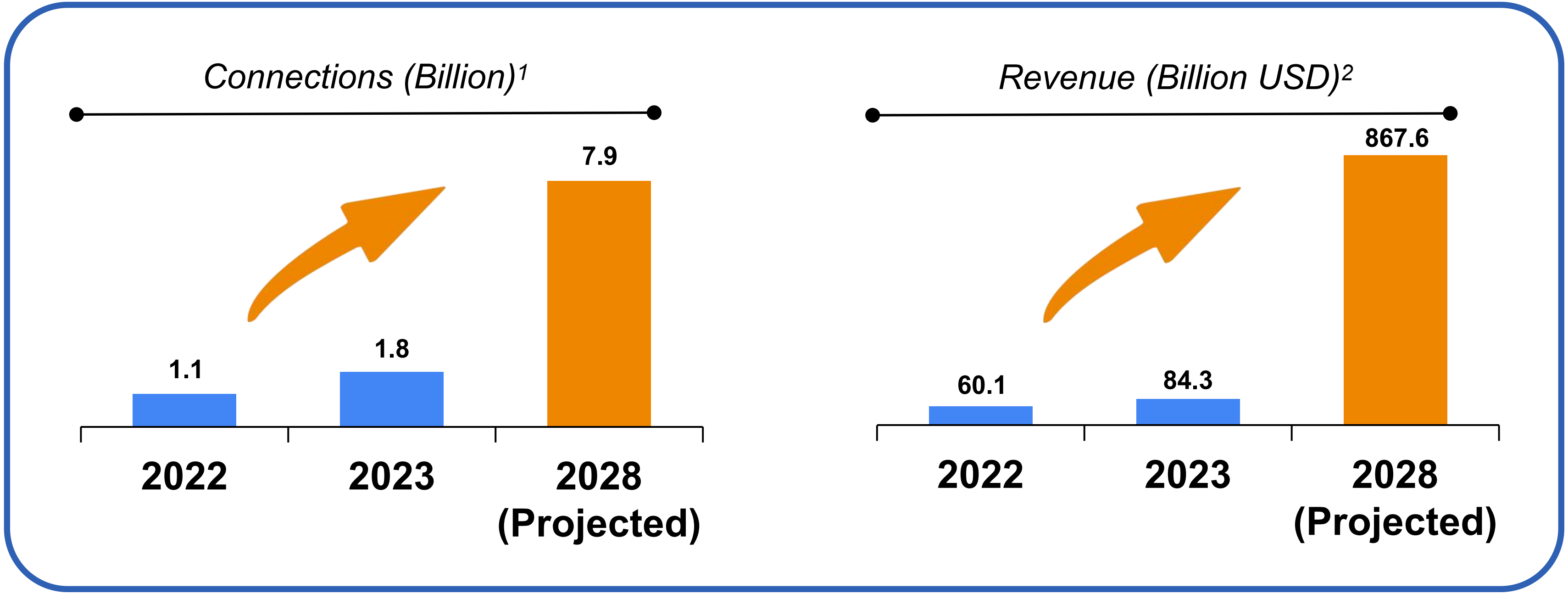
Towards 5G Security

Zhaowei Tan
November 14, 2024

CRESP Industry Day

UC RIVERSIDE

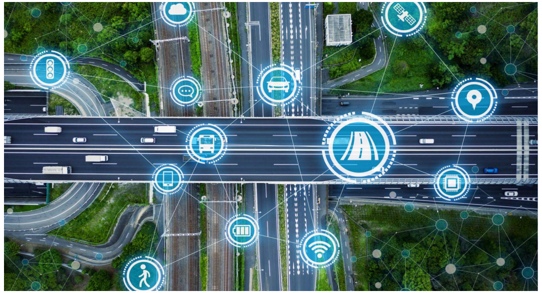
5G: Anytime, Anywhere Networks



UC RIVERSIDE

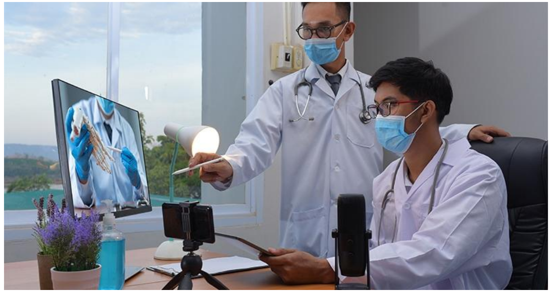
1. https://www.5gamericas.org/global-5g-connections-surge-to-1-76-billion-66-percent-growth-year-over-year-as-north-america-leads-charge/
2. https://www.grandviewresearch.com/industry-analysis/5g-services-market

A Spectrum of Usage Scenarios



Smart City

Manufacturing



Healthcare

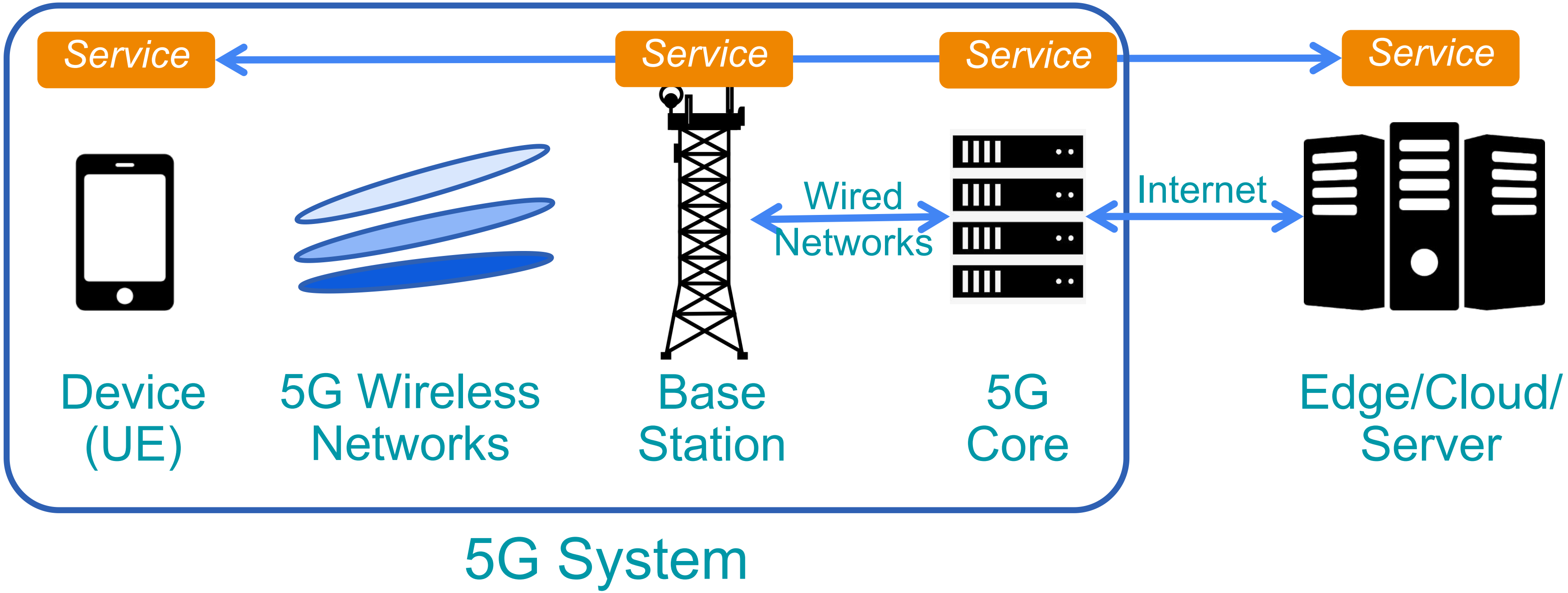
Agriculture

AR/VR

My Research:
Resilient 5G against Attacks

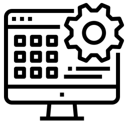
Important Objective for Government & Industry

5G's Simplified Architecture



UC RIVERSIDE

My research for 5G (and beyond) security

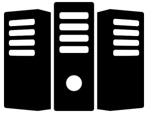


Service

Security for cellular vehicle-to-everything, emergency calls, cellular IoT, …

Network

Study on network protocols: New attacks and countermeasures



System

Security for base station sub-systems, 5G core network, and devices

Security about 5G Services

Service	*Security for cellular vehicle-to-everything, **emergency calls**, cellular IoT, …*
Network	*Study on network protocols: New attacks and countermeasures*
System	*Security for base station sub-systems, 5G core network, and devices*

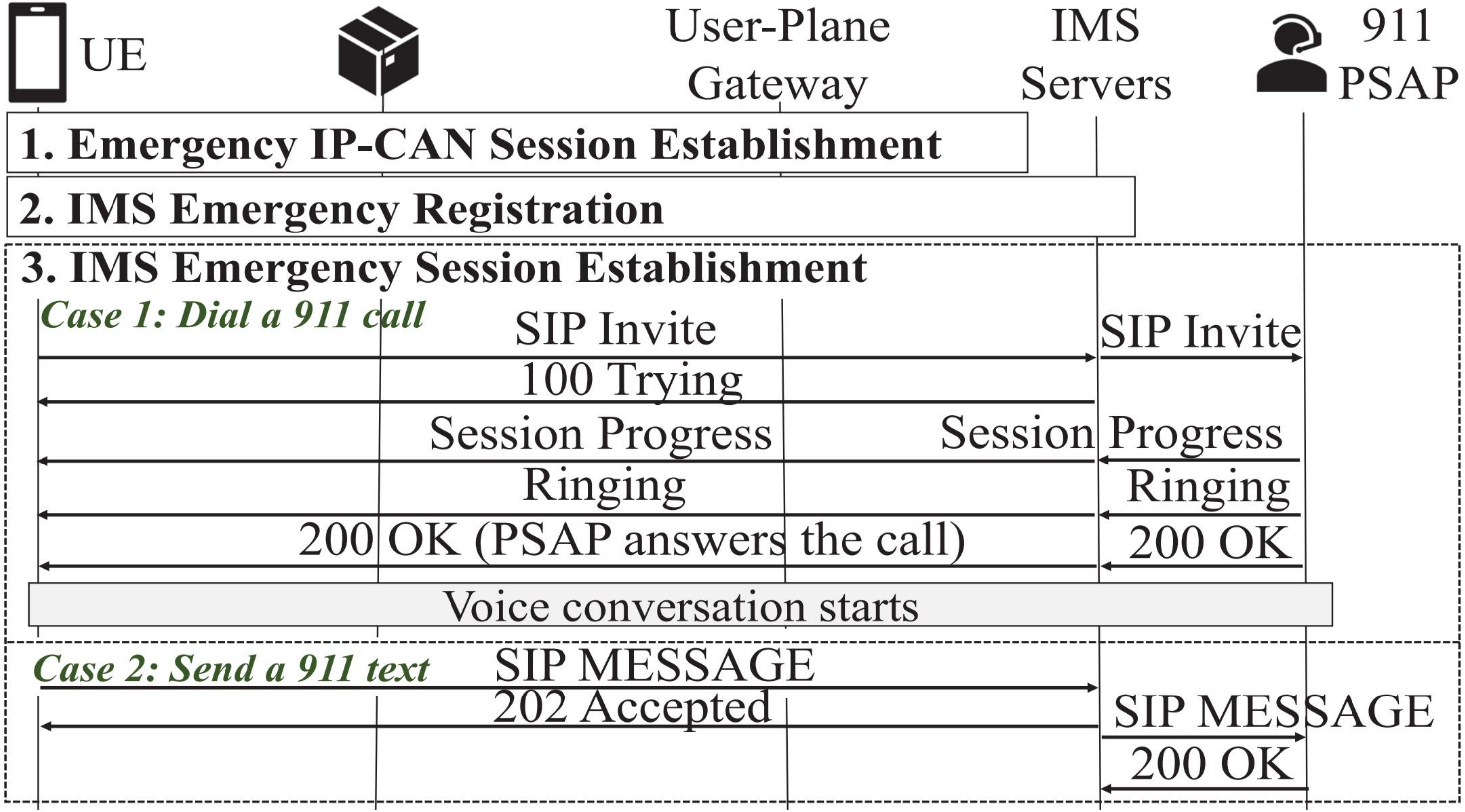
UC RIVERSIDE

Practice of Cellular Emergency Service

To ensure the availability of cellular emergency services,

- In the U.S., Federal Communications Commission (FCC) stipulates that cellular carriers must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point (PSAP).
- The GSM Association (GSMA) standard requires emergency services must be supported by all mobile phones even without SIM cards and be free of charge for mobile users.
- The 3GPP standard requires emergency services to be provided with higher priority than other cellular services.

How Emergency Service Works



Our Findings

- Test three US major carriers using device and SDR
  - … In a responsible way! (No actual emergency calls/text messages are sent to IMS servers or PSAPs)
- We found that cellular emergency services (in US) are deniable and abusable
  - Four insecure designs from 3GPP cellular emergency service standards
- Enabling attacks such as Denial of Emergency Service and Session Hijacking

V1: Unverifiable emergency IP-CAN requests

- Per FCC Title 47, U.S. carriers need to support non-service-initialized devices (denoted anonymous UE) to access emergency services
  - Only one emergency IP-CAN session can be established per UE

Reality: The network cannot differentiate whether the second IP-CAN session establishment request is sent by a benign user or an attacker.

UE1 IP — IMS Server IP

No.	Time	Source	Destination	Protocol	Leng	Info
4	2.0...	2600:1009:11f...	2001:4888:5:f...	TCP	80	38698 -> 5060 [SYN]
5	2.1...	2001:4888:5:f...	2600:1009:11f...	TCP	72	5060 -> 38698 [SYN,
6	2.1...	2600:1009:11f...	2001:4888:5:f...	TCP	60	38698-> 5060 [ACK]
...			...			...
72	18....	2001:4888:5:f...	2600:1009:11f...	TCP	60	5060 -> 38708 [FIN,
73	18....	2600:1009:11f...	2001:4888:5:f...	TCP	60	38708 -> 5060 [ACK]
74	20....	2600:1009:11f...	2001:4888:5:f...	TCP	80	38710 -> 5060 [SYN]
75	21....	2600:1009:11f...	2001:4888:5:f...	TCP	80	[TCP Retransmission]
76	24....	2600:1009:11f...	2001:4888:5:f...	TCP	80	38712 -> 5060 [SYN]
77	25....	2600:1009:11f...	2001:4888:5:f...	TCP	80	[TCP Retransmission]

The UE1 was implicitly detached.

UE2 IP — IMS Server IP

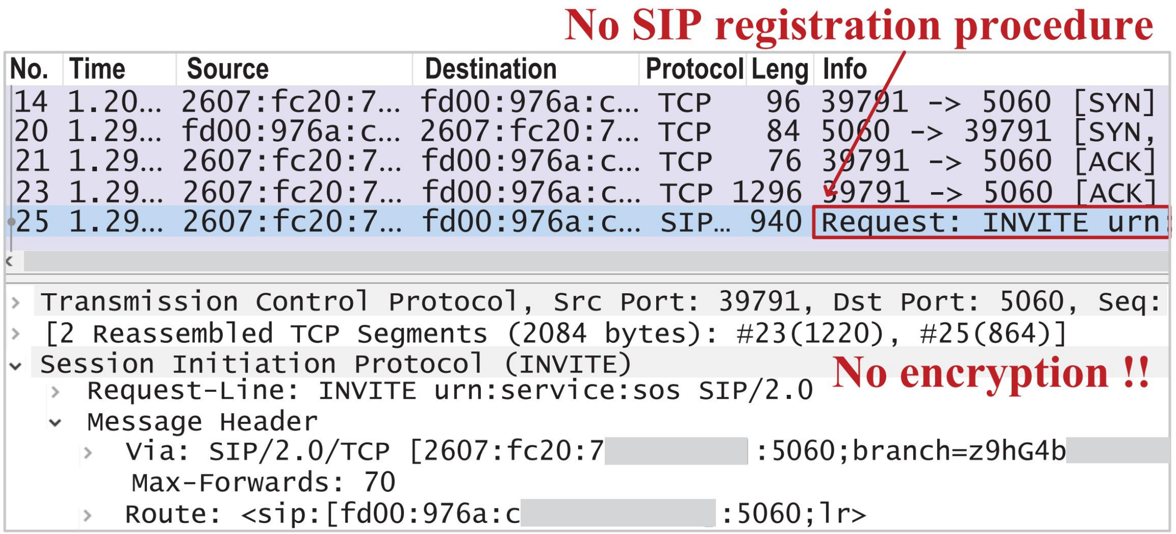
No.	Time	Source	Destination	Protocol	Leng	Info
1	0.0...	fe80::4a:11:1...	ff02::1	ICM...	88	Router Advertisement
2	7.0...	2600:1009:10f...	2001:4888:5:f...	TCP	80	41212 -> 5060 [SYN]
3	7.1...	2001:4888:5:f...	2600:1009:10f...	TCP	72	5060 -> 41212 [SYN,
4	7.1...	2600:1009:10f...	2001:4888:5:f...	TCP	60	41212 -> 5060 [ACK]
5	7.1...	2600:1009:10f...	2001:4888:5:f...	TCP	60	41212 -> 5060 [FIN,

The UE2 began to communicate with the IMS server.

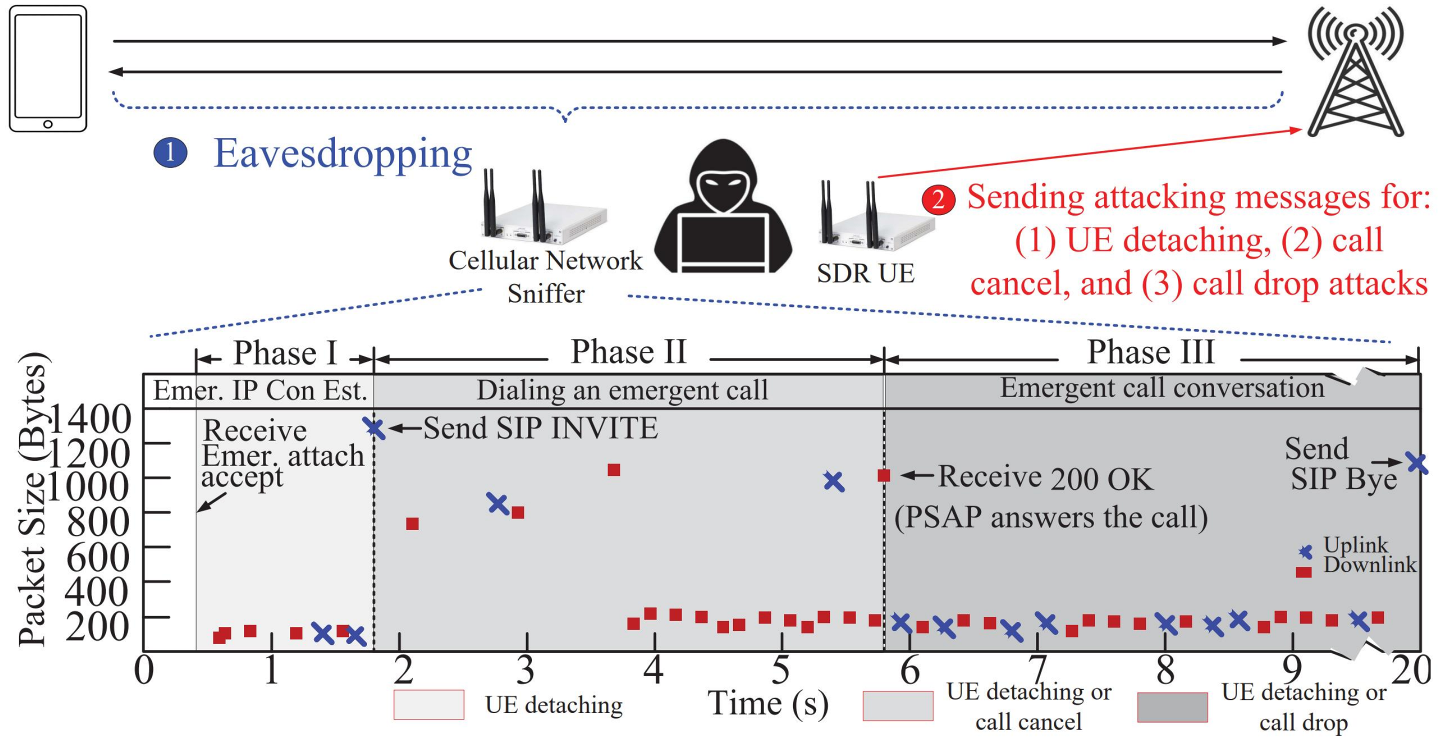
V2: Improper cross-layer security binding

- Normal IMS session set up is bound to IPSec

Reality: No key exchange during emergency services IMS



Attack: Denial of Cellular Emergency Service



V3: Non-atomic service initialization

Three emergency service initialization actions should be performed without any interruption - Atomicity

Reality: Adversaries can send data in the middle of session setup

The destination is not necessarily to be the IMS server.

UE IP (emergency) Google DNS Server IP

No.	Time	Source	Destination	Protocol	Leng	Info
1	0.0...	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
2	1.0...	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
3	2.0...	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
		...	...			...
21	19....	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
22	20....	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
23	21....	2600:1009:110...	2001:4860:486...	ICMPv6	104	Echo (ping) request
24	24....	2600:1009:110...	2001:4888:2:f...	TCP	80	50730 -> 5060 [SYN]
25	24....	2001:4888:2:f...	2600:1009:110...	TCP	72	5060 -> 50730 [SYN,
26	24....	2600:1009:110...	2001:4888:2:f...	TCP	60	50730 -> 5060 [ACK]

The emergency IP connectivity still exists.

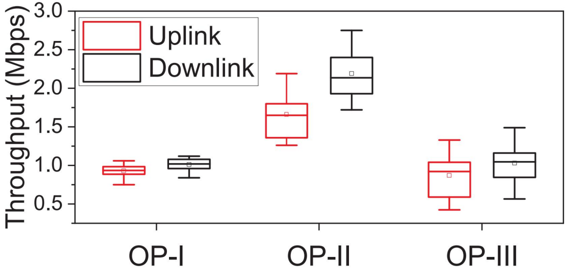
UC RIVERSIDE

V4: Improper Access Control on Sessions

- The access of emergency IP-CAN session should be restricted to IMS servers
  - Done by PCF (Policy Control Function)

Reality: *All carriers allow various mobile-to-mobile communications when bypassing internal firewall protection*

Carriers	Mobile-to-Internet	Mobile-to-Mobile		
		E2E	E2IMS	E2D
OP-I	X	O	X	X
OP-II	X	O	X	O
OP-III	X	O	O	O



E2E Attack Throughput

UC RIVERSIDE

5G Networking Security Research

Service

Security for cellular vehicle-to-everything, emergency calls, cellular IoT, …

Network

Study on network protocols:
New attacks and ***countermeasures***

System

Security for base station sub-systems, 5G core network, and devices

5G Control vs. Data Plane

Control plane: Session and state control -> Well-studied

Data plane: Per-packet data delivery

- *Largely unexplored research: Challenging* with per-packet overhead
- Both application packets and data-plane signaling

UC RIVERSIDE

Data-Plane: Overlooked but Problematic

Control Packets ✓
Data Packets ✓
Data-Plane Signaling Messages

Commands

- **DRX Command**
- **Time Advance**

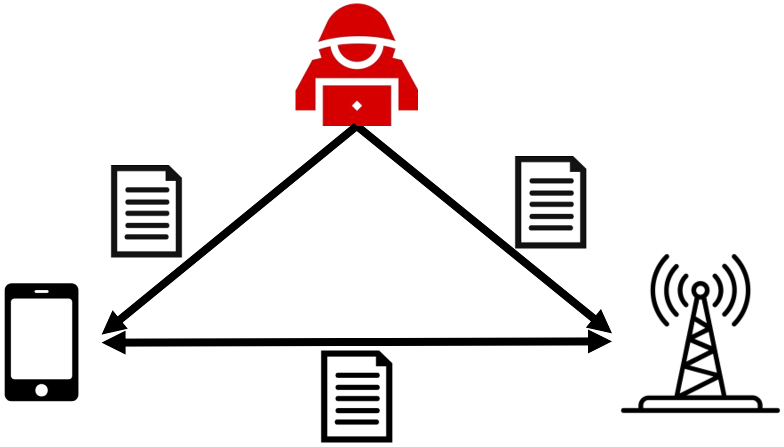
...

Status Sync-Up

- **Power Headroom**
- **Buffer Status Report**

...

Data-Plane Signaling Attacks



Power draining,
Connection reset,
Resource draining,
…

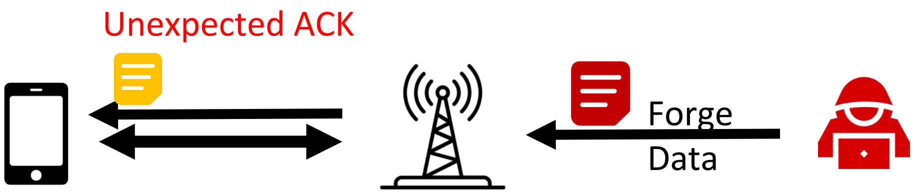
CDS (MobiCom '21)

Proactive protection is impractical with high overhead ->
Can we design reactive solutions to detect such attacks?

Signaling Verification for Attack Detection

Design guideline 1: ***Verify what's right*** instead of targeting *certain threats*

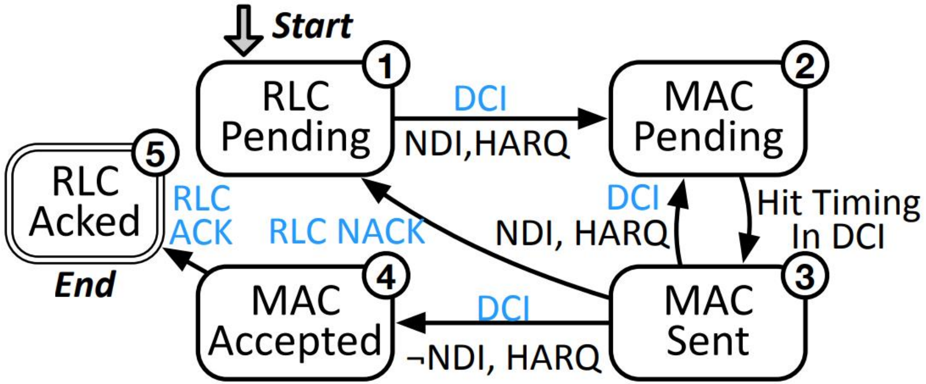
Design guideline 2: ***Verify data-plane signaling message*** instead of *per packet monitoring*



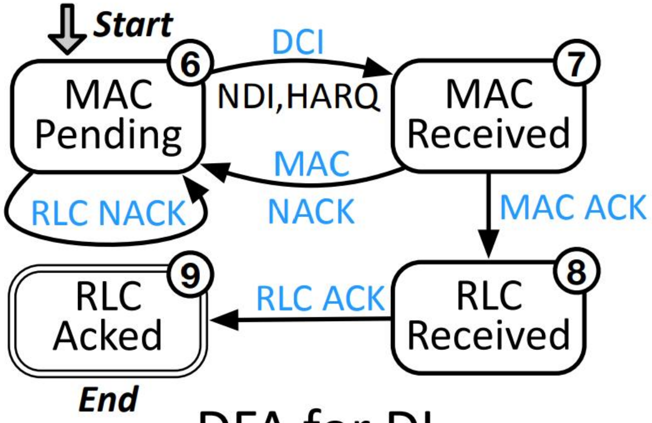
UC RIVERSIDE

Cross-Layer, State-Dependent Detection

CellDAM: State-dependent checks on 9 states



DFA for UL



DFA for DL

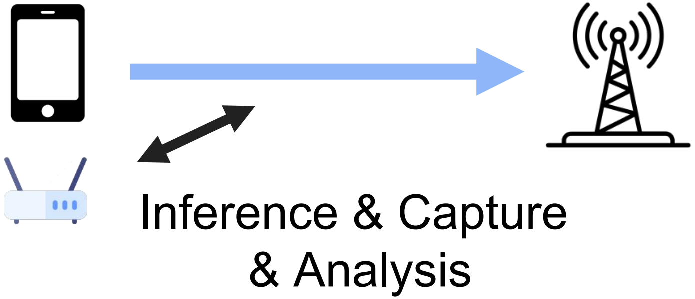
Enable CellDAM without Firmware Access

With firmware access

Directly inspect the signaling messages

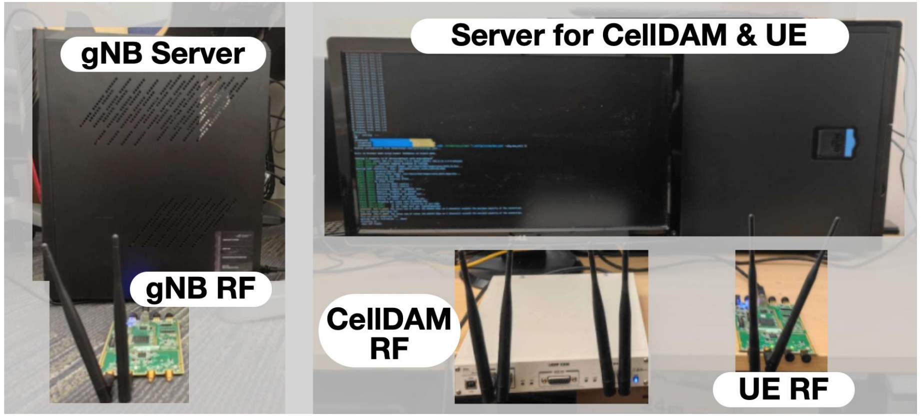
No firmware access

Use a companion node to capture signals for detection



Evaluation Results on CellDAM

- Can detect *5 known classes of attacks* (incl. all data-attacks and common signaling attacks) and find *3 new attacks*
- Incur *0.9%* overhead compared to per-packet processing



5G System Security Research

Service

Security for cellular vehicle-to-everything, emergency calls, cellular IoT, …

Network

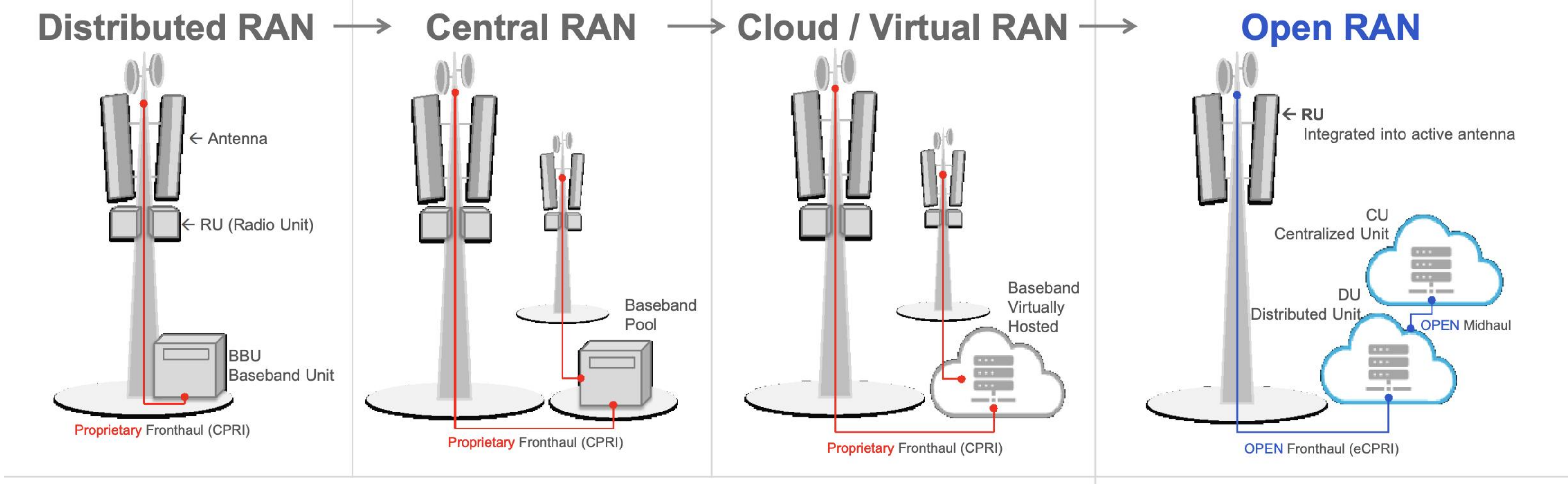
Study on network protocols: New attacks and countermeasures

System

*Security for **base station sub-systems**, 5G core network, and devices*

Trend: Softwarization of base stations

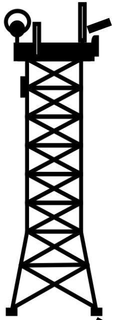
Open Radio Access Networks (O-RAN): *Nonproprietary, intelligent* upgrade for 5G base station



O-RAN Components

RAN Intelligent Controller (RIC):

Monitors other components, runs multiple AI models for intelligent network management



O-CU: Data security with encryption/decryption/integrityy, QoS

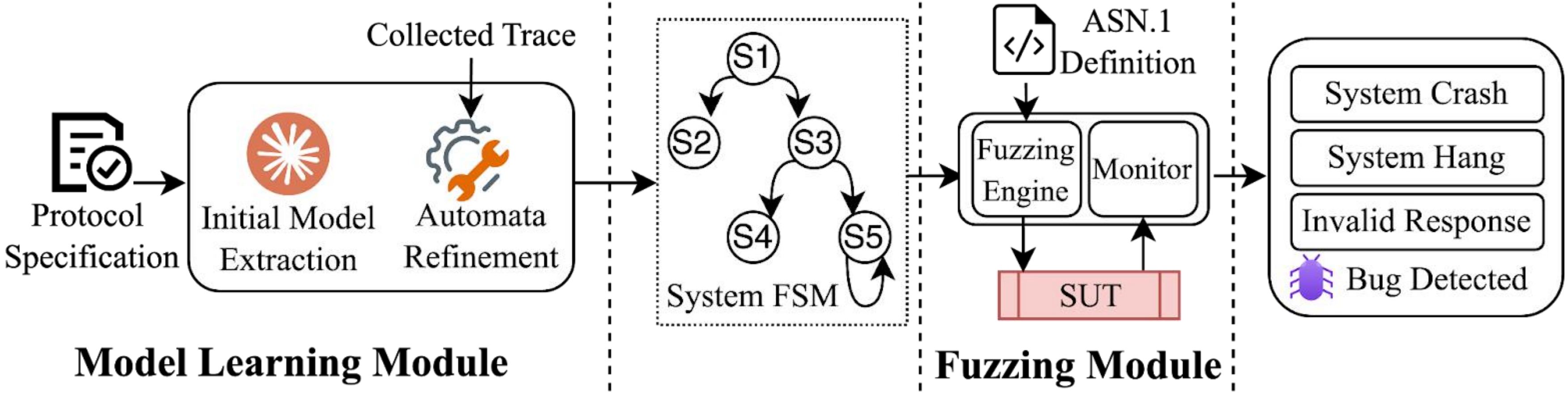
O-DU: High-PHY (e.g., scrambling), MAC layer, Reliable data transfer

O-RU: Low-layer PHY procedures such as digital-to-analog converter

O-RAN Security: A sample of questions

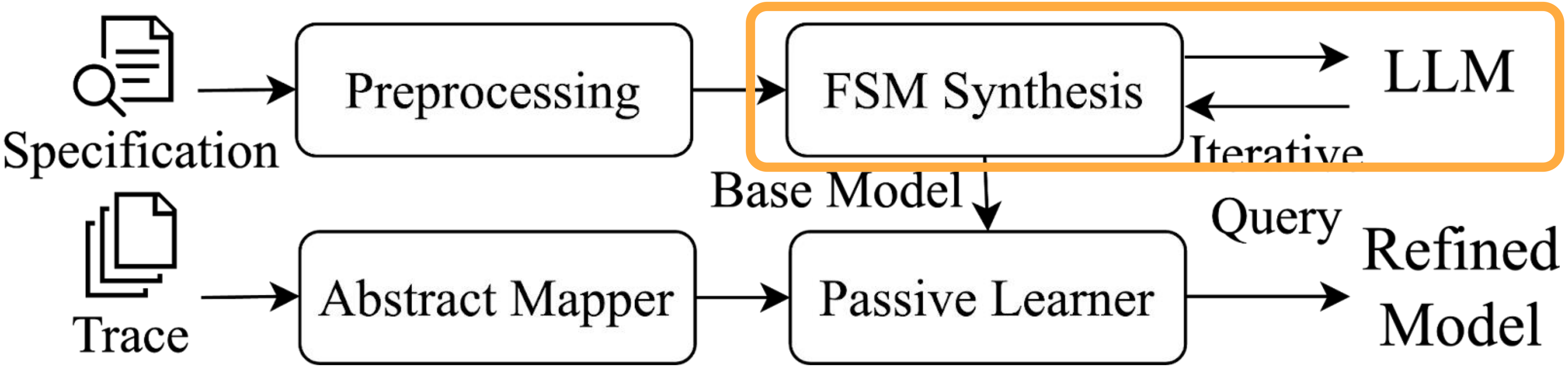
- Conformance: Does each component work correctly?
  - Black-box component with room for customizable implementation
- Interoperability: Would O-RAN components interaction expose additional vulnerabilities?
  - Different components are from different vendors
- Security, privacy, and safety for AI models?
  - AI models can make incorrect or conflicting decisions

Our First Attempt:
ARCANE: Model-Based O-RAN Fuzzing



LLM-Assisted Modeling Learning

- Apply LLM and design prompts for
- Refine the model by incorporating traces



Main Findings

- Tested on open-source SDR implementation of 5G O-RAN
- 149 bugs with 9 root causes
- Can be leveraged to launch three categories of attacks
  - Authentication bypass, DoS, and network failures

UC RIVERSIDE

Summary

Threats against specialized 5G services

Protecting data plane with detection

Security implication in the O-RAN era

Support & Collab.

Thank you!

Questions?

Zhaowei Tan (ztan@ucr.edu)

https://cs.ucr.edu/~ztan

UC RIVERSIDE