32ND USENIX SECURITY SYMPOSIUM

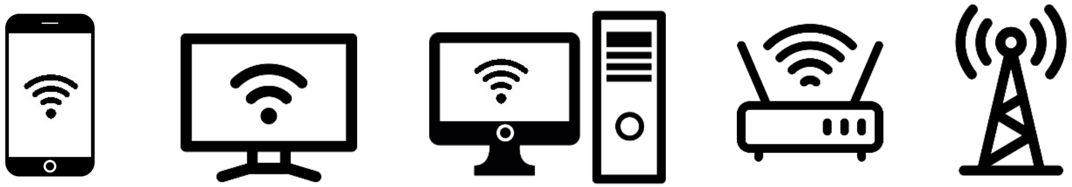
Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting

Tao Ni[*], Guohao Lan[†], Jia Wang[§], Qingchuan Zhao[*], Weitao Xu[*]

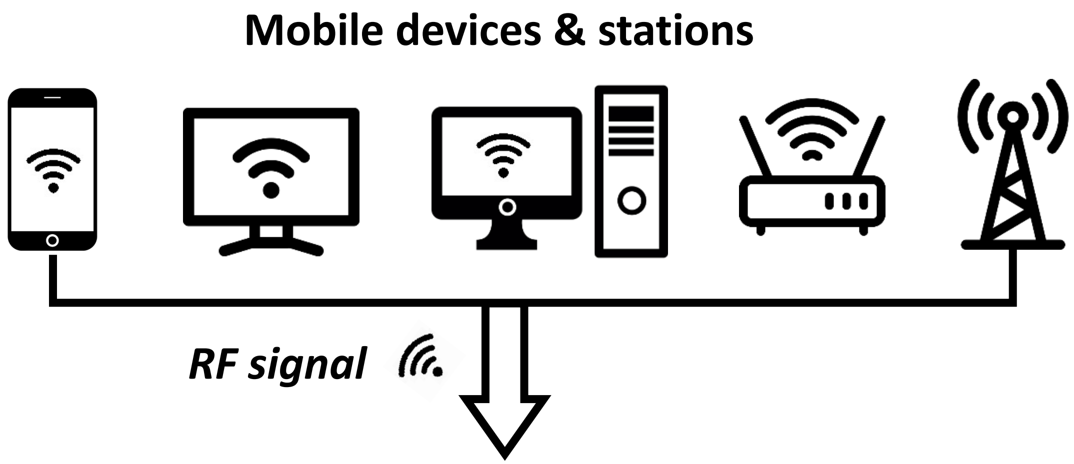
[*]City University of Hong Kong [†]Delft University of Technology [§]Shenzhen University

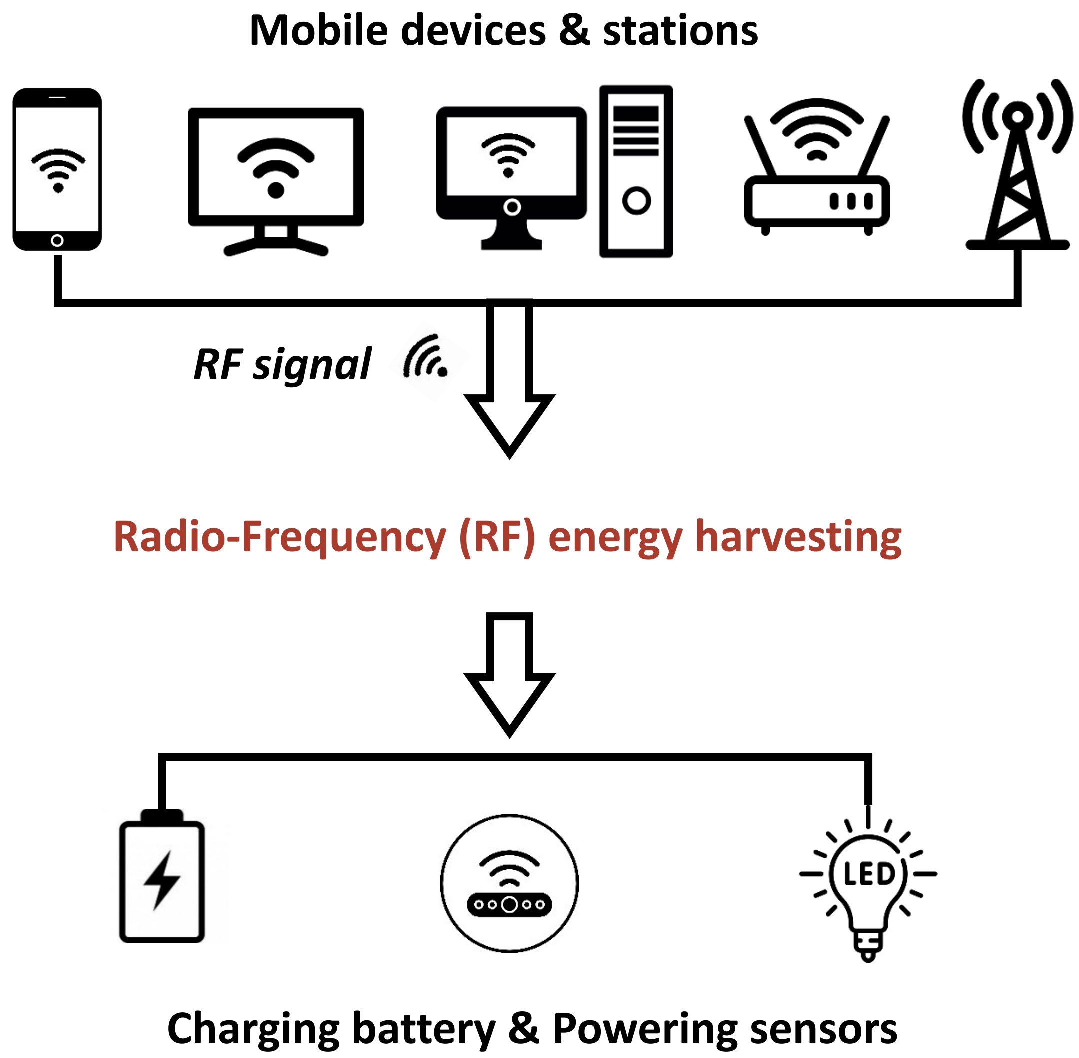
Introduction

Mobile devices & stations



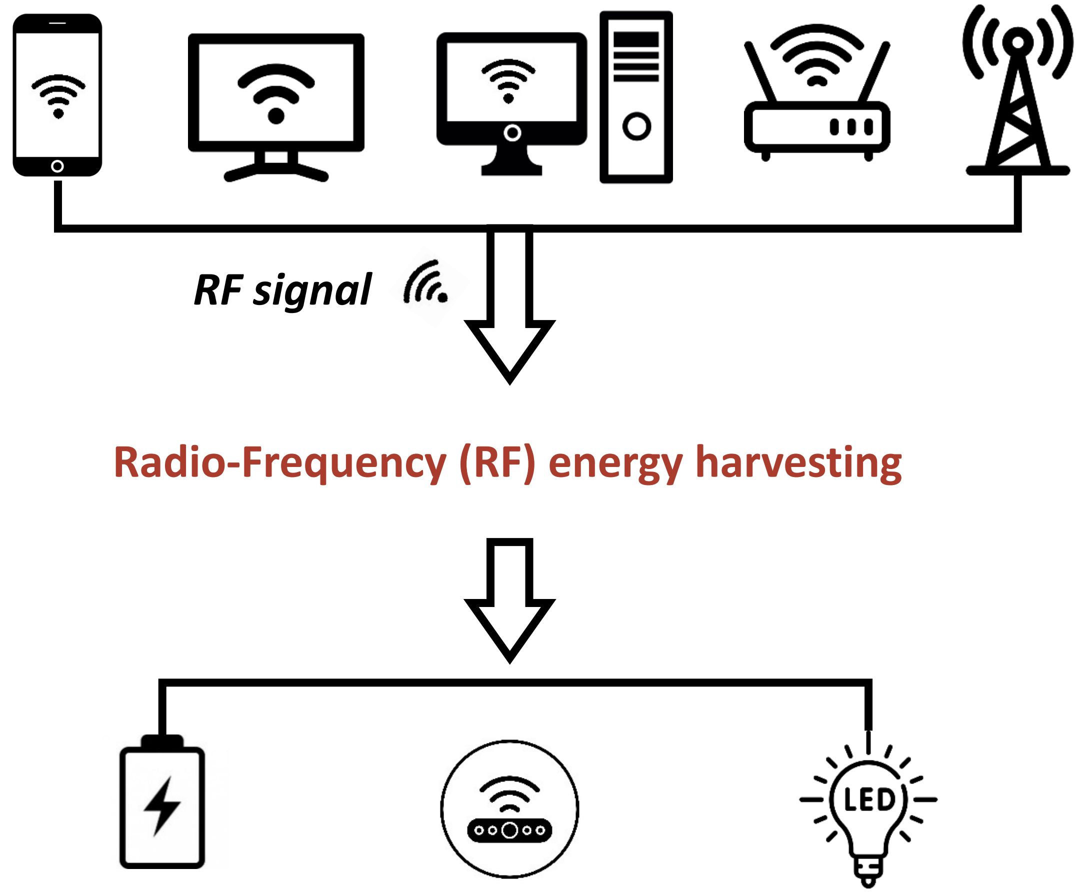
Introduction



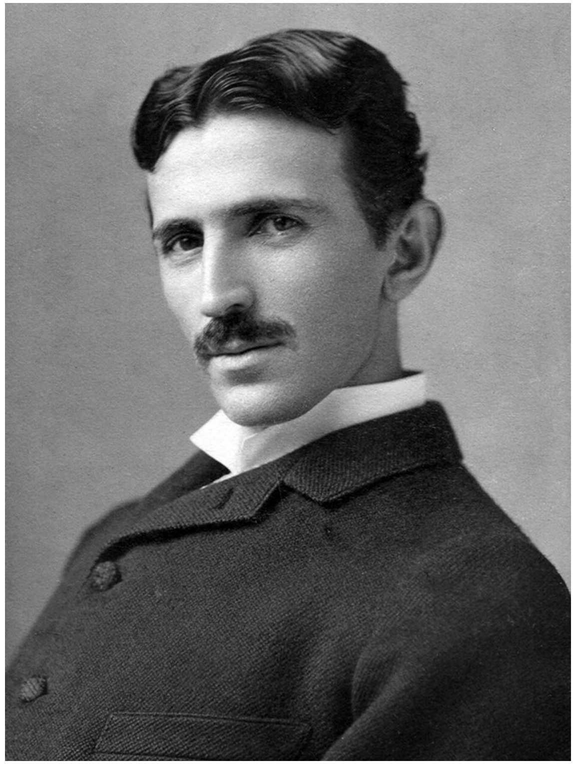

Mobile devices & stations
RF signal
Radio-Frequency (RF) energy harvesting
LED
Charging battery & Powering sensors

Introduction

Mobile devices & stations



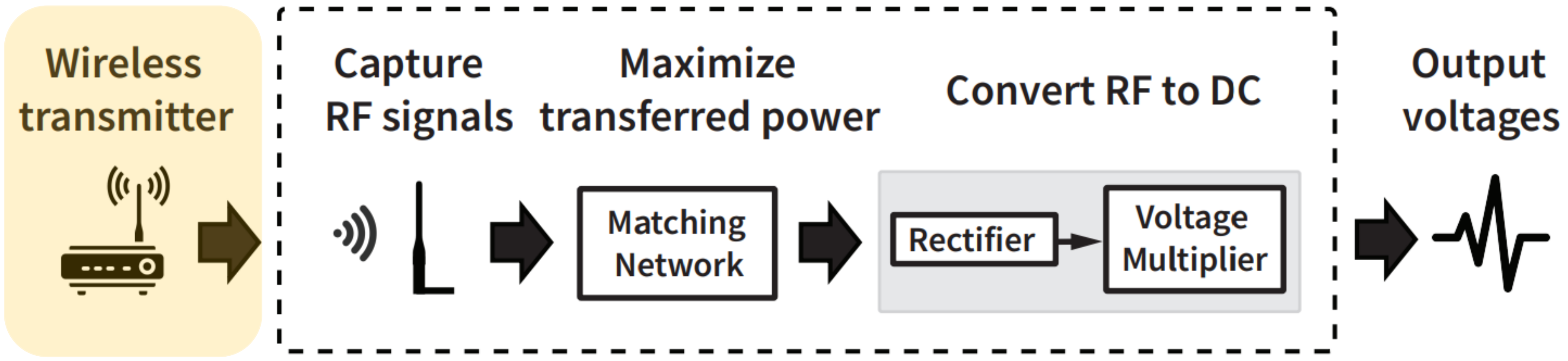
Charging battery & Powering sensors



Nikola Tesla (1856 - 1943)

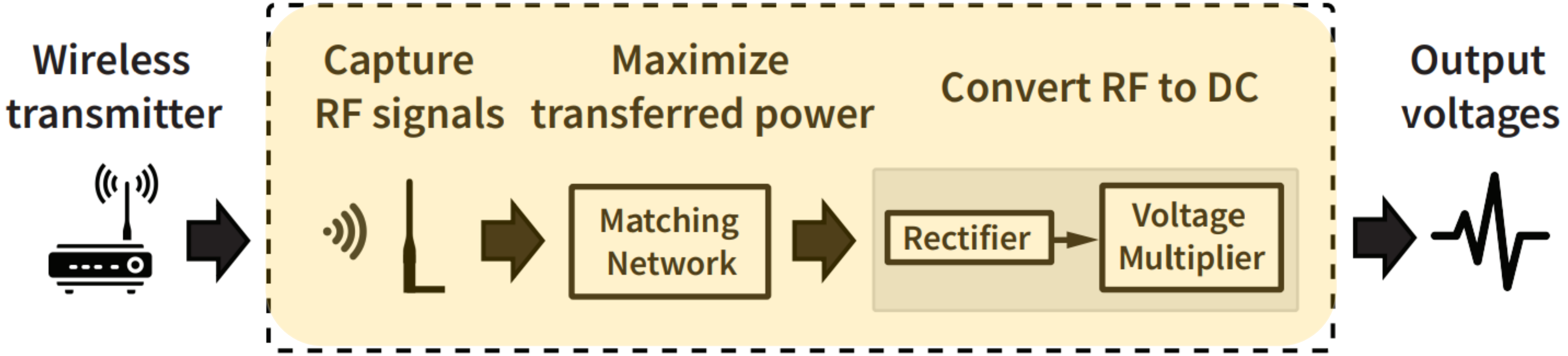
“power every device through the air”

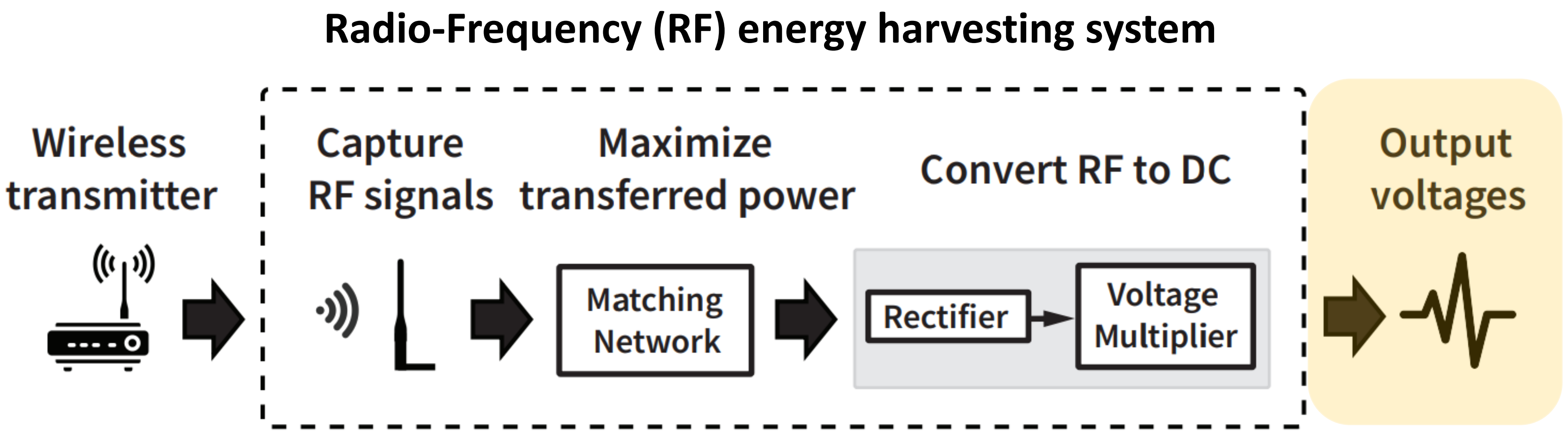
Radio-Frequency (RF) energy harvesting system



RF Energy Harvesting

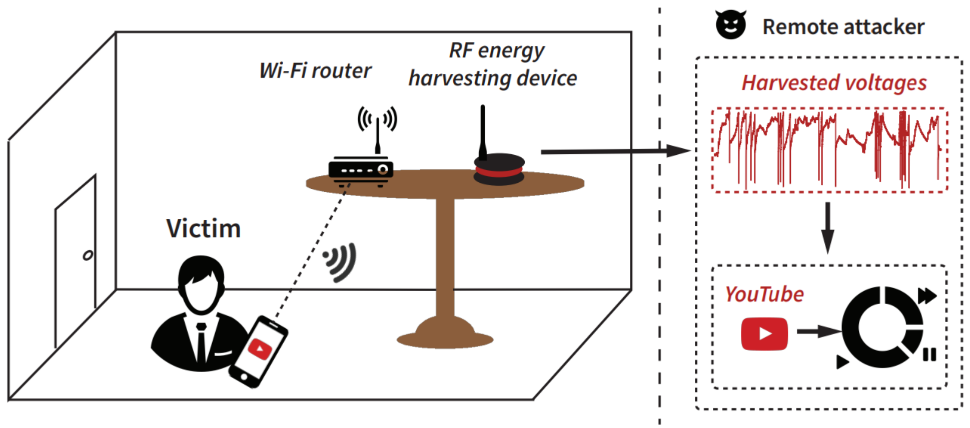
Radio-Frequency (RF) energy harvesting system




Radio-Frequency (RF) energy harvesting system
Wireless transmitter
Capture RF signals
Maximize transferred power
Convert RF to DC
Output voltages
Matching Network
Rectifier
Voltage Multiplier

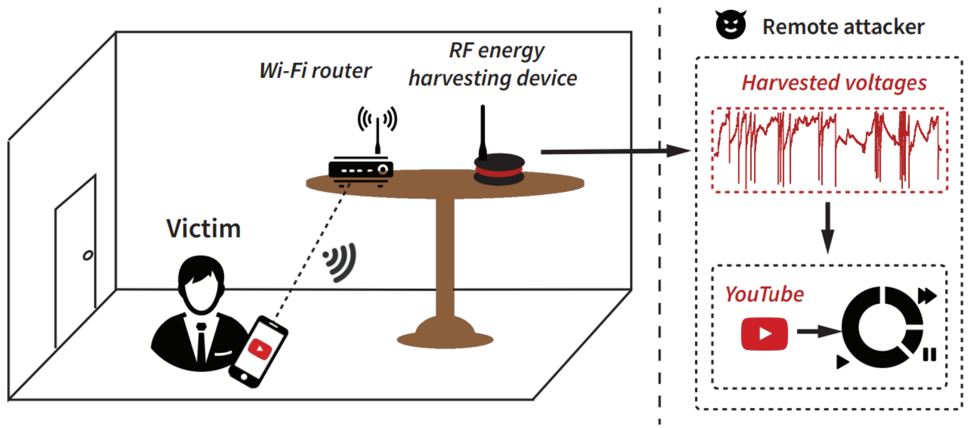
A Motivating Example

Attack scenario

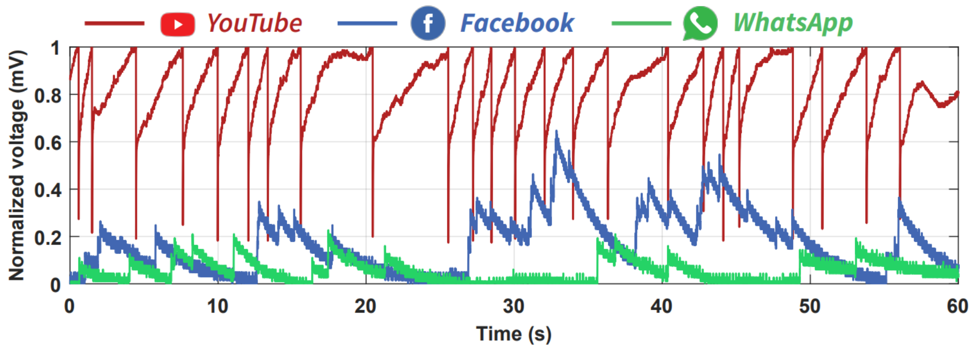


A Motivating Example

Attack scenario

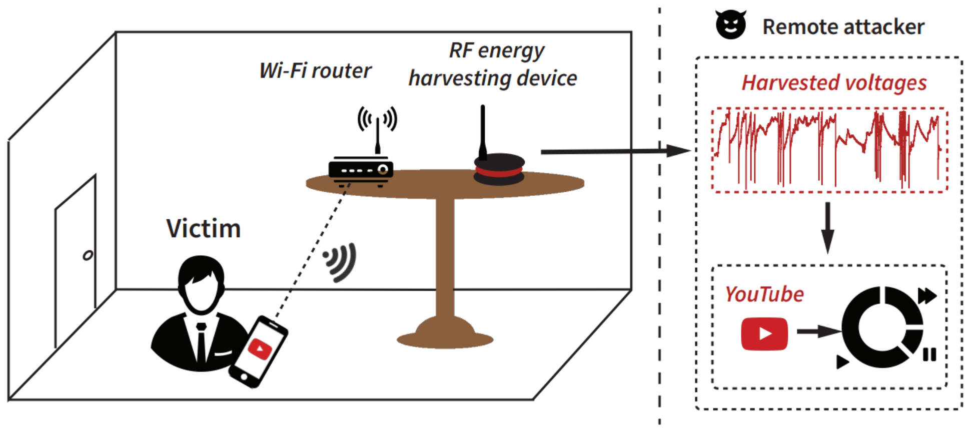


Harvested voltage signal of three apps

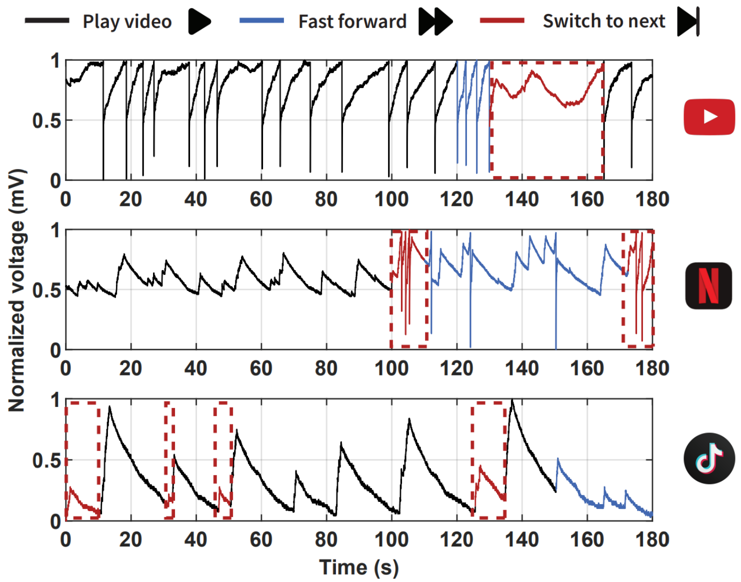


A Motivating Example

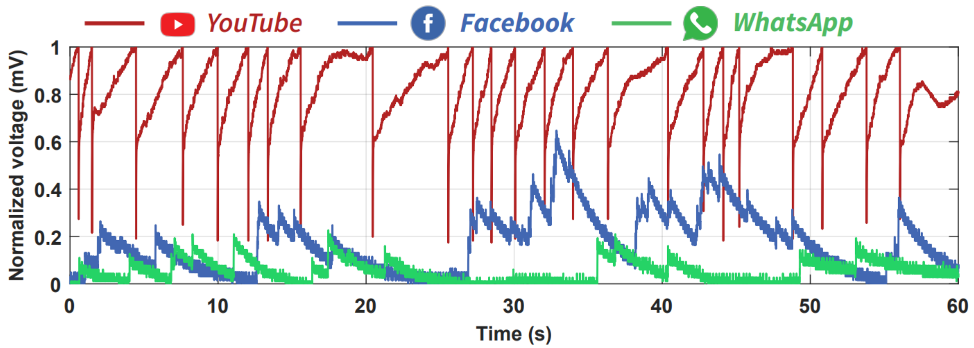
Attack scenario



Harvested voltage signal of apps & activities

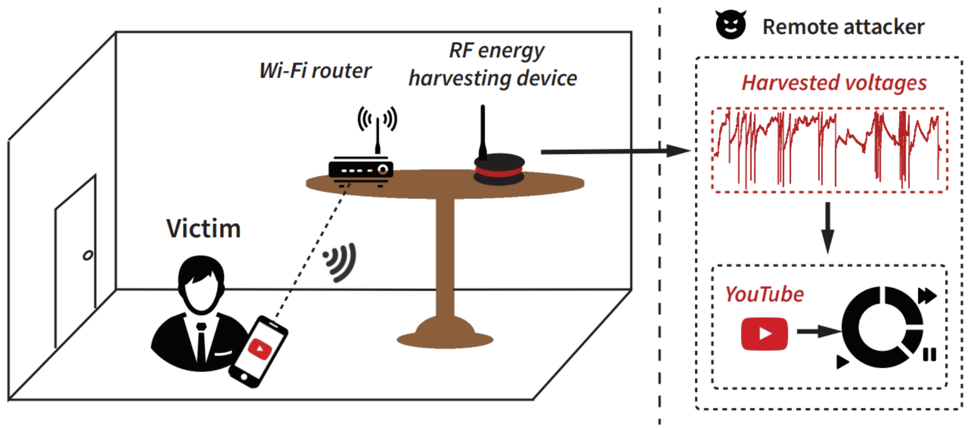


Harvested voltage signal of three apps

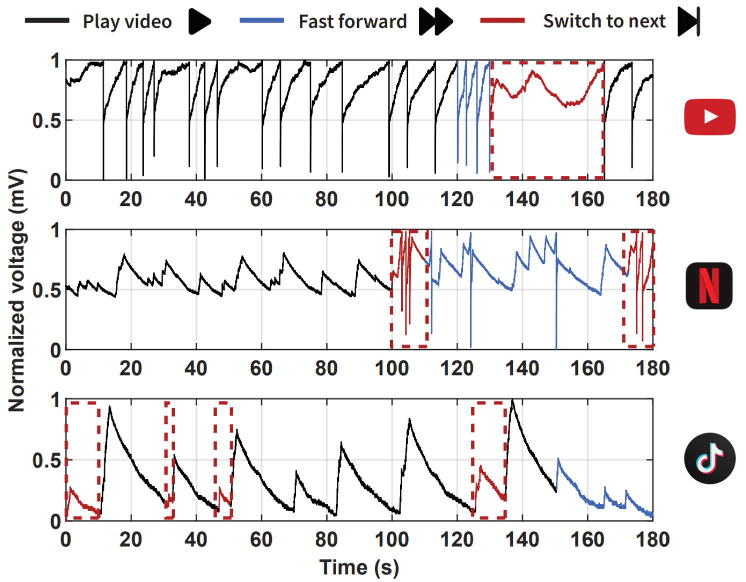


A Motivating Example

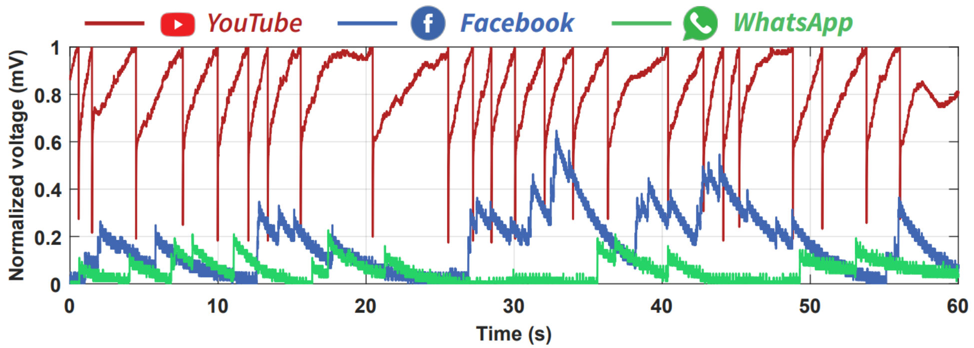
Attack scenario



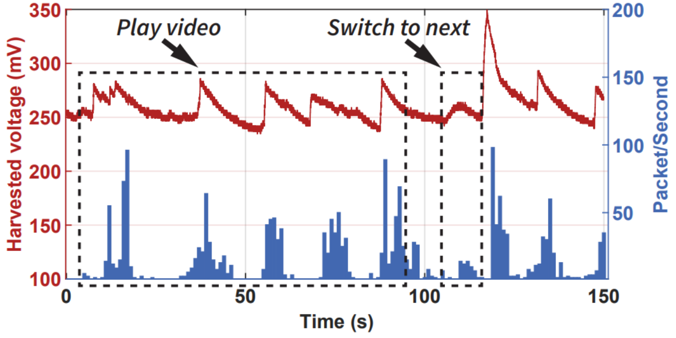
Harvested voltage signal of apps & activities



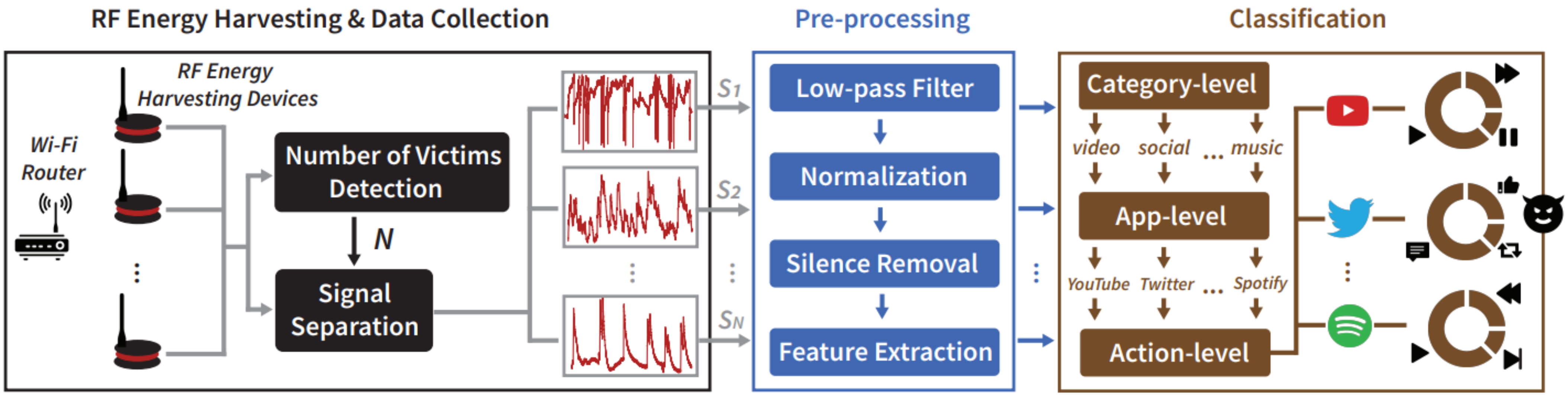
Harvested voltage signal of three apps



RF energy vs. Packets per second



Overview of *AppListener*

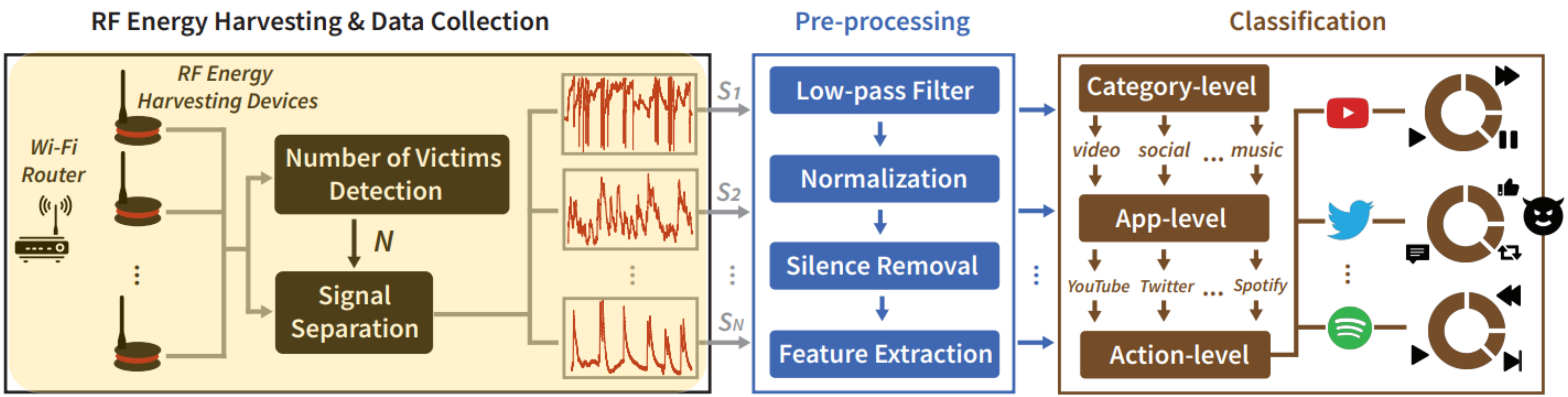


Comparison with Prior Works

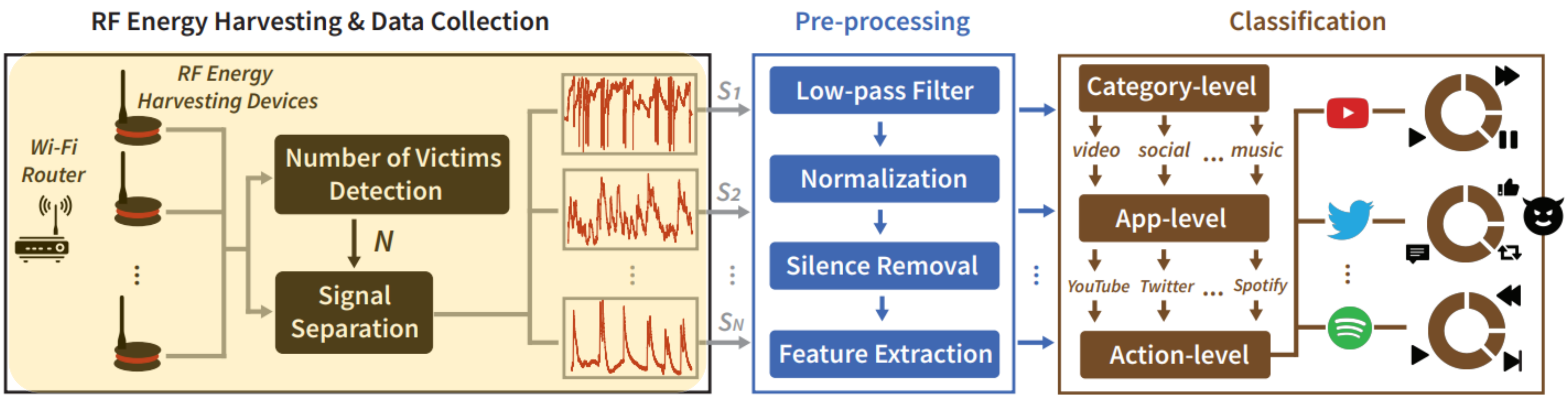
Works	Side Channel	w/o IP/Destination	Encrypted Network	In-app Activity	Number of Features	Multi-victim Attack
DECANTeR [1]	Network Traffic	✗	✗	✗	6	✗
AppScanner [2]	Network Traffic	✗	✓	✗	54	✗
NetScope [3]	Network Traffic	✗	✓	✓	N/A	✗
MIMETIC [4]	Network Traffic	✗	✓	✗	N/A	✗
Liu et al. [5]	Network Traffic	✗	✓	✓	30	✗
ActiveTracker [6]	Network Traffic	✓	✓	✓	N/A	✗
FlowPrint [7]	Network Traffic	✗	✓	✓	110	✗
FOAP [8]	Network Traffic	✓	✓	✓	123	✓
AppListener (Ours)	RF Energy	✓	✓	✓	31	✓

[1] Riccardo Bortolameotti, Thijs van Ede, Marco Caselli, Maarten H Everts, Pieter Hartel, Rick Hofstede, Willem Jonker, and Andreas Peter. Decanter: Detection of anomalous outbound http traffic by passive application fingerprinting. *In Proceedings of ACSAC*, 2017.
[2] Vincent F Taylor, Riccardo Spolaor, Mauro Conti, and Ivan Martinovic. Appscanner: Automatic fingerprinting of smartphone apps from encrypted network traffic. *In Proceedings of the IEEE EuroS&P*, 2016.
[3] Brendan Saltaformaggio, Hongjun Choi, Kristen Johnson, Yonghwi Kwon, Qi Zhang, Xiangyu Zhang, Dongyan Xu, and John Qian. Eavesdropping on fine-grained user activities within smartphone apps over encrypted network traffic. *In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2016.
[4] Giuseppe Aceto, Domenico Ciuonzo, Antonio Montieri, and Antonio Pescapè. Mimetic: Mobile encrypted traffic classification using multimodal deep learning. *Computer Networks*, 165:106944, 2019.
[5] Junming Liu, Yanjie Fu, Jingci Ming, Yong Ren, Leilei Sun, and Hui Xiong. Effective and real-time in-app activity analysis in encrypted internet traffic streams. *In Proceedings of the ACM KDD*, 2017.
[6] Ding Li, Wenzhong Li, Xiaoliang Wang, Cam-Tu Nguyen, and Sanglu Lu. Activetracker: Uncovering the trajectory of app activities over encrypted internet traffic streams. *In Proceedings of the IEEE SECON*, 2019.
[7] Thijs van Ede, Riccardo Bortolameotti, Andrea Continella, Jingjing Ren, Daniel J Dubois, Martina Lindorfer, David Choffnes, Maarten van Steen, and Andreas Peter. Flowprint: Semi-supervised mobile-app fingerprinting on encrypted network traffic. *In Proceedings of NDSS*, 2020.
[8] Jianfeng Li, Hao Zhou, Shuohan Wu, Xiapu Luo, Ting Wang, Xian Zhan, and Xiaobo Ma. Foap: Fine-grained open-world android app fingerprinting. *In Proceedings of USENIX Security Symposium*, 2022.

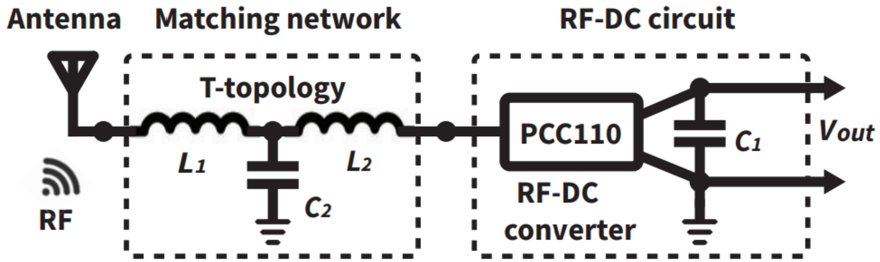
RF energy harvester & Portable attacking device



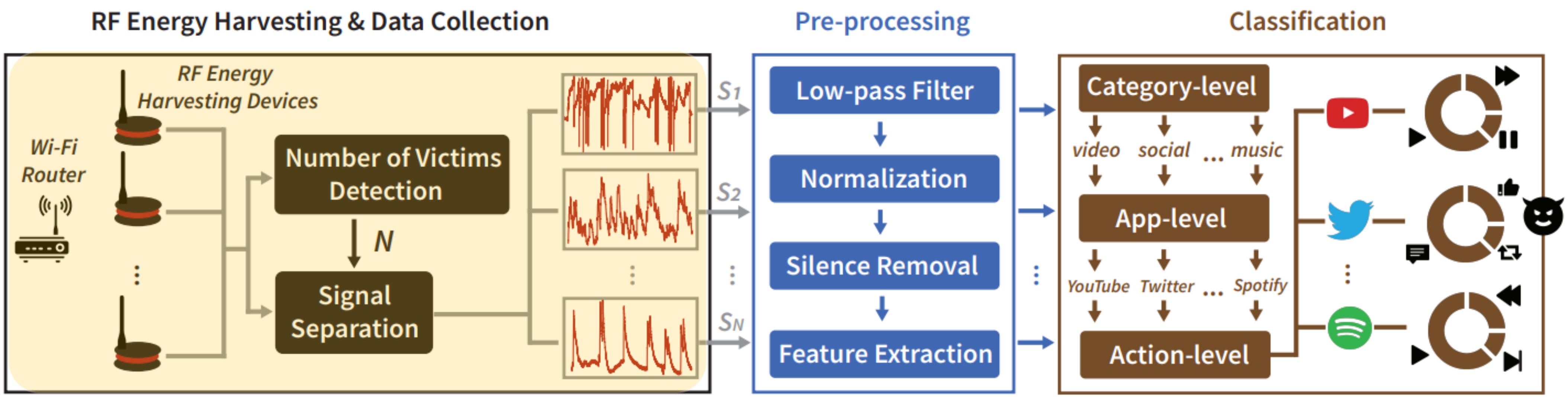
RF energy harvester & Portable attacking device



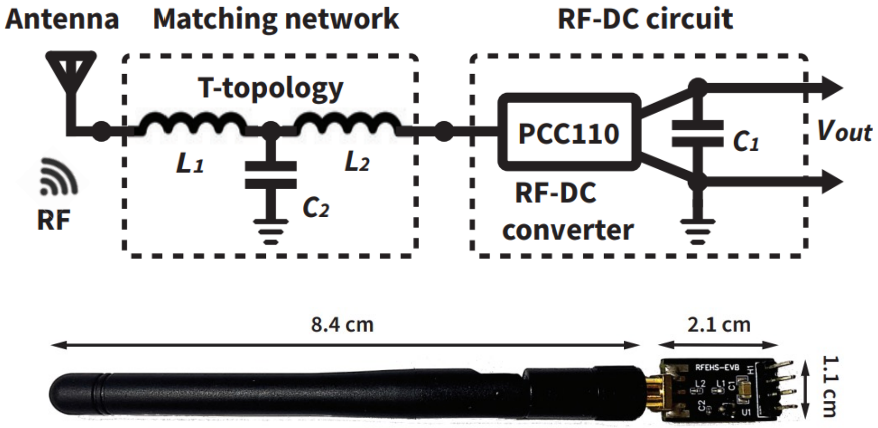
RF energy harvester



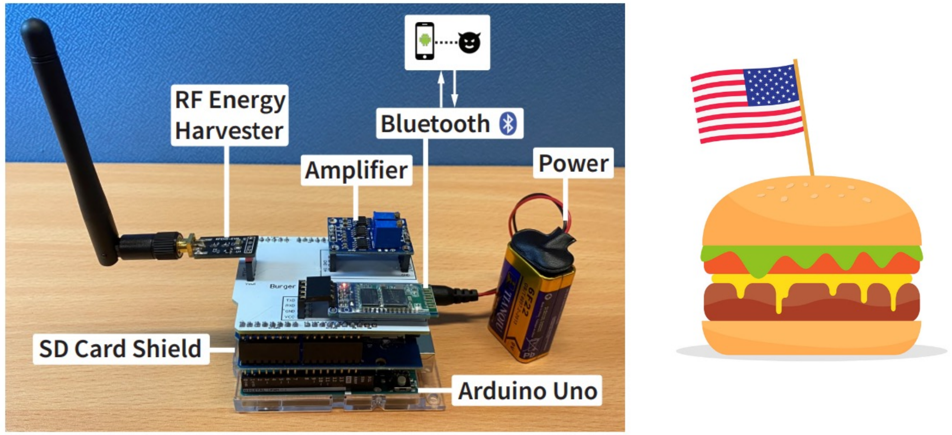
RF energy harvester & Portable attacking device



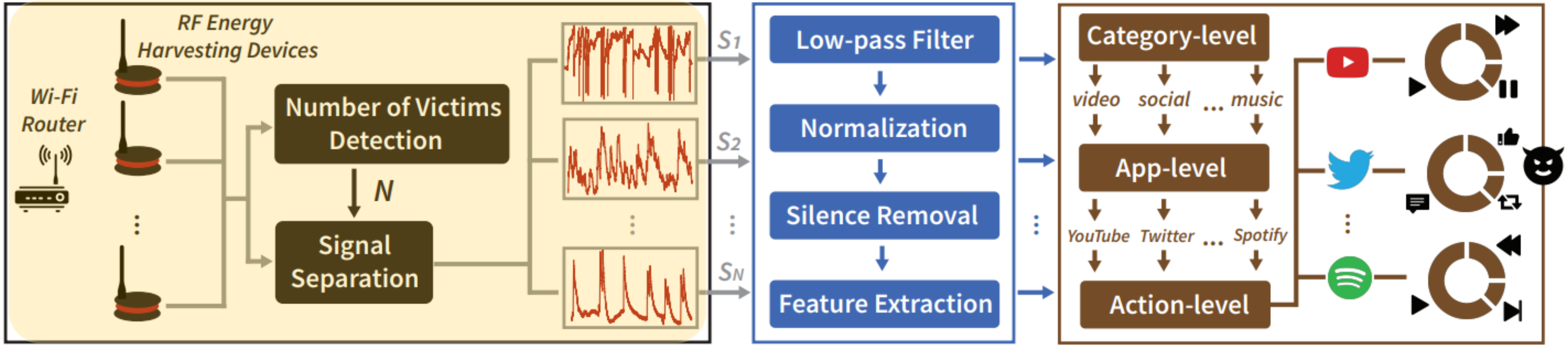
RF energy harvester



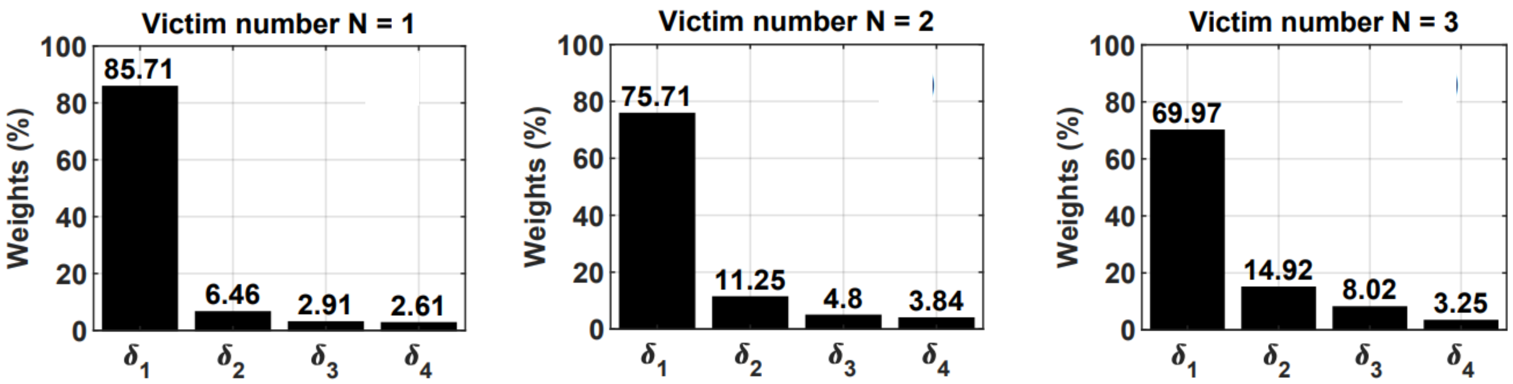
The “*Burger Model*”



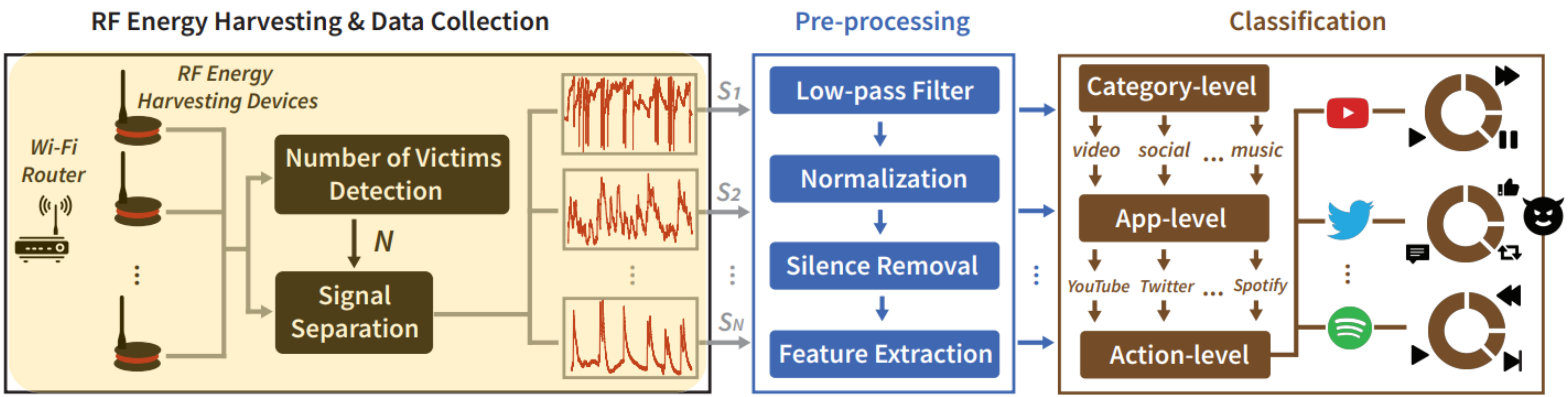
Number of Victims Detection



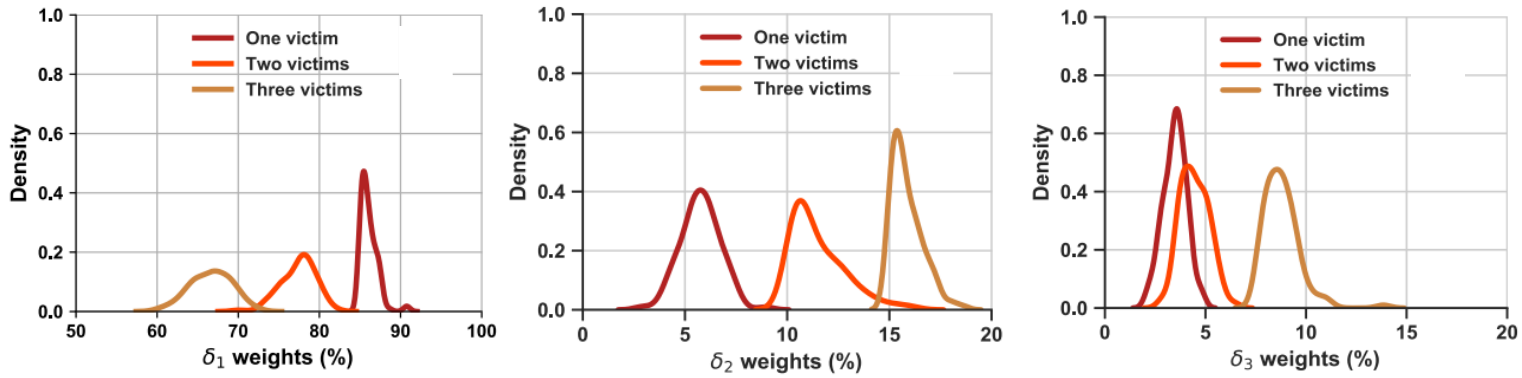
Decomposed singular values when the number of victims = 1, 2, and 3



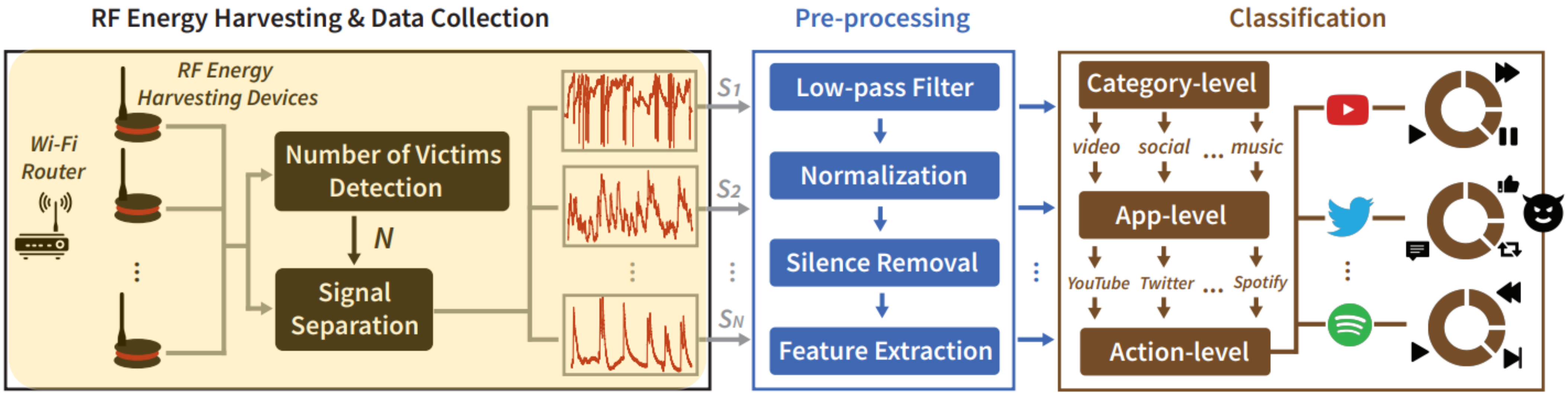
Number of Victims Detection



Density distribution of singular values δ_1, δ_2 and δ_3 (# of victims = 1, 2, and 3)



Signal Separation



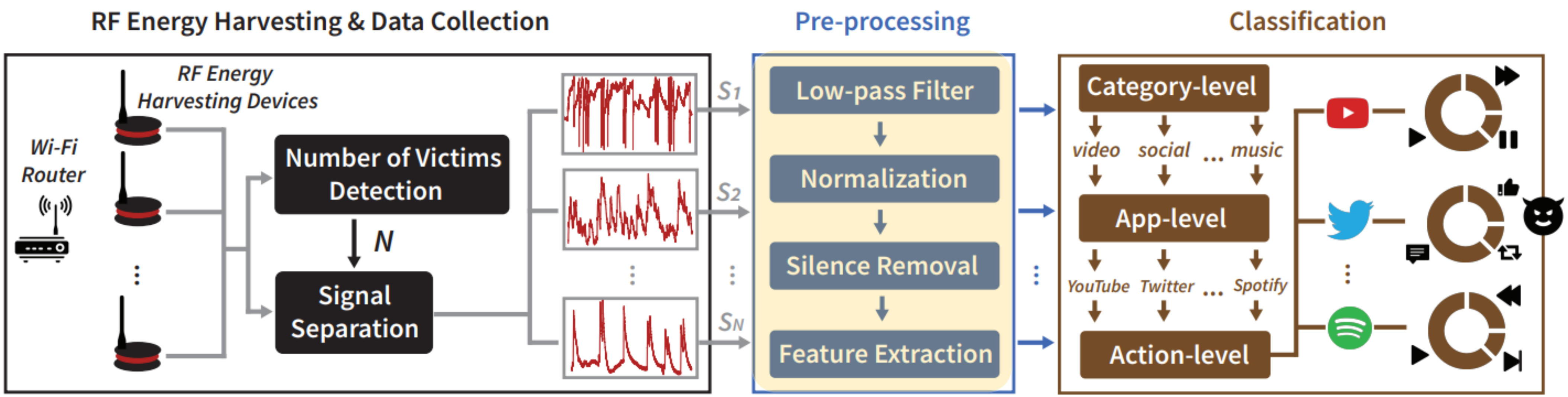
***FastICA* - Blind Source Separation**

Algorithm 1: Signal Separation Algorithm

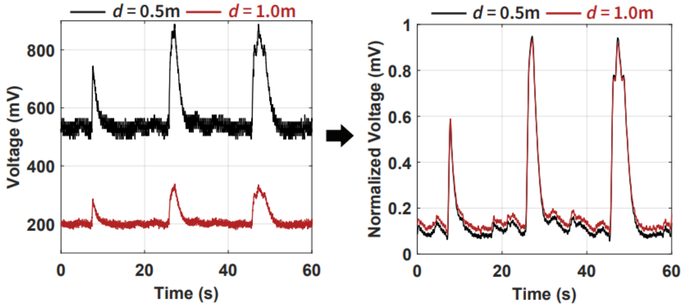
Input: N: Number of desired components (victims).
$Y \in \mathbb{R}^{N\times L}$: Observed L-length voltage signals from N devices.
Output: $A^{-1} \in \mathbb{R}^{N\times N}$: Inverse mixing matrix. $X \in \mathbb{R}^{N\times L}$: Independent voltage signals.

Initialize an empty array A^{-1}
for $i \leftarrow 1$ **to** N **do**
  Initialize a random N-length vector a_i
  while *a_i is not converged* **do**
    $a_i^* = \frac{1}{L} Y g(a_i^T Y)^T - \frac{1}{L} g'(a_i^T Y) 1_L a_i$ `// ` 1_L `is a` L`-dimension column vector of 1's`
    $a_i^* = a_i - \sum_{j=1}^{i-1} (a_i^T a_j) a_j$
    $a_i = \frac{a_i^*}{\|a_i^*\|}$
  end while
  $A^{-1} = [a_1, a_2, \ldots, a_i]$, if converged, add to A^{-1}
end for
$A^{-1} = [a_1, a_2, \ldots, a_N]$, obtain inverse mixing matrix.
$X = A^{-1} Y$, calculate independent voltage signals.

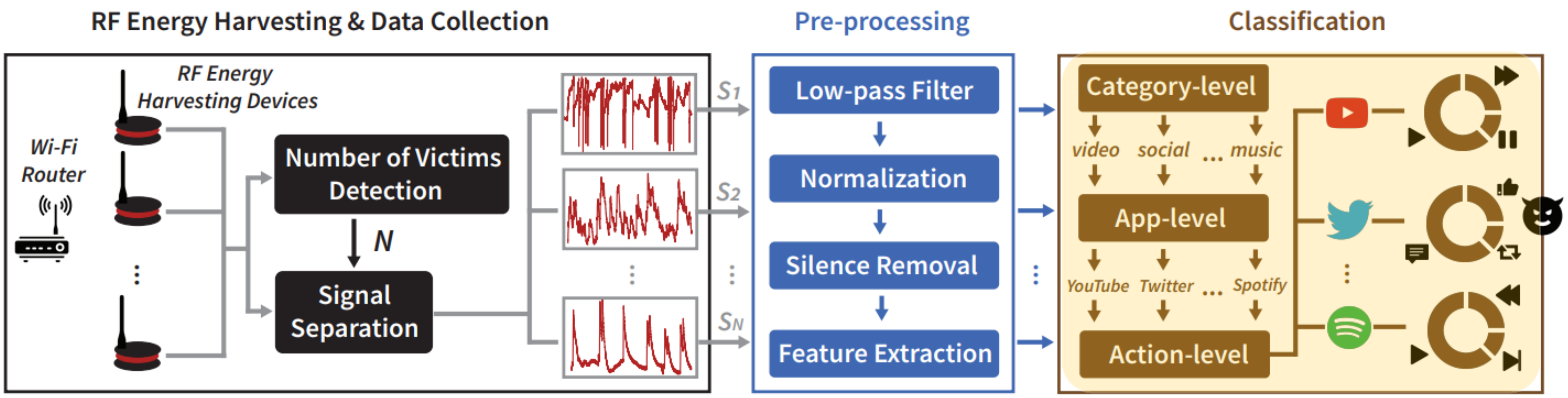
Pre-processing



- Low-pass filter: *Savitzky-Golay* (S-G) filter to remove high-frequency noise
- Data normalization: reduce impact of distance
- Silence removal: deduct the DC offset
- Feature extraction: time-domain and frequency domain.

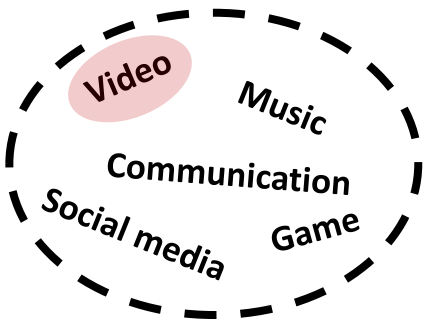


Classification

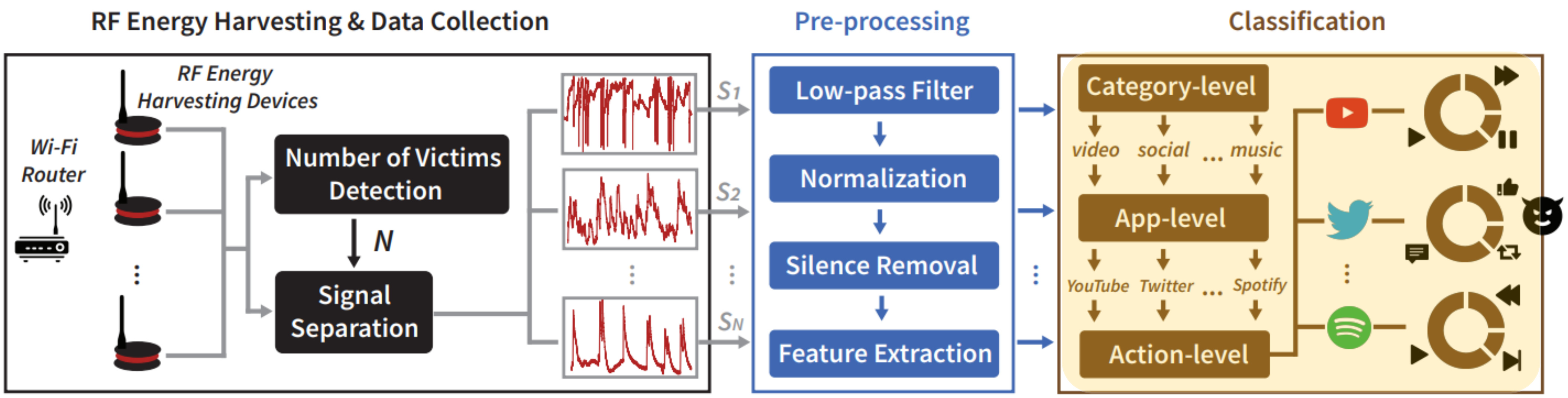


Three-tier classification framework

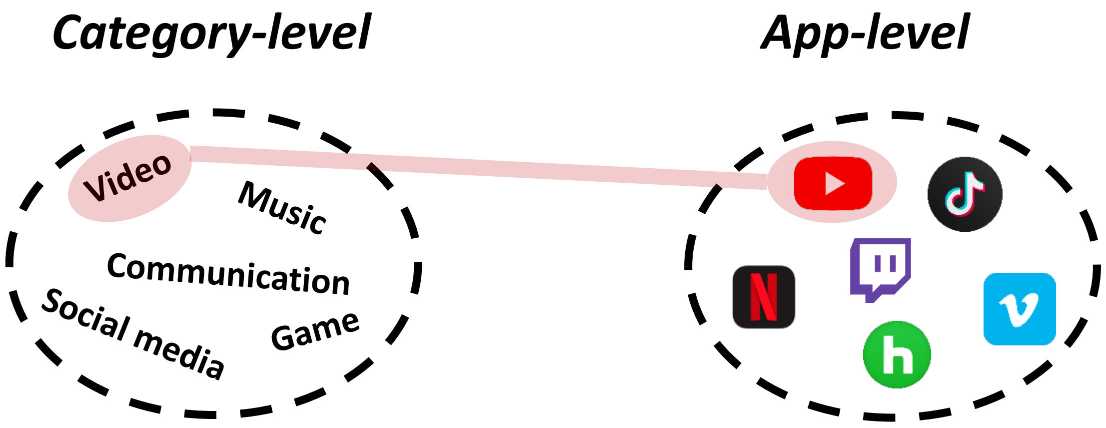
Category-level



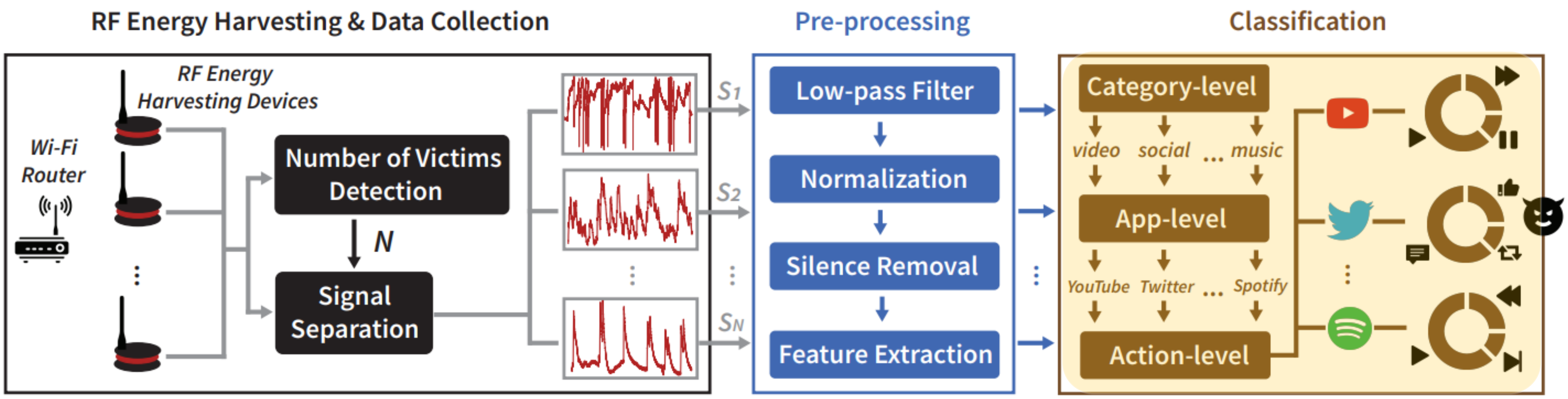
Classification



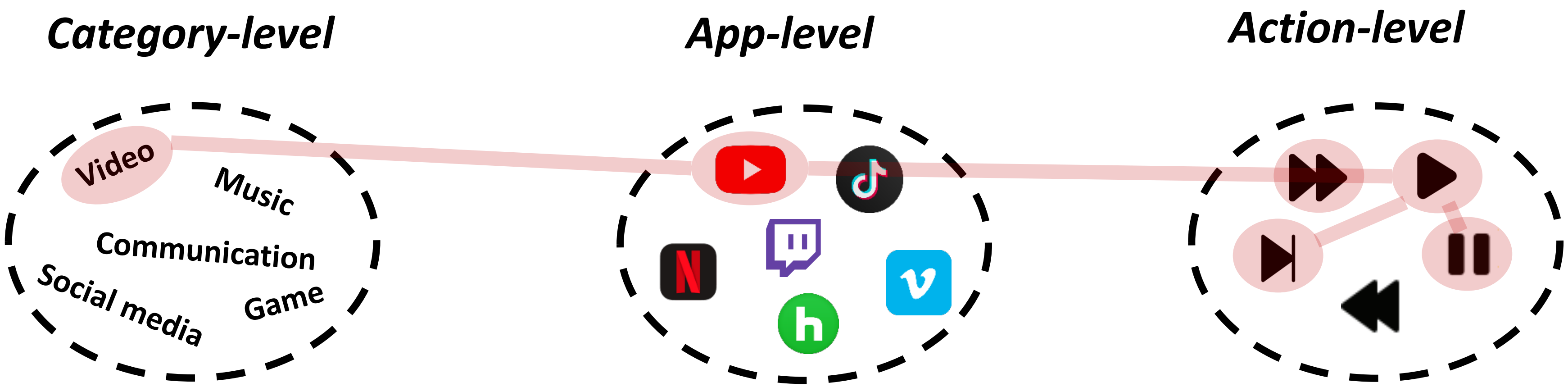
Three-tier classification framework



Classification



Three-tier classification framework



Evaluation – Experiment Setup

5 categories, 40 mobile apps, 5 in-app activities

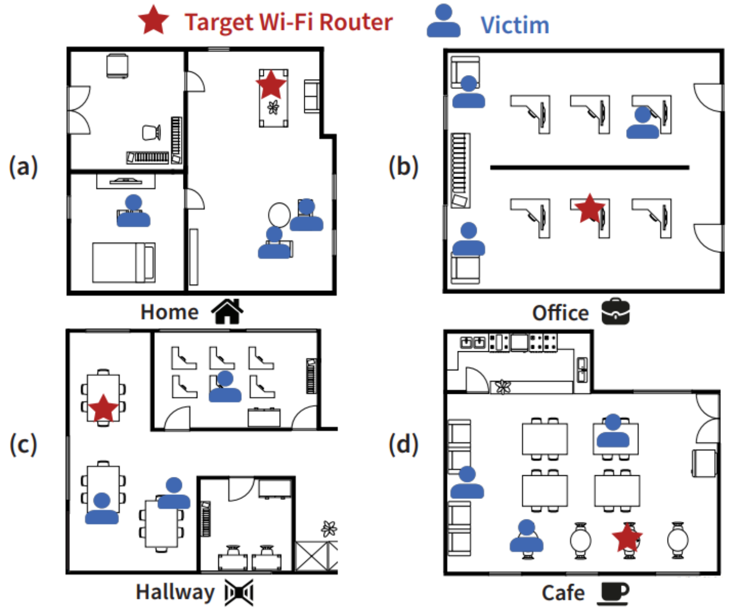
Video Apps				Activity
YouTube	TikTok	Netflix	Vimeo	Play Next Pause
Hulu	TED Talk	Disney+	Twitch	Forward Backward
Music Apps				**Activity**
Spotify	Apple Music	YouTube Music	SoundCloud	Play Next Pause
Shazam	Netease Cloud	Kugou Music	QQ Music	Forward Backward
Social Media Apps				**Activity**
Facebook	Twitter	Instagram	LinkedIn	Repost Refresh Share
Reddit	Pinterest	Quora	Sina Weibo	Thumb-up Comment
Communication Apps				**Activity**
WhatsApp	Line	Telegram	Messenger	Text Images Videos
WeChat	Snapchat	Hangouts	Discord	Send voice Video call
Game Apps				**Activity**
PUBG	Minecraft	Arena of Valor	FIFA	Loading Entering Gaming
Genshin	Hearthstone	LoL Wild Rift	UNO	Matching Exit game

Evaluation – Experiment Setup

5 categories, 40 mobile apps, 5 in-app activities

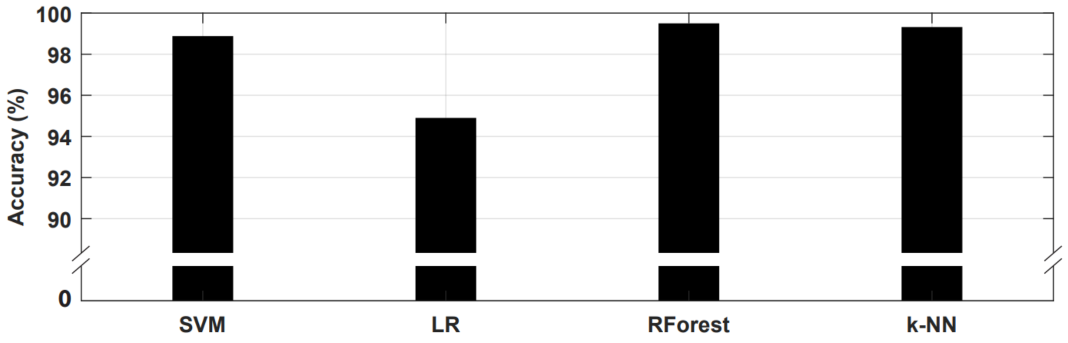
Video Apps				Activity
YouTube	TikTok	Netflix	Vimeo	▶Play ⏭Next ⏸Pause
Hulu	TED Talk	Disney+	Twitch	⏩Forward ⏪Backward
Music Apps				**Activity**
Spotify	Apple Music	YouTube Music	SoundCloud	▶Play ⏭Next ⏸Pause
Shazam	Netease Cloud	Kugou Music	QQ Music	⏩Forward ⏪Backward
Social Media Apps				**Activity**
Facebook	Twitter	Instagram	LinkedIn	Repost Refresh Share
Reddit	Pinterest	Quora	Sina Weibo	Thumb-up Comment
Communication Apps				**Activity**
WhatsApp	Line	Telegram	Messenger	Text Images Videos
WeChat	Snapchat	Hangouts	Discord	Send voice Video call
Game Apps				**Activity**
PUBG	Minecraft	Arena of Valor	FIFA	Loading Entering Gaming
Genshin	Hearthstone	LoL Wild Rift	UNO	Matching Exit game

4 common scenarios



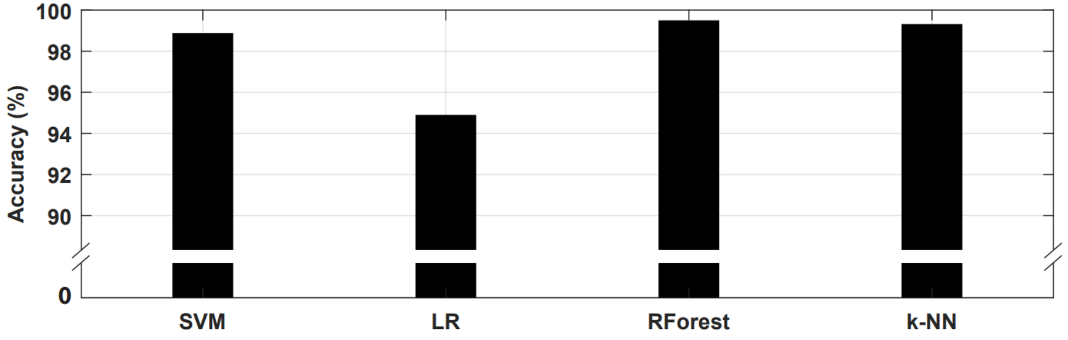
Overall Effectiveness

Identify app's category

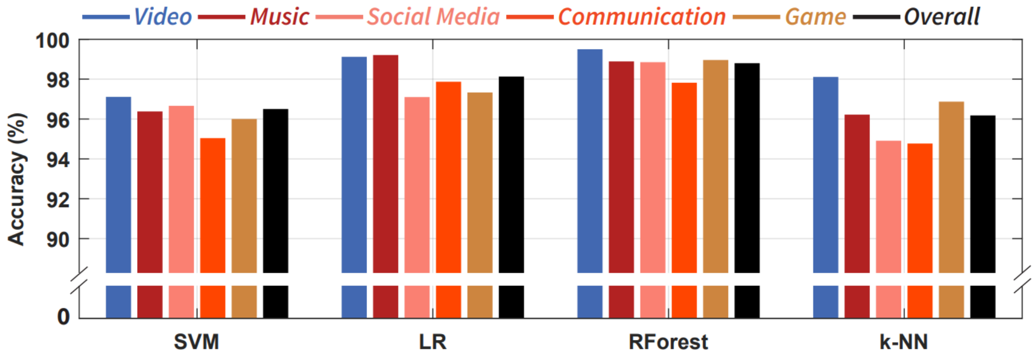


Overall Effectiveness

Identify app's category

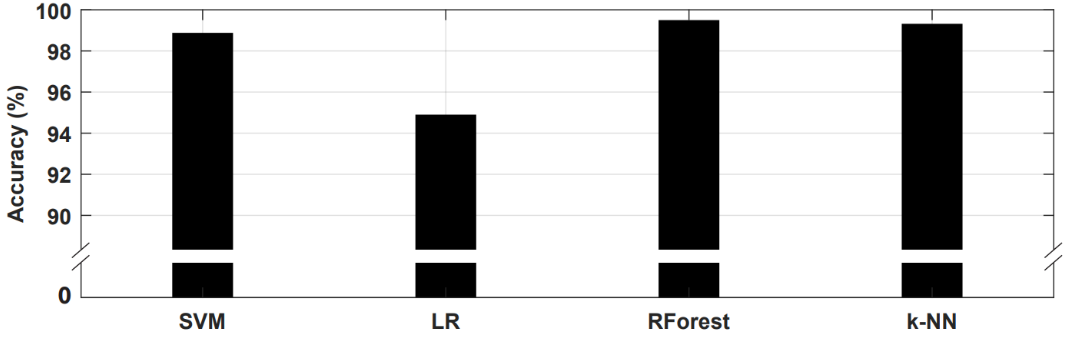


Identify app

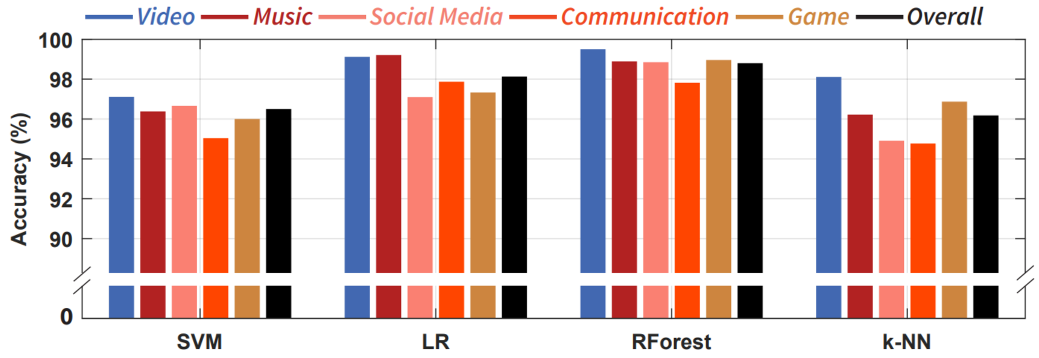


Overall Effectiveness

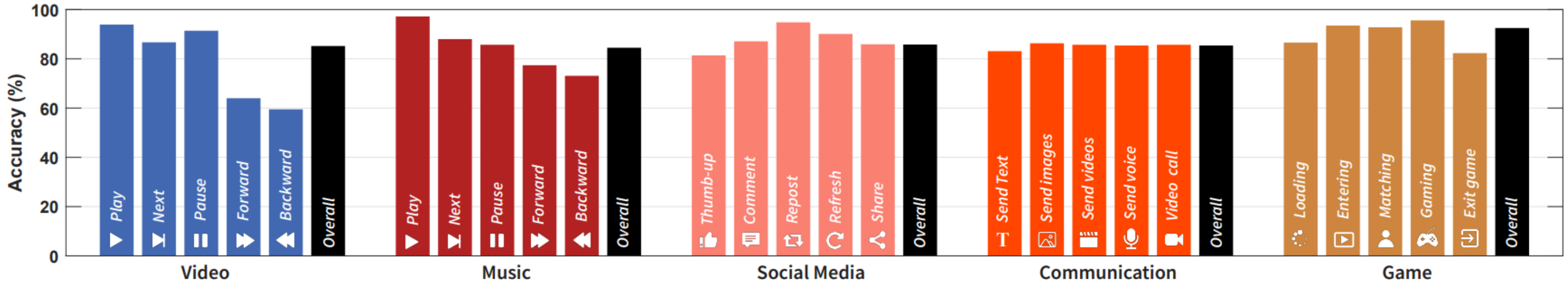
Identify app's category



Identify app

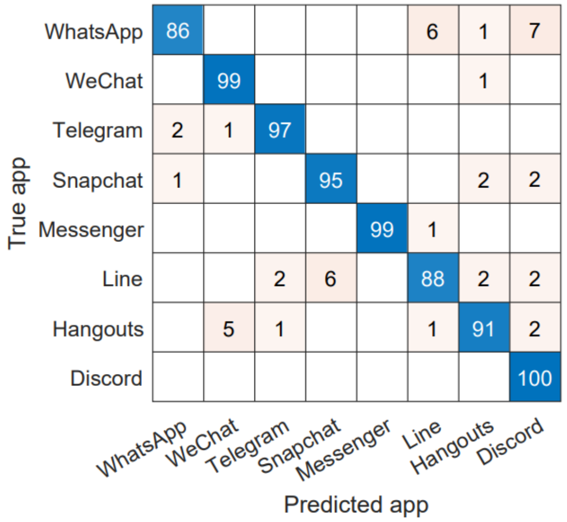


Identify in-app activity

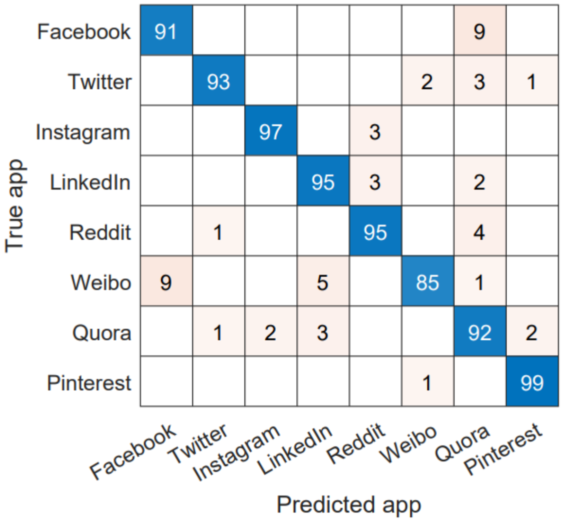


Further Analysis

Communication



Social Media



Further Analysis

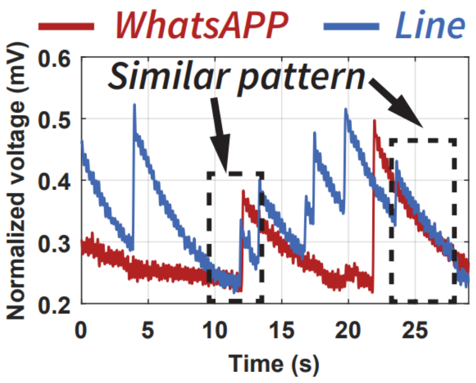
Communication

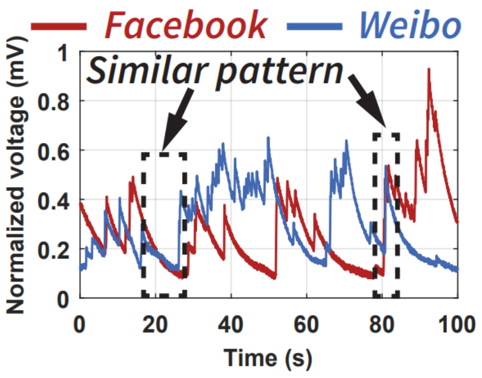
True app \ Predicted app	WhatsApp	WeChat	Telegram	Snapchat	Messenger	Line	Hangouts	Discord
WhatsApp	86					6	1	7
WeChat		99					1	
Telegram	2	1	97					
Snapchat	1			95			2	2
Messenger					99	1		
Line			2	6		88	2	2
Hangouts		5	1			1	91	2
Discord								100

Social Media

True app \ Predicted app	Facebook	Twitter	Instagram	LinkedIn	Reddit	Weibo	Quora	Pinterest
Facebook	91						9	
Twitter		93				2	3	1
Instagram			97		3			
LinkedIn				95	3		2	
Reddit		1			95		4	
Weibo	9			5		85	1	
Quora		1	2	3			92	2
Pinterest						1		99

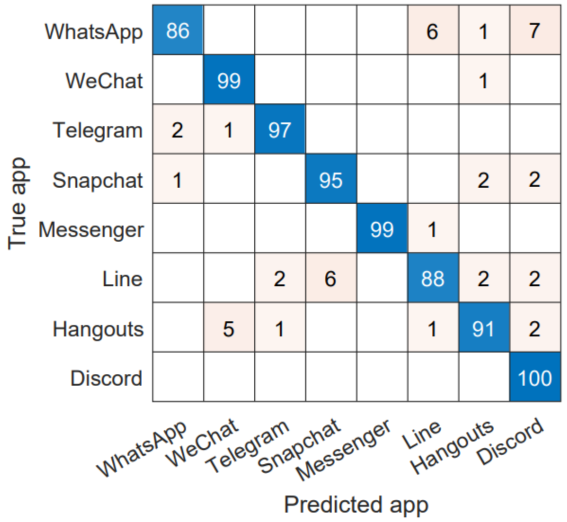
Misprediction Analysis



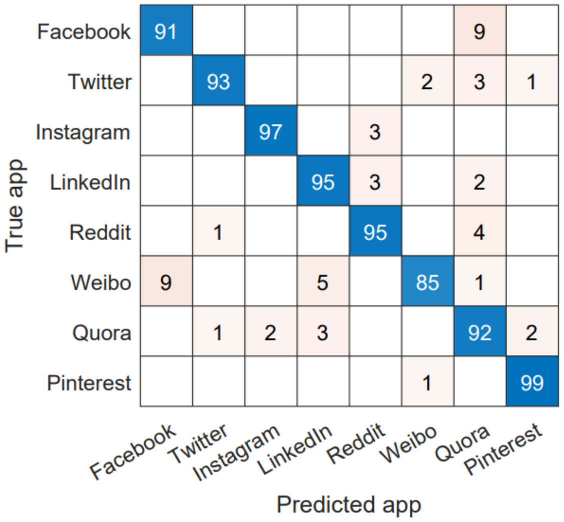


Further Analysis

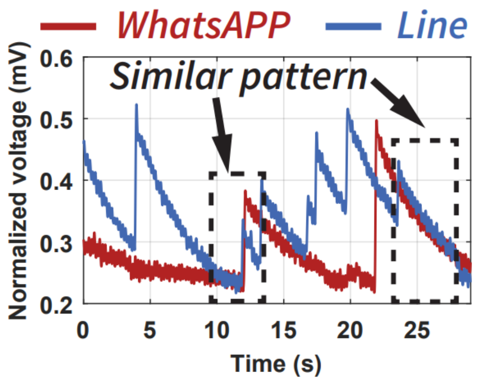
Communication

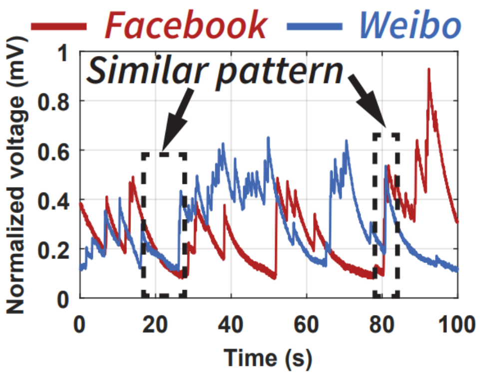


Social Media



Misprediction Analysis



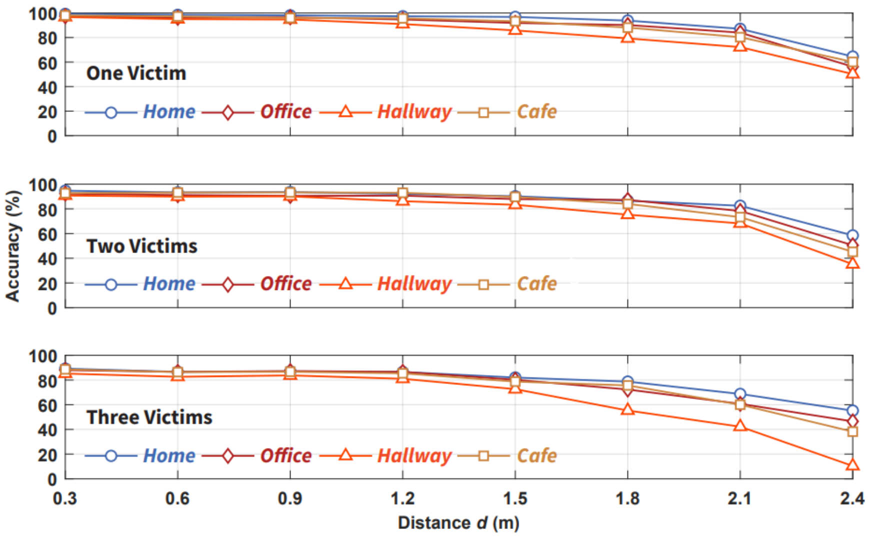


Multi-victim Attacks

	App Combinations										Acc. (%)	App Combinations										Acc. (%)
Two Victims Scenario	●	●	○	○	○	○	○	○	○	○	99.6	○	○	●	○	○	○	●	○	○	○	96.1
	●	○	●	○	○	○	○	○	○	○	91.1	○	○	●	○	○	○	○	●	○	○	95.8
	●	○	○	●	○	○	○	○	○	○	89.2	○	○	●	○	○	○	○	○	●	○	87.7
	●	○	○	○	●	○	○	○	○	○	93.8	○	○	●	○	○	○	○	○	○	●	90.6
	●	○	○	○	○	●	○	○	○	○	98.9	○	○	○	●	●	○	○	○	○	○	87.9
	●	○	○	○	○	○	●	○	○	○	92.5	○	○	○	●	○	●	○	○	○	○	88.5
	●	○	○	○	○	○	○	●	○	○	93.1	○	○	○	●	○	○	●	○	○	○	87.7
	●	○	○	○	○	○	○	○	●	○	96.9	○	○	○	●	○	○	○	●	○	○	89.5
	●	○	○	○	○	○	○	○	○	●	92.4	○	○	○	●	○	○	○	○	●	○	93.2
	○	●	●	○	○	○	○	○	○	○	92.2	○	○	○	●	○	○	○	○	○	●	92.6
	○	●	○	●	○	○	○	○	○	○	95.2	○	○	○	○	●	●	○	○	○	○	98.5
	○	●	○	○	●	○	○	○	○	○	90.3	○	○	○	○	●	○	●	○	○	○	96.1
	○	●	○	○	○	●	○	○	○	○	97.5	○	○	○	○	●	○	○	●	○	○	97.2
	○	●	○	○	○	○	●	○	○	○	90.0	○	○	○	○	●	○	○	○	●	○	95.6
	○	●	○	○	○	○	○	●	○	○	87.7	○	○	○	○	●	○	○	○	○	●	91.1
	○	●	○	○	○	○	○	○	●	○	92.0	○	○	○	○	○	●	●	○	○	○	92.6
	○	●	○	○	○	○	○	○	○	●	89.0	○	○	○	○	○	●	○	●	○	○	91.9
	○	○	●	●	○	○	○	○	○	○	96.8	○	○	○	○	○	●	○	○	●	○	95.1
	○	○	●	○	●	○	○	○	○	○	95.6	○	○	○	○	○	●	○	○	○	●	95.8
	○	○	●	○	○	●	○	○	○	○	98.8	○	○	○	○	○	○	●	●	○	○	96.5
Three Victims Scenario	●	●	●	○	○	○	○	○	○	○	89.3	●	○	○	●	○	○	○	○	○	●	87.4
	●	●	○	●	○	○	○	○	○	○	87.4	●	○	○	○	●	●	○	○	○	○	87.8
	●	●	○	○	●	○	○	○	○	○	84.8	●	○	○	○	●	○	●	○	○	○	85.6
	●	●	○	○	○	●	○	○	○	○	86.5	●	○	○	○	●	○	○	●	○	○	86.1
	●	●	○	○	○	○	●	○	○	○	86.7	●	○	○	○	●	○	○	○	●	○	84.6
	●	●	○	○	○	○	○	●	○	○	87.9	●	○	○	○	●	○	○	○	○	●	85.4
	●	●	○	○	○	○	○	○	●	○	87.7	●	○	○	○	○	●	●	○	○	○	86.9
	●	●	○	○	○	○	○	○	○	●	84.7	●	○	○	○	○	●	○	●	○	○	87.4
	●	○	●	●	○	○	○	○	○	○	86.4	●	○	○	○	○	●	○	○	●	○	86.3
	●	○	●	○	●	○	○	○	○	○	90.2	●	○	○	○	○	●	○	○	○	●	85.4
	●	○	●	○	○	●	○	○	○	○	88.0	●	○	○	○	○	●	○	○	○	●	89.0
	●	○	●	○	○	○	●	○	○	○	85.3	●	○	○	○	○	○	●	●	○	○	87.2
	●	○	●	○	○	○	○	●	○	○	85.6	●	○	○	○	○	○	●	○	●	○	86.9
	●	○	●	○	○	○	○	○	●	○	87.2	●	○	○	○	○	○	●	○	○	●	84.7
	●	○	●	○	○	○	○	○	○	●	84.5	●	○	○	○	○	○	○	●	●	○	84.2
	●	○	○	●	●	○	○	○	○	○	86.5	●	○	○	○	○	○	○	●	○	●	83.8
	●	○	○	●	○	●	○	○	○	○	88.0	○	●	●	●	○	○	○	○	○	○	86.5
	●	○	○	●	○	○	●	○	○	○	87.5	○	●	●	○	●	○	○	○	○	○	83.7
	●	○	○	●	○	○	○	●	○	○	90.0	○	●	●	○	○	●	○	○	○	○	85.6
	●	○	○	●	○	○	○	○	●	○	86.9	○	●	●	○	○	○	●	○	○	○	86.0

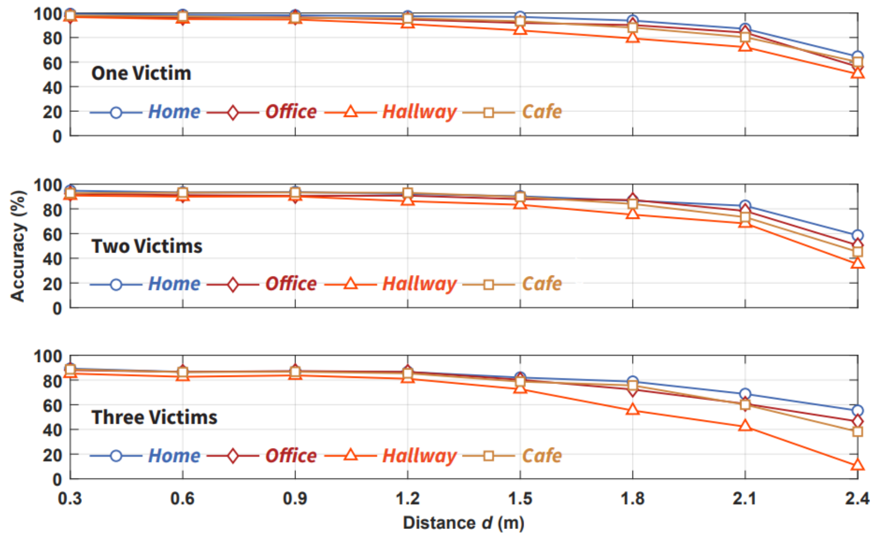
Impact Factors

Impact of distance

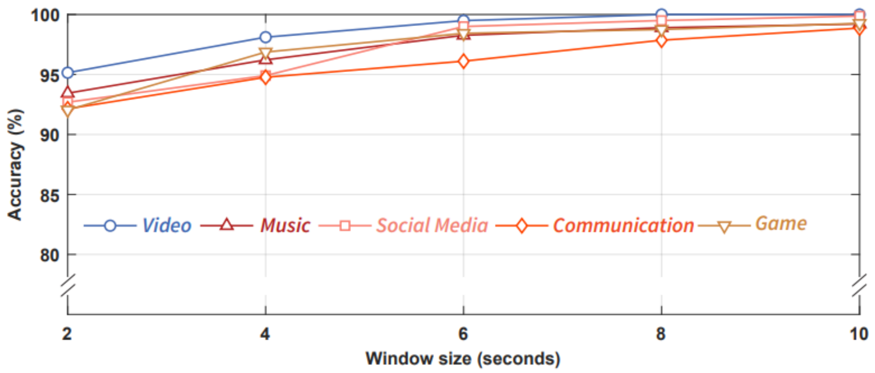


Impact Factors

Impact of distance

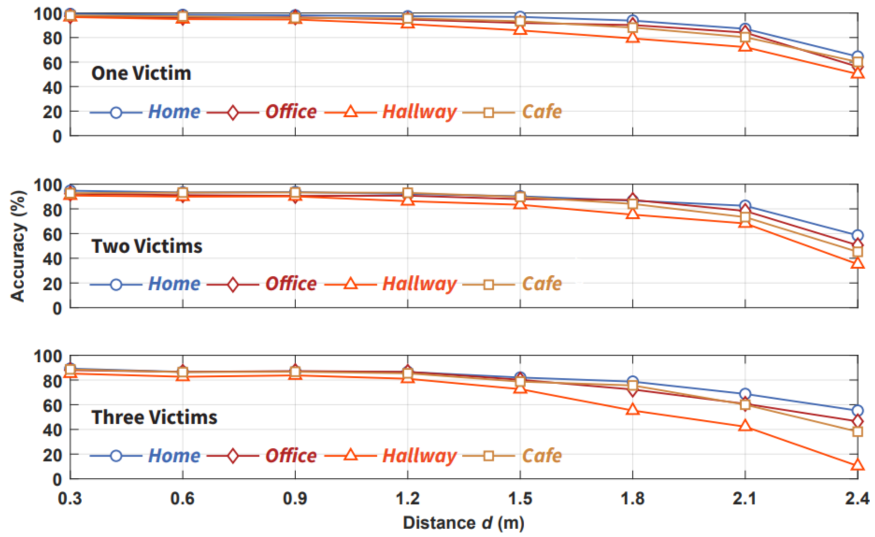


Impact of sliding window

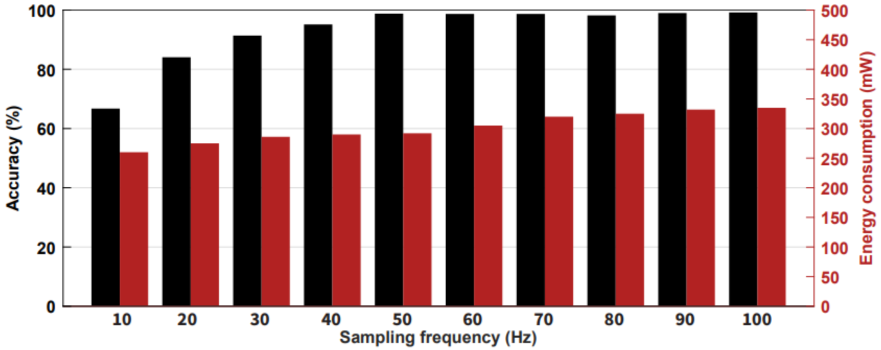


Impact Factors

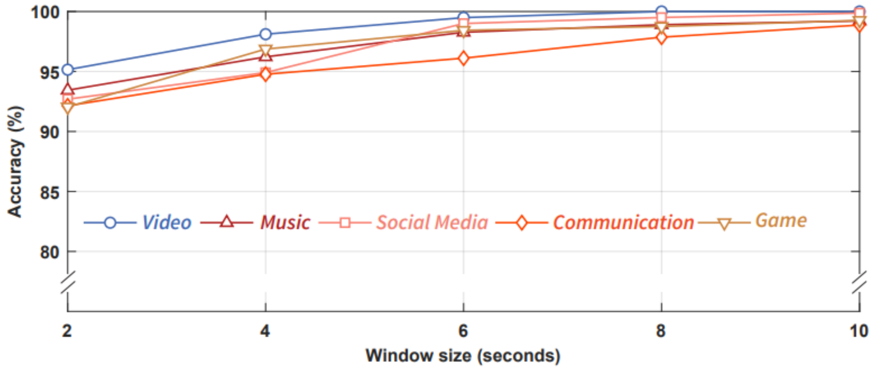
Impact of distance



Impact of sampling frequency

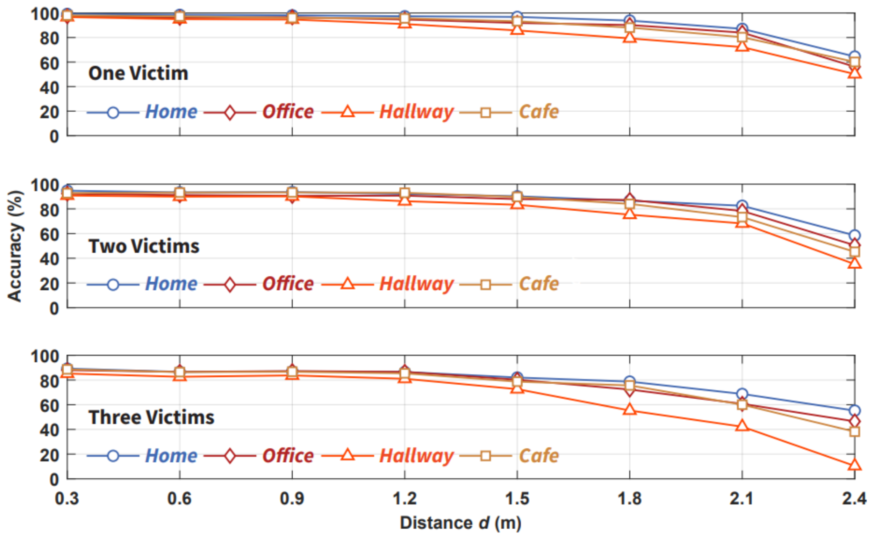


Impact of sliding window

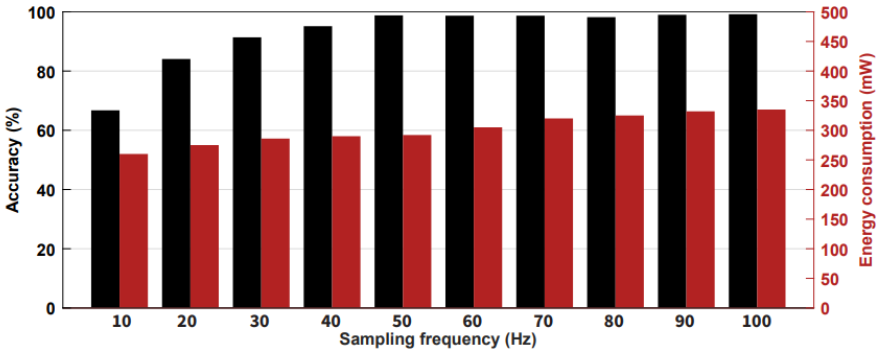


Impact Factors

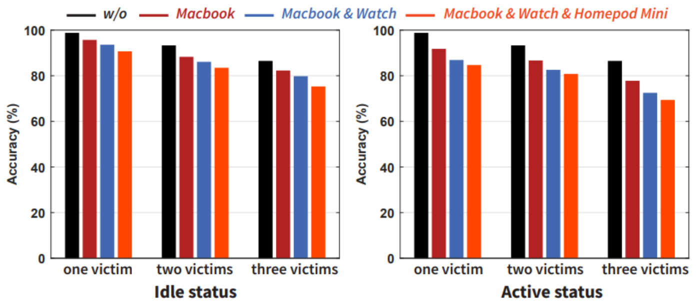
Impact of distance



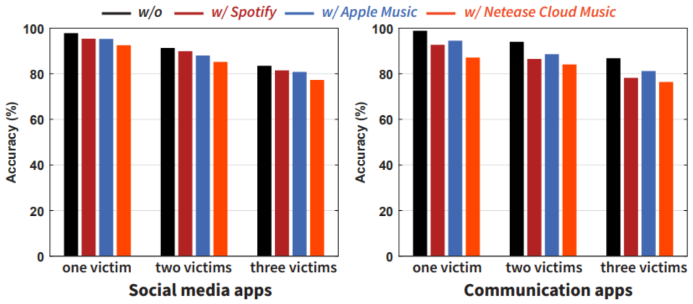
Impact of sampling frequency



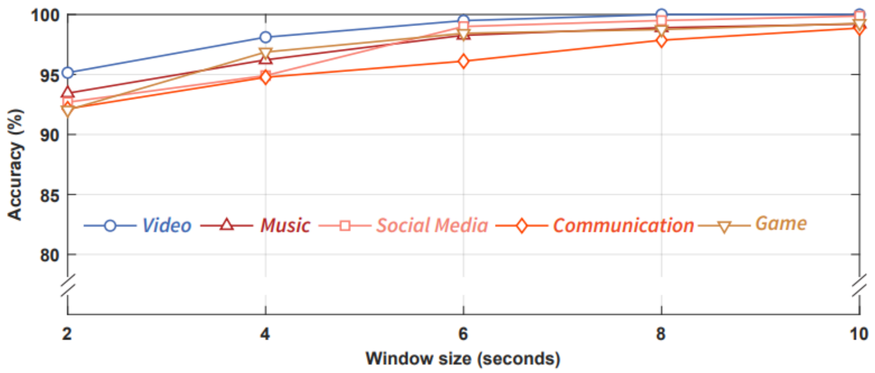
Impact of non-target devices



Impact of background apps

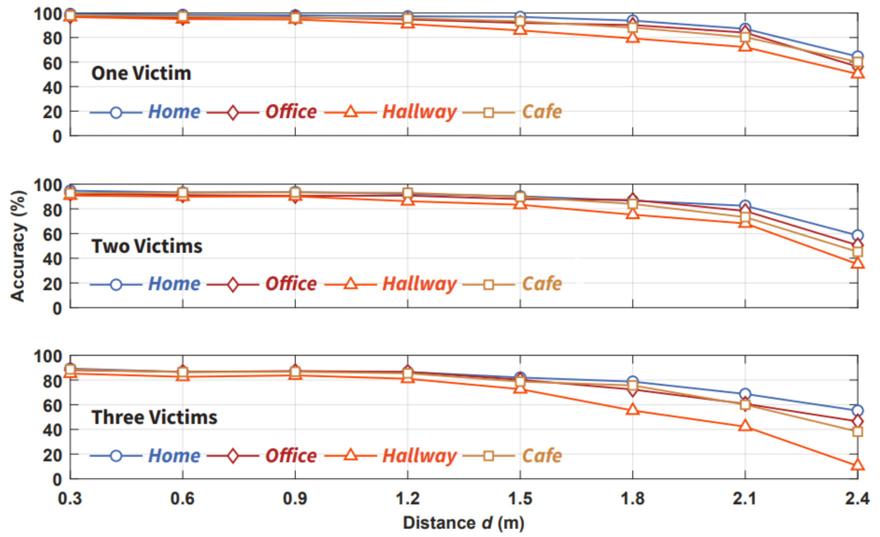


Impact of sliding window

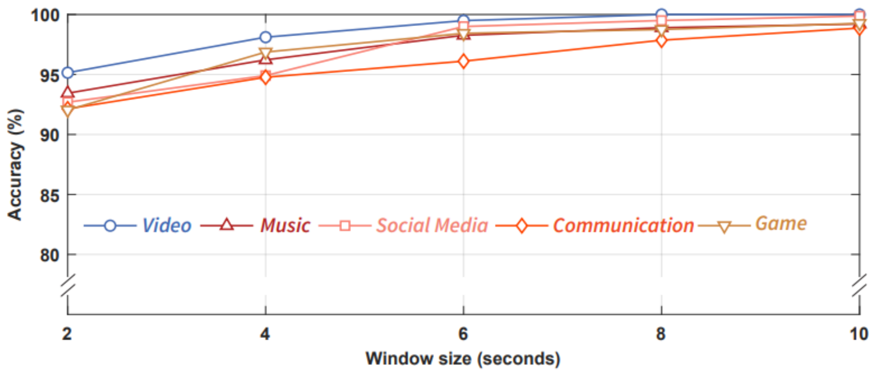


Impact Factors

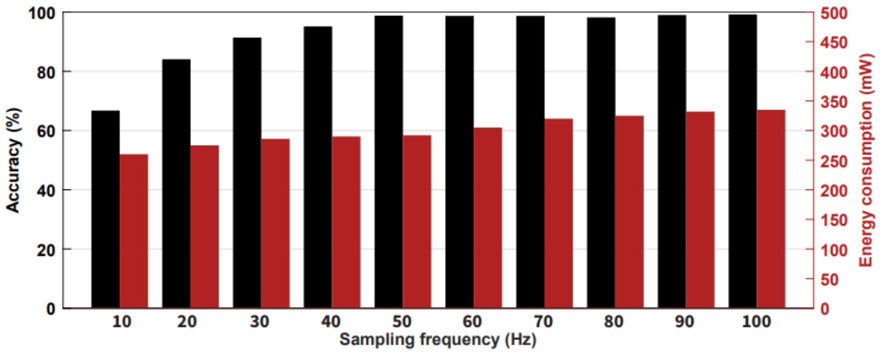
Impact of distance



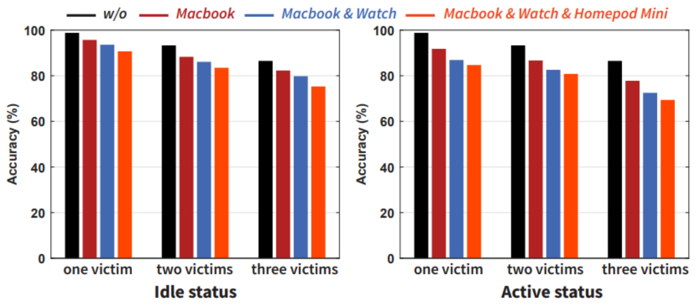
Impact of sliding window



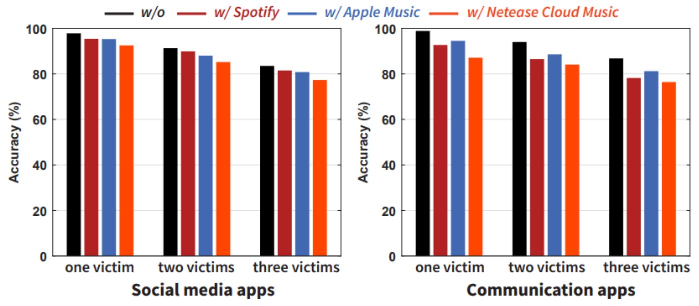
Impact of sampling frequency



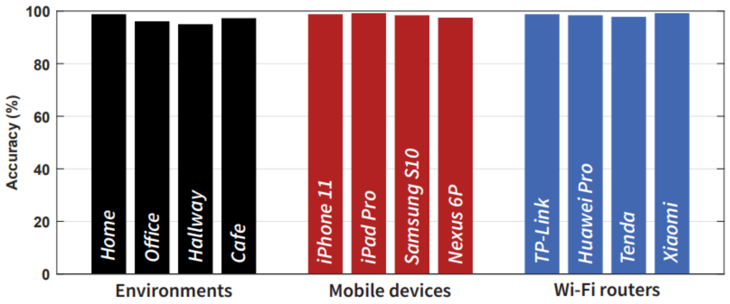
Impact of non-target devices



Impact of background apps



Impact of environment and hardware



Generalization, Improvement, and Through-Wall Attacks

Cross environment, cross mobile devices, and cross Wi-Fi routers

Accuracy (%)		Test environments					Test mobile devices					Test Wi-Fi routers			
		Home	Office	Hallway	Cafe		iPhone 11	iPad Pro	Samsung	Nexus 6P		TP-Link	Huawei	Tenda	Xiaomi
Training model	Home	98.8	96.5	94.3	98.2	iPhone 11	98.8	96.5	90.2	88.0	TP-Link	98.8	95.4	97.7	98.0
	Office	95.3	96.1	92.3	95.8	iPad Pro	94.3	99.2	91.6	90.2	Huawei	95.8	98.4	95.4	96.2
	Hallway	94.3	91.5	95.0	92.1	Samsung	89.3	88.6	98.4	93.1	Tenda	94.3	96.5	97.8	95.5
	Cafe	96.6	96.1	95.0	97.3	Nexus 6P	87.7	88.0	92.9	97.5	Xiaomi	94.5	95.2	97.3	99.2

Generalization, Improvement, and Through-Wall Attacks

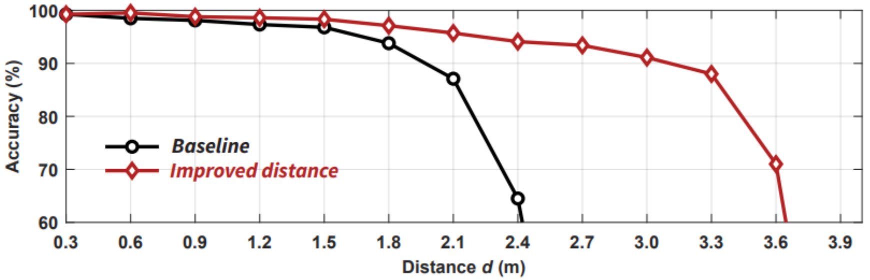
Cross environment, cross mobile devices, and cross Wi-Fi routers

Accuracy (%) — Training model	Test environments: Home	Office	Hallway	Cafe
Home	98.8	96.5	94.3	98.2
Office	95.3	96.1	92.3	95.8
Hallway	94.3	91.5	95.0	92.1
Cafe	96.6	96.1	95.0	97.3

Accuracy (%) — Training model	Test mobile devices: iPhone 11	iPad Pro	Samsung	Nexus 6P
iPhone 11	98.8	96.5	90.2	88.0
iPad Pro	94.3	99.2	91.6	90.2
Samsung	89.3	88.6	98.4	93.1
Nexus 6P	87.7	88.0	92.9	97.5

Accuracy (%) — Training model	Test Wi-Fi routers: TP-Link	Huawei	Tenda	Xiaomi
TP-Link	98.8	95.4	97.7	98.0
Huawei	95.8	98.4	95.4	96.2
Tenda	94.3	96.5	97.8	95.5
Xiaomi	94.5	95.2	97.3	99.2

Improving attack distance with two RF-DC converters

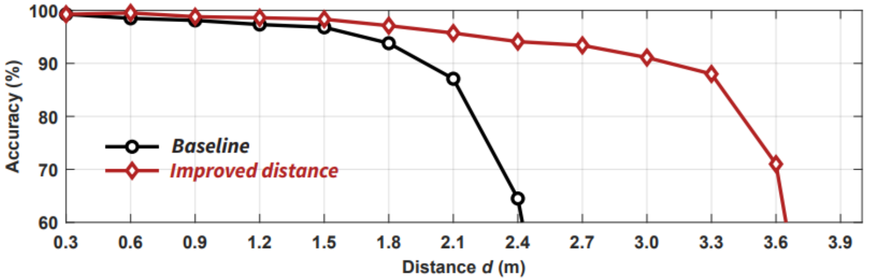


Generalization, Improvement, and Through-Wall Attacks

Cross environment, cross mobile devices, and cross Wi-Fi routers

Accuracy (%)	Test environments					Test mobile devices					Test Wi-Fi routers			
Training model	Home	Office	Hallway	Cafe		iPhone 11	iPad Pro	Samsung	Nexus 6P		TP-Link	Huawei	Tenda	Xiaomi
Home	98.8	96.5	94.3	98.2	iPhone 11	98.8	96.5	90.2	88.0	TP-Link	98.8	95.4	97.7	98.0
Office	95.3	96.1	92.3	95.8	iPad Pro	94.3	99.2	91.6	90.2	Huawei	95.8	98.4	95.4	96.2
Hallway	94.3	91.5	95.0	92.1	Samsung	89.3	88.6	98.4	93.1	Tenda	94.3	96.5	97.8	95.5
Cafe	96.6	96.1	95.0	97.3	Nexus 6P	87.7	88.0	92.9	97.5	Xiaomi	94.5	95.2	97.3	99.2

Improving attack distance with two RF-DC converters



Harvested voltage & Accuracy vs. Blocking items

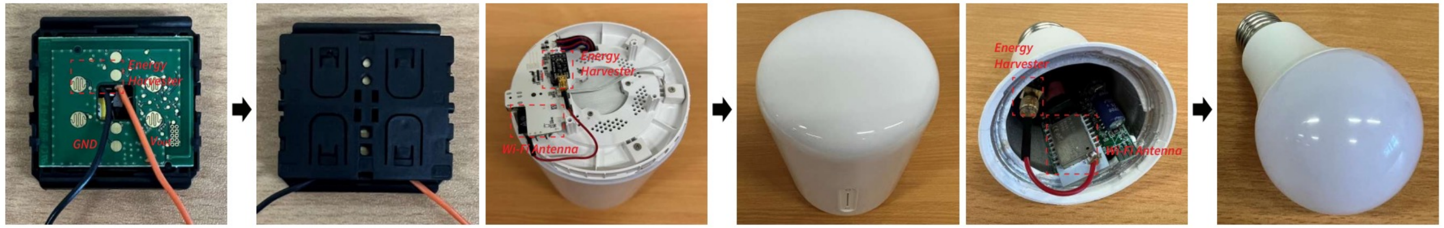
Blocking item	Thickness (cm)	Harvested voltage (mV)	Acc. (%)
Non-blocking	–	429	98.4
Partition board	2.8	359	97.7
Wooden door	6.1	241	96.8
Thin wall	8.0	122	93.1
Thick wall	27.4	0	–

Attack IoT Devices

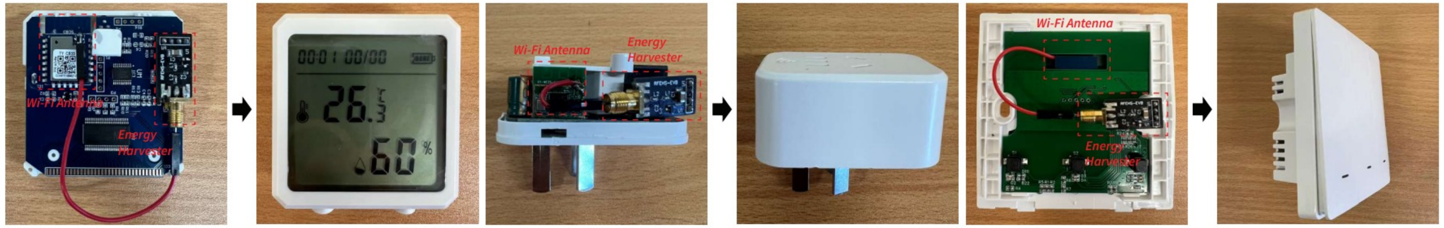
Result of attacking IoT devices

Commodity Product	Energy Harvester	Antenna	Gain	BLE	Acc. (%) of Multi-Victim Scenarios			Max. Distance (m) (One Acc. > 90%)
					One	Two	Three	
ZF Energy Harvesting BLE Push-button [46]	●	●	N/A	●	93.6	89.5	82.2	~ 1.05
Xiaomi Mi Bedside Smart Lamp [47]	○	●	N/A	●	90.9	83.0	77.1	~ 0.60
GHome Smart LED Bulb [48]	○	●	N/A	○	91.8	86.2	80.7	~ 1.50
Tuya Wi-Fi Temperature and Humidity Sensor [49]	○	●	1.3 dBi	●	86.9	83.1	78.1	~ 0.45
Tuya Smart Plug (With Metering) [50]	○	●	1.0 dBi	○	89.4	83.6	76.9	~ 0.45
Zinguo Wi-Fi Smart Switch [51]	○	●	3.0 dBi	○	91.8	85.8	81.6	~ 0.90

Integrating *AppListener* into different commodity IoT devices



(a) Energy Harvesting BLE Pushbutton. (b) Xiaomi Mi Bedside Smart Lamp (c) GHome Smart LED Bulb



(d) Wi-Fi Temperature and Humidity Sensor (e) Tuya Smart Plug (With Metering) (f) Zinguo Wi-Fi Smart Switch

Countermeasures

- **Traffic obfuscation: transmitting redundant packets to interfere harvested voltages.**

- **Dynamic power adaptation: bursting transmission in low-power mode while transmitting small packets in high-power mode.**

Thank you!

Speaker: Tao Ni

Personal website: tony520.github.io

City University of Hong Kong