MobiCom 2023

Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning

Tao Ni[*], Jianfeng Li[†], Xiaokuan Zhang[‡], Chaoshun Zuo[¶],
Wubing Wang[‖], Weitao Xu[*], Xiapu Luo[§], Qingchuan Zhao[*]

[*]*City University of Hong Kong* [†]*Xi'an Jiaotong University* [‡]*George Mason University*
[¶]*The Ohio State University* [‖]*DBAPP Security Co., Ltd* [§]*The Hong Kong Polytechnic University*

Introduction

USB Cables

Cable-based Power Banks

Wireless Chargers

Introduction

USB Cables

Cable-based Power Banks

Wireless Chargers

Charger-Surfing (USENIX-SEC'20)

WIGHT (Oakland'22)

GhostTalk (NDSS'22)

Cour *et al.* (CCS'21)

Wu *et al.* (ACSAC'21)

EM-Surfing (TDSC'22)

Dai *et al.* (Oakland'23)

Wireless Charging Power Banks

Wireless Charging Power Banks

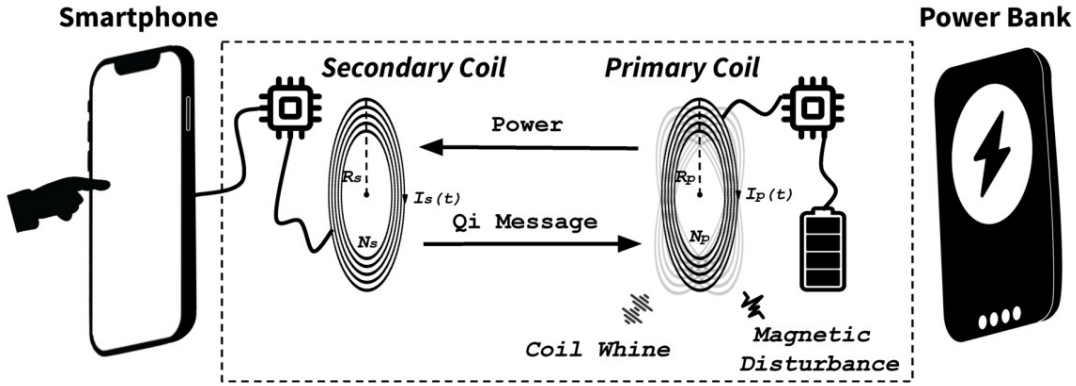
Wireless Charging Power Banks

Is this contactless charging accessory safe?

Wireless Charging Power Banks

Wireless Charging Power Banks

Charging Principles

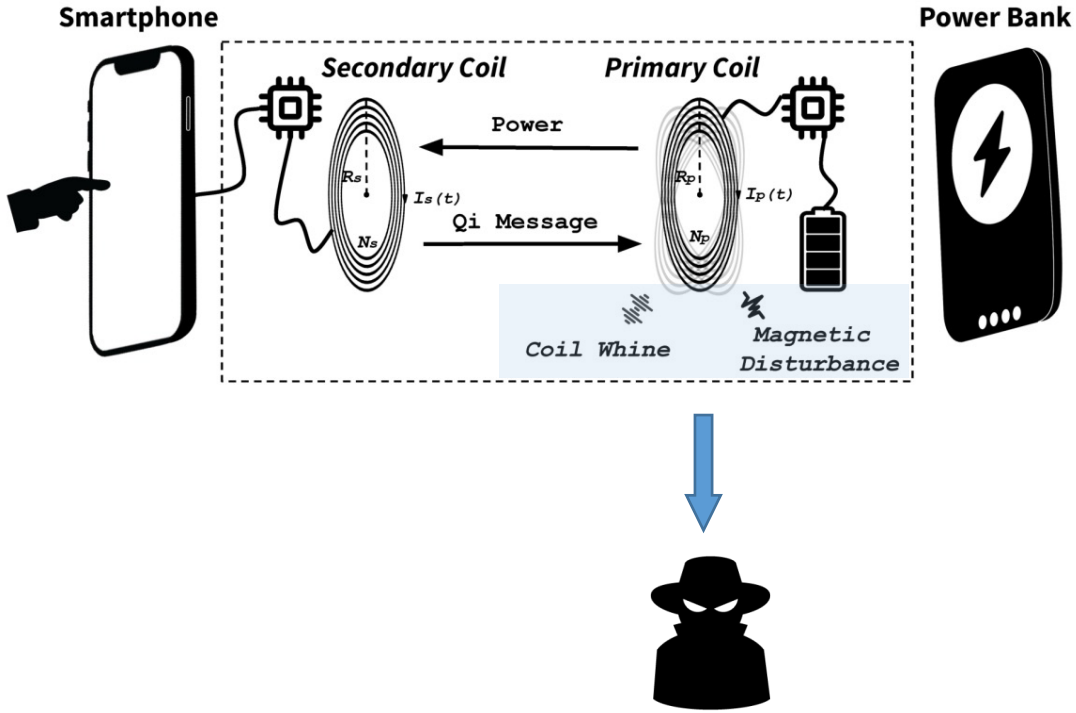


Is this contactless charging accessory safe?

Wireless Charging Power Banks

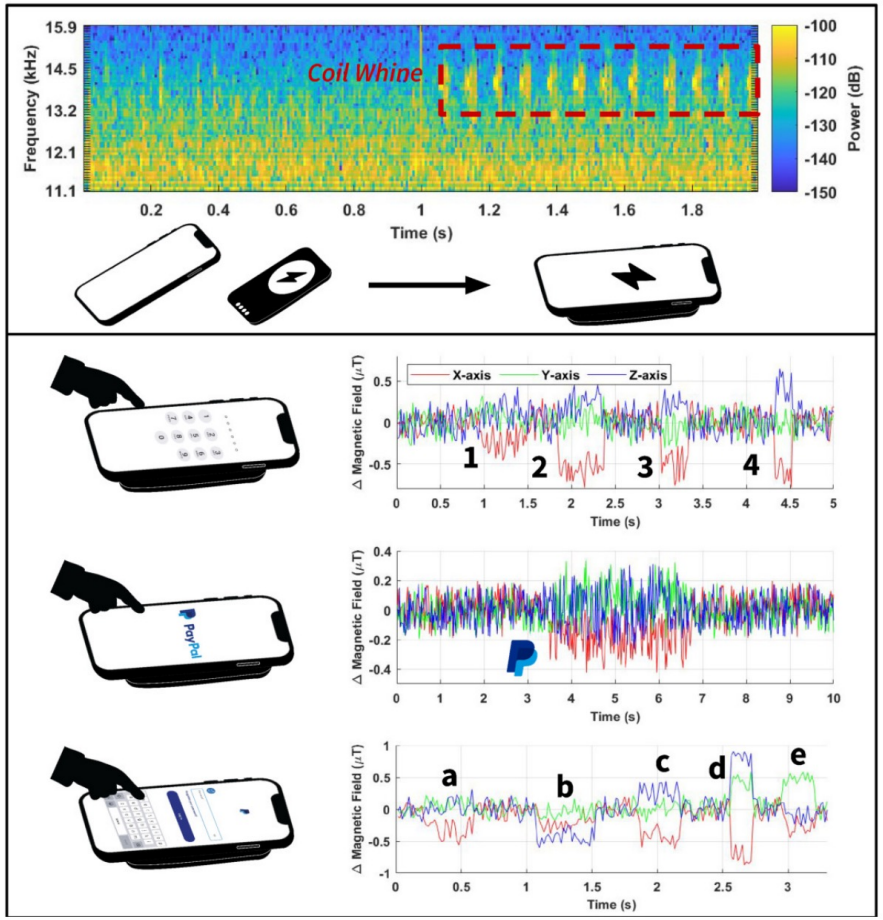
Wireless Charging Power Banks

Charging Principles

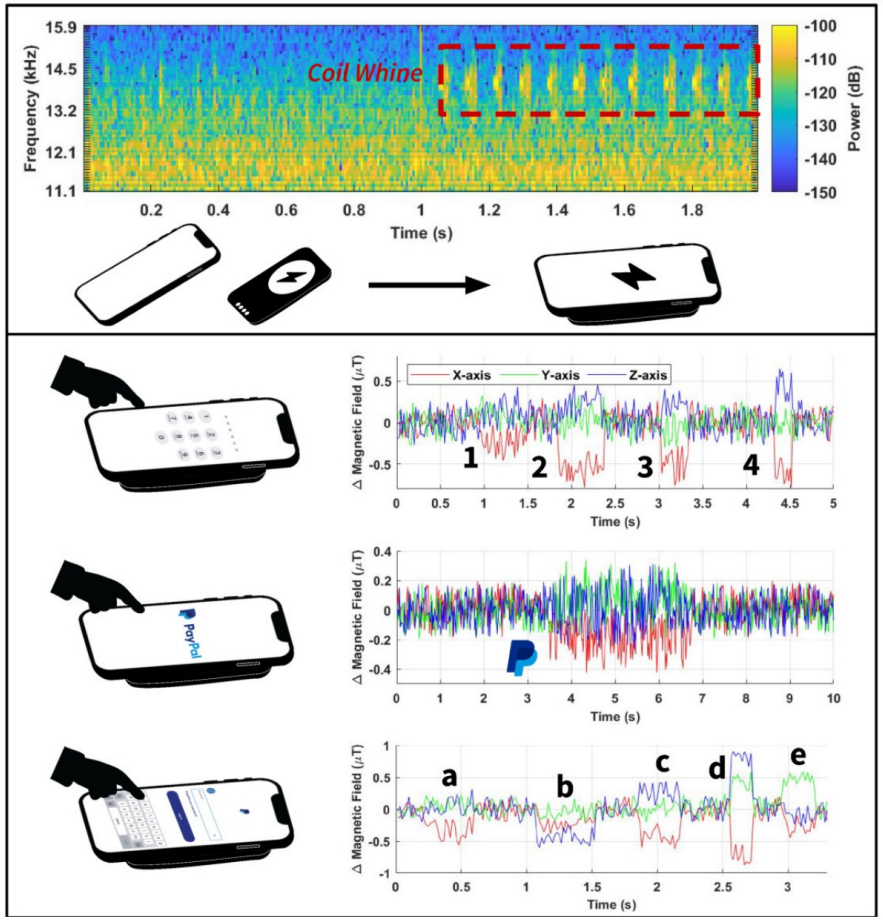


Is this contactless charging accessory safe?

Motivating Example & Physical Phenomena



Motivating Example & Physical Phenomena

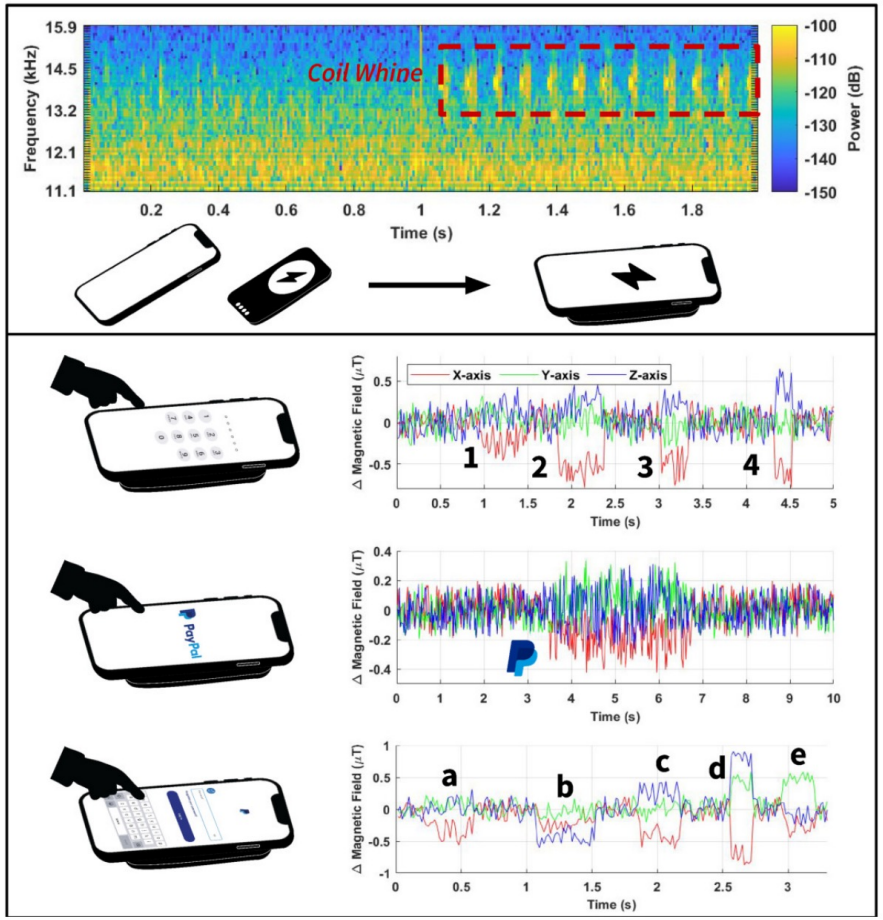


Coil Whine

Vibration and deformation of the coil

- Maxwell stress tensor
- Magnetostriction
- Lorentz force

Motivating Example & Physical Phenomena



Coil Whine

Vibration and deformation of the coil

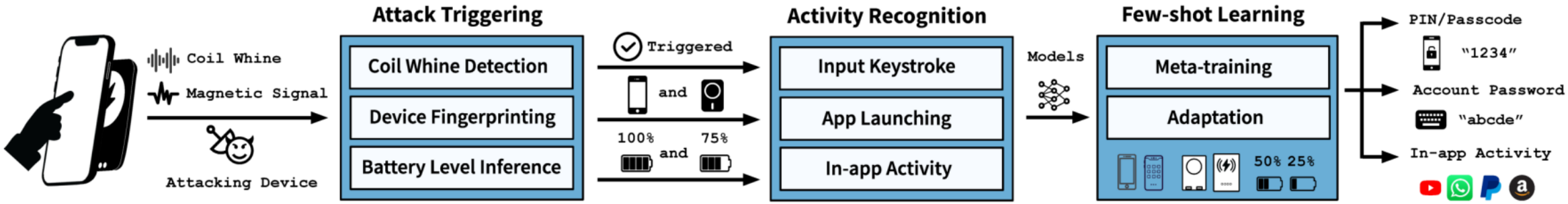
- Maxwell stress tensor
- Magnetostriction
- Lorentz force

Magnetic Field Disturbance

Perturbations of ambient magnetic field

- Load changes (Charging smartphone)
- Touchscreen characteristics
- Finger-coupling effects

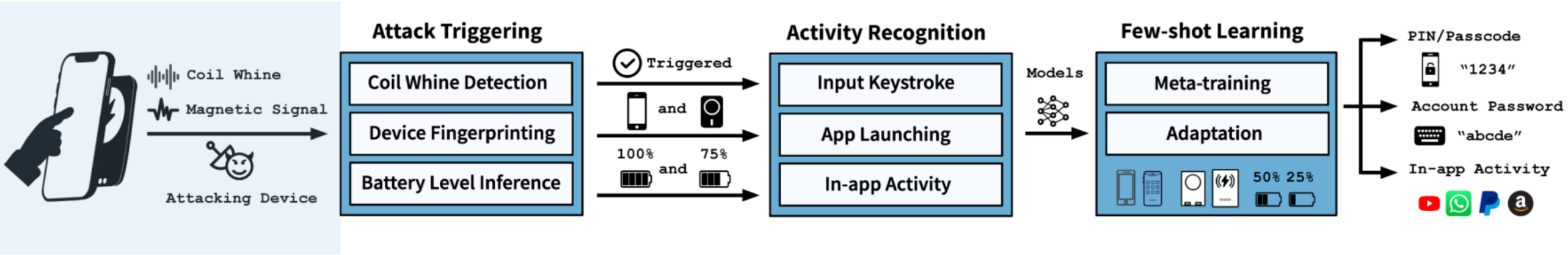
BankSnoop – A Contactless Side-Channel Attack Framework



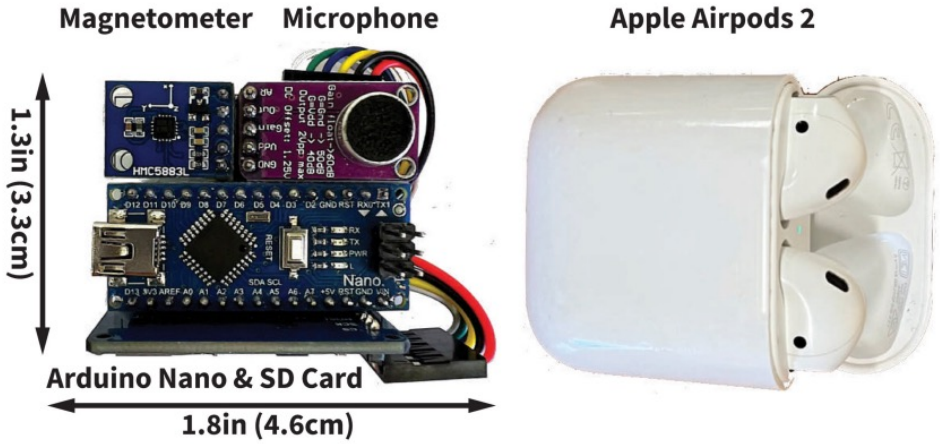
Comparison with Prior Works

Attacks	Attack surface	Contactless	No need to Compromise devices	No prior knowledge of devices	Fine-grained user privacy	Domain adaptive
Cour et al. (CCS'21)	Current in power line	✗	✗	✗	✗	✗
Wu et al. (ACSAC'21)	Inductive current	✓	✓	✗	✗	✗
EM-Surfing (TDSC'22)	Inductive voltage	✗	✗	✗	✓	✗
Charger-Surfing (Security'20)	Current in USB cable	✗	✗	✗	✓	✗
GhostTalk (NDSS'22)	Current in USB cable	✗	✗	✗	✓	✗
BankSnoop (Our work)	*Coil whine and Magnetic field*	✓	✓	✓	✓	✓

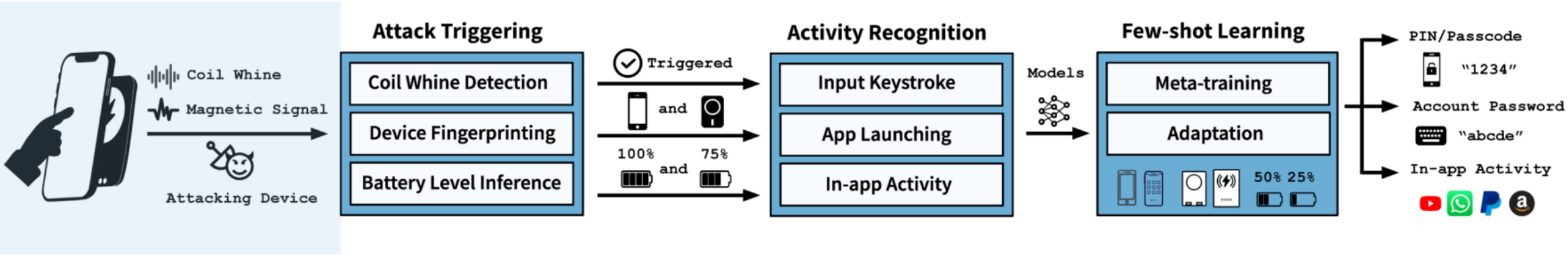
Attacking Device & Scenarios



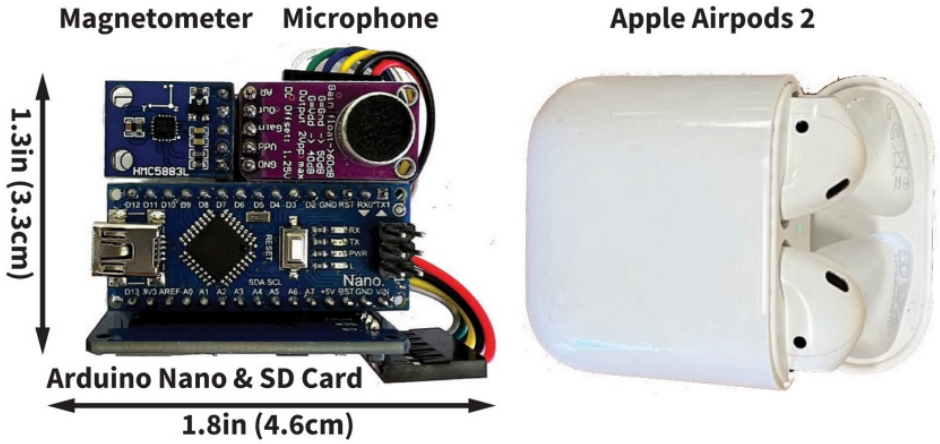
Attacking Device



Attacking Device & Scenarios



Attacking Device

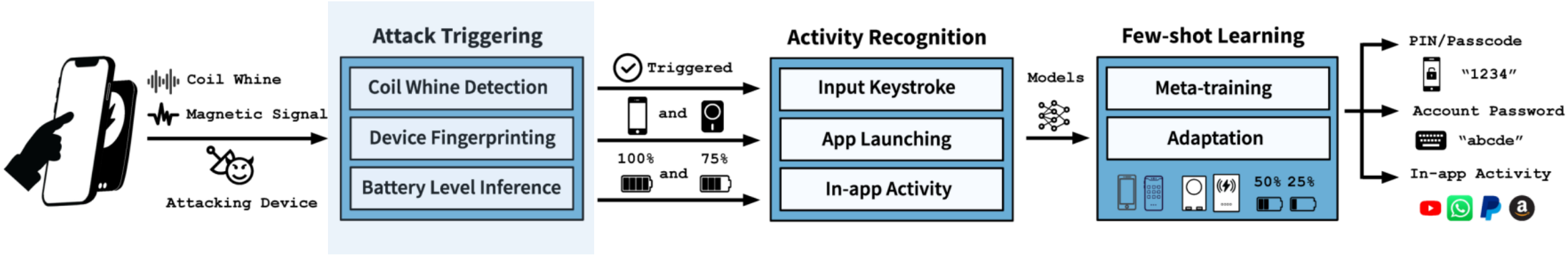


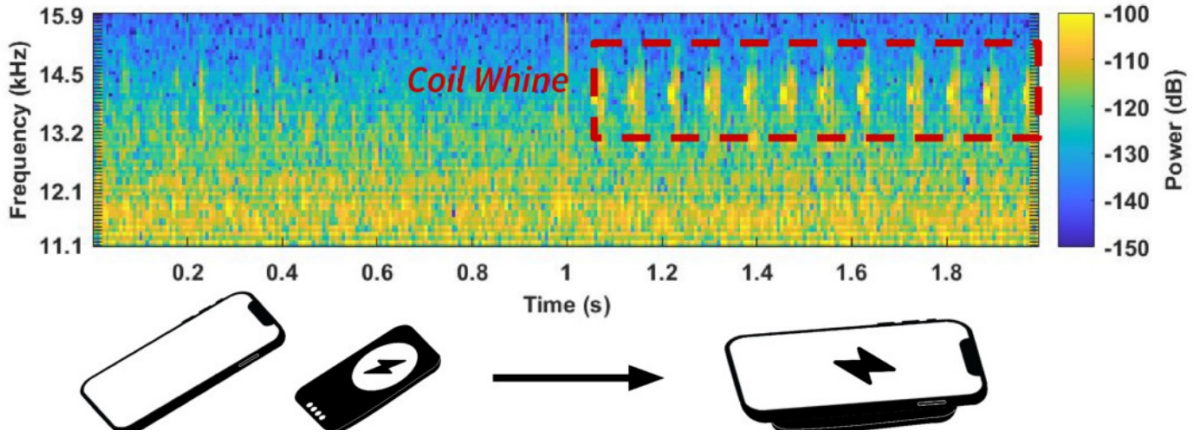
Attack Scenarios

Underneath table

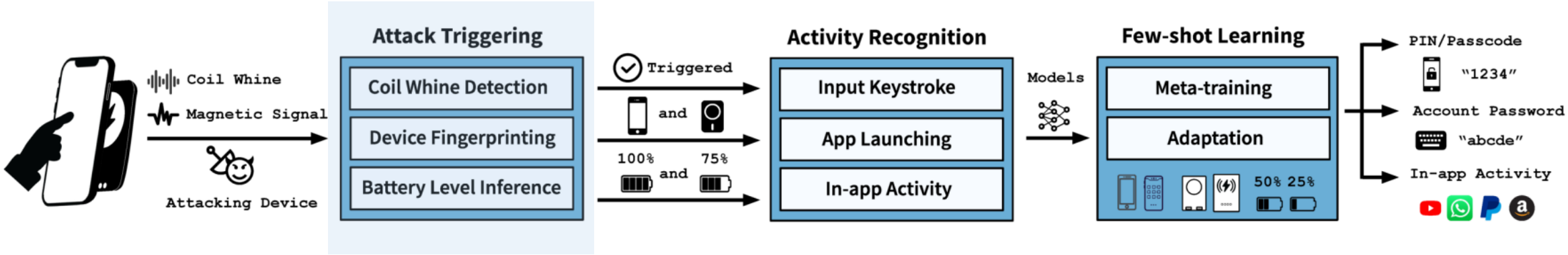
Near the devices

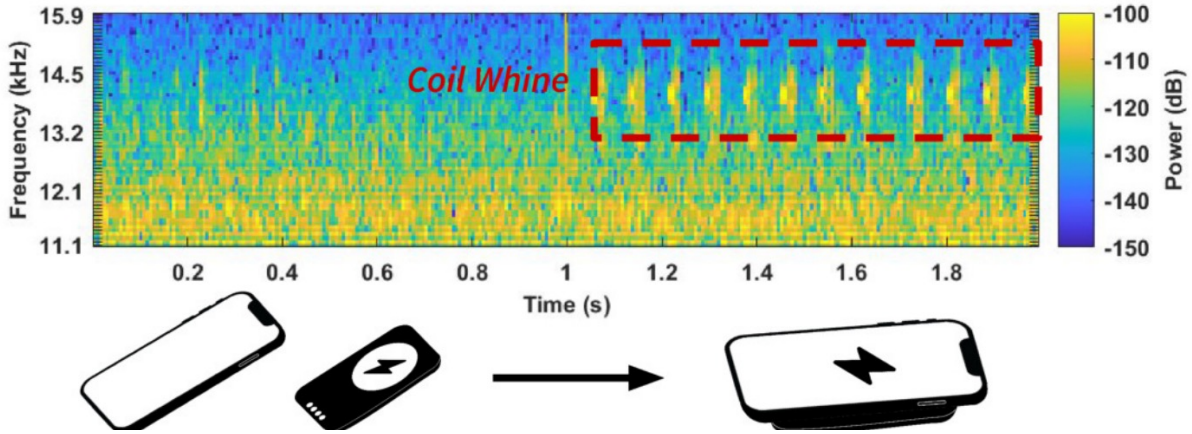
Attack Triggering – Coil Whine Detection

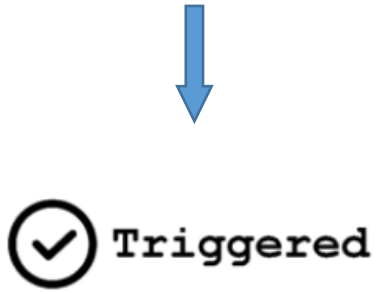




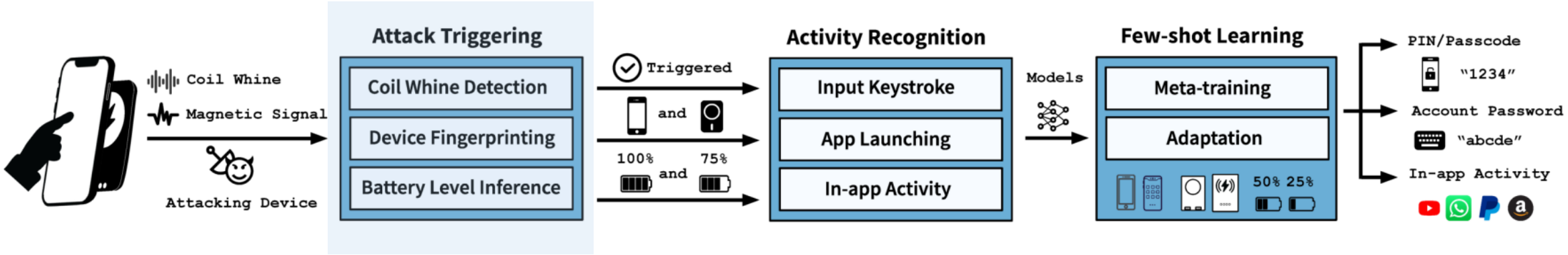
Attack Triggering – Coil Whine Detection







Attack Triggering – Device Fingerprinting



Power Banks

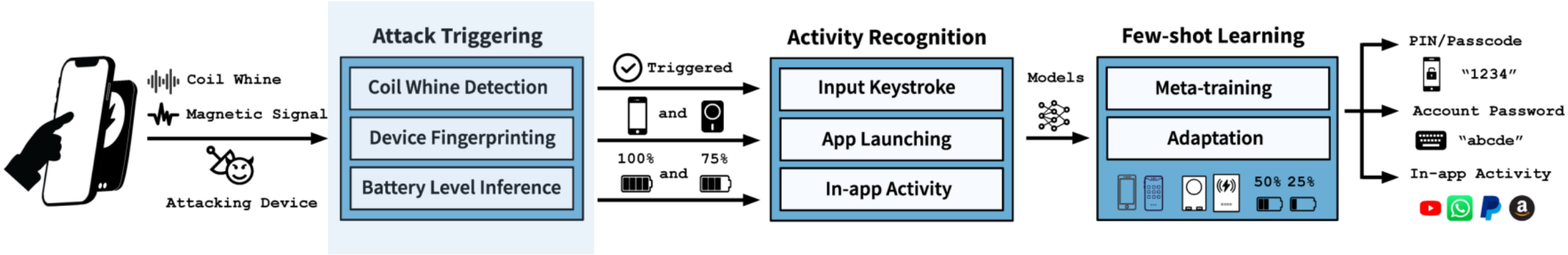
- P_1 : EGO MAGPOWER 2
- P_2 : Anker MagGo
- P_3 : Apple MagSafe Battery Pack
- P_4 : Belkin BOOSTCHARGE

×

Smartphones

- S_1 : iPhone 13 Pro
- S_2 : iPhone 12
- S_3 : iPhone 11
- S_4 : Samsung S10

Attack Triggering – Device Fingerprinting



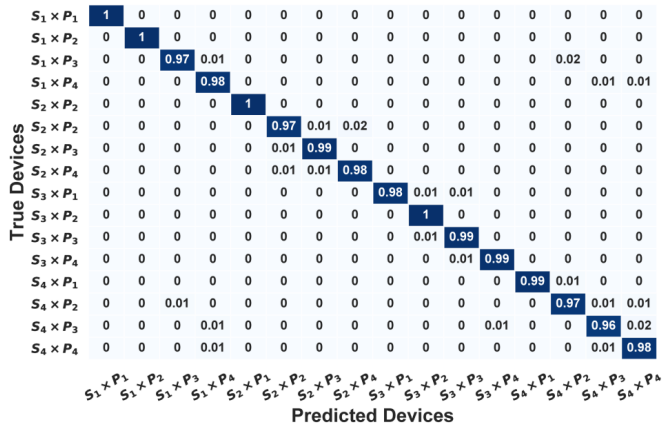
Power Banks

- P_1 : EGO MAGPOWER 2
- P_2 : Anker MagGo
- P_3 : Apple MagSafe Battery Pack
- P_4 : Belkin BOOSTCHARGE

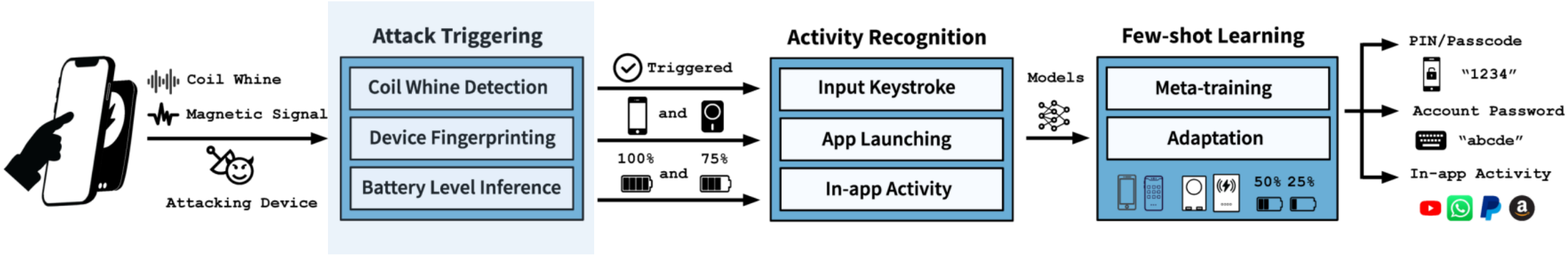
×

Smartphones

- S_1 : iPhone 13 Pro
- S_2 : iPhone 12
- S_3 : iPhone 11
- S_4 : Samsung S10

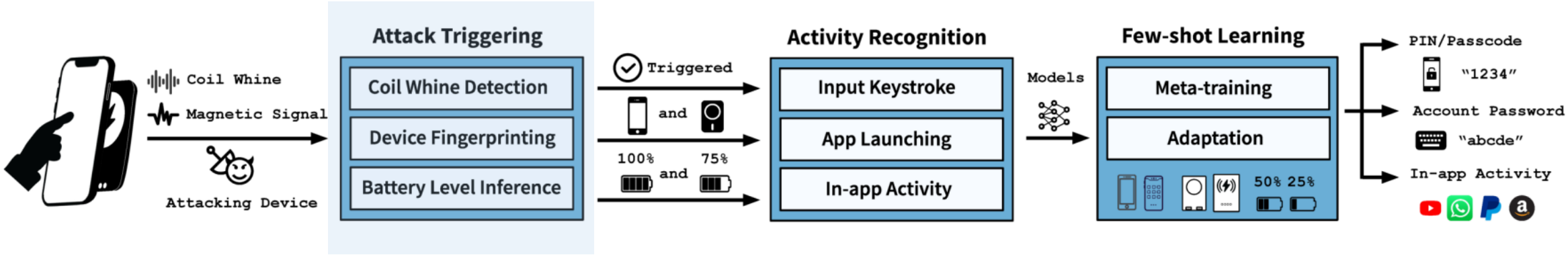


Attack Triggering – Battery Level Inference



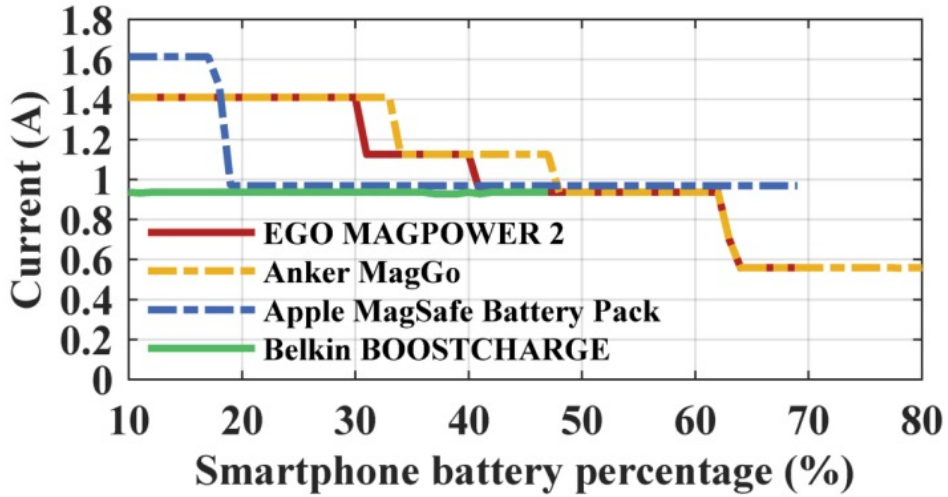
RQ1: Do different power banks present different battery levels in a wireless charging process?

Attack Triggering – Battery Level Inference

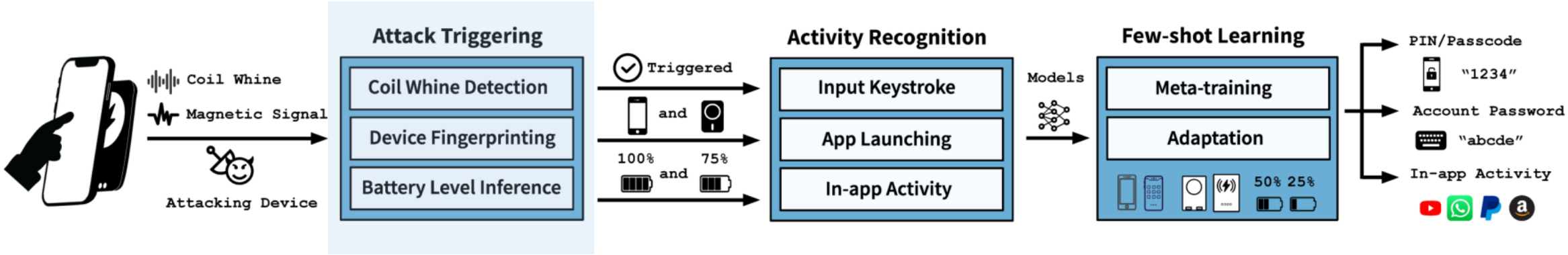


RQ1: Do different power banks present different battery levels in a wireless charging process?

Answer to RQ1: Different power banks present different charging patterns, and some (e.g., EGO MAGPOWER 2, Anker MagGo) present ladder-like battery levels.

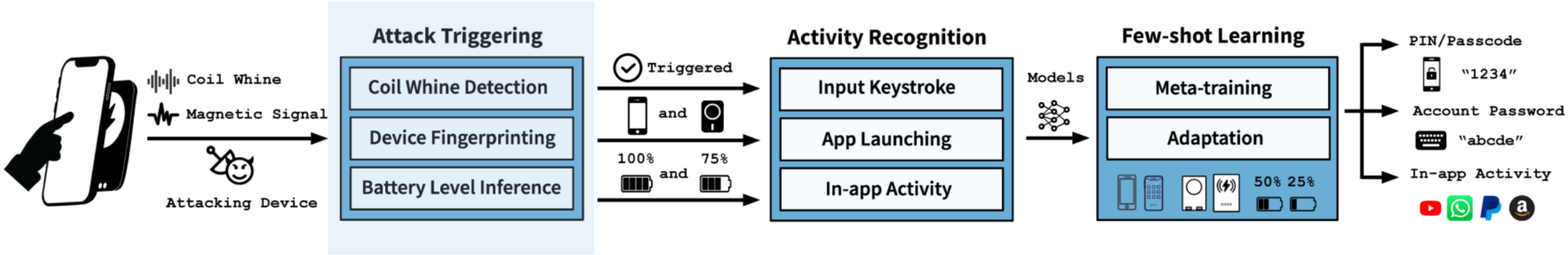


Attack Triggering – Battery Level Inference



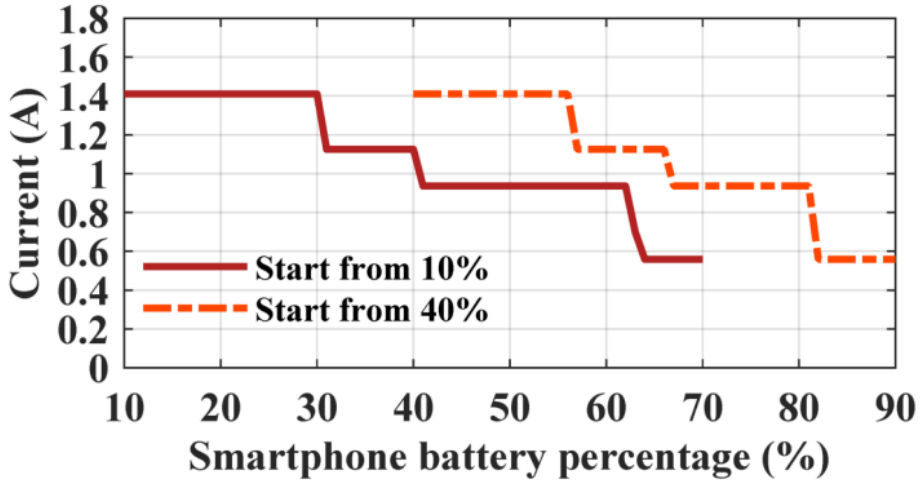
RQ2: Does the initial battery percentage of the smartphone impacts the inductive charging current?

Attack Triggering – Battery Level Inference

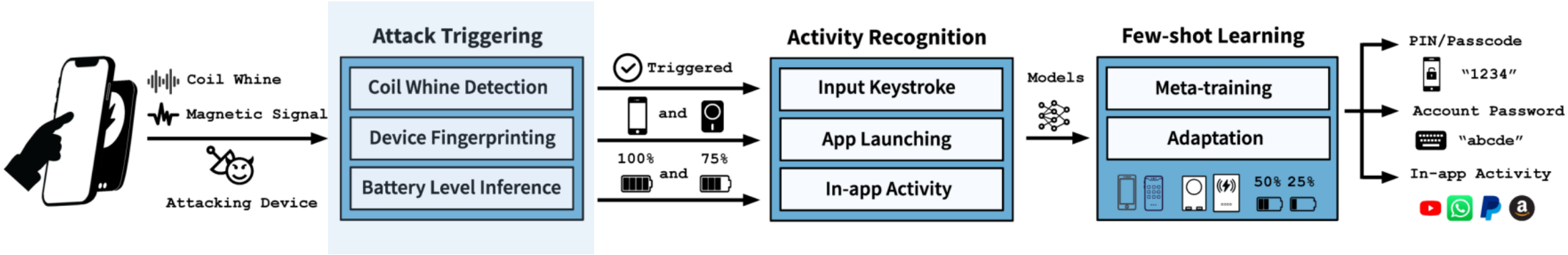


RQ2: Does the initial battery percentage of the smartphone impacts the inductive charging current?

Answer to RQ2: The inductive charging current in the secondary coil depends on the battery level of the power bank regardless of the smartphone's initial battery percentage.

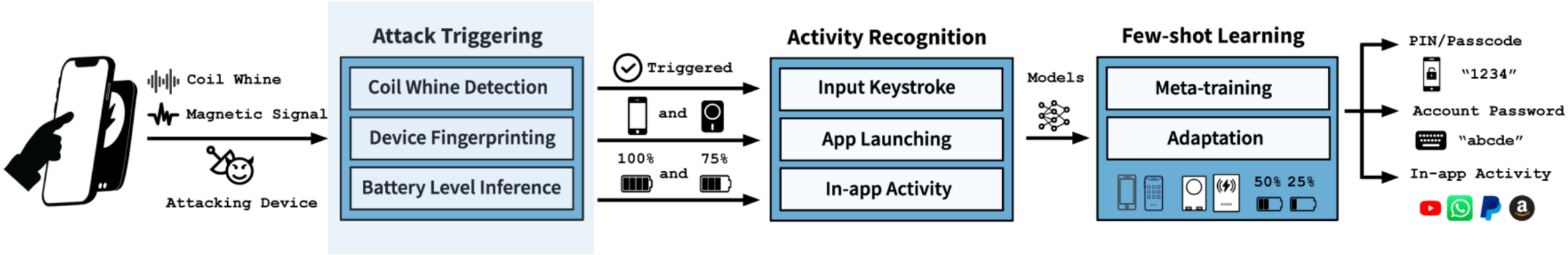


Attack Triggering – Battery Level Inference



RQ3: Can CDFs of magnetic field strength differences distinguish the battery levels of a power bank?

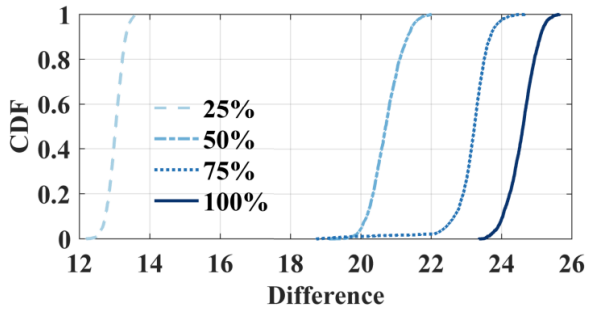
Attack Triggering – Battery Level Inference



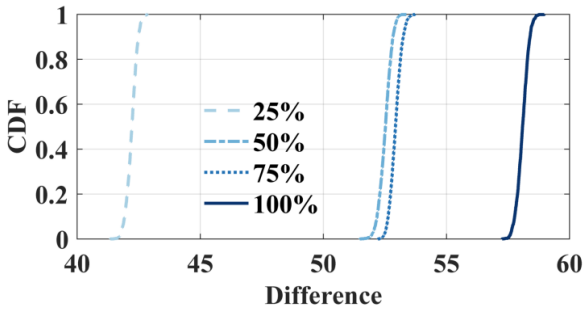
RQ3: Can CDFs of magnetic field strength differences distinguish the battery levels of a power bank?

$$Mag_s(t) = \sqrt{Mag_x^2(t) + Mag_y^2(t) + Mag_z^2(t)}$$

Answer to RQ3: We can use CDFs of the magnetic field strength differences as the measurement to distribute different battery levels of a wireless charging power bank.

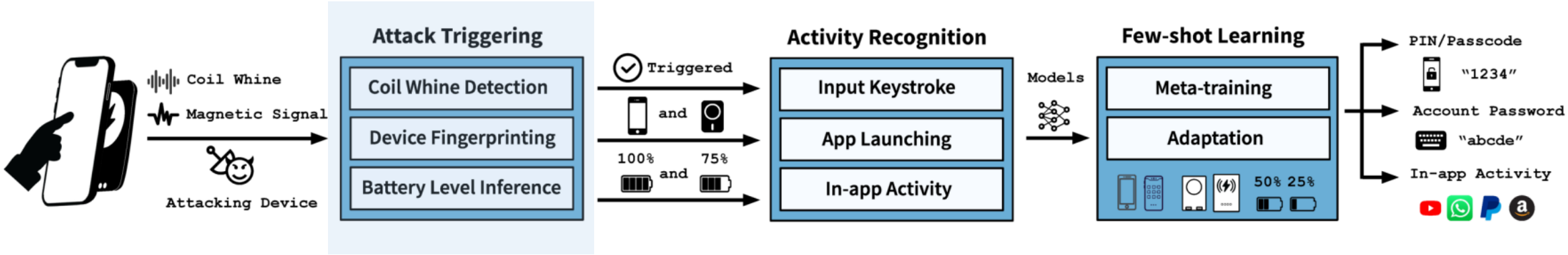


(a) EGO MAGPOWER 2.



(b) Anker MagGo.

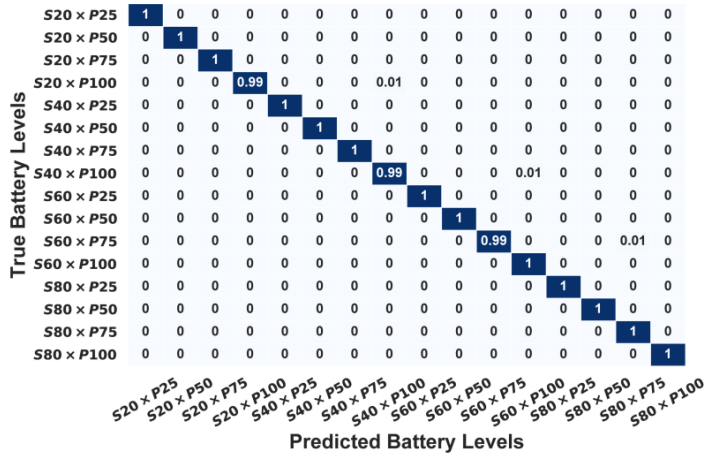
Attack Triggering – Battery Level Inference



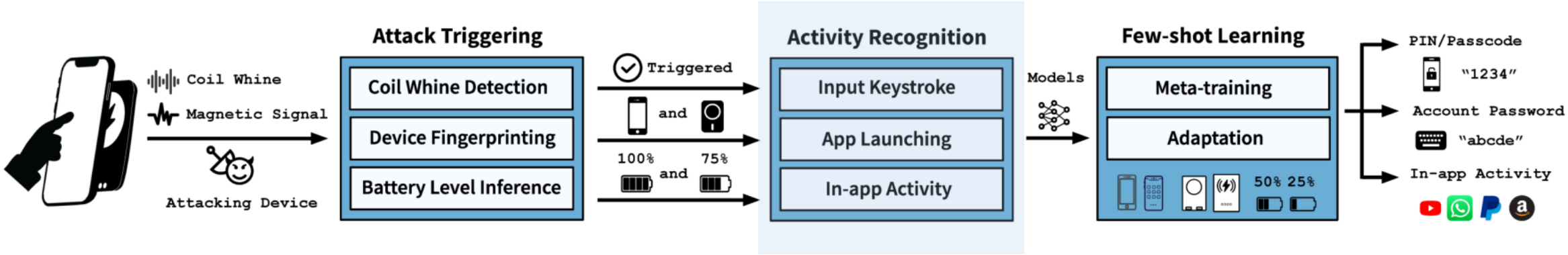
RQ3: Can CDFs of magnetic field strength differences distinguish the battery levels of a power bank?

Answer to RQ3: We can use CDFs of the magnetic field strength differences as the measurement to distribute different battery levels of a wireless charging power bank.

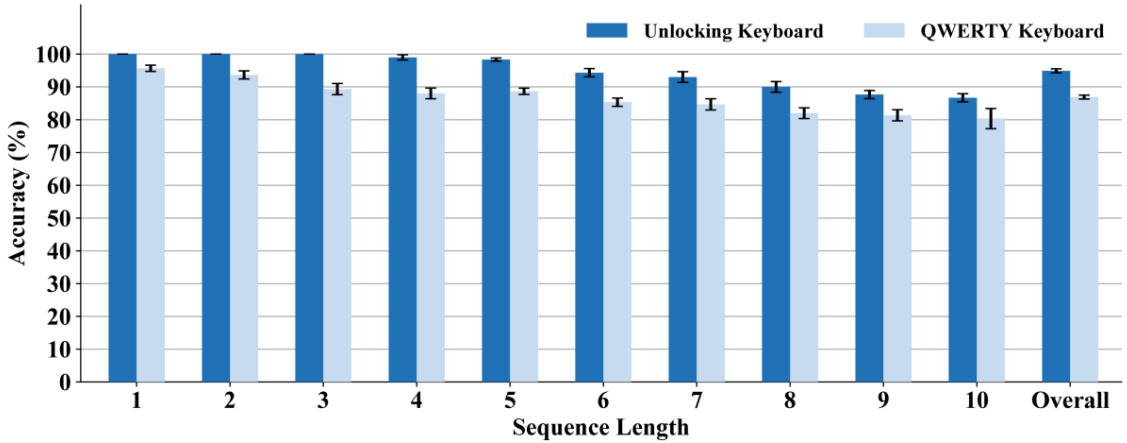
$$Mag_s(t) = \sqrt{Mag_x^2(t) + Mag_y^2(t) + Mag_z^2(t)}$$



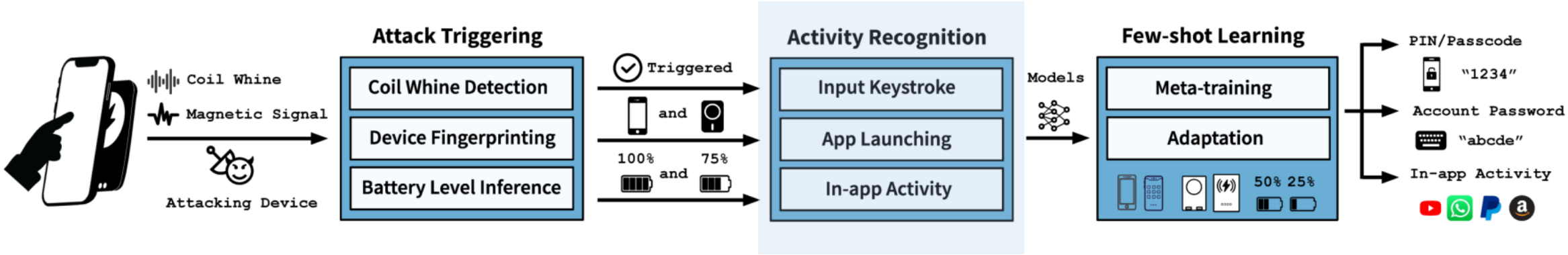
Activity Recognition – Input Keystroke



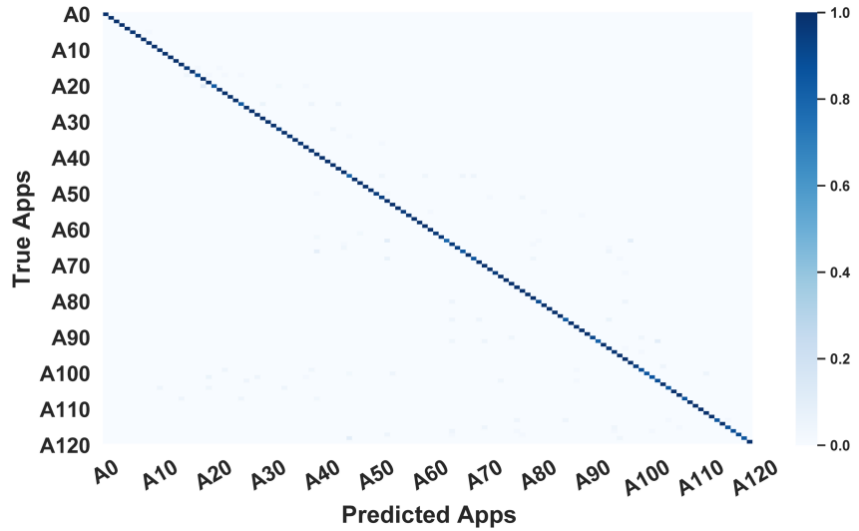
Input Keystrokes



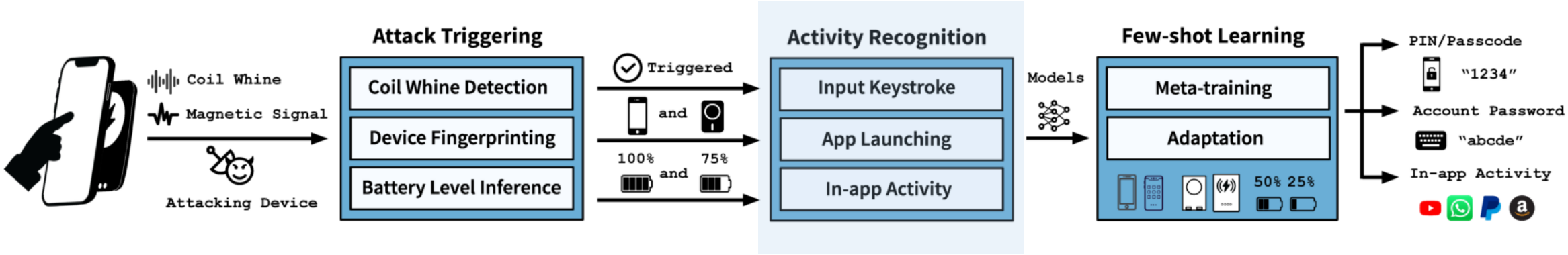
Activity Recognition – App Launching



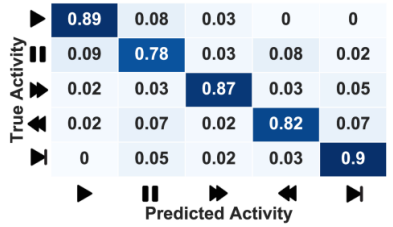
Launching Apps



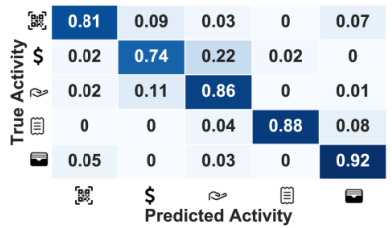
Activity Recognition



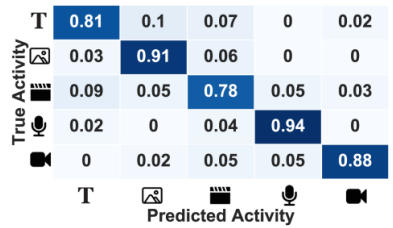
In-App Activities



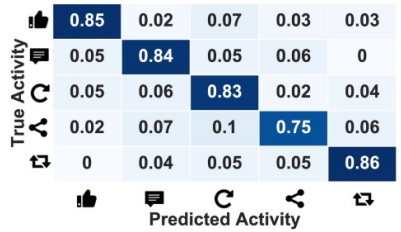
(a) YouTube



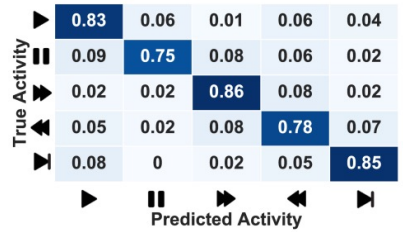
(b) PayPal



(c) WhatsApp

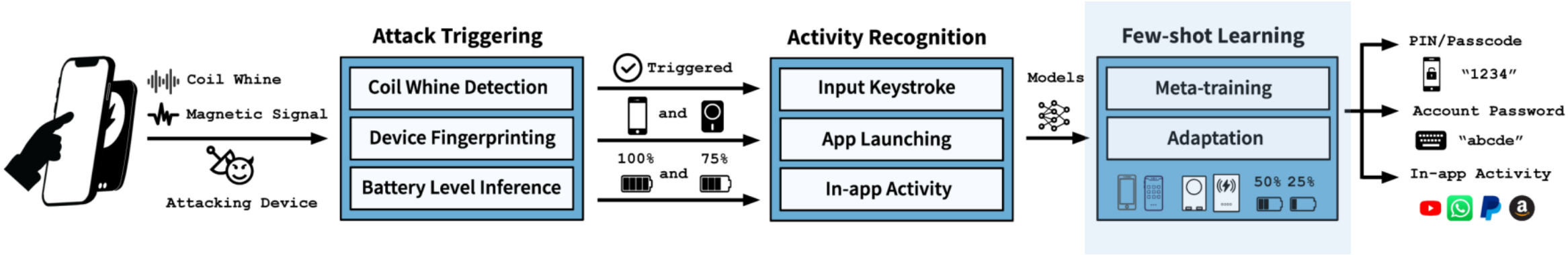


(d) Facebook



(e) Spotify

Few-Shot Learning – Fast Adaptation



Algorithm 1: Meta-training for magnetic classifier

Input: $\mathcal{D}_S$: source dataset. f: magnetic signal classifier. α and β: learning rate hyperparameters.

Output: f_{θ^*}: trained magnetic signal classifier with optimized parameters θ^*.

$\theta \leftarrow \theta_0$, $f_\theta \leftarrow f_{\theta_0}$ ▷ random initialize f_θ with parameters θ_0

while *not finished* **do**

  $\mathcal{T} \leftarrow$ generate a batch of tasks from $\mathcal{D}_S$

  for *each task* $\mathcal{T}_i \in \mathcal{T}$ **do**

    $\mathcal{S}_{\mathcal{T}_i} \leftarrow K \times N$ support samples from $\mathcal{T}_i$

    $\mathcal{S}_{\mathcal{Q}_i} \leftarrow K \times N$ query samples from $\mathcal{T}_i$ $(\mathcal{S}_{\mathcal{T}_i} \cap \mathcal{S}_{\mathcal{Q}_i} = \phi)$

    Evaluate $\nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_\theta)$ with $\mathcal{S}_{\mathcal{T}_i}$ and loss $\mathcal{L}_{\mathcal{T}_i}(f_\theta, \mathcal{S}_{\mathcal{T}_i})$

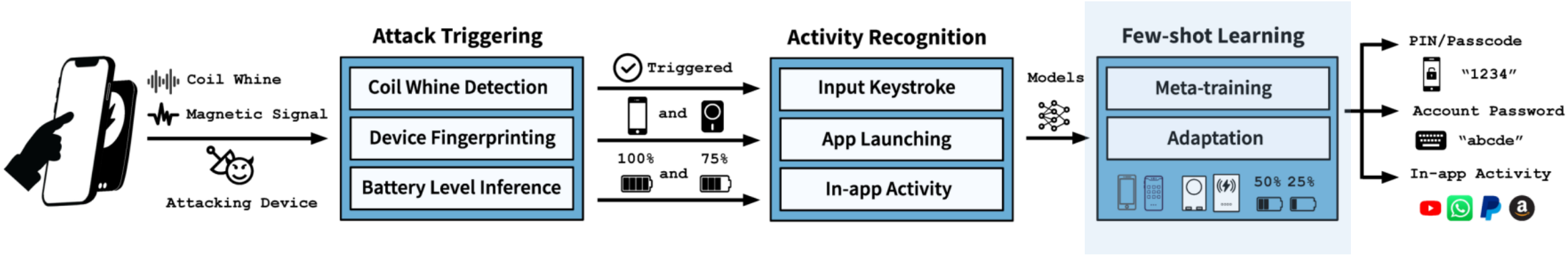
    $\theta'_{\mathcal{T}_i} \leftarrow \theta_0 - \alpha \nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, \mathcal{S}_{\mathcal{T}_i})$ ▷ obtain task-specific parameters $\theta'_{\mathcal{T}_i}$ of $\mathcal{T}_i$ using gradient descent.

    Evaluate $\mathcal{L}_{\mathcal{T}_i}(f_{\theta'_{\mathcal{T}_i}})$ with query set $\mathcal{S}_{\mathcal{Q}_i}$.

  $\theta^* \leftarrow \theta_0 - \beta \nabla_\theta \sum_{\mathcal{T}_i \in \mathcal{T}} \mathcal{L}_{\mathcal{T}_i}(f_{\theta'_{\mathcal{T}_i}}, \mathcal{S}_{\mathcal{Q}_i})$ ▷ obtain the optimized parameters θ^* that minimizes all task losses

Output classifier f_{θ^*} with optimized parameters θ^*

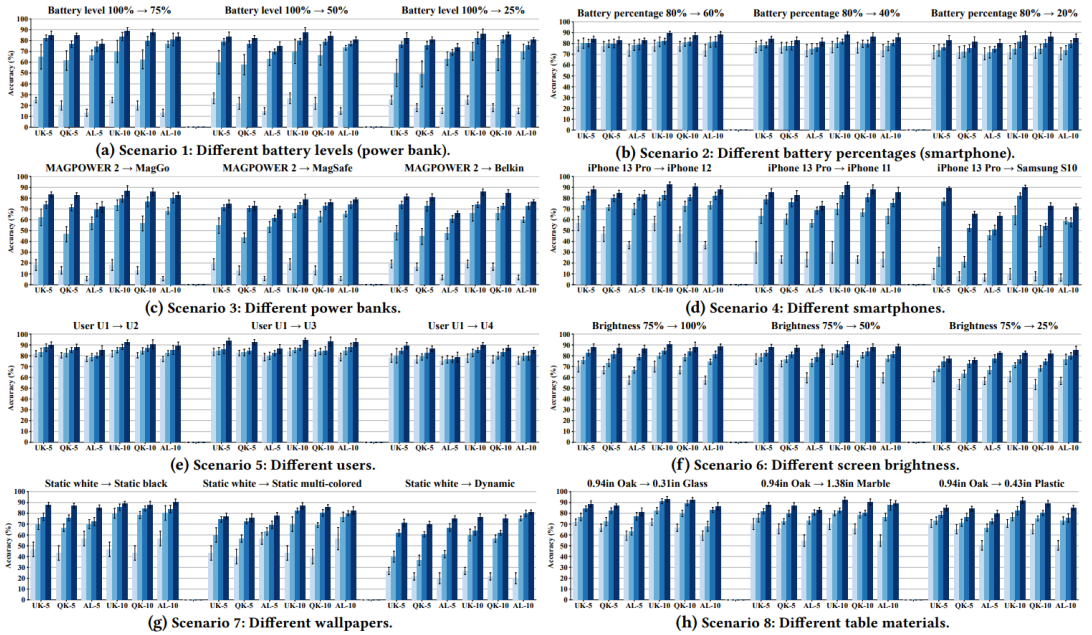
Few-Shot Learning – Fast Adaptation



Algorithm 1: Meta-training for magnetic classifier

Input: $\mathcal{D}_S$: source dataset. f: magnetic signal classifier. α and β: learning rate hyperparameters.
Output: f_{θ^*}: trained magnetic signal classifier with optimized parameters θ^*.

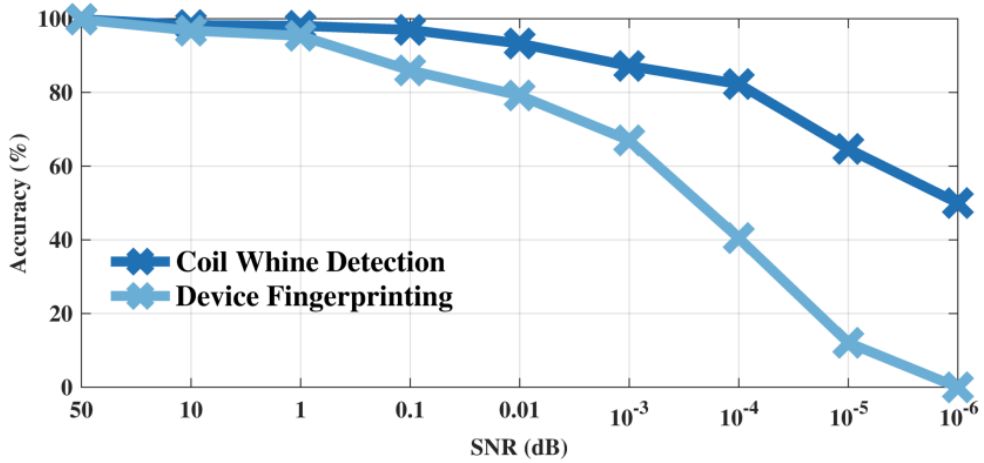
$\theta \leftarrow \theta_0$, $f_\theta \leftarrow f_{\theta_0}$ ▷ random initialize f_θ with parameters θ_0
while *not finished* **do**
  $\mathcal{T} \leftarrow$ generate a batch of tasks from $\mathcal{D}_S$
  for *each task* $\mathcal{T}_i \in \mathcal{T}$ **do**
    $\mathcal{S}_{\mathcal{T}_i} \leftarrow K \times N$ support samples from $\mathcal{T}_i$
    $\mathcal{S}_{\mathcal{Q}_i} \leftarrow K \times N$ query samples from $\mathcal{T}_i$ $(\mathcal{S}_{\mathcal{T}_i} \cap \mathcal{S}_{\mathcal{Q}_i} = \phi)$
    Evaluate $\nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_\theta)$ with $\mathcal{S}_{\mathcal{T}_i}$ and loss $\mathcal{L}_{\mathcal{T}_i}(f_\theta, \mathcal{S}_{\mathcal{T}_i})$
    $\theta'_{\mathcal{T}_i} \leftarrow \theta_0 - \alpha \nabla_\theta \mathcal{L}_{\mathcal{T}_i}(f_{\theta_0}, \mathcal{S}_{\mathcal{T}_i})$ ▷ obtain task-specific parameters $\theta'_{\mathcal{T}_i}$ of $\mathcal{T}_i$ using gradient descent.
    Evaluate $\mathcal{L}_{\mathcal{T}_i}(f_{\theta'_{\mathcal{T}_i}})$ with query set $\mathcal{S}_{\mathcal{Q}_i}$.
  $\theta^* \leftarrow \theta_0 - \beta \nabla_\theta \sum_{\mathcal{T}_i \in \mathcal{T}} \mathcal{L}_{\mathcal{T}_i}(f_{\theta'_{\mathcal{T}_i}}, \mathcal{S}_{\mathcal{Q}_i})$ ▷ obtain the optimized parameters θ^* that minimizes all task losses
Output classifier f_{θ^*} with optimized parameters θ^*



(a) Scenario 1: Different battery levels (power bank).
(b) Scenario 2: Different battery percentages (smartphone).
(c) Scenario 3: Different power banks.
(d) Scenario 4: Different smartphones.
(e) Scenario 5: Different users.
(f) Scenario 6: Different screen brightness.
(g) Scenario 7: Different wallpapers.
(h) Scenario 8: Different table materials.

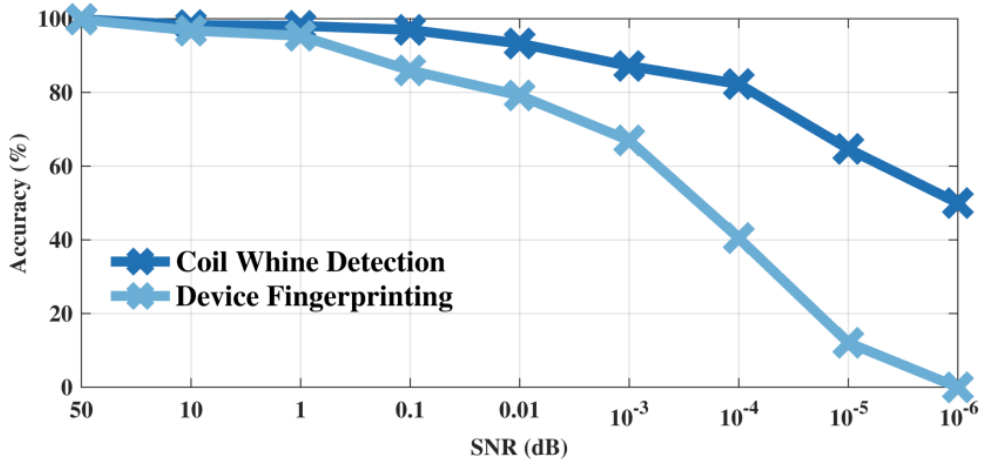
Analysis of Other Impact Factors

Environmental Noise

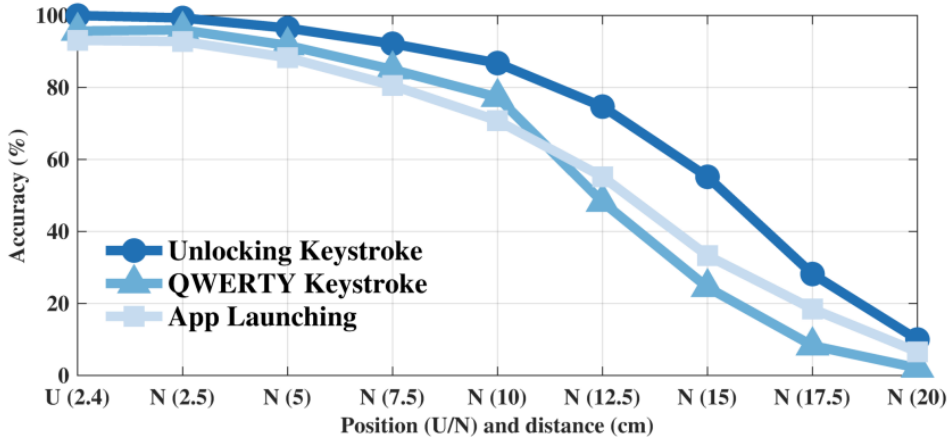


Analysis of Other Impact Factors

Environmental Noise



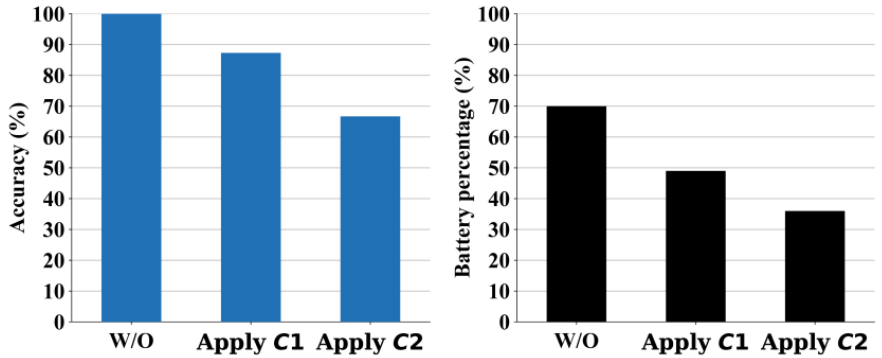
Position and Distance



Countermeasures

Countermeasure 1: Shield magnetic field.

Countermeasure 2: Signal obfuscation.



(a) Recognition accuracy. (b) Battery after charging.

Conclusion

- **A novel contactless side-channel attack**

Conclusion

- **A novel contactless side-channel attack**
- **A new attack framework**

Conclusion

- **A novel contactless side-channel attack**
- **A new attack framework**
- **Comprehensive evaluation with fast adaptation**

Thank you!

Speaker: Tao Ni (Tony)

Personal website: tony520.github.io

Email: taoni2-c@my.cityu.edu.hk

City University of Hong Kong

I will be on the 2024 job market!

Read the paper