signal?

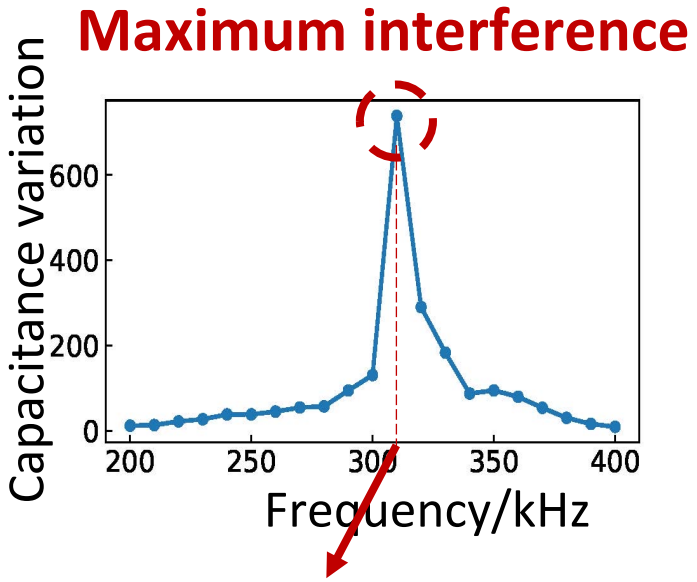
- In practice, due to the asymmetric circuit, an attack signal will create a voltage difference between the TX and RX electrodes such that change the excitation signal.



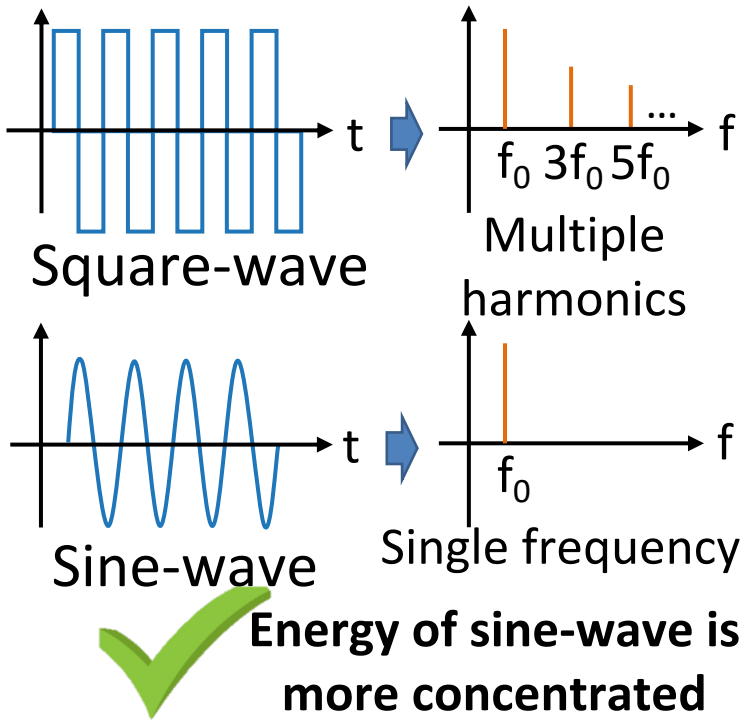
How to select an attack signal?

➢ Enhance the interference intensity and generate ghost touches.

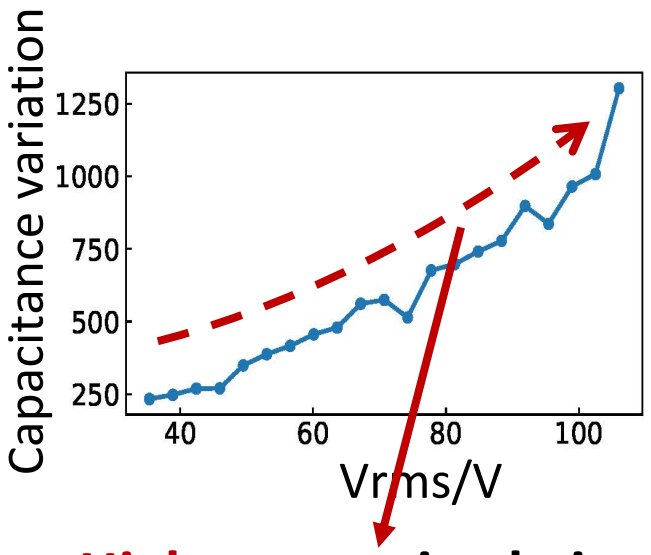
a. Attack Signal Frequency



b. Attack Signal Type



c. Attack Signal Magnitude



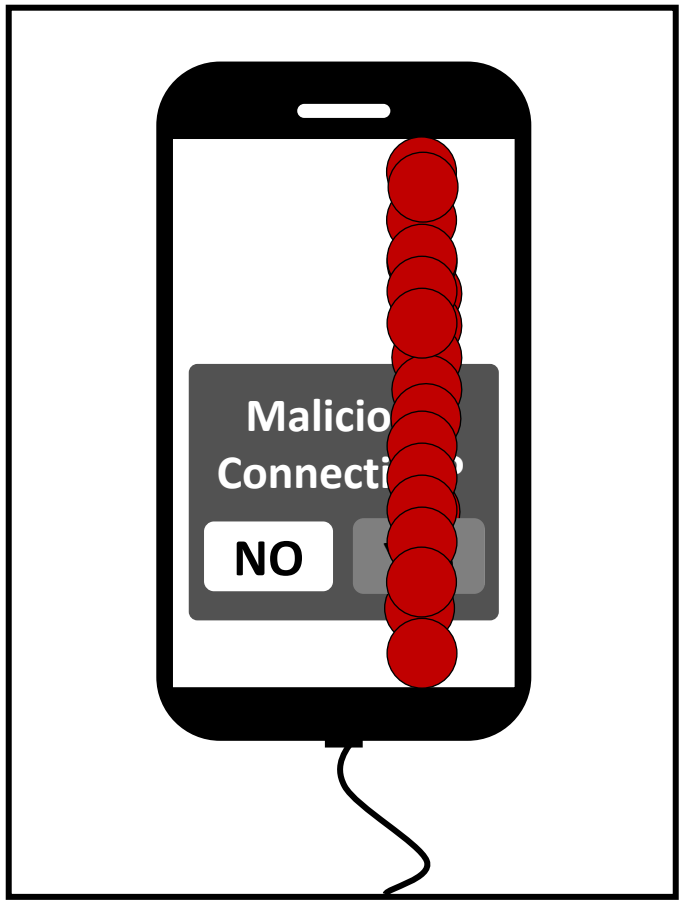
Attack design

➢ **Step1: Generate ghost touches**

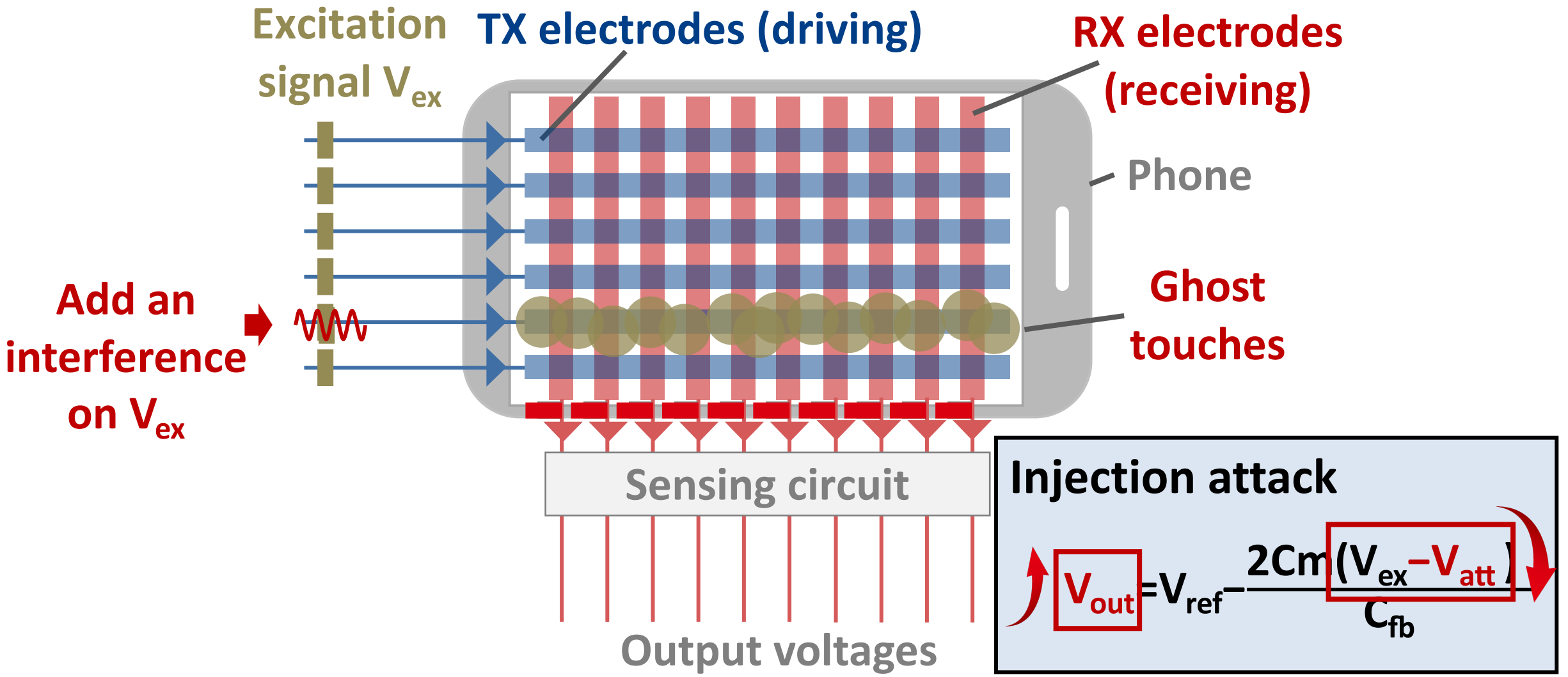
- Where to inject attack signal?
- How to select an attack signal?

➢ **Step2: Control ghost touches**

- Where are targeted positions?
- When to inject attack signals?



Step2: Control ghost touches



Injection attack

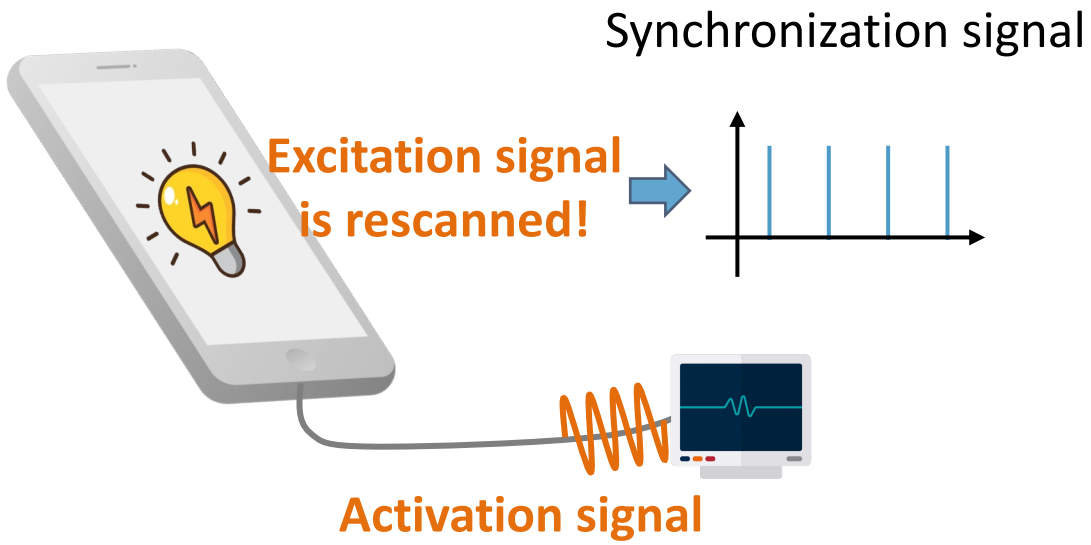
$$V_{out} = V_{ref} - \frac{2C_m(V_{ex} - V_{att})}{C_{fb}}$$

Step2: Control ghost touches

➢ Acquire synchronization signal.

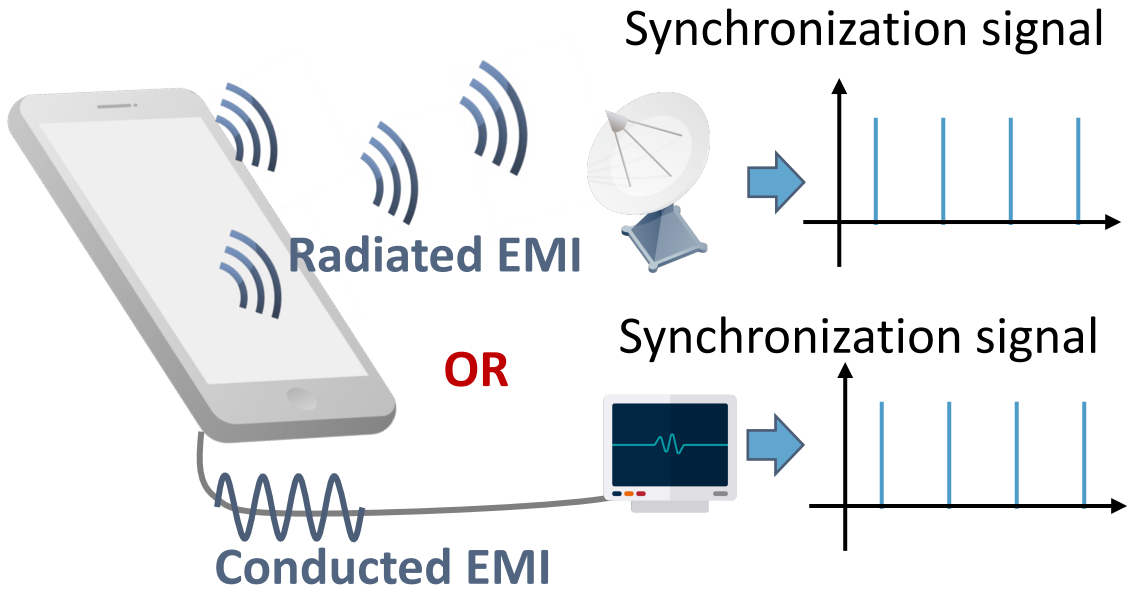
Method1: Active synchronization

- Smartphone can adaptively adjust its refresh rate



Method2: Passive synchronization

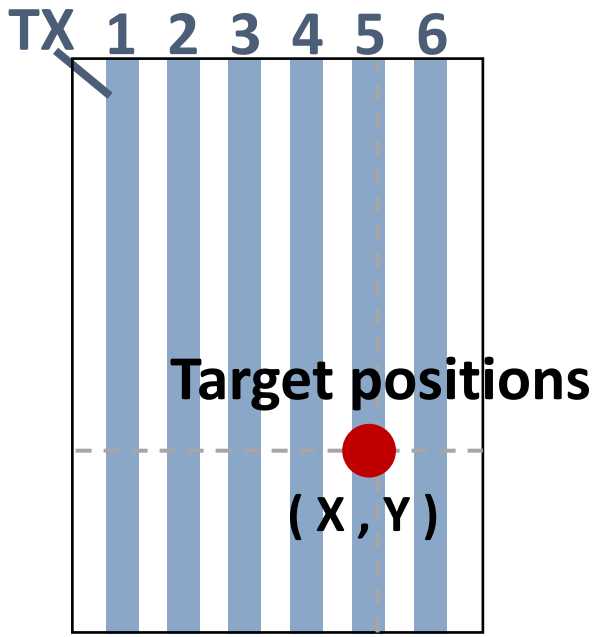
- Extract synchronization signal from the radiated or conducted EMI.



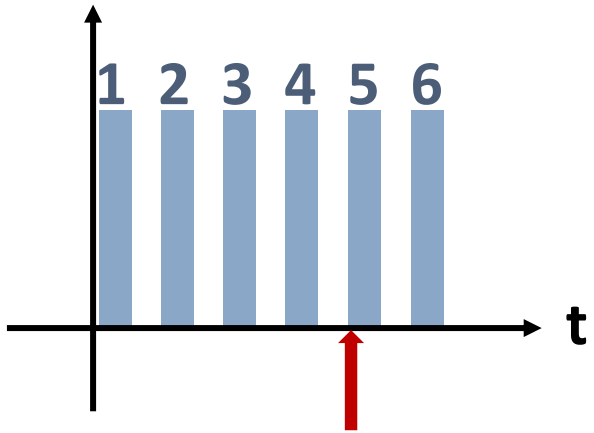
Step2: Control ghost touches

➢Estimate target positions and calculate the transmission time.

1. Where are the target positions of touches?

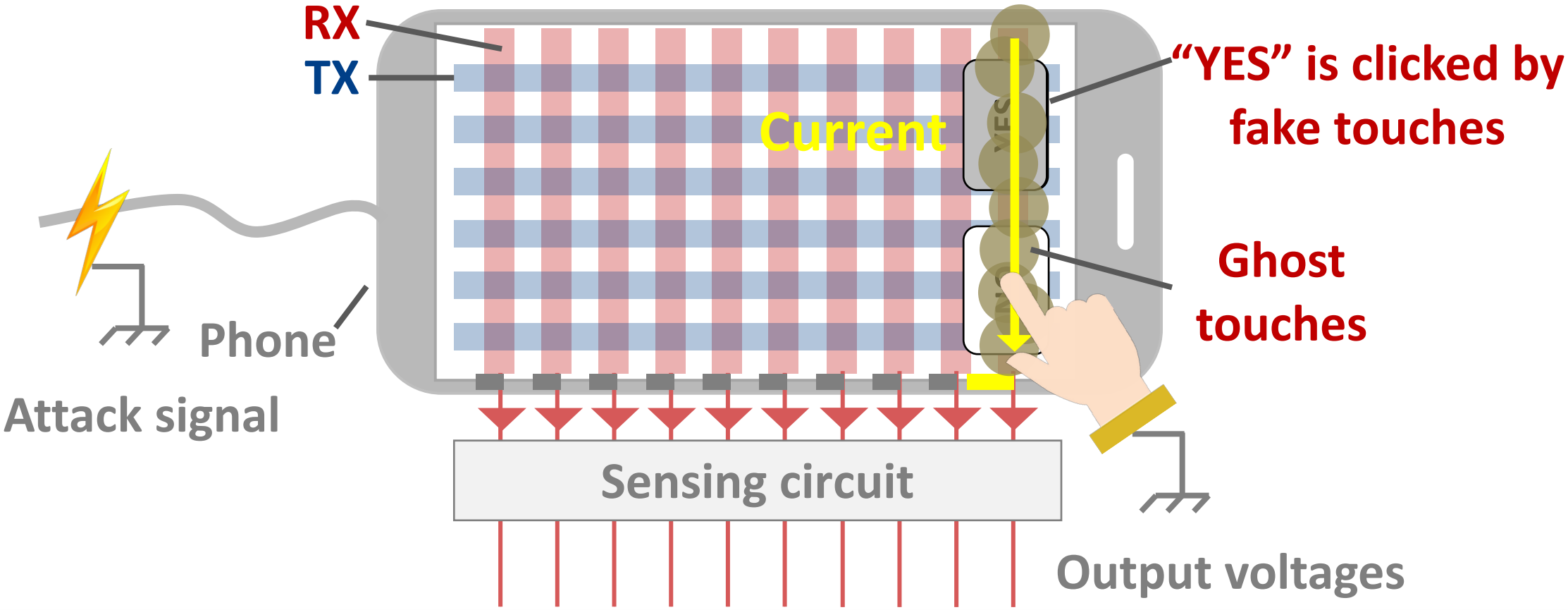


2. When to inject attack signals?



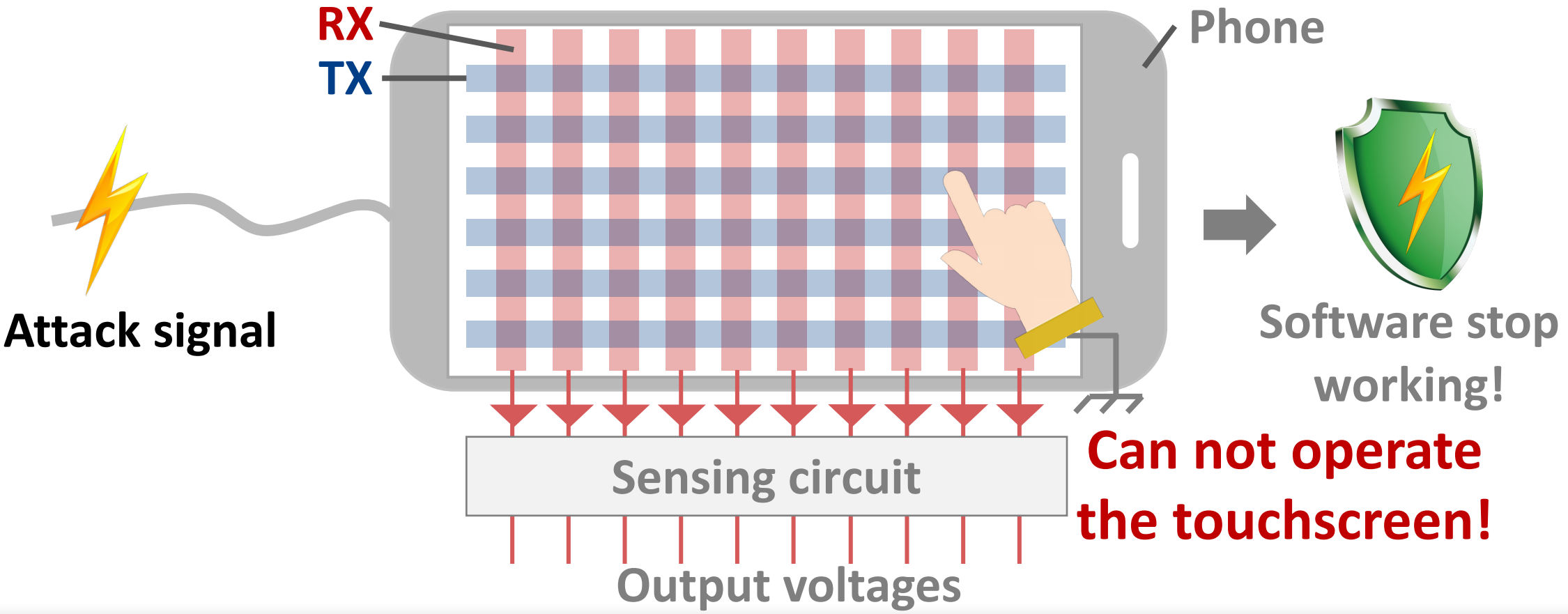
Alteration attack

➢ Human's finger will absorb charges and create a current on the RX electrode.



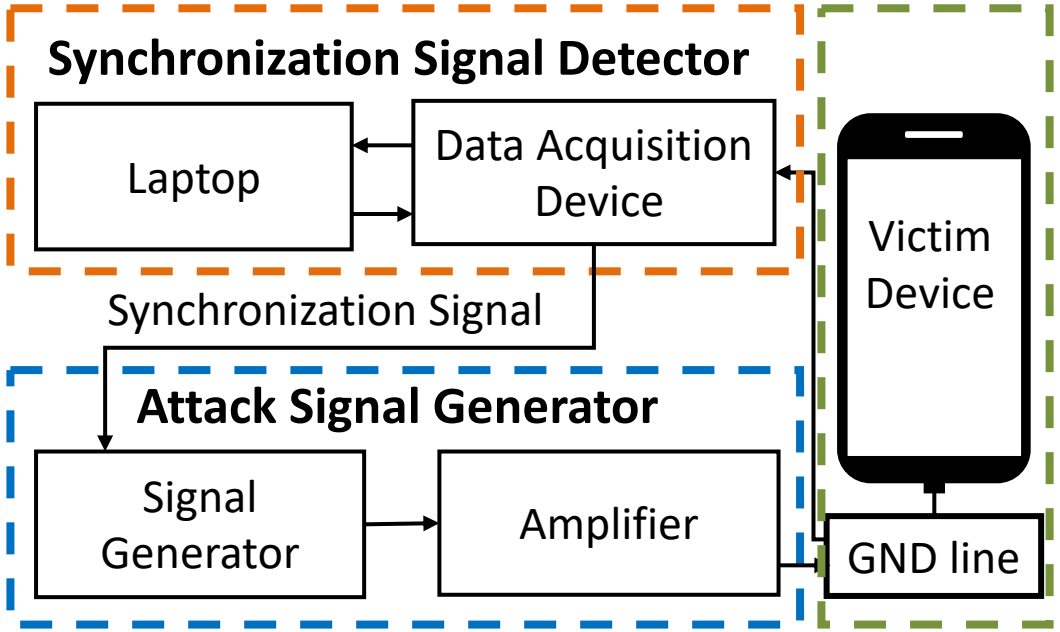
Denial-of-Service attack

➢ DoS attack exploits the electrostatic discharge(ESD)-induced soft failure mechanism and disable the touch service.

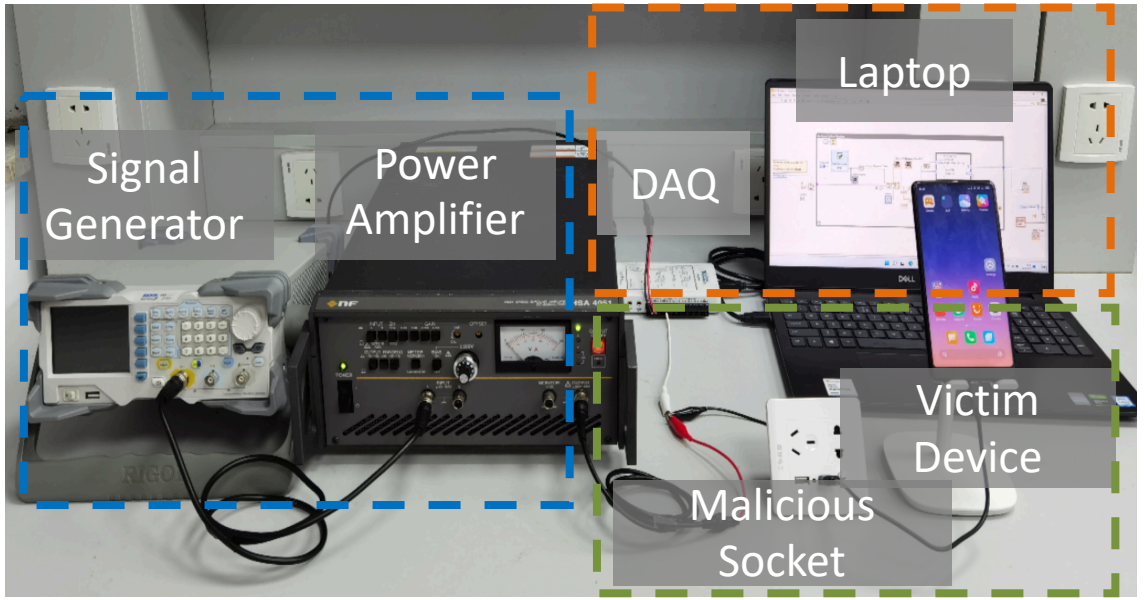


Experimental setup

WIGHT Attack System



Physical Setup



Target devices: 6 smartphones, **1** tablet, **2** standalone touchscreen panels.

Overall performance

Models	spec.	dir.	ref. / kHz	exc/ kHz	Injection attack			RX-targeted attack			DoS attack		
					f./kHz	vrms /V	succ.	f./kHz	vrms /V	succ.	f./kHz	vrms /V	succ.
Xiaomi Mi Mix 2	USB-C	V	119.7	323	309	310	**19/30**	322	220	**20/30**	230	60	**30/30**
Huawei nova 2	USB-C	V	116.2	140.7	18.83	448	**14/30**	133	250	**16/30**	130	330	**10/30**
Apple iPhone SE	Lightning	H	60	303	12	300	**17/30**	120	300	**11/30**	20	220	**30/30**
Apple iPhone 7	Lightning	H	60	120	12	230	**19/30**	120	200	**10/30**	300	200	**28/30**
Samsung Galaxy S20 FE	USB-C	H	118.12	416	420	300	**13/30**	416	70	**18/30**	416	230	**30/30**
LG Nexus 5X	USB-C	H	120	278	278	300	**25/30**	290	110	**9/30**	290	200	**30/30**
Asus Google Nexus 7	Micro	H	120	129	300	280	**13/30**	129	30	**14/30**	85	270	**30/30**
CAPATIVATE-PHONE	Micro	V	30	120	120	300	**29/30**	120	130	**13/30**	300	260	**28/30**
9-inch touch panel	USB-A	V	70	185	185	300	**19/30**	185	70	**16/30**	243	260	**16/30**

WIGHT can achieve injection, alteration, DoS attacks at average success rates of 62.2%, 47%, 86.9%, respectively.

Factors

1. Magnitudes

Vrms./V	53	71	88	110	113
Xiaomi MIX2	0%	0%	0%	50%	65%
LG Nexus X5	0%	80%	85%	90%	90%

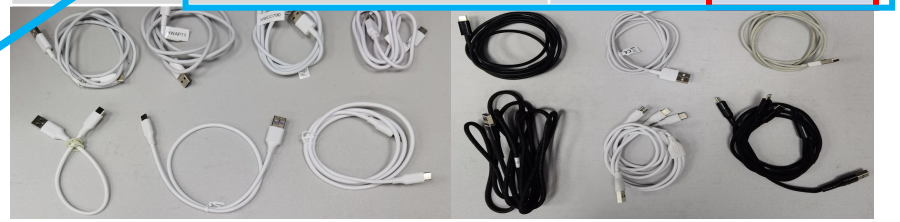
1. **Higher signal magnitudes** ⇩ **Higher success rate**

2. **WIGHT is effective with charging cables and power adapters**

3. **Small-brand cables with lower power efficiency but are safer to attack**

2. Charging cables

	Charging cable	Eff.	Succ.
Big-brand charging cables	HUAWEI CP51	62%	8/10
	HUAWEI AP71	100%	7/10
	HUAWEI CC790	99%	7/10
	HUAWEI AP70	93%	3/10
	iPhone	100%	8/10
	ZMI	100%	8/10
Samll-brand charging cables	QOOVI CC-500C	47%	7/10
	SmartDevil A51-104	100%	8/10
	SmartDevil A51-106	100%	7/10
	SmartDevil A51-110	100%	8/10
	PISEN LS-TC09-2000	16%	0/10
	QOOVI CC-022A	50%	0/10
	Remax	57%	0/10



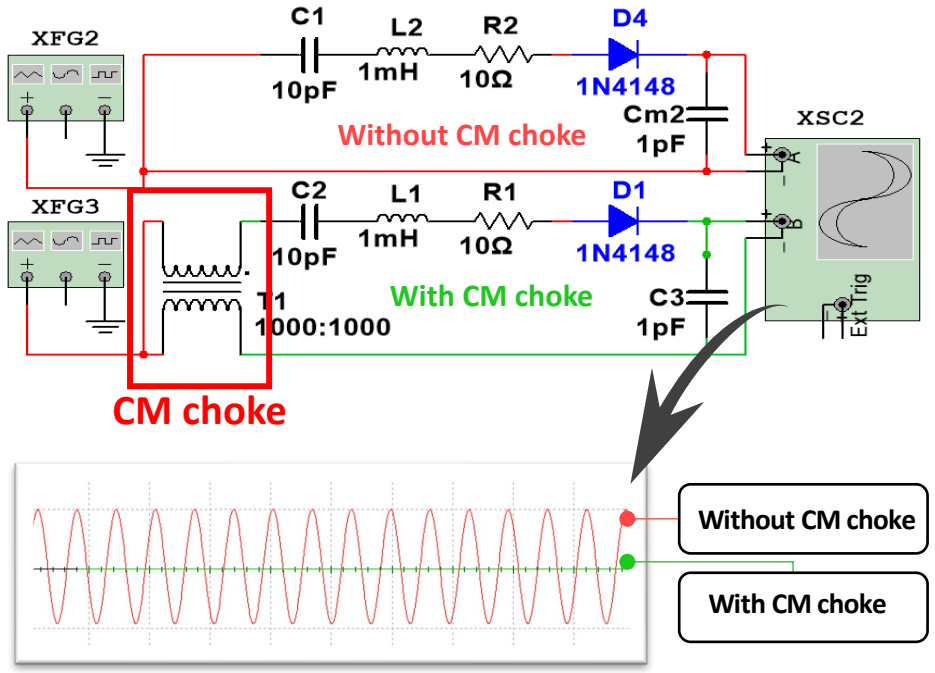
3. Power adapters

Adapters	Effi	Succ.
OPPO VCA7GACH	116%	7/10
RECCI RCT-N02C	97%	9/10
QOOVI C213	96%	9/10
HUAWEI-050200	88%	7/10
Xiaomi A319-050100U	53%	6/10
SKK-S258	97%	7/10

Countermeasures

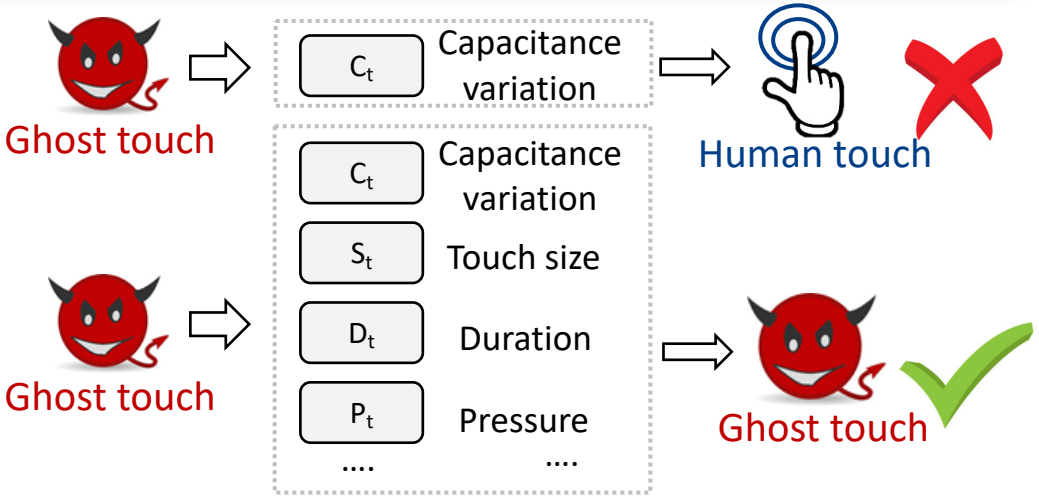
❑ Hardware-based Suppression

Ghost Blocker： Add a **CM choke** to block the path and suppress the attack signal.



❑ Software-based Detection

Use **multiple touch features** to differentiate human touches and ghost touches.



❑ Authentication

Database of trustworthy public charging stations.

Responsible disclosure

We have contacted the product security team at Apple, Samsung, Xiaomi and TEXAS INSTRUMENTS, and received their feedback.

Thank you for contacting the Apple Product Security team. Your message is important to us and will be reviewed by an Apple Representative.

Please use this email only to report security issues in Apple products or services. You may receive additional emails from us if we need additional information or clarification about a reported security issue in an Apple product or service. Apple Product Security does not respond to requests for technical support.

AppleCare

If you have received a phone call claiming to be from Apple, please contact Apple Support at https://support.apple.com/contact.

Please include the line below in follow-up emails for this request. Follow-up: 797077907 Hello Yan,

Thanks again for your report. Are you able to reproduce this when the device is locked?

Best regards,
Niklas
Apple Product Security

Hello Yan Jiang,

This is a confirmation that we have received the email, and thank you for reaching out to us regarding a security concern you have found.

If you are interested in our rewards program, you may also visit our official site below for reporting guidance and report us through the website.
Also note that you need to submit through "Create Report" in below page in order to be eligible for the rewards program:
https://security.samsungmobile.com/secu
https://security.samsungmobile.com/rew

Thank you very much.

Very Respectfully,
Samsung Mobile Security

小米安全中心 Xiaomi Security Center front page Submit a security bug Subm

oduce a simple attack: (1) (1) Connect the mobile phone (Xiaomi MIX2) with a sta
to the GND line of the charging cable, and the negative pole is left floating. (3) C
with a frequency of 309 kHz and an amplitude of 320 Vpp. (4) Synchronize the C
acts on the expected TXs.
y questions, you can contact us by email (Yan Jiang (Zhejiang University) yj98@
r
g University) yj98@zju.edu.cn
University) xji@zju.edu.cn
g University) eekaiwang@zju.edu.cn
hnical University of Darmstadt) richard.mitev@trust.tu-darmstadt.de
g University) yanchen@zju.edu.cn
ghi (Technical University of Darmstadt) ahmad.sadeghi@trust.tu-darmstadt.de
iang University) wyxu@zju.edu.cn

under review under repair Repa

Vulnerability: Touchscreen Component Vulnerability
bility has been assigned an auditor to follow up, please be patient
bility has been confirmed, you will get 30 contribution points and 30 c

Subject: RE: [EXTERNAL] Vulnerability report: injecting controlled ghost touches on TEXAS products via the charging cable

Hi Yan Jiang,

Thank you for your submission to the TI PSIRT. We will review your submission and respond in approximately 3-5 business days. Feel free to reach out to the TI PSIRT in case you have any questions on status or to provide additional information that would be helpful in evaluating your submission.

We also ask that you review the TI PSIRT Responsible Handling Policy, so that you can be aware of the expectations TI has for PSIRT submissions

Regards,
TI PSIRT

Conclusion

- Proposed **WIGHT**, the first ghost touch attack against capacitive touchscreens by injecting CM signals via a charging cable.
- Analyzed the **underlying principle** of successful ghost-touch injection theoretically and experimentally.
- Validated the **feasibility** of WIGHT on 9 commercial touchscreen devices and proposed **countermeasures** to mitigate the threat.

WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens

USSLAB Website: www.usslab.org

System Security Lab Website: www.informatik.tu-darmstadt.de/systemsecurity/system_security_lab_sys

Corresponding authors:

xji@zju.edu.cn

wyxu@zju.edu.cn

ZHEJIANG UNIVERSITY

TECHNISCHE UNIVERSITÄT DARMSTADT