AIM: Amplifying Intelligence in Mobile Networks

A Brief Summary

Chunyi Peng

Purdue University

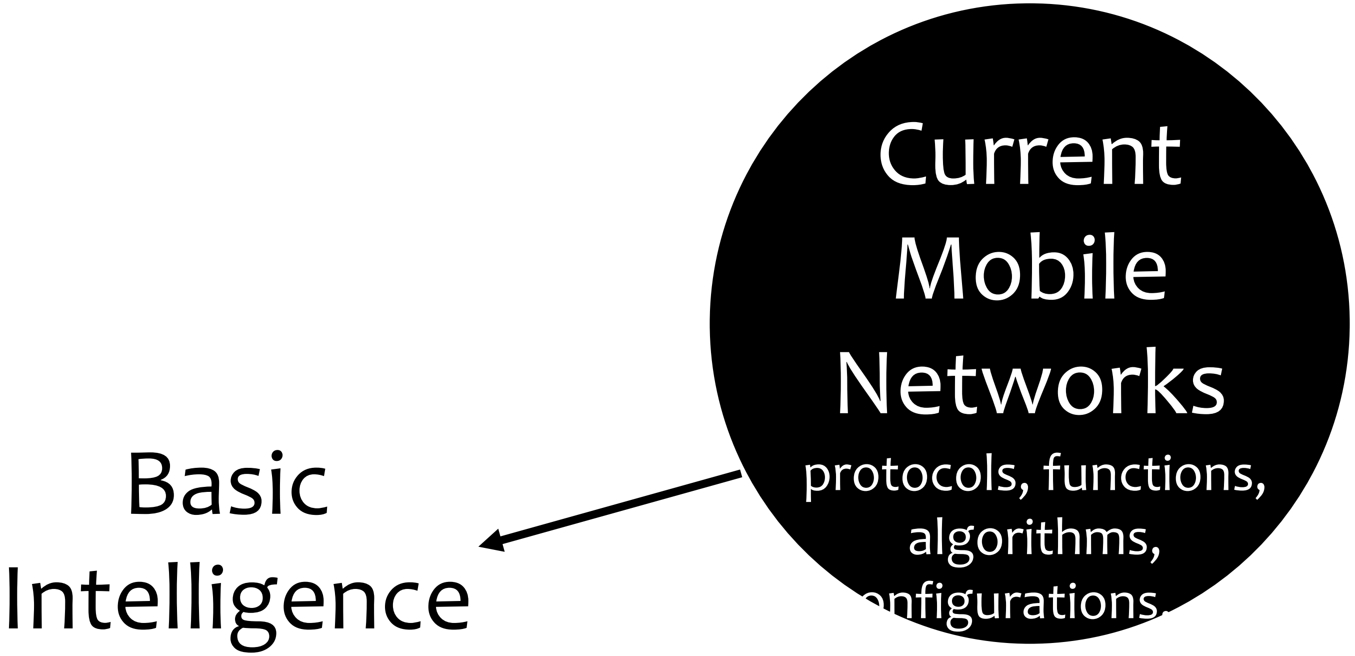
Nov 2018

What is AIM?

Our vision

Make it open and more intelligent

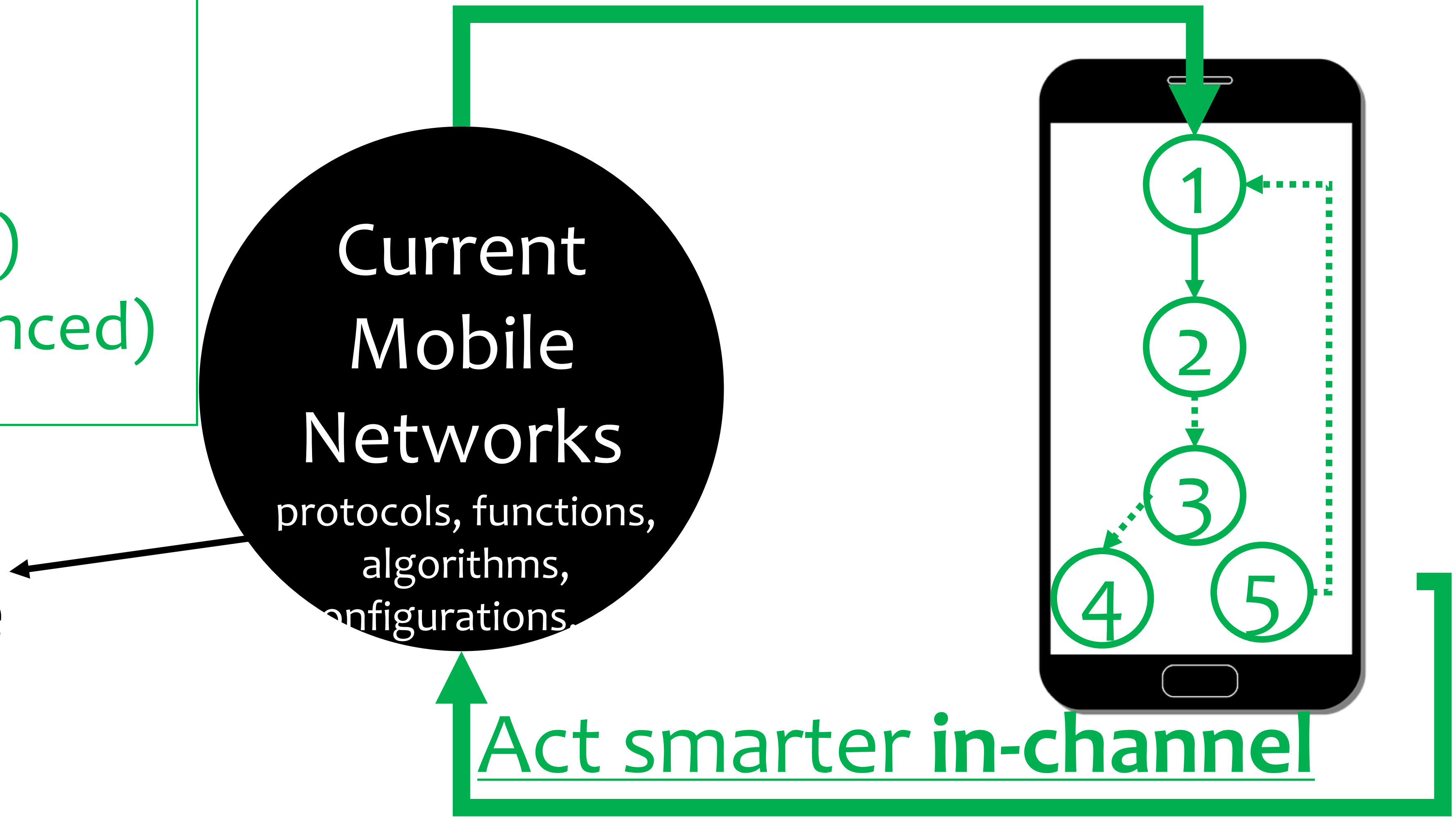
Current problem:
“blackbox”
to users and researchers
(hard to do research)



Make it open and more intelligent

Enable a data-driven **secondary-channel** to learn and reason

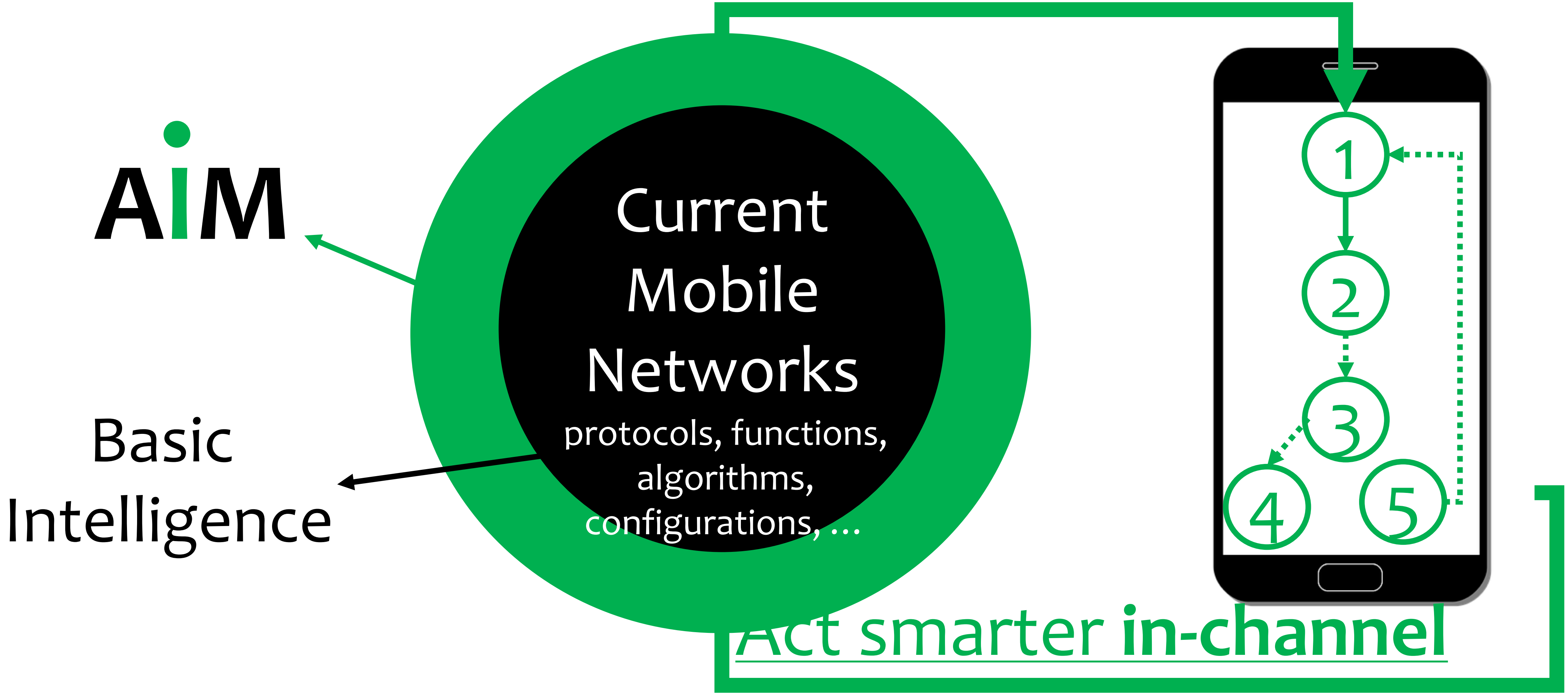
① Open data
② Learning
③ Reasoning
④ Acting (basic)
⑤ Acting (advanced)


Current Mobile Networks
protocols, functions, algorithms, onfigurations,
1
2
3
4
5
Act smarter **in-channel**

Basic Intelligence

Make it open and more intelligent

Enable a data-driven **secondary-channel** to learn and reason



AiM

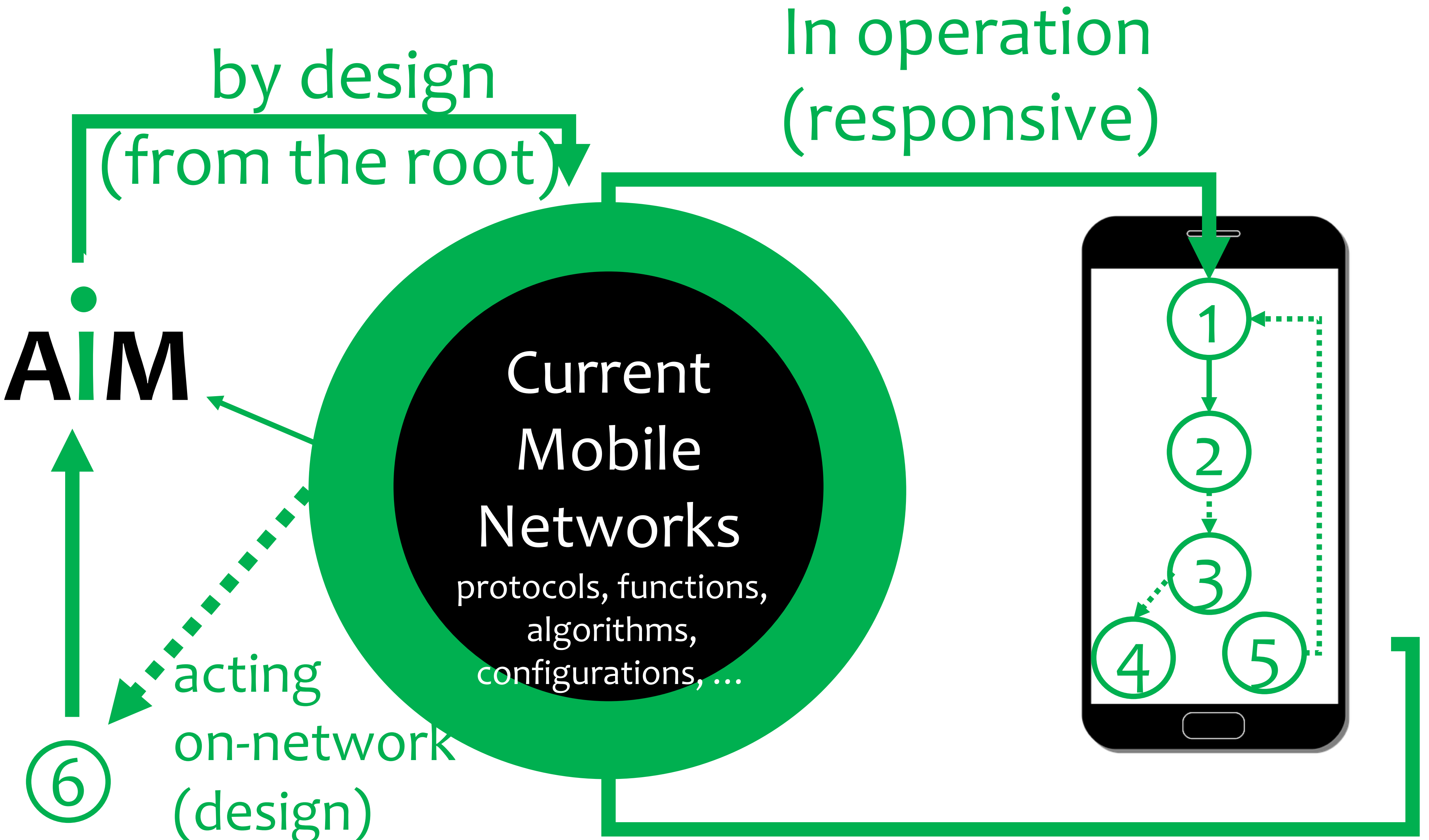
Basic Intelligence

Current Mobile Networks

protocols, functions, algorithms, configurations, …

Act smarter **in-channel**

From operation to design



by design (from the root)

In operation (responsive)

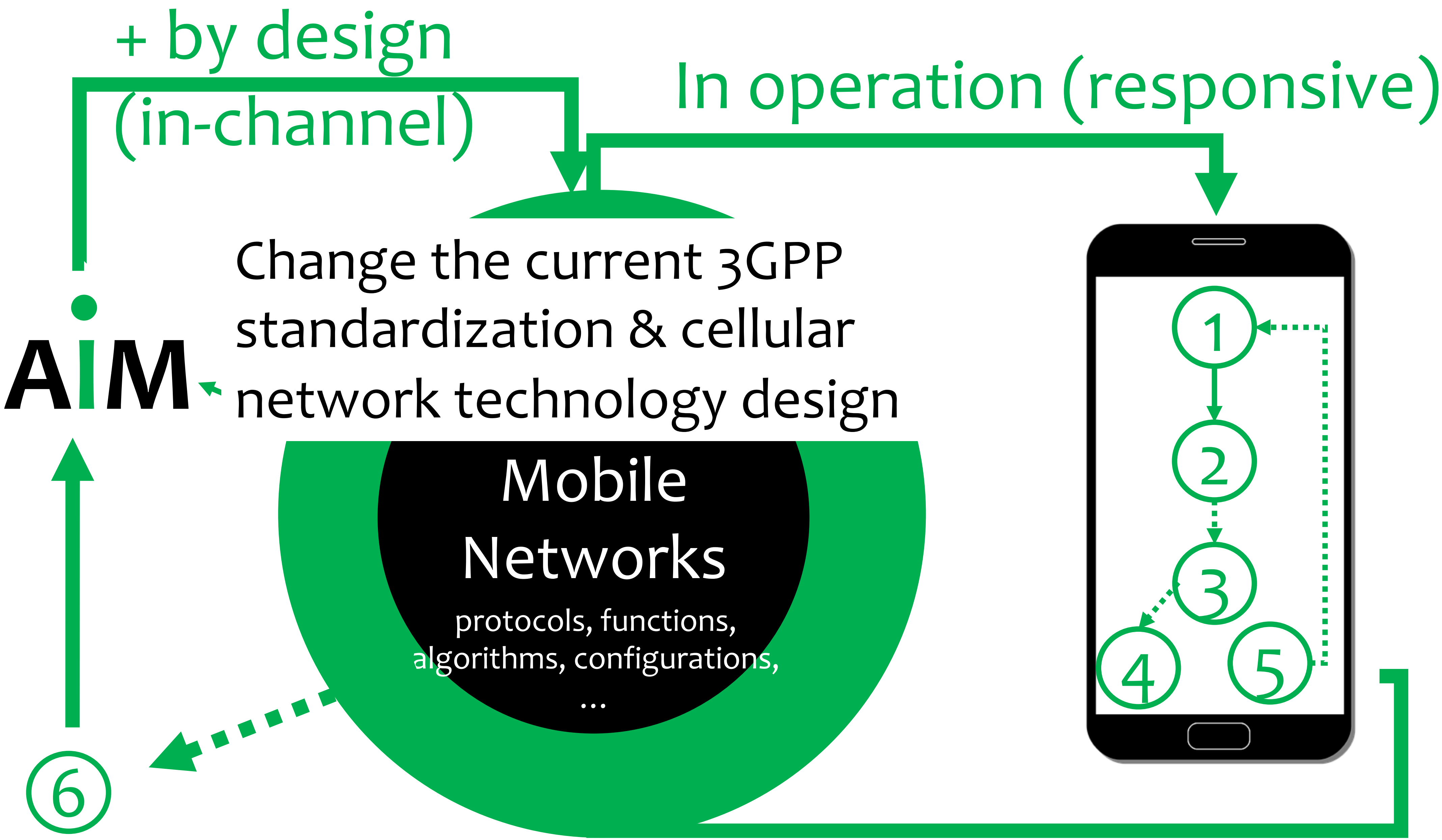
AiM

Current Mobile Networks

protocols, functions, algorithms, configurations, …

acting on-network (design)

From operation to design



+ by design (in-channel)

In operation (responsive)

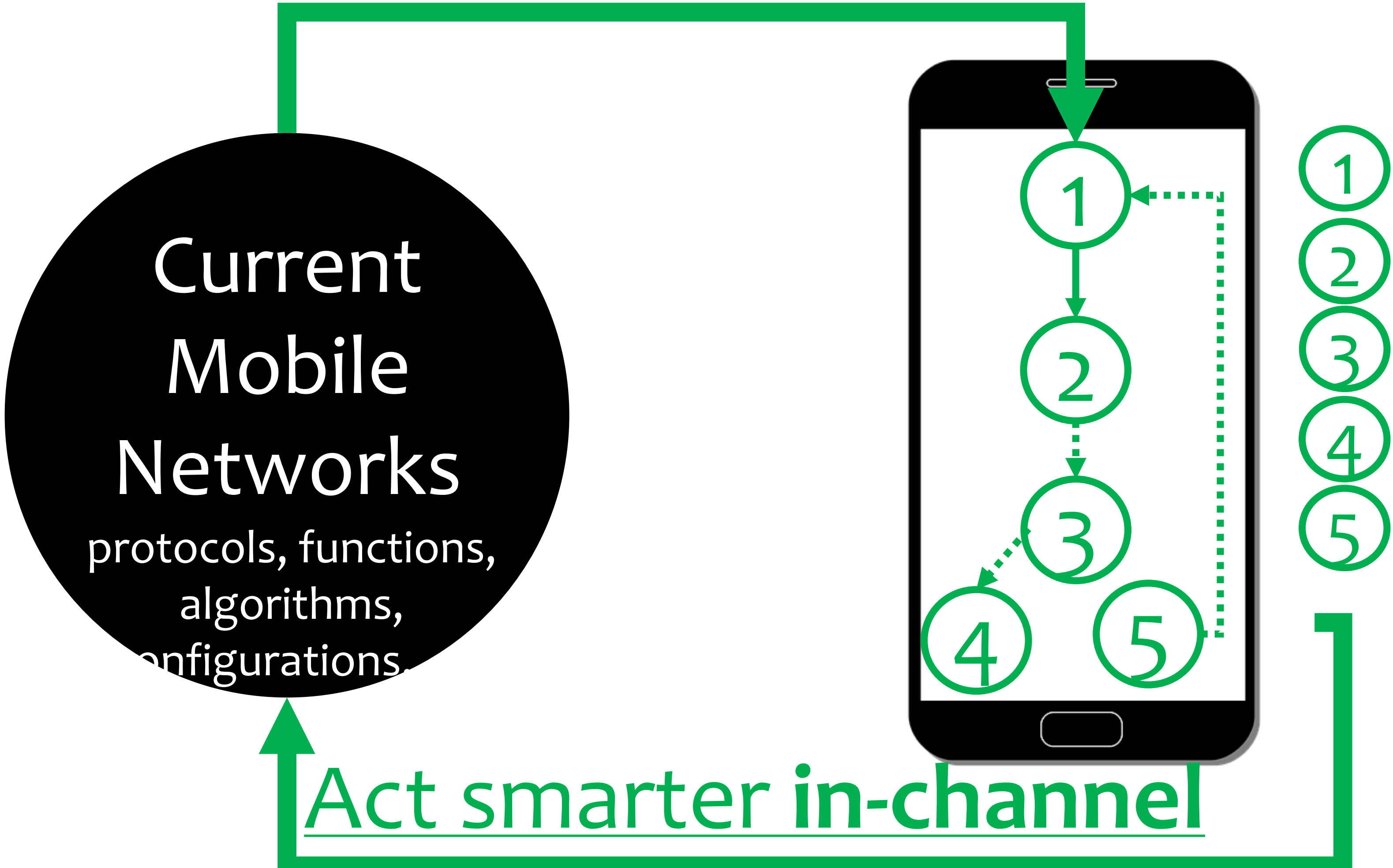
Change the current 3GPP standardization & cellular network technology design

What we have done for AIM?

Our approaches & progress

Empower device-side intelligence

Enable a data-driven **secondary-channel** to learn and reason

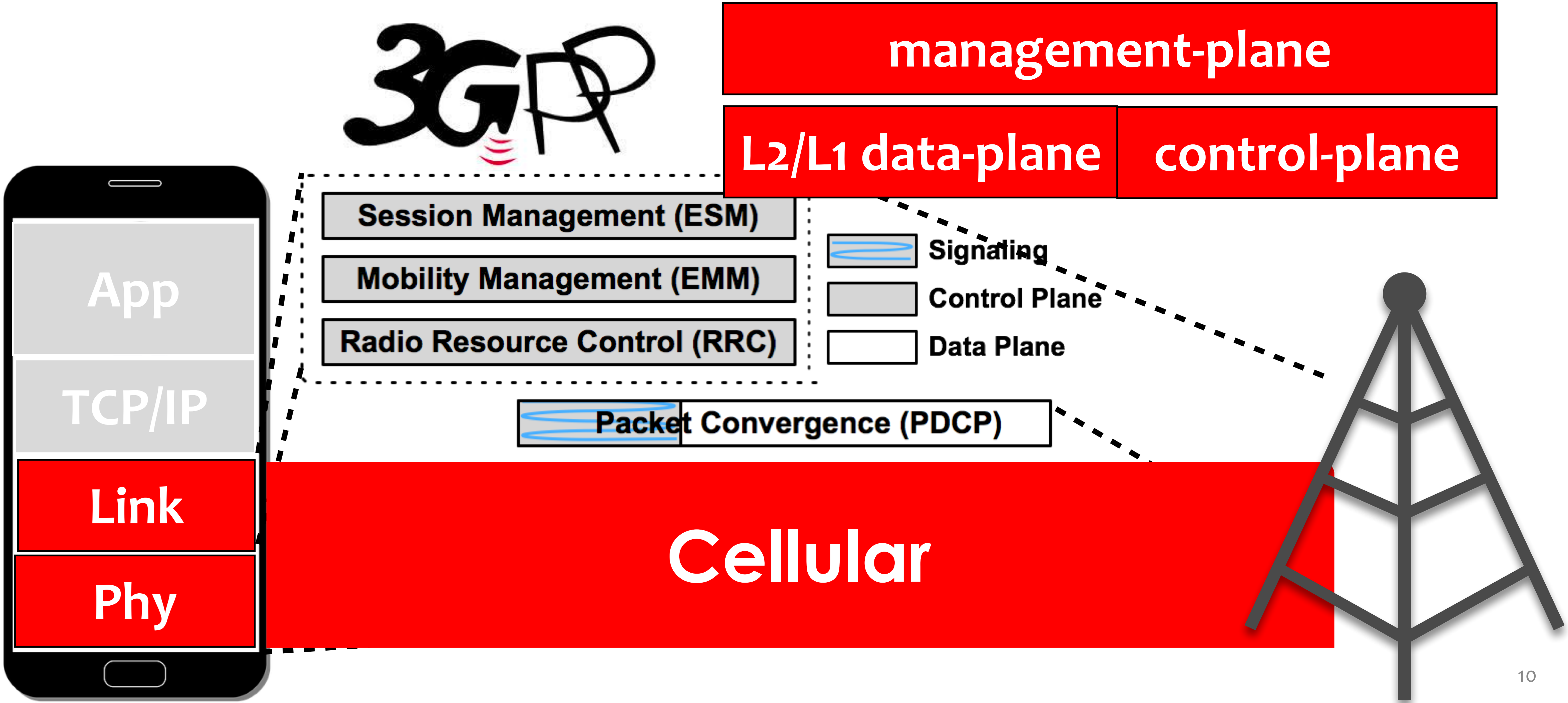


Act smarter **in-channel**

1 Open data
2 Learning
3 Reasoning
4 Acting (basic)
5 Acting (advanced)

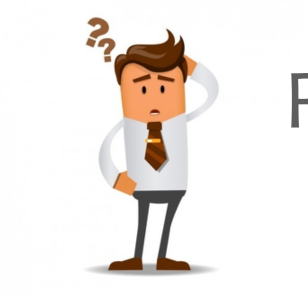
Our solution #1: Make it open

① Open it (data-driven)



It is hard to get data

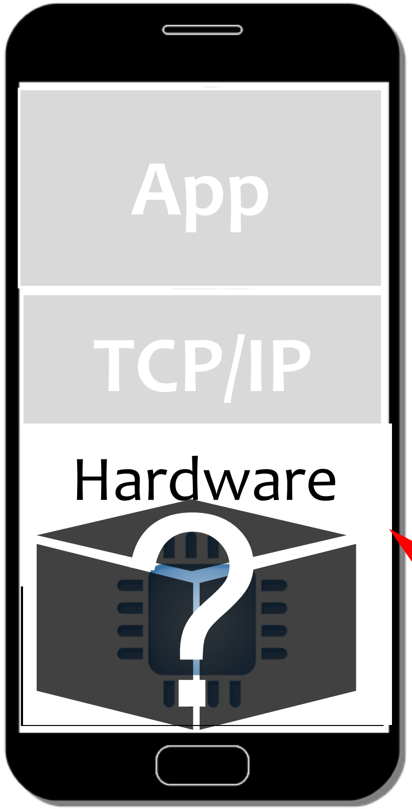
- A long-standing barrier in academia



Researcher
(like you)

Operators

Oh we cannot tell you unless you sign an NDA

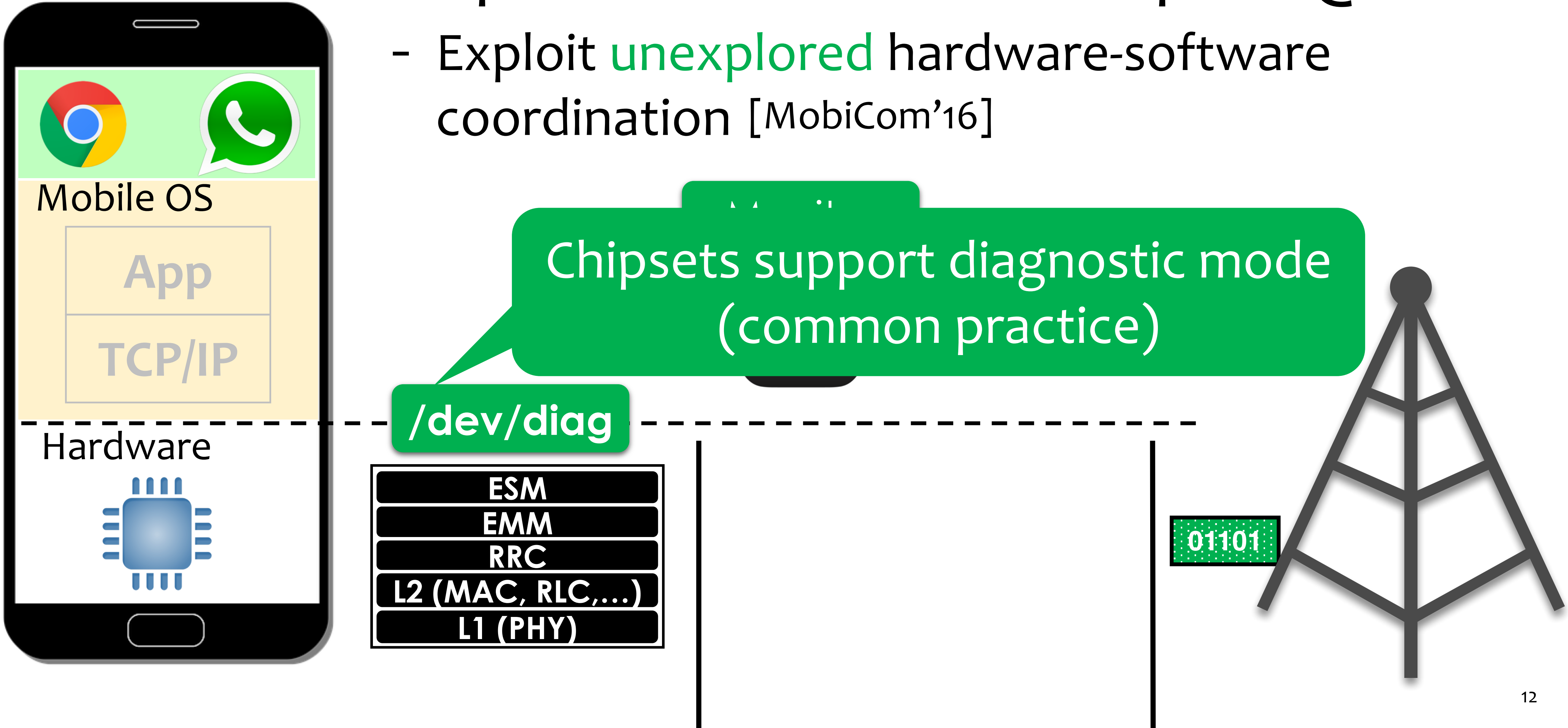


OS/chipset

Whoops!
No API. No data exposed

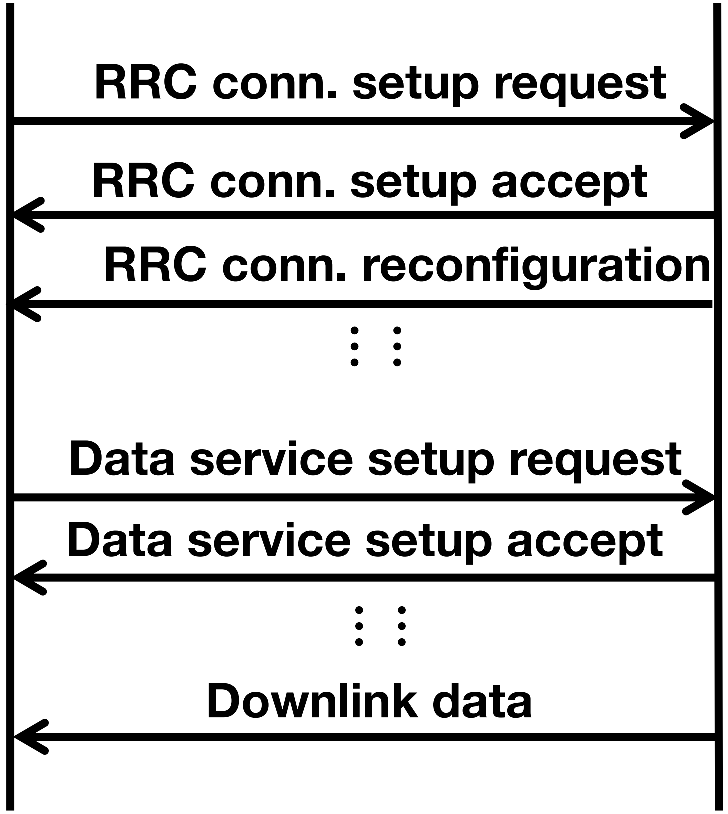
Our solution #1 via MobileInsight

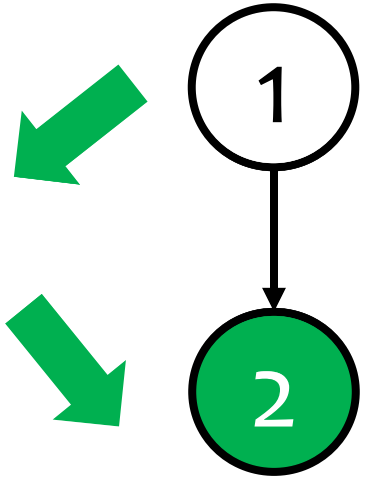
- Expose data to software space @device
  - Exploit unexplored hardware-software coordination [MobiCom'16]



Chipsets support diagnostic mode (common practice)

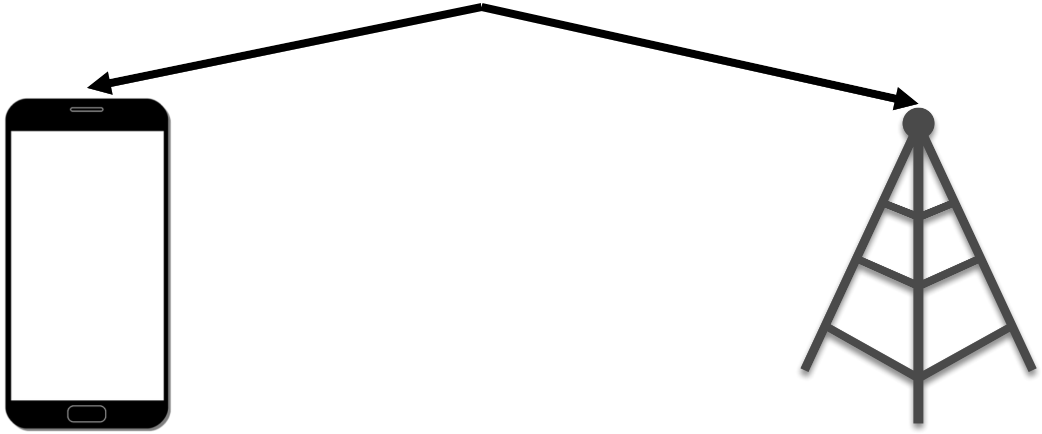
Our solution #2: Learning


RRC conn. setup request
RRC conn. setup accept
RRC conn. reconfiguration
Data service setup request
Data service setup accept
Downlink data



Open it (data-driven)

Learn what (inference and analytics)



Tracking local states

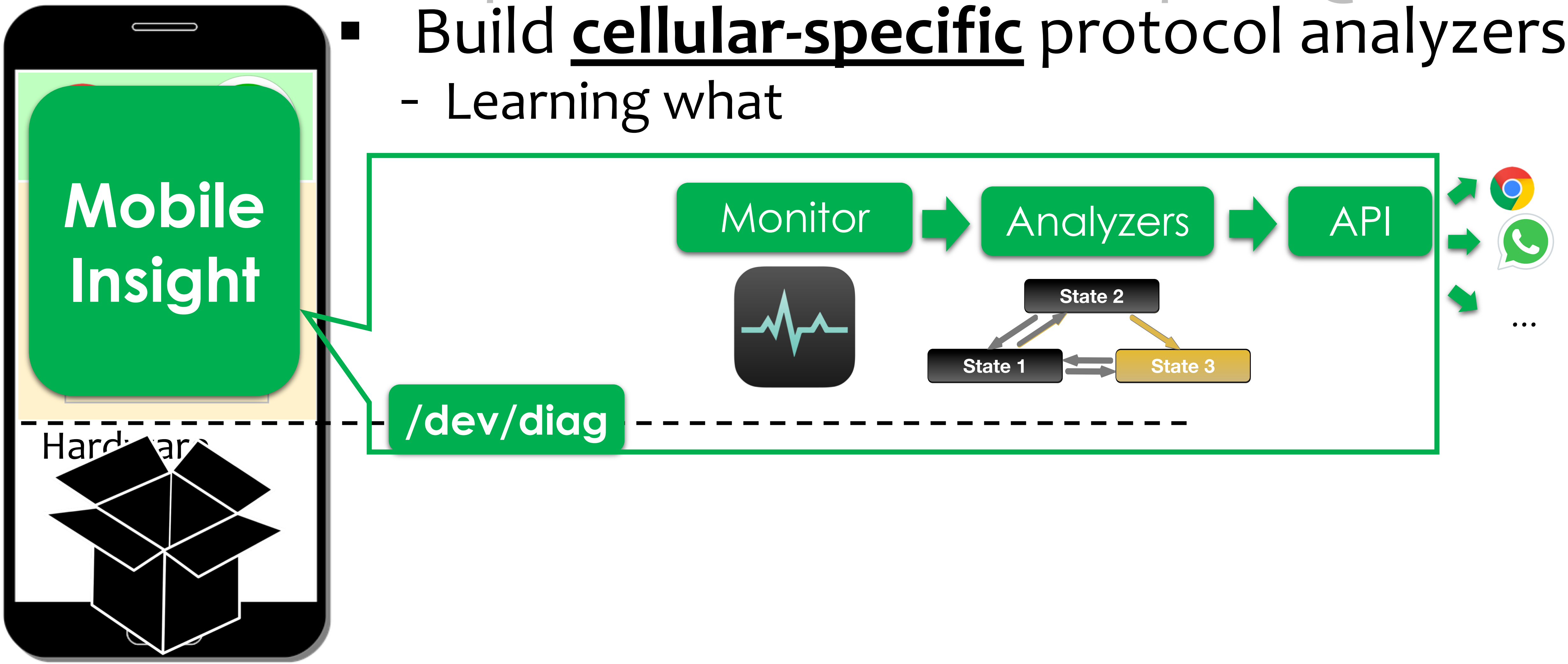
Inferring operation logic

✓ Leverage domain knowledge (protocol state machine models from 3GPP)

✓ Plus learning algorithms (details in Mobicom'16)

MobileInsight: Data + Learning

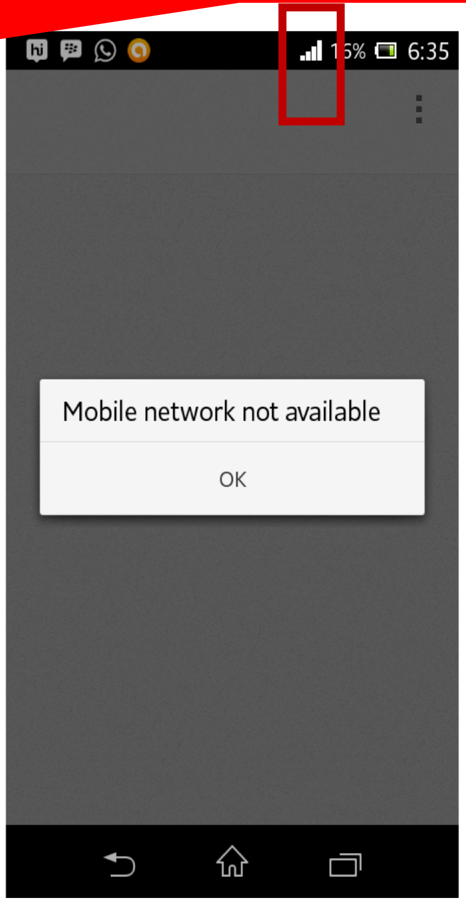
- Expose data to software space @device
- Build **cellular-specific** protocol analyzers
  - Learning what



Now, we open the box to learn what is happening (and likely why)

Back to the example

Why no network access?

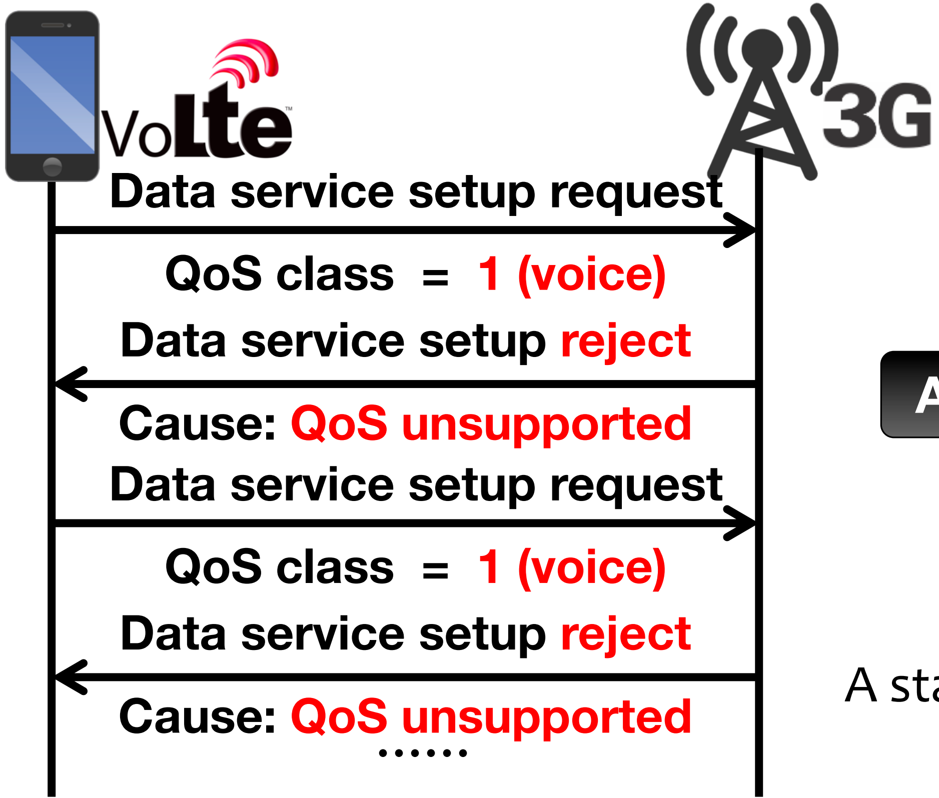


Mobile network not available

Wireless quality & speed look good!

By tracking protocol states …

- **Cause:** device-side misconfiguration
  - **Easy fix:** disable VoLTE when the device in 3G



Data service setup request

QoS class = 1 (voice)

Data service setup reject

Cause: QoS unsupported

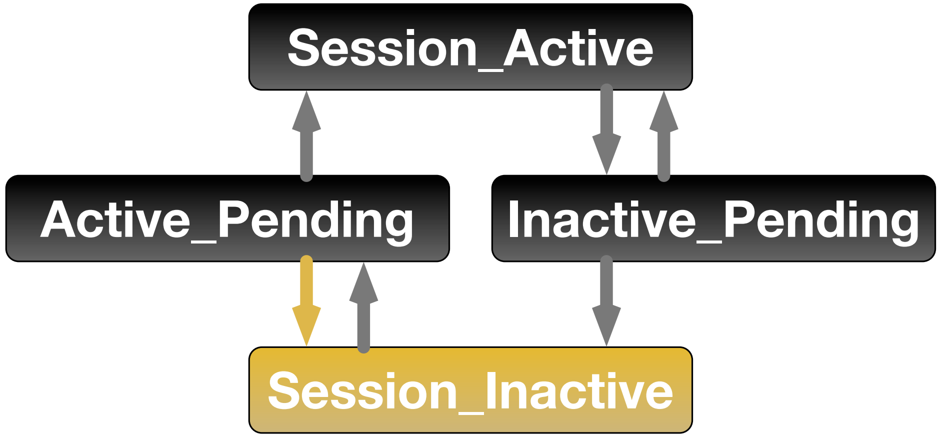
Data service setup request

QoS class = 1 (voice)

Data service setup reject

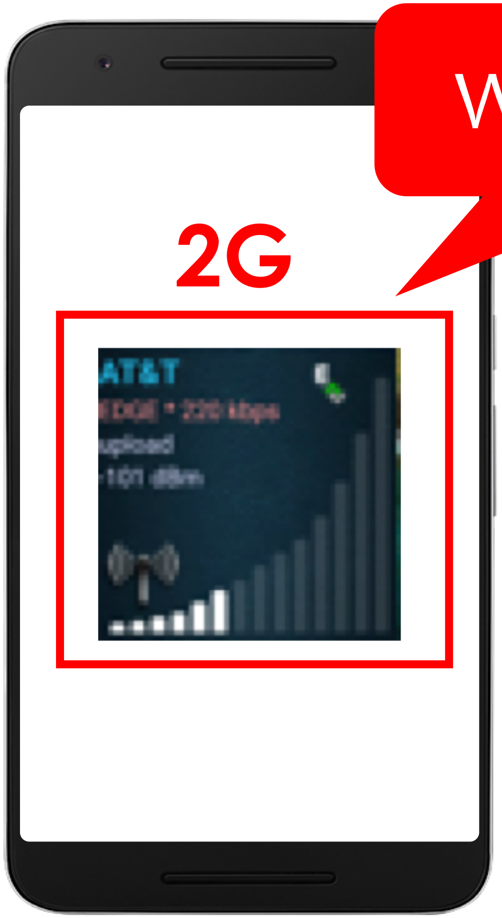
Cause: QoS unsupported

……



A state machine of session establishment @ Device

Back to another example

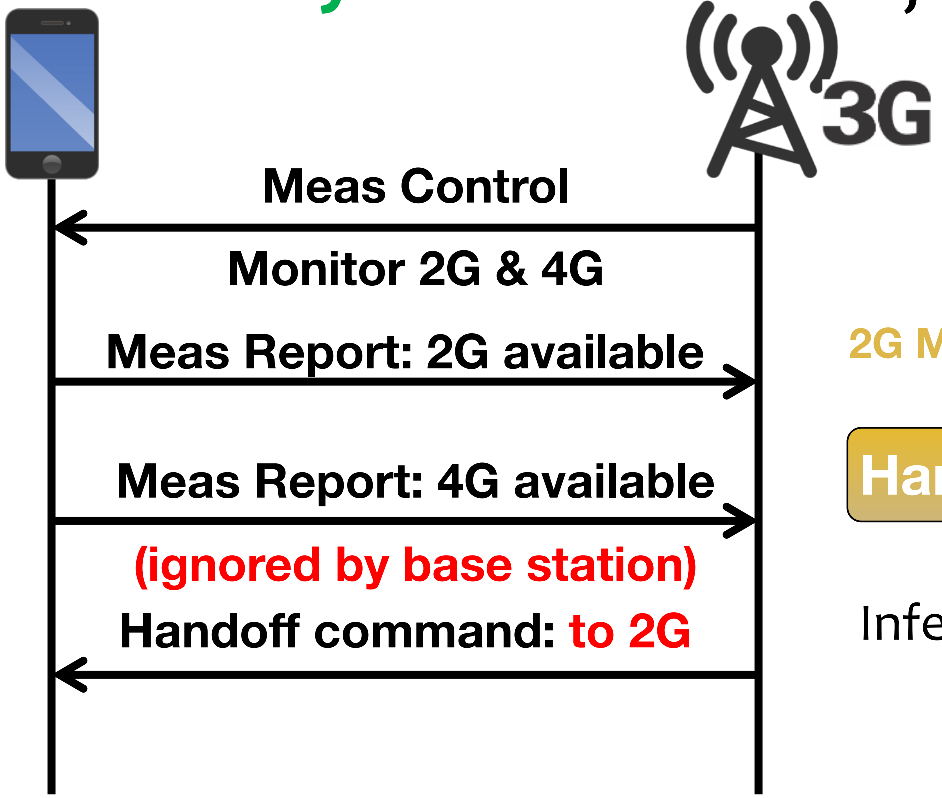


Why slow 2G?

When 4G is available

By inferring handoff decision logic…

- **Cause:** inconsistent policies at device and network (FCFS@base station)
  - **Easy fix:** the device just switches to 4G



Meas Control

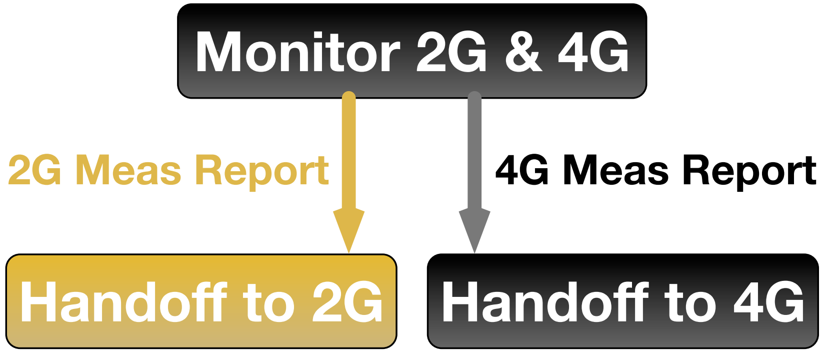
Monitor 2G & 4G

Meas Report: 2G available

Meas Report: 4G available

(ignored by base station)

Handoff command: to 2G



Monitor 2G & 4G

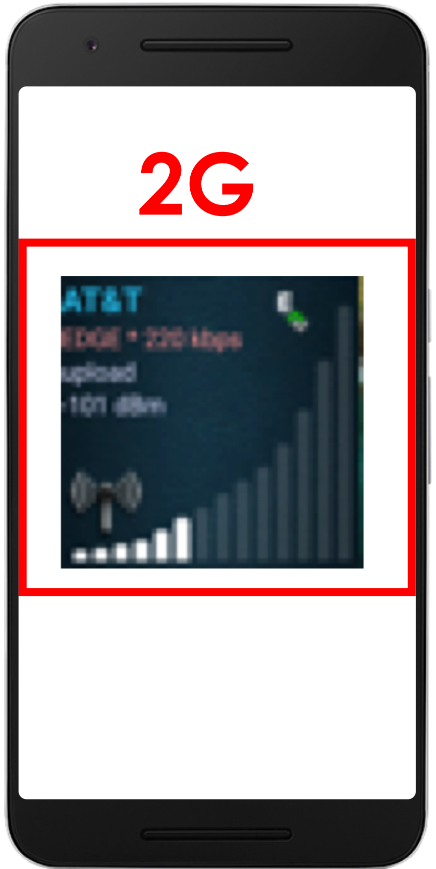
2G Meas Report

4G Meas Report

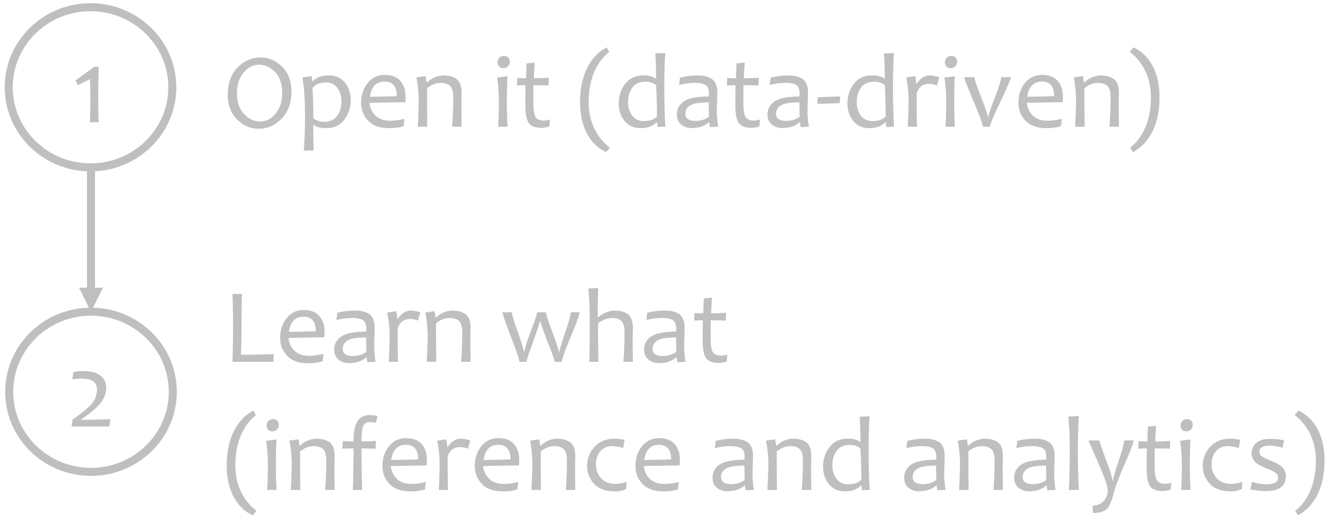
Handoff to 2G

Handoff to 4G

Inferred state machine of handoff



What is Next?



1 Open it (data-driven)

2 Learn what (inference and analytics)

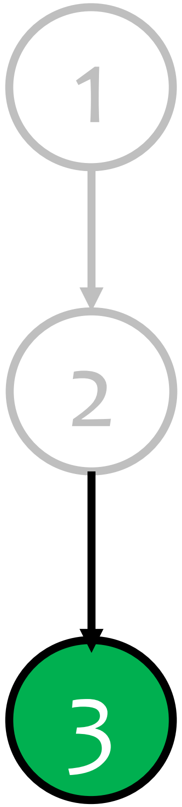
Solve the problem if wrong

- or improvement on performance, reliability, security …

Reason why (by design)

- From the root
- Is it correct? Can it be solved/improved?

What is Next?



Open it (data-driven)

Learn what (inference and analytics)

Reason why (by design)

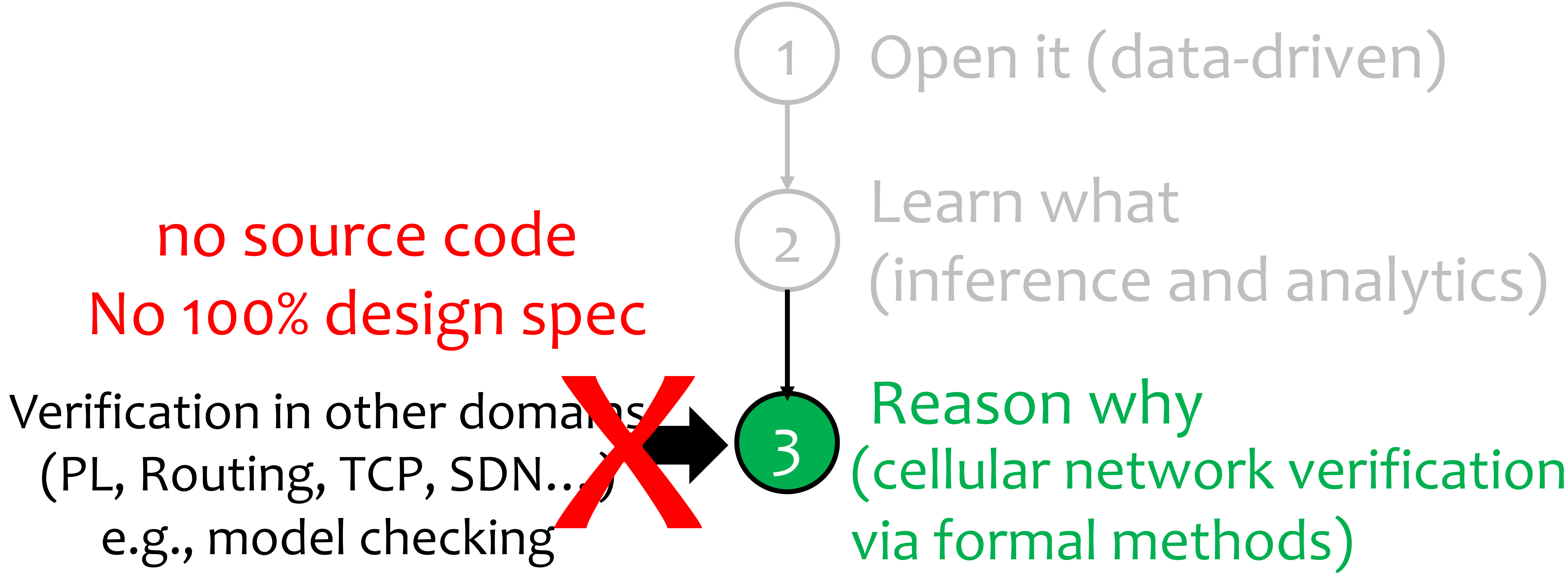
- From the root
- Is it correct? Can it be solved/improved?

Be rigorous (scientific)

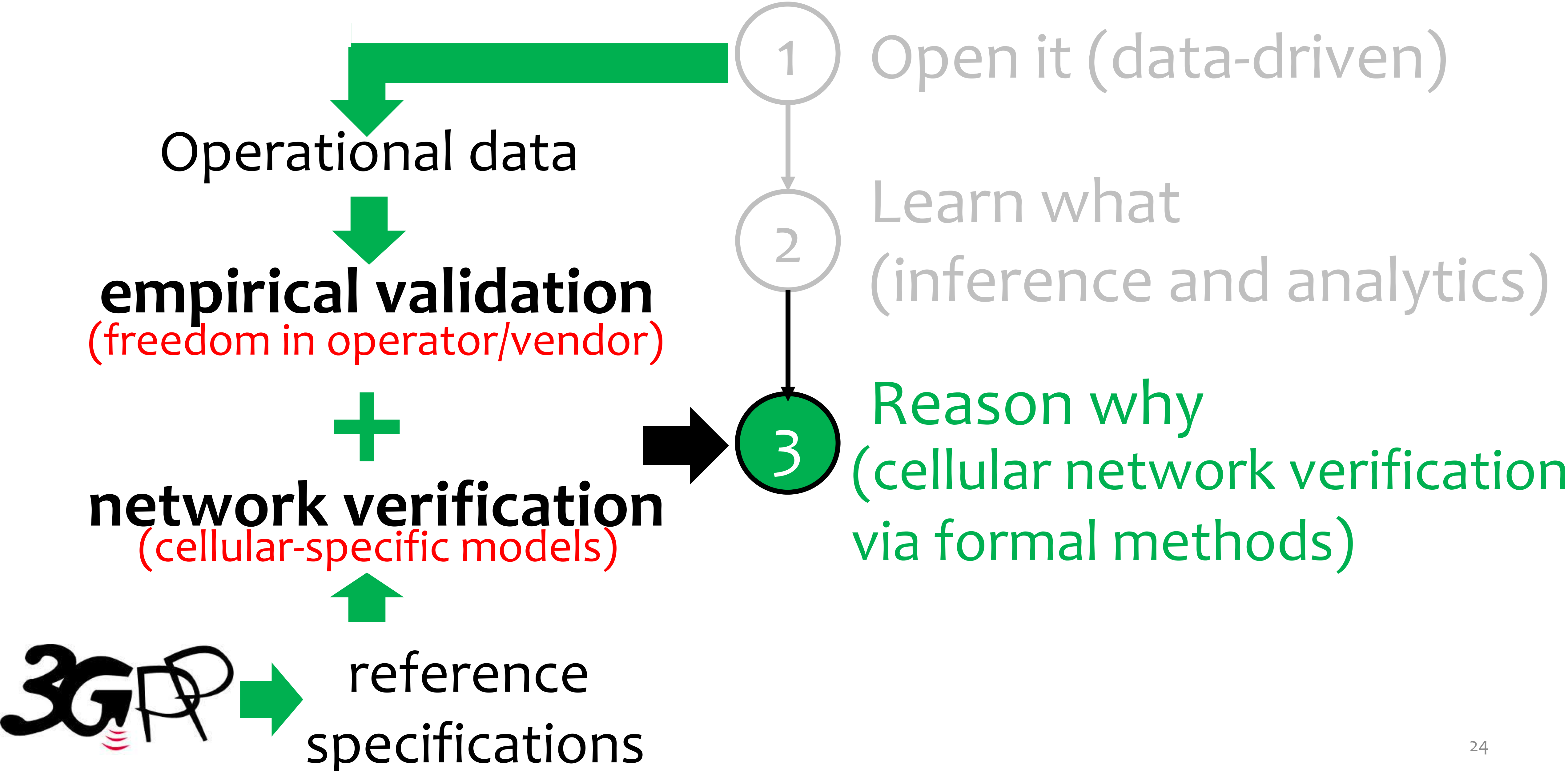
✓ Failure diagnosis (above examples)

- **From operation to design**
  - Fundamentally reason about the current operation: whether and why it goes wrong
- **Goal: provable correctness by design**
  - Engineering artifact over decades of industry practice
  - Error-prone: complex protocol stack & configurations, rich interactions and possibilities
  - Lessons/insights for new design
- **Our approach: cellular network verification**

Our solution #3: Reasoning



Our solution #3: Reasoning



1 Open it (data-driven)

2 Learn what (inference and analytics)

3 Reason why (cellular network verification via formal methods)

Operational data

empirical validation
(freedom in operator/vendor)

+

network verification
(cellular-specific models)

3GPP reference specifications

2 main results: correctness violated

- **incorrect control-plane protocol interactions** in 3G/4G [SIGCOMM'14]
  - Individual protocol is well designed $\nRightarrow$ proper interactions among them are ~~not~~ guaranteed.

	Necessary but problematic cooperation	**Independent but coupled operations**
Cross-layer (e.g., MM-RRC)		
Cross-domain (voice-data)		
Cross-system (3G-4G)		

2 main results: correctness violated

- **instability** and **unreachability** **in mobility management** [SIGMETRICS'16, ICCCN'16, MobiCom'18b]
  - From control-plane to management plane (policy/ config.)
    - Still via modeling and empirical validation
  - Structural deficiencies rooted in misconfigurations and/or policy conflicts
  - A new form of BGP routing instability [SIGMETRICS'00, L Gao, J Rexford)
    - But policies within the same AS (carrier)

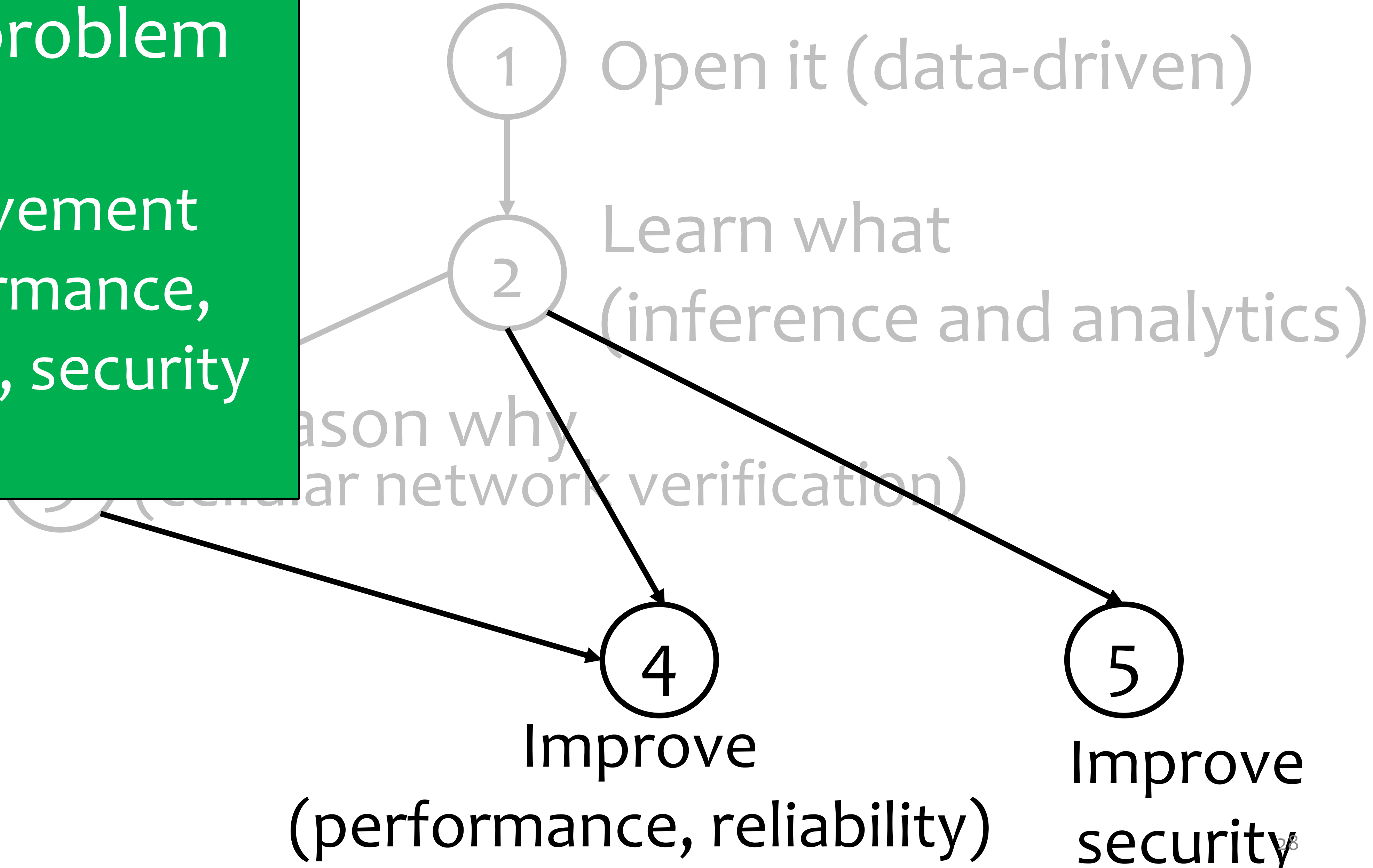
What’s More?

- From stability to unreachability [ICCCN’16]
  - Handoff converges but to a poor choice (e.g., 2G not 4G)
- From single-carrier to multi-carrier [Mobicom’18b]
  - In both theory and practice
  - Google project Fi: one sim card, multi-carrier access
  - Persistent loops caused by policy conflicts
    - between inter-carrier switch policies and intra-carrier switch policies (handoffs)
- From stability to performance [IMC’18]
  - Quantify the performance impacts of handoff configurations
  - Disclose more “problematic” instances

Our Solution #4: Acting for better

Solve the problem if wrong

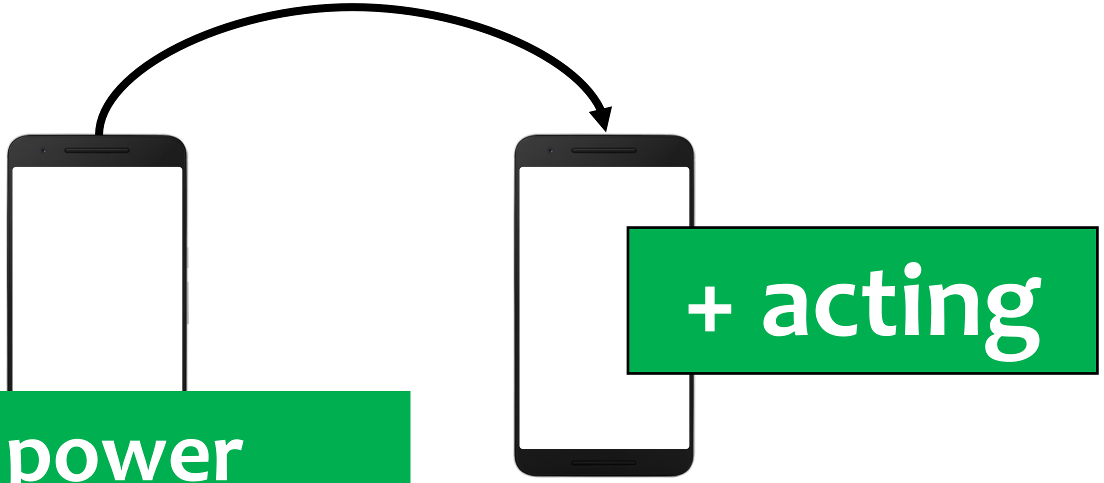
- or improvement on performance, reliability, security …



Our solution #4 via proactive devices

- Approach: Passive → proactive

Device-centric
Software-based



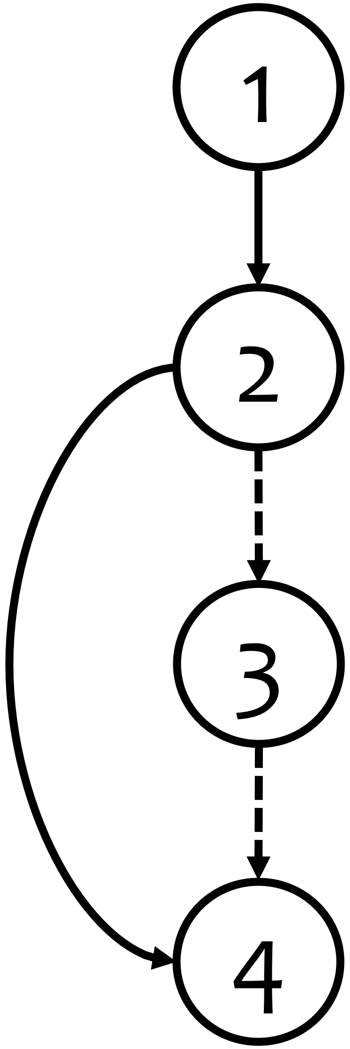
+ acting

- ✓ Explore unexplored power
- ✓ Be responsive (at runtime)
- ✓ Easier to deploy (immediately)
- ✓ Accessible for us (academy)

4
Improve
(performance, reliability)

5
Improve
(security)

A general solution flow



Monitor:
open data at runtime

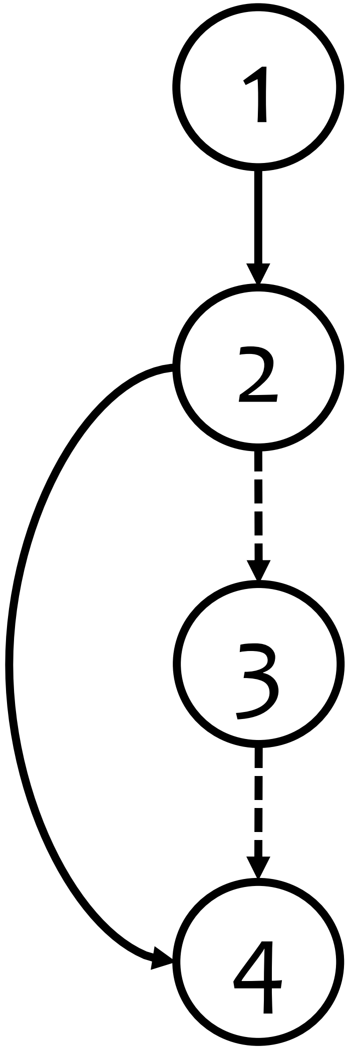
Learn what

Reason why

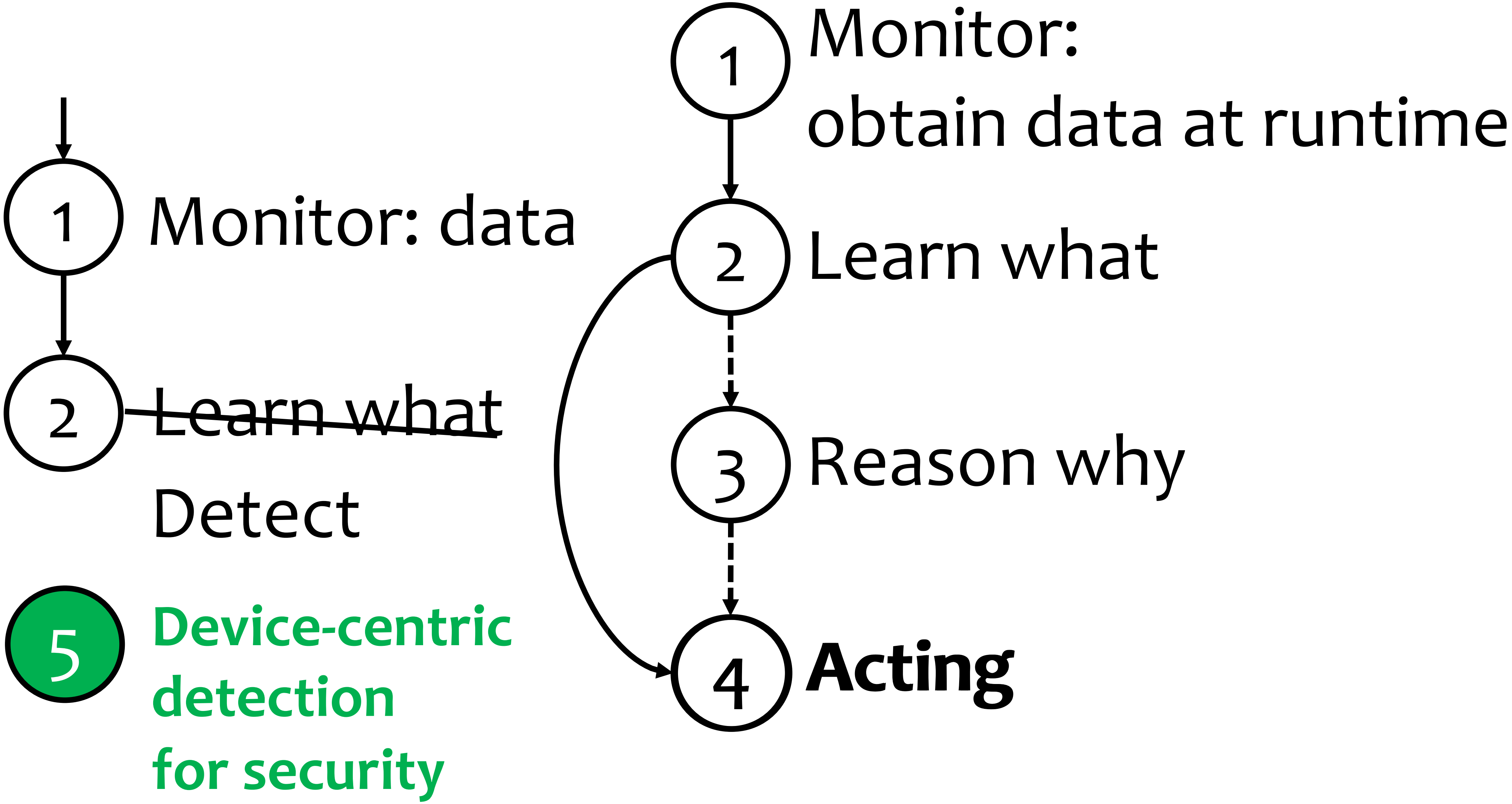
Acting

Many exciting results already

- **Empowered by data→ learning/reasoning →acting**
- **Our work**
  - ✓ [NSDI'16]: multi-carrier access in Google Fi
  - ✓ [MobiCom'17]: control latency reduction
  - ✓ **[Mobicom'18]: combating caller ID spoofing**
- **by other researchers (trend ⇈)**
  - ✓ [Mobisys'17]: web optimization
  - ✓ [SIGMETRICS'17]: energy efficiency
  - ✓ [CoNext'17]: 360 video optimization
  - ✓ [SIGMETRICS'18]: VR latency reduction
  - ✓ [MobiCom'19]: video optimization



Alternative device-side option



1 Monitor: data

2 ~~Learn what~~

Detect

5 Device-centric detection for security

1 Monitor: obtain data at runtime

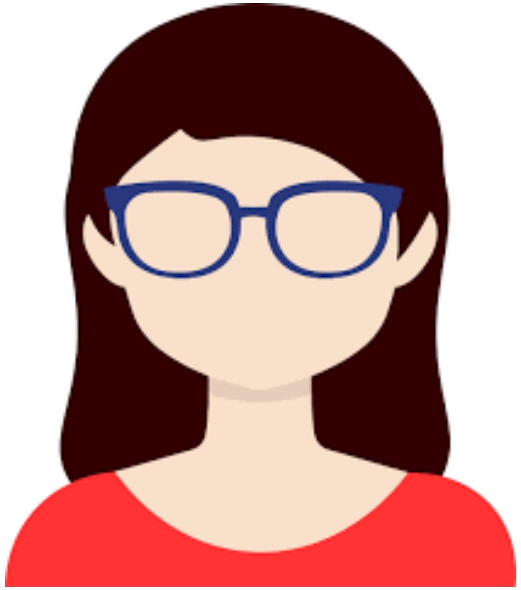
2 Learn what

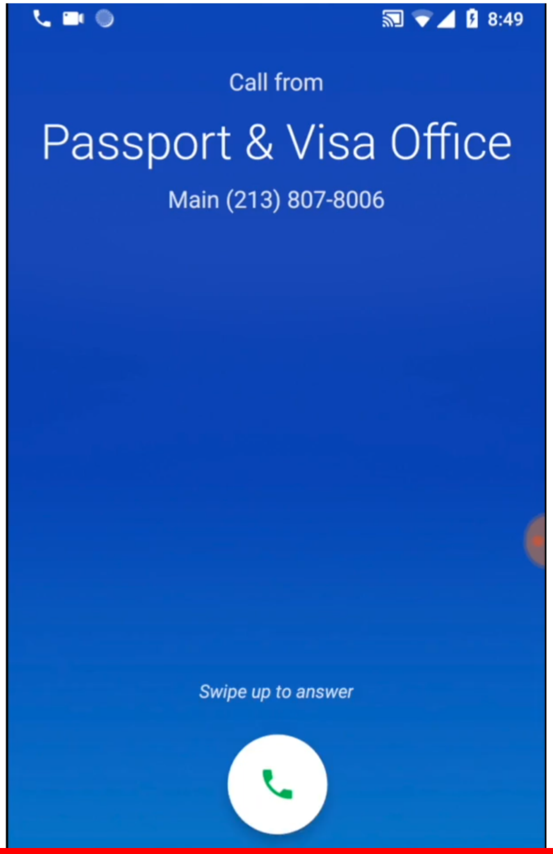
3 Reason why

4 **Acting**

Case study: CEIVE

[MobiCom'18a]





8:49

Call from

Passport & Visa Office

Main (213) 807-8006

Swipe up to answer

中国驻美总领事馆最后一次通知，您有一份紧急重要文件，即将影响您的出入境，如需查询请按9，由人工为您说明・・・・・・

This is the last call from Consulate General of the People's Republic of China. You have an urgent and important document that will

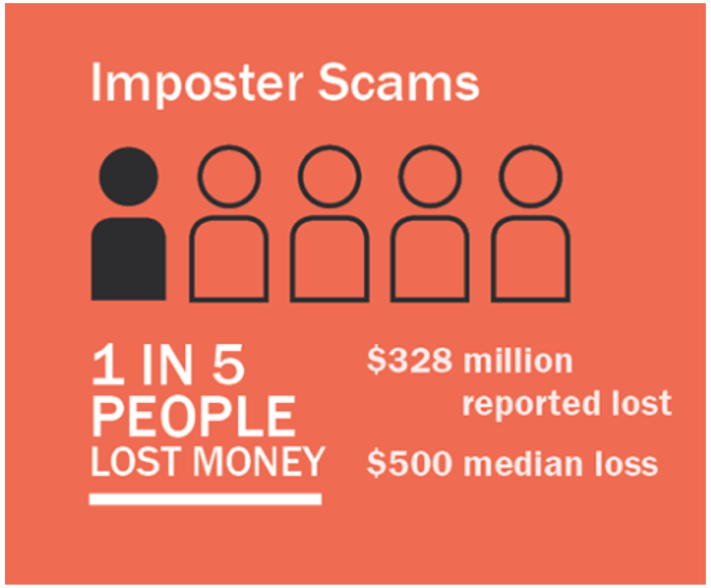
Yes. It was a scam!

A big threat, ↑ at an alarming rate

FEDERAL TRADE COMMISSION

Consumer Information

"top fraud is again Imposter Scams"



Imposter Scams

1 IN 5 PEOPLE LOST MONEY

$328 million reported lost

$500 median loss

$720 median fraud loss

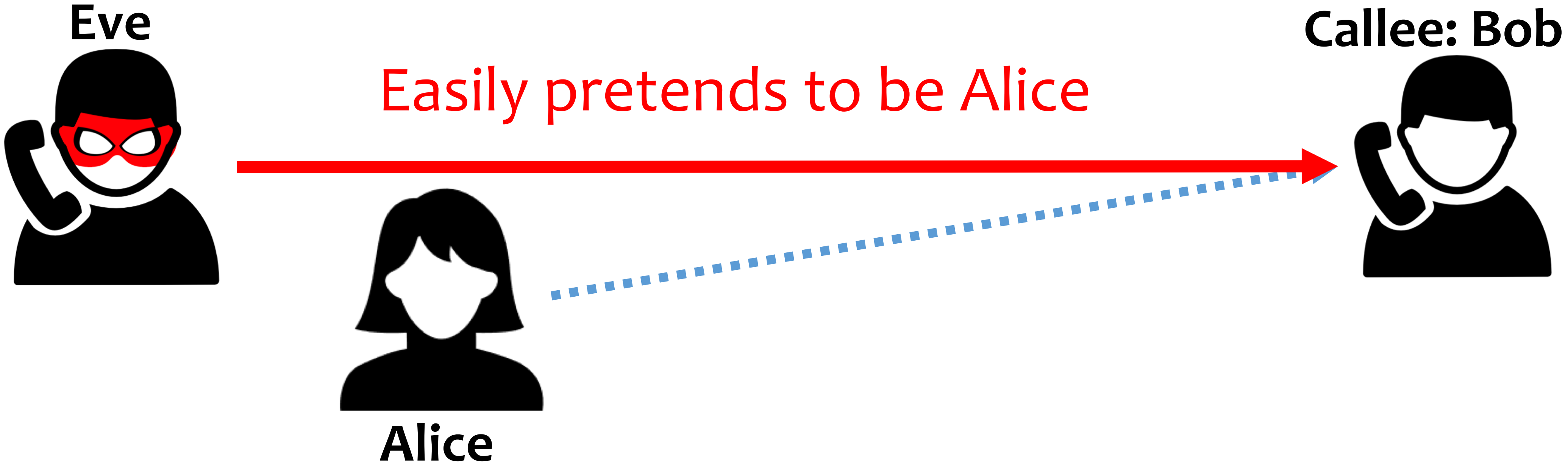
by phone in 2017

$430 in 2017

$274 in 2016

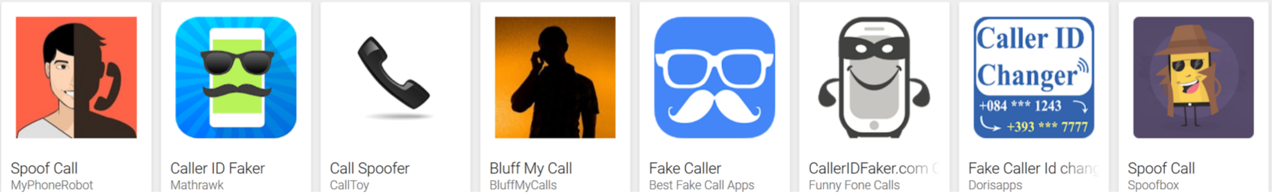
Not only in US, but globally

Because of caller ID spoofing



Easy to launch, but hard to defend

So many public tools available …



Spoof Call
MyPhoneRobot

Caller ID Faker
Mathrawk

Call Spoofer
CallToy

Bluff My Call
BluffMyCalls

Fake Caller
Best Fake Call Apps

CallerIDFaker.com C
Funny Fone Calls

Fake Caller Id chang
Dorisapps

Spoof Call
Spoofbox

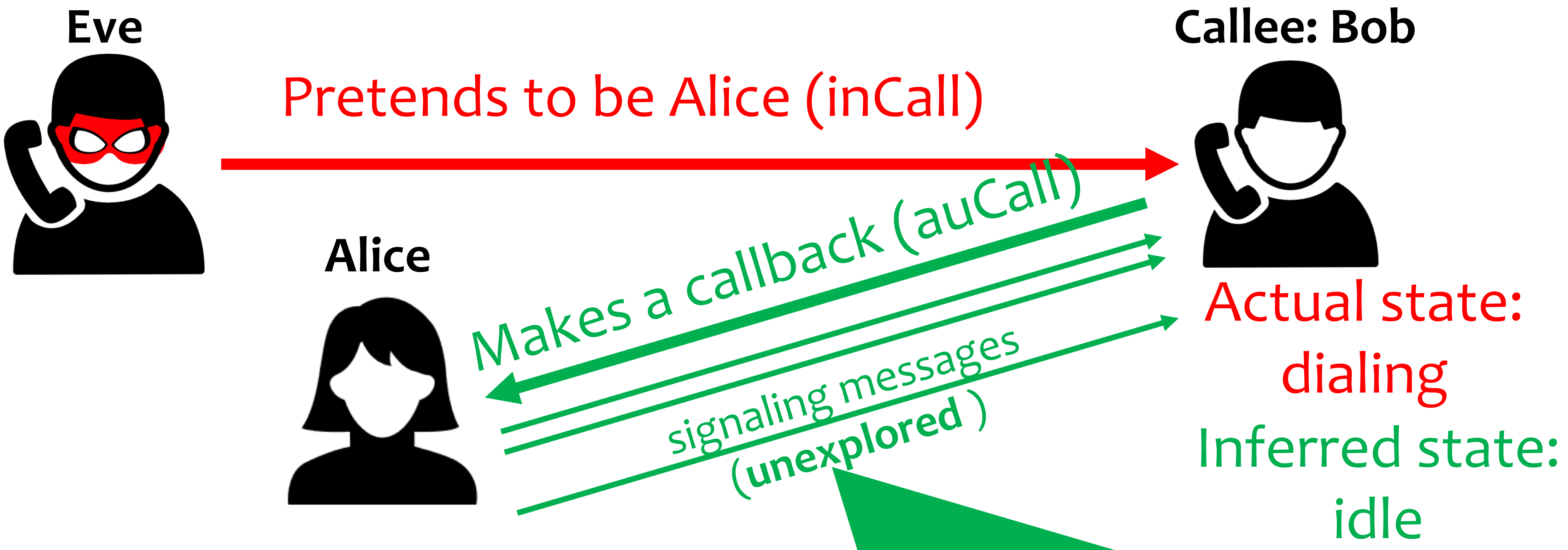
No practical solutions…

~~Global Certificate Authority~~

~~Challenge-and-response:~~

~~Caller ID app~~

CEIVE: callee-only solution



state@auCall: Idle ≠ state@inCall: dialing

Spoofing Detected!

Devil in the details

Call state ambiguity

Diversity from operators

CEIVE aware attack

CEIVE: multi-phase learning (verification) with domain-specific feature selection, training and detection

almost 100% effective in 4 major US carriers within several (< 20) seconds

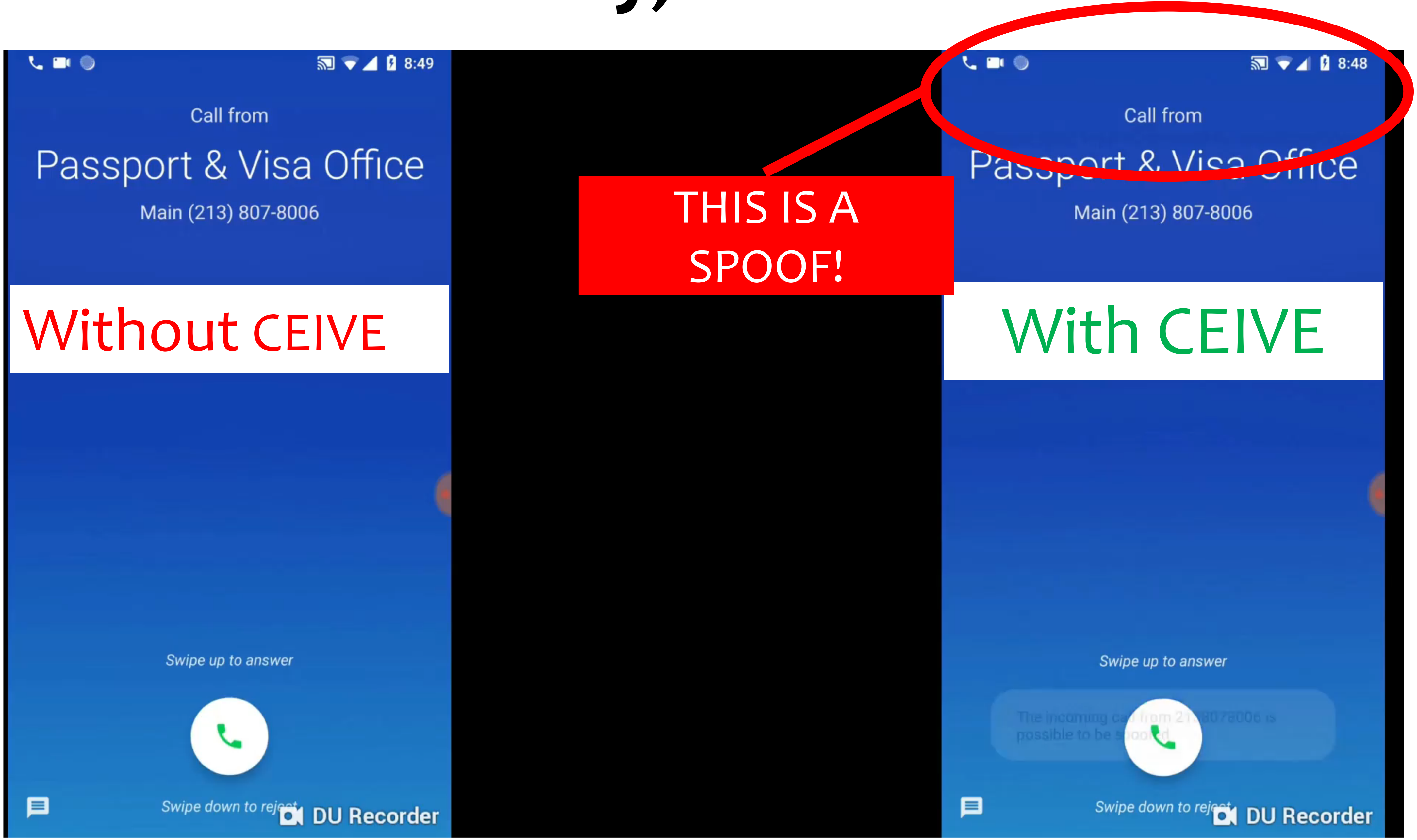
at&t

T Mobile

Sprint

verizon

Back to that day,



8:49

Call from

Passport & Visa Office

Main (213) 807-8006

Without CEIVE

Swipe up to answer

Swipe down to reject

DU Recorder

THIS IS A SPOOF!

8:48

Call from

Passport & Visa Office

Main (213) 807-8006

With CEIVE

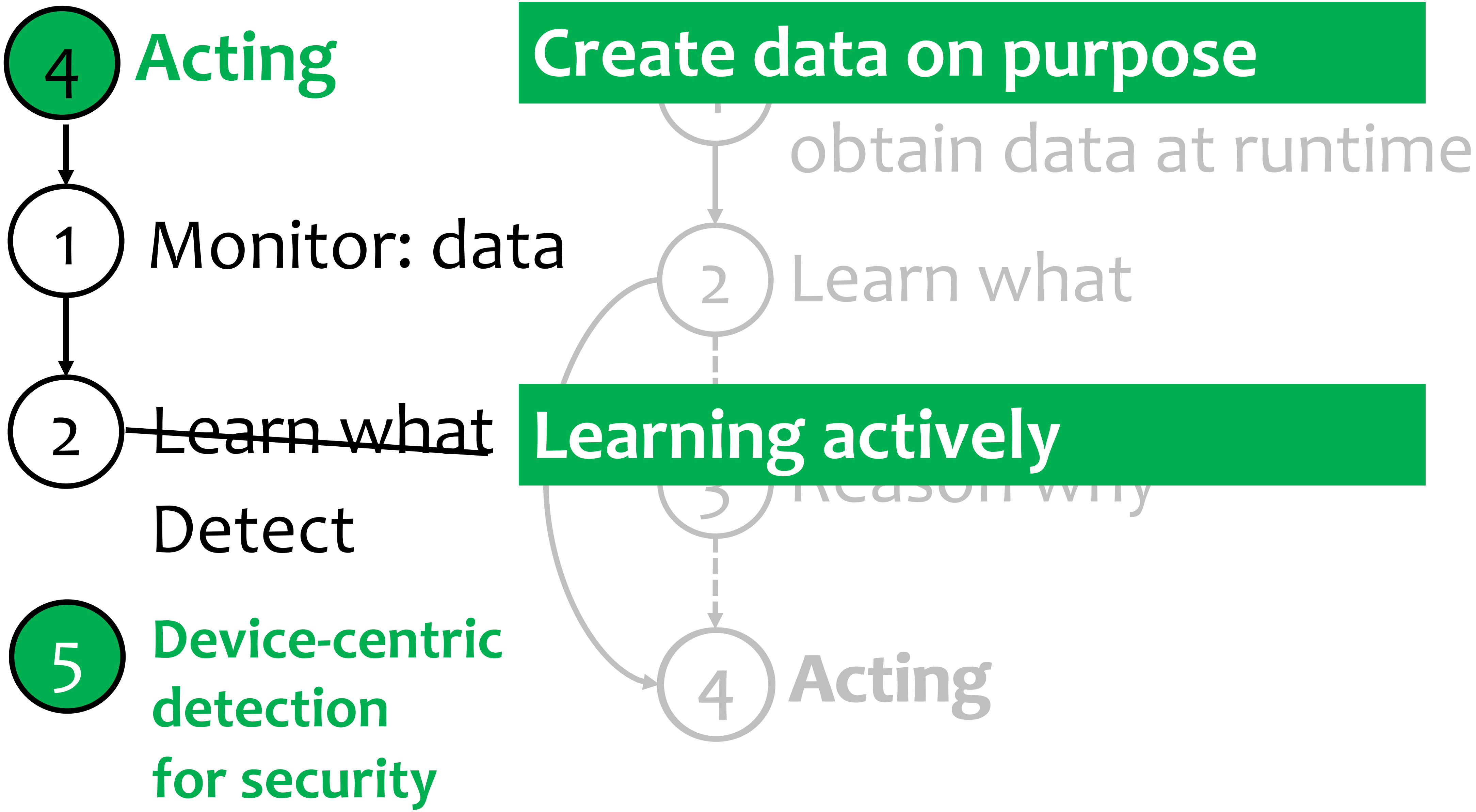
Swipe up to answer

The incoming call from 2138078006 is possible to be spoofed.

Swipe down to reject

DU Recorder

Alternative device-side option



4 Acting

1 Monitor: data

2 ~~Learn what~~

Detect

5 Device-centric detection for security

Create data on purpose

1 obtain data at runtime

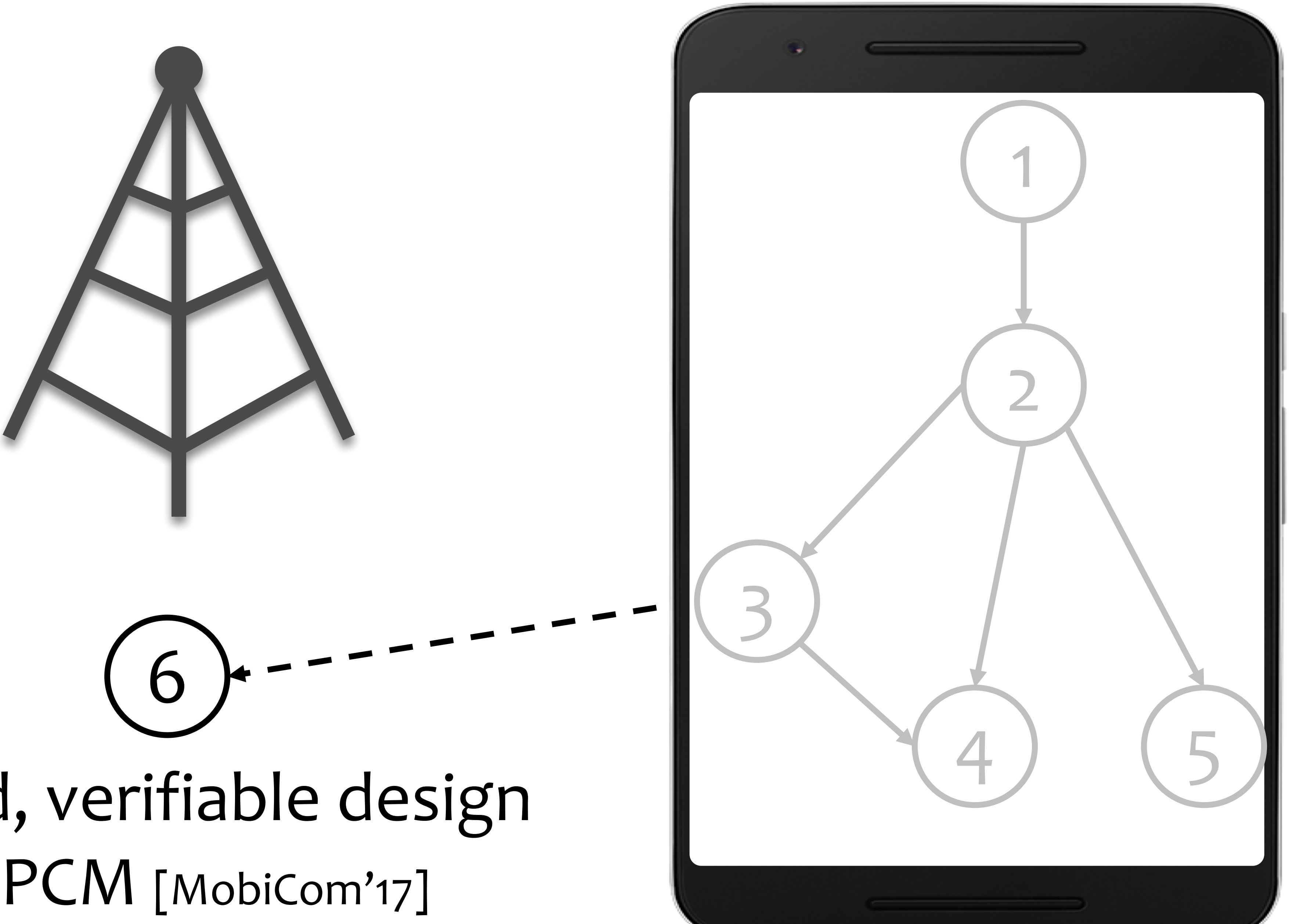
2 Learn what

Learning actively

3 Reason why

4 Acting

From device to network

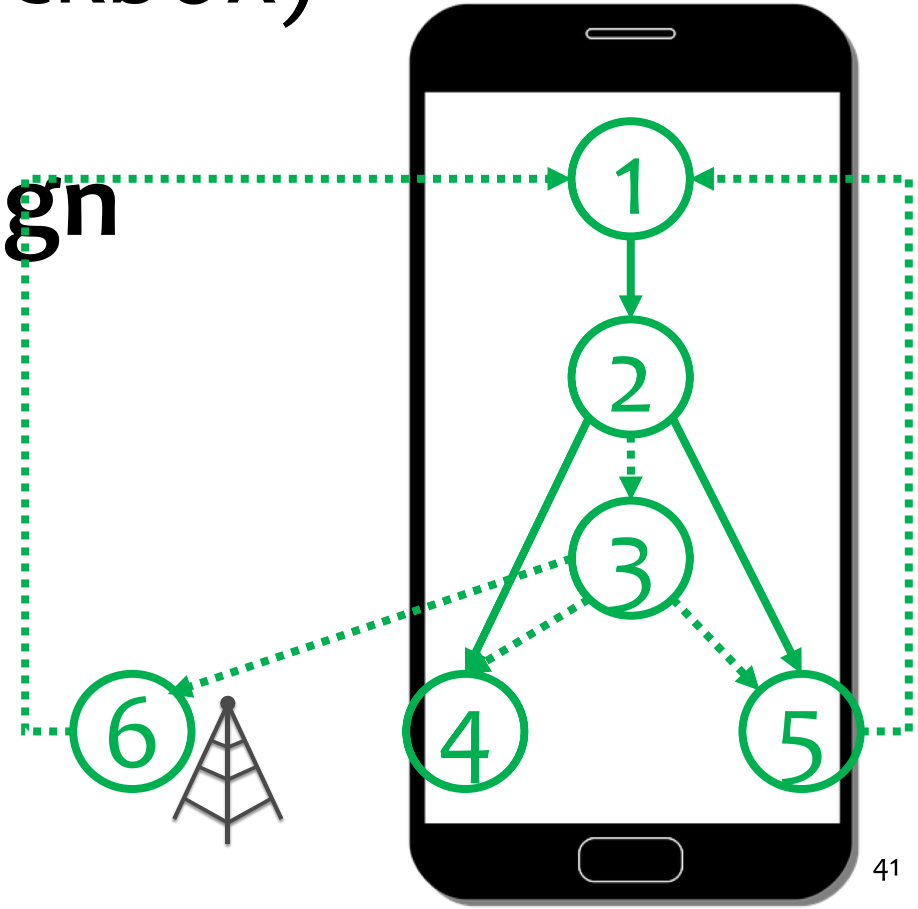


simplified, verifiable design

e.g.,DPCM [MobiCom'17]

Summary of AIM approaches

- **device-centric** (what we can change)
  - Not not limited to devices only (see item 6)
- **data-driven** (open the blackbox)
- **Learning, reasoning, acting**
- **Verification + verifiable design**
  - Be scientific
  - Formal correctness
- **Software-defined actions**
  - Be practical
  - Explore unexplored device power



What's NEXT?

Extending and using AIM

Still, tips of the iceberg

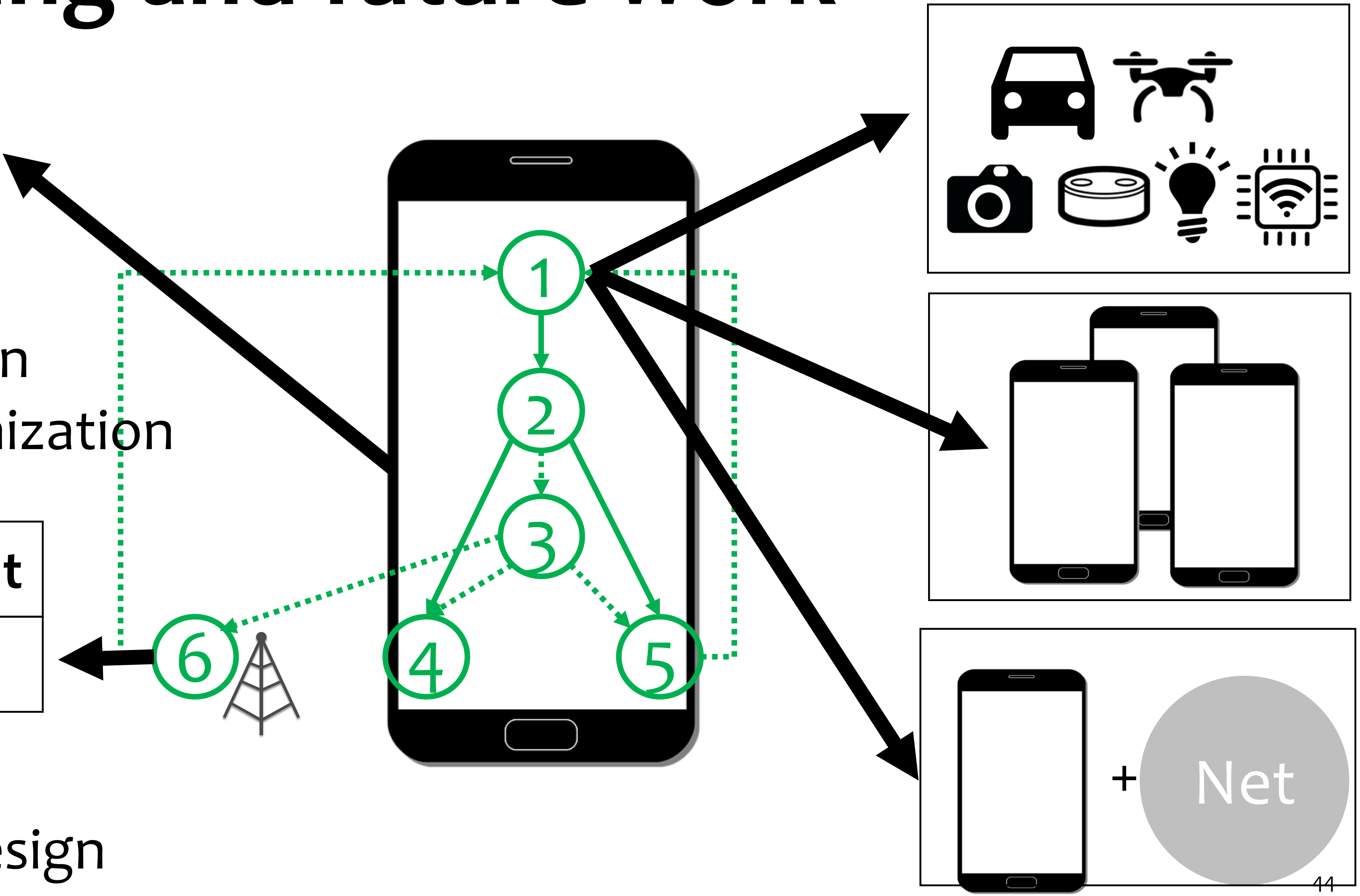
- Open up amble research space
- When you learn, reason and take actions in situations where we could not before

Ongoing and future work

App

TCP/IP

Cross-layer optimization and customization



Ctrl & mgmt

L2/L1

Simplified & verifiable design

Empower research for “You”

- **By other researchers**
  - ✓ [Mobisys’17]: web optimization
  - ✓ [SIGMETRICS’17]: energy efficiency
  - ✓ [CoNext’17]: 360 video optimization
  - ✓ [SIGMETRICS’18]: VR latency reduction
  - ✓ [NDSS’18]: LTE security
  - ✓ [IEEENetwor’18]: handoff stability
  - ✓ [MobiCom’19]: video optimization
  - ✓ [MobiCom’19]: high-speed mobility
  - ✓ …
- Used by both industry & academy
  - AT&T, Verizon, Nokia, Microsoft, Xiaomi,
  - Stanford, Berkley, UCLA, UCSD, GaTech …

MobileInsight

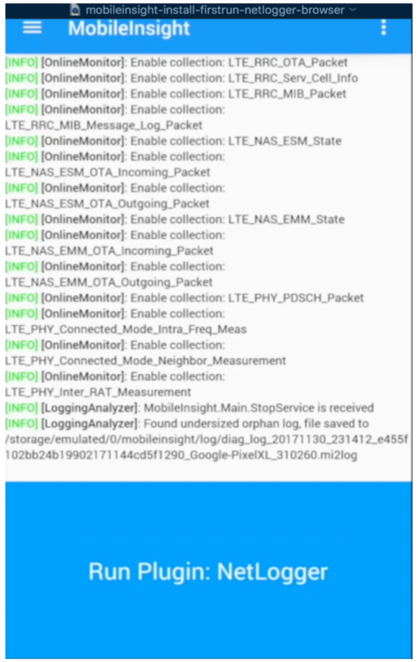
ver. 3.4

http://www.mobileinsight.net

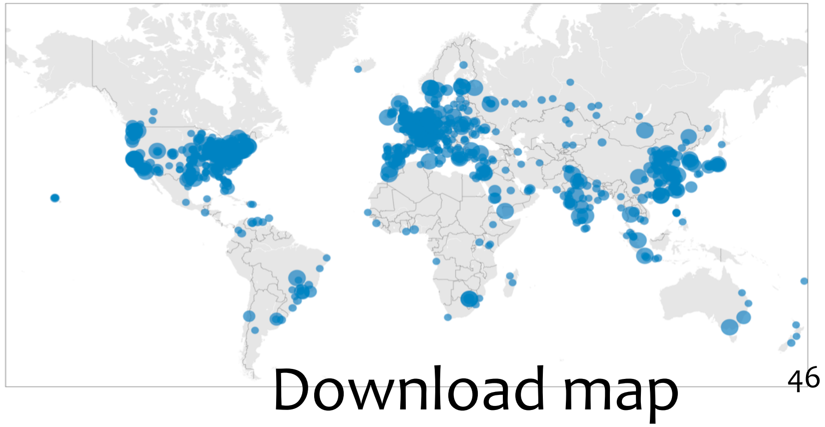
MobileInsight status

http://mobileinsight.net/

- Open source and dataset
  - Latest release: v3.4
- Android app (rooted)
  - Full 4G/3G control + core L1/L2
  - Built-in 4G/3G control analyzers
- Increasing use by companies, starts-up, and universities



```
[INFO] [OnlineMonitor]: Enable collection: LTE_RRC_OTA_Packet
[INFO] [OnlineMonitor]: Enable collection: LTE_RRC_Serv_Cell_Info
[INFO] [OnlineMonitor]: Enable collection: LTE_RRC_MIB_Packet
[INFO] [OnlineMonitor]: Enable collection:
LTE_RRC_MIB_Message_Log_Packet
[INFO] [OnlineMonitor]: Enable collection: LTE_NAS_ESM_State
[INFO] [OnlineMonitor]: Enable collection:
LTE_NAS_ESM_OTA_Incoming_Packet
[INFO] [OnlineMonitor]: Enable collection:
LTE_NAS_ESM_OTA_Outgoing_Packet
[INFO] [OnlineMonitor]: Enable collection: LTE_NAS_EMM_State
[INFO] [OnlineMonitor]: Enable collection:
LTE_NAS_EMM_OTA_Incoming_Packet
[INFO] [OnlineMonitor]: Enable collection:
LTE_NAS_EMM_OTA_Outgoing_Packet
[INFO] [OnlineMonitor]: Enable collection: LTE_PHY_PDSCH_Packet
[INFO] [OnlineMonitor]: Enable collection:
LTE_PHY_Connected_Mode_Intra_Freq_Meas
[INFO] [OnlineMonitor]: Enable collection:
LTE_PHY_Connected_Mode_Neighbor_Measurement
[INFO] [OnlineMonitor]: Enable collection:
LTE_PHY_Inter_RAT_Measurement
[INFO] [LoggingAnalyzer]: MobileInsight.Main.StopService is received
[INFO] [LoggingAnalyzer]: Found undersized orphan log, file saved to
/storage/emulated/0/mobileinsight/log/diag_log_20171130_231412_e455f
102bb24b19902171144cd5f1290_Google-PixelXL_310260.mi2log
```



Download map

MobileInsight-LAB (MI-LAB)

http://milab.cs.purdue.edu/

- **From one to many**
- Open testbed for in-phone cellular network experimentation, data, analyzer **at scale**

- **You publish your task**
- **MI-LAB runs it 'everywhere'**
  - For community and by community

MI-LAB

Takeaways

- AIM aims to open ”closed” cellular network access in today’s operations

- AIM mainly via device-centric data-driven approaches
  - Inter-disciplined: DS, ML (AI), PL, SYS, NET
  - From operation to design
  - From device to network

- Opportunities ahead
  - Open-source tools available

http://mobileinsight.net/

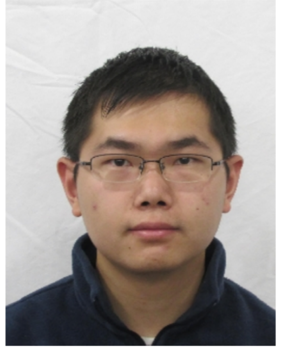
http://milab.cs.purdue.edu/

Acknowledgement

Prof. Lu (UCLA)

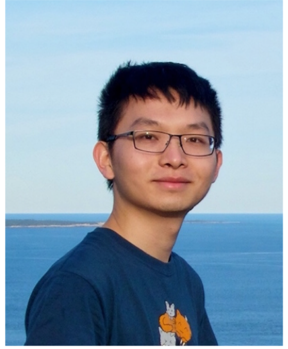
Prof. Li (NCTU)

Prof. Tu (MSU)



Yuanjie Li

Haotian Deng



Zengwen Yuan

…

MobileInsight core team

Students at Purdue

- Haotian Deng
- Andrew B Groenewold
- Jiayi Meng
- Zhuo Jiang
- Ans Fida
- Jiawei Lu
- Guocheng Wei
- Kelvin Zhang
- Youssef Elabd

& students at OSU

& visiting students

Many collaborators …

(Microsoft, Adobe, Qualcomm, Tsinghua, MSU, SJTU, …)

Reference (1/4)

[imc18] Haotian Deng, Chunyi Peng, Ans Fida, Jiayi Meng, and Charlie Hu, Mobility Support in Cellular Networks: A Measurement Study on Its Configurations and Implications, Nov. 2018

[mobicom18a] Haotian Deng, Weicheng Wang, and Chunyi Peng, CEIVE: Combating Caller ID Spoofing on 4G Mobile Phones Via Callee-Only Inference and Verification, Oct 2018. **(with Best Demo Award)**

[mobicom18b] Zengwen Yuan, Qianru Li, Yuanjie Li, Songwu Lu, Chunyi Peng, and George Varghese, Resolving Policy Conflicts in Multi-Carrier Cellular Access, Oct 2018.

[sigcomm18] Li Li, Ke Xu, Tong Li, Kai Zheng, Chunyi Peng, Dan Wang, Xiangxiang Wang, Meng Shen and Rashid Mijumbi , *A Measurement Study on Multi-path TCP with Multiple Cellular Carriers on High-speed Rails*, Aug. 2018

[icccn18] Zengwen Yuan, Yuanjie Li, Chunyi Peng, Songwu Lu, Haotian Deng, Zhaowei Tan and Taqi Raza, A Machine Learning Based Approach to Mobile Network Analysis, July 2018 (Invited Paper)

Reference (2/4)

[cns18] Tian Xie,Guan-Hua Tu,Chi-Yu Li,Chunyi Peng, Jiawei Li,and Mi Zhang, The Dark Side of Operational Wi-Fi Calling Services, May 2018 **(Best Paper Award)**

[mobicom17] Yuanjie Li, Zengwen Yuan, Chunyi Peng, A Control-Plane Perspective on Reducing Data Access Latency in LTE Networks, MobiCom'17, Snowbird, Utah, Oct 2017.

[icccn17] Haotian Deng, Qianru Li, Yuanjie Li, Songwu Lu, Chunyi Peng, Taqi Raza,Zhao wei Tan, Zengwen Yuan, Zhehui Zhang, Towards Automated Intelligence in 5G Systems, ICCCN'17, Vancouver, Canada, August 2017.

[mobicom16] Yuanjie Li, Chunyi Peng, Zengwen Yuan, Jiayao Li, Haotian Deng and Tao Wang, *MobileInsight: Extracting and Analyzing Cellular Network Information on Smartphones*, MobiCom'16, New York, USA, Oct. 2016. **(Best Community Paper Award)**

[sigmetrics16] Yuanjie Li, Haotian Deng, Jiayao Li, Chunyi Peng and Songwu Lu, *Instability in Distributed Mobility Management: Revisiting Configuration Management in 3G/4G Mobile Networks*, France, June 2016.

Reference (3/4)

[ccs16] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Yuanjie Li and Songwu Lu, New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks, CCS'16, Vienna, Austria, Oct. 2016.

[icccn16] Chunyi Peng and Yuanjie Li, *Demystify Undesired Handoff in Cellular Networks*, Waikoloa, Hawaii, Aug. 2016.

[infocom16] Chunyi Peng, Yuanjie Li, Zhuoran Li, Jie Zhao and Jiaqi Xu, *Understanding and Diagnosing Real-World Femtocell Performance Problems*, INFOCOM'16, San Francisco, CA, April 2016.

[nsdi16] Yuanjie Li, Haotian Deng, Chunyi Peng, Zengwen Yuan, Guan-Hua Tu, Jiayao Li and Songwu Lu, *iCellular: Device-Customized Cellular Network Access on Commodity Smartphones*, NSDI'16, Santa Clara, CA, March 2016.

[ccs15] Chiyu Li, Guanhua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, Xinbing Wang, Insecurity of Voice Solution VoLTE in LTE Mobile Networks, CCS'15, Denver, Oct. 2015.

Reference (4/4)

[cns15] Guanhua Tu, Chiyu Li, Chunyi Peng, Songwu Lu, *How Voice Call Technology Poses Security Threats in 4G LTE Networks*, CNS'15, Florence, Italy, Sep. 2015.

[infocom15] Li Li, Ke Xu, Dan Wang, Chunyi Peng, Qingyang Xiao and Rashid Mijumbi, *A Measurement Study on TCP Behaviors in HSPA+ Networks on High-speed Rails*, INFOCOM'15, Hong Kong, China, April, 2015.

[ccs14] Chunyi Peng, Chiyu Li, Hongyi Wang, Guanhua Tu and Songwu Lu, *Real Threats to Your Data Bills: Security Loopholes and Defense in Mobile Data Charging*, CCS'14, Scottsdale, Arizona, Nov. 2014.

[sigcomm14] Guanhua Tu, Yuanjie Li, Chunyi Peng, Chiyu Li, Hongyi Wang, Songwu Lu, *Control-Plane Protocol Interactions in Cellular Networks*, SIGCOMM'14, Chicago, Aug. 2014.