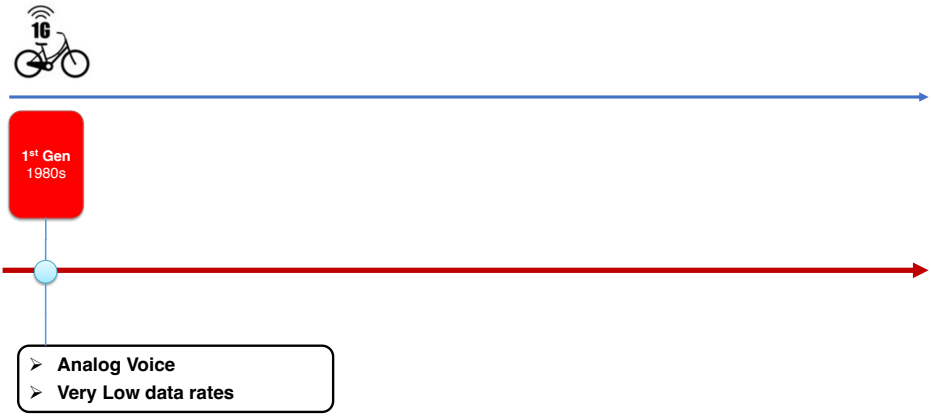
Security-Enhanced Radio Access Networks for 5G OpenRAN

Dr. Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

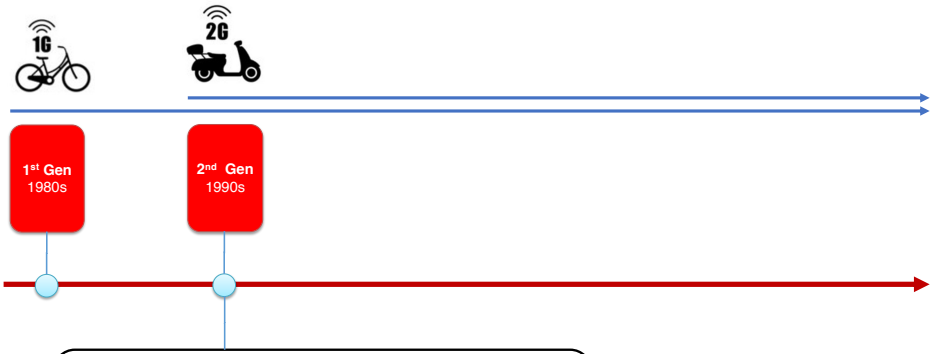
Joint work with Haohuang Wen, Prakhar Sharma, Phil Porras, Vinod Yegneswaran, and Ashish Gehani

11/21/2024

Evolution of Cellular Network

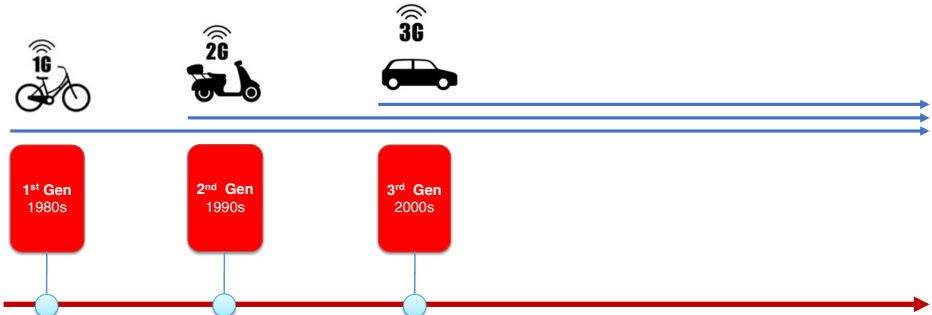


Evolution of Cellular Network



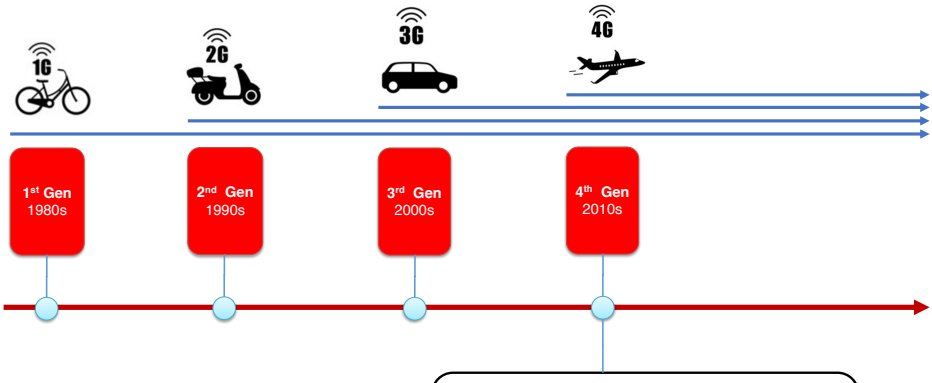
- Digital Communication
- SMS (Short Message Service)
- GSM (Global System for Mobile Communications)

Evolution of Cellular Network

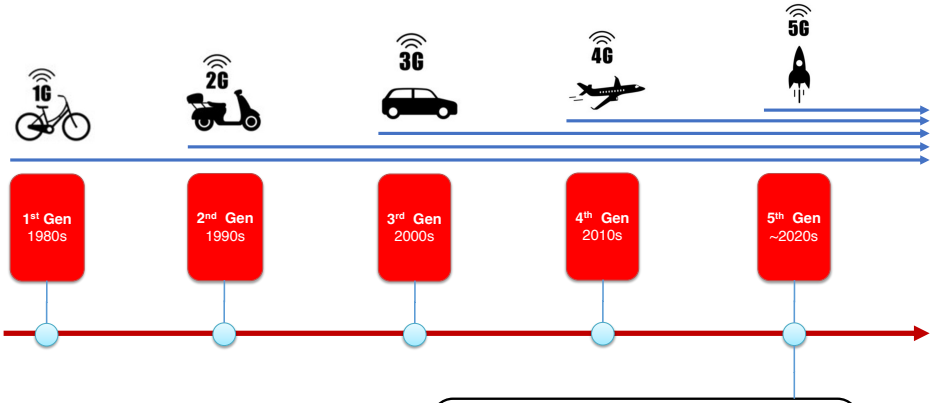


- **Mobile Internet (Kbps)**
- **Video Calls**
- **UMTS (Universal Mobile Telecommunications System)**

Evolution of Cellular Network



Evolution of Cellular Network



Why 5G is not Secure

Why do we care about 5G Security and Privacy?

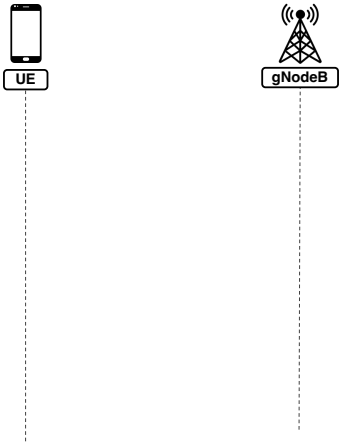
Why 5G is not Secure

Why do we care about 5G Security and Privacy?

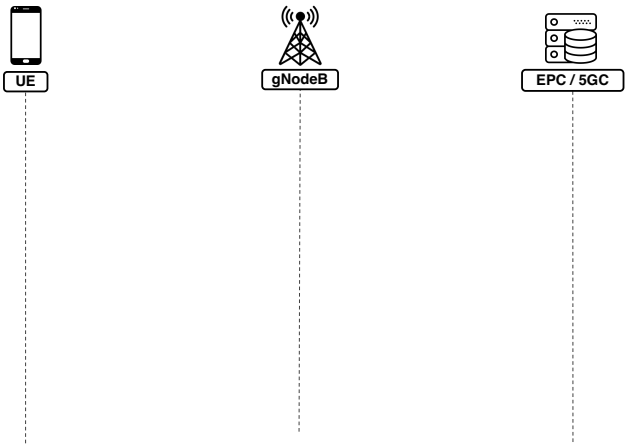
The vulnerable cellular network standard

Why 5G is not Secure

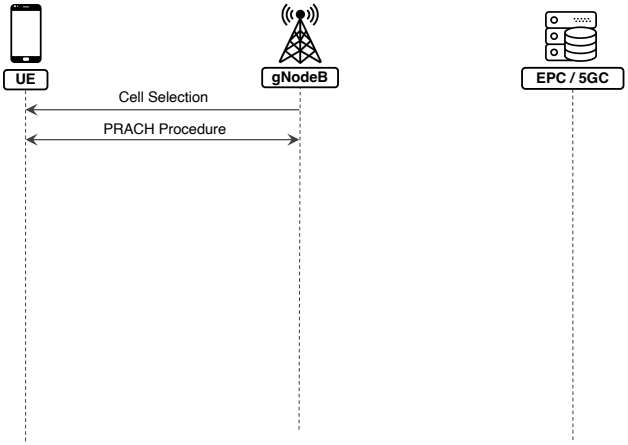
Why 5G is not Secure



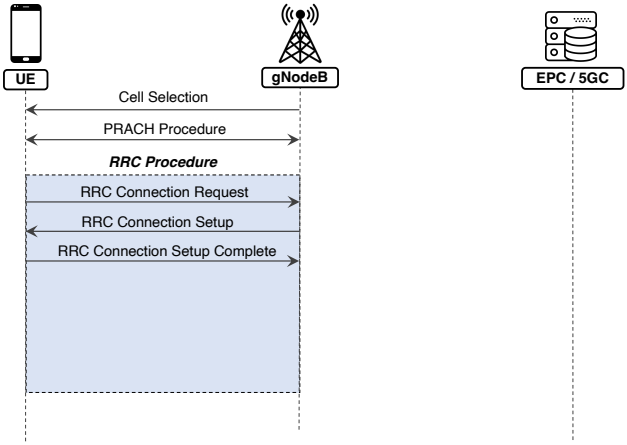
Why 5G is not Secure



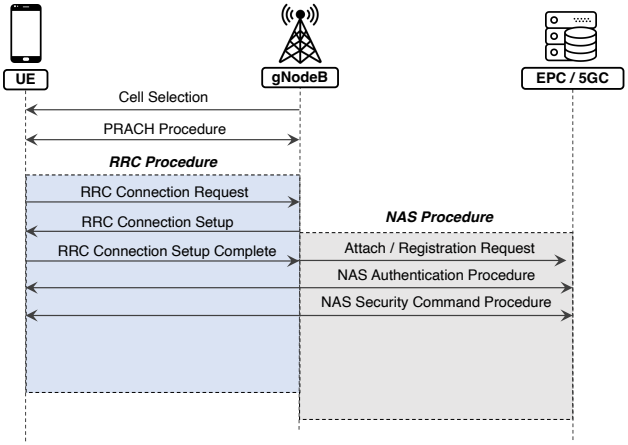
Why 5G is not Secure



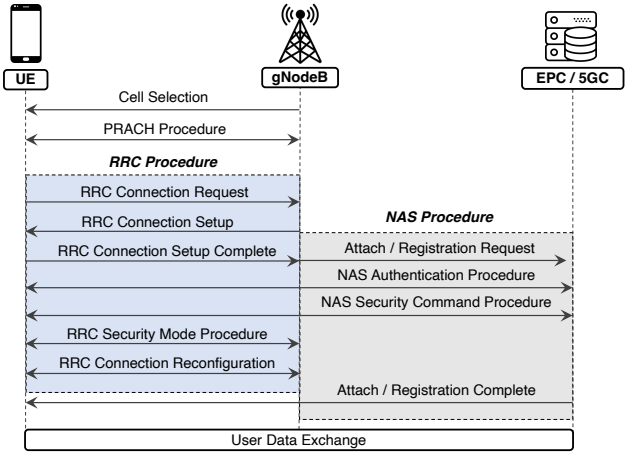
Why 5G is not Secure



Why 5G is not Secure

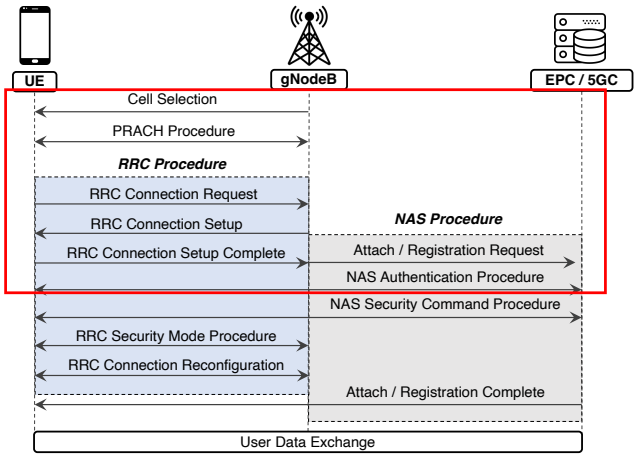


Why 5G is not Secure

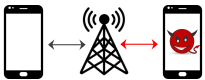


Why 5G is not Secure

Initial Messages Not Encrypted & Integrity Protected

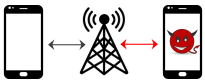


Threat Model



Adversary UEs

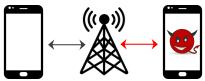
Threat Model



Adversary UEs

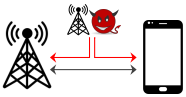
Man-In-the-Middle Attacker

Threat Model



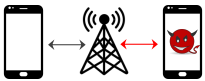
Adversary UEs

Man-In-the-Middle Attacker



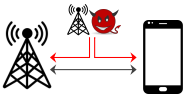
Signal Injector

Threat Model



Adversary UEs

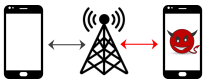
Man-In-the-Middle Attacker



Signal Injector

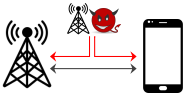
USRP B210 ($2000)

Threat Model



Adversary UEs

Man-In-the-Middle Attacker



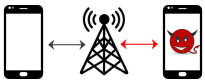
Signal Injector

USRP B210 ($2000)

+

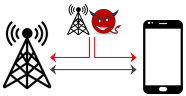
Raspberry Pi ($80)

Threat Model



Adversary UEs

Man-In-the-Middle Attacker



Signal Injector

USRP B210 ($2000)

+

Raspberry Pi ($80)

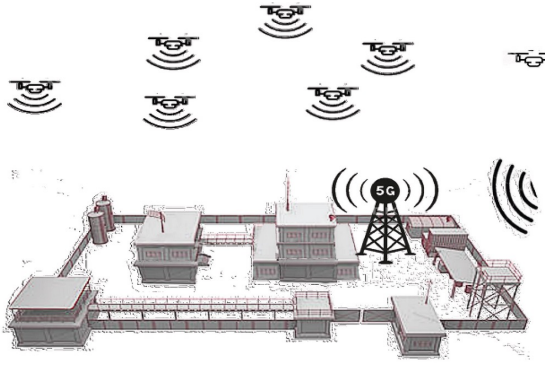
+

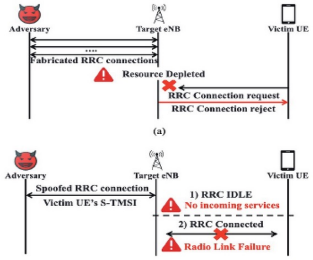
OPEN AIR INTERFACE

OpenAirInterface 5G (Free)

Attack Scenarios

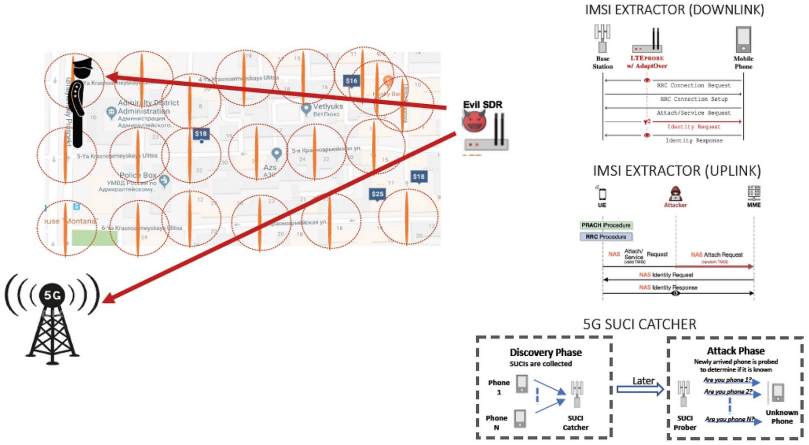
5G Base Station Distributed Denial-of-Service (DDoS) Attack Scenario





H. Kim, J. Lee, E. Lee and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," 2019 IEEE Symposium on Security and Privacy (SP), 2019.

Attack Scenarios



Attack Scenarios

Can we fix the standards to eliminate these attacks?

Attack Scenarios

Can we fix the standards to eliminate these attacks?

Currently very challenging due to numerous concerns

- Extremely Complicated Standard
- Backward Compatibility
- Performance and User Experience
- Overhead Constraint
- .....

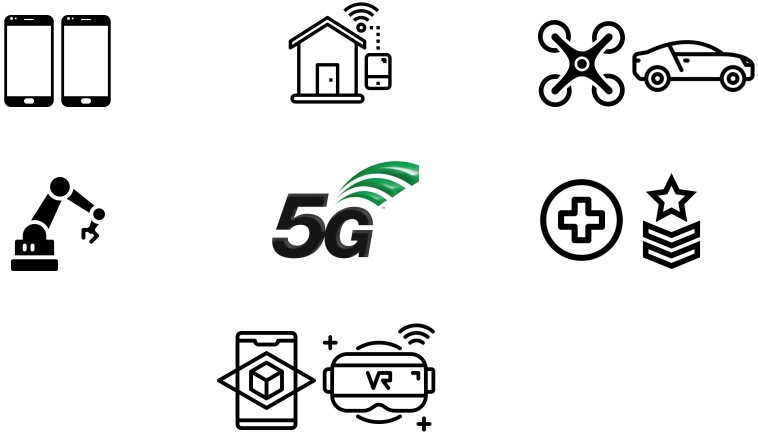
Attack Scenarios

~~Can we fix the standard body to eliminate these attacks?~~

~~Currently very challenging due to various concerns~~

How to defend against these attacks?

The Security Opportunities Enabled by OpenRAN



The Security Opportunities Enabled by OpenRAN

The Security Opportunities Enabled by OpenRAN

O-RAN provides new opportunities to integrate modular **security services** into 5G / Future G cellular networks

The Security Opportunities Enabled by OpenRAN

What is OpenRAN (O-RAN) [o-r]

- Represent a new software-defined open cellular network architecture

The Security Opportunities Enabled by OpenRAN

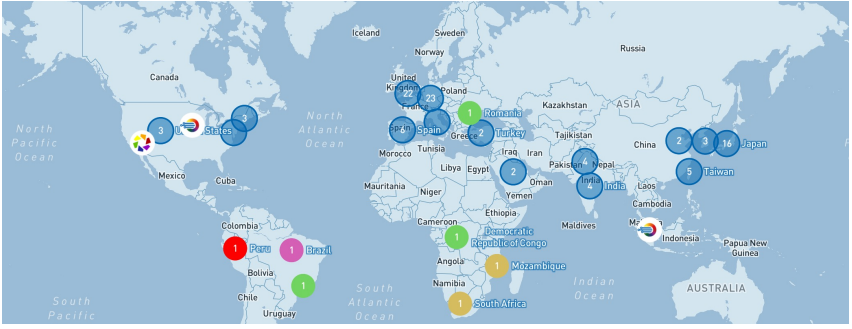
What is OpenRAN (O-RAN) [o-r]

- Represent a new software-defined open cellular network architecture
- Founded in 2018 by O-RAN Alliance

The Security Opportunities Enabled by OpenRAN

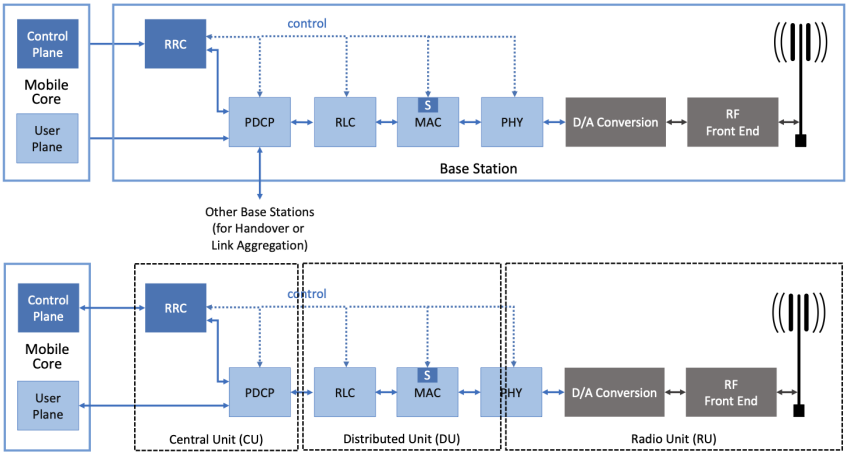
What is OpenRAN (O-RAN) [o-r]

- Represent a new software-defined open cellular network architecture
- Founded in 2018 by O-RAN Alliance
- Adopted by 32 mobile network operator worldwide (as of 2/2024)



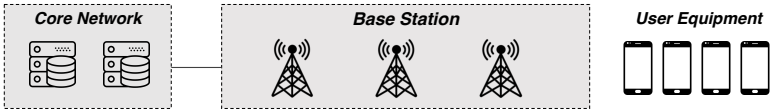
Deployments of O-RAN based technology and solutions from map.o-ran.org

Traditional RAN vs. OpenRAN



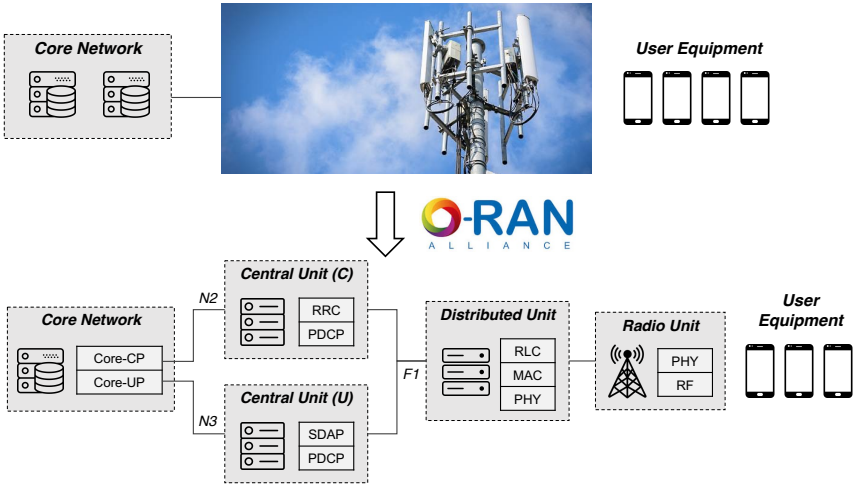
Source: https://5g.systemsapproach.org/ran.html

Traditional RAN vs. OpenRAN

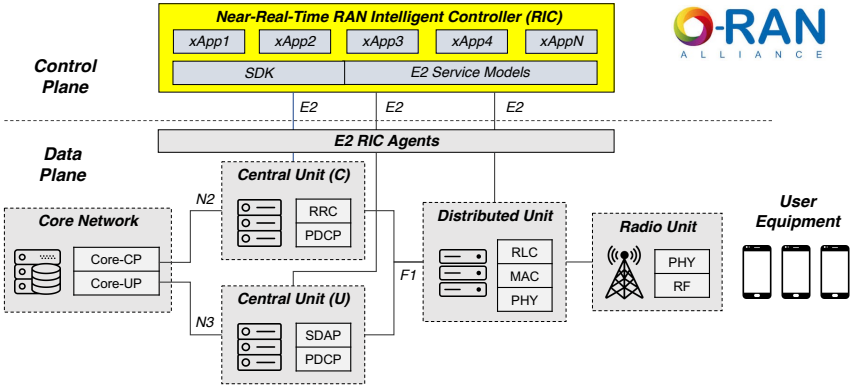


Traditional RAN vs. OpenRAN

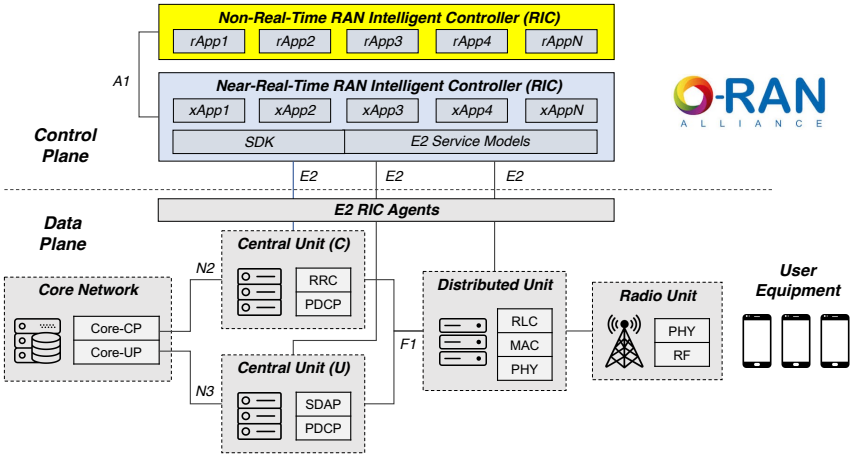
Traditional RAN vs. OpenRAN



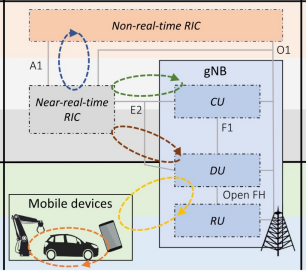
Traditional RAN vs. OpenRAN



Traditional RAN vs. OpenRAN

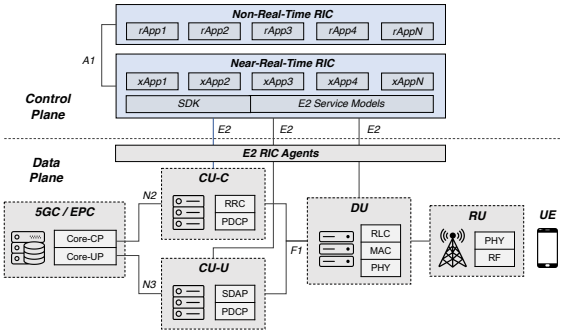


OpenRAN Architecture and Requirement

Control and learning objective	Scale (devices)	Input data	Timescale	Architecture	Challenges and limitations	
Policies, models, slicing	> 1000	Infrastructure KPMs	Non-real-time > 1 s		Orchestration of large-scale deployments	Supported by O-RAN
User Session Management e.g., load balancing, handover	> 100	CU KPMs e.g., number of sessions, PDCP traffic	Near-real-time 10-1000 ms		Process streams from multiple CUs and sessions	
Medium Access Management e.g., scheduling policy, RAN slicing	> 100	MAC KPMs e.g., PRB utilization, buffering	Near-real-time 10-1000 ms		Small time scales, control many DUs/UEs	
Radio Management e.g., scheduling, beamforming	~10	MAC/PHY KPMs e.g., PRB utilization, channel estimation	Real-time < 10 ms		Custom real-time loops not supported	For further study
Device DL/UL Management e.g., modulation	1	I/Q samples	Real-time < 1 ms		Device- and RU-level standardization	

O-RAN requirements and the closed-loop control enabled by the O-RAN architecture, and possible extensions. The control loops are represented by the dashed arrows [PBD+22]

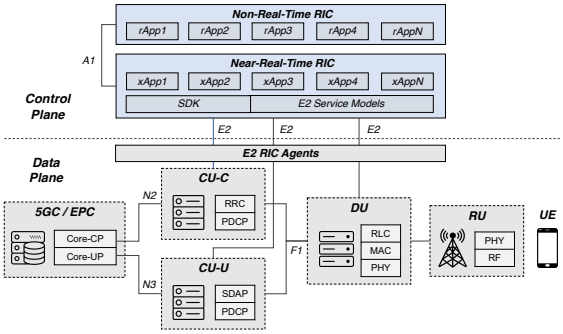
OpenRAN Architecture and Requirement



O-RAN's Key Capabilities

1. Disaggregation

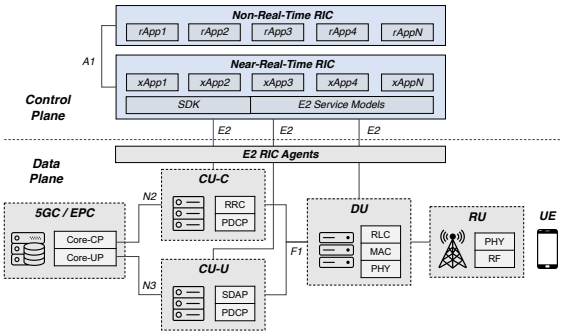
OpenRAN Architecture and Requirement



O-RAN's Key Capabilities

1. Disaggregation
2. Modularization (xApps / rApps)

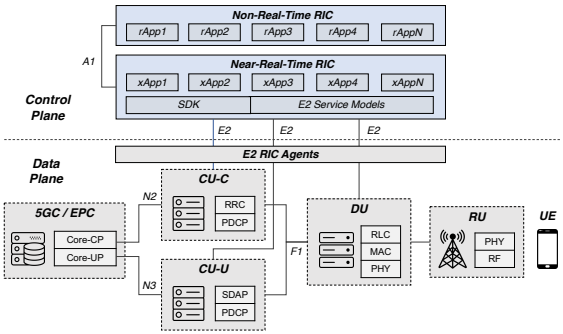
OpenRAN Architecture and Requirement



O-RAN's Key Capabilities

1. Disaggregation
2. Modularization (xApps / rApps)
3. Interoperability (Open Interfaces)

OpenRAN Architecture and Requirement



O-RAN's Key Capabilities

1. Disaggregation
2. Modularization (xApps / rApps)
3. Interoperability (Open Interfaces)
4. Virtualization

Challenges and Opportunities

1. **Visibility**
2. **Detection**
3. **Mitigation**

- The ability for O-RAN xApps to observe various threat modality at the edge.

Challenges and Opportunities

1. **Visibility**
   - The ability for O-RAN xApps to observe various threat modality at the edge.
2. **Detection**
   - The ability to perform security analytics and detect adversarial attacks.
3. **Mitigation**

Challenges and Opportunities

1. **Visibility**
   - The ability for O-RAN xApps to observe various threat modality at the edge.
2. **Detection**
   - The ability to perform security analytics and detect adversarial attacks.
3. **Mitigation**
   - The ability to automatically respond to emerging anomalies and attacks when they happen.

Challenges and Opportunities

1. **Visibility**
2. **Detection**
3. **Mitigation**

Existing O-RAN Applications and Service Models

Challenges and Opportunities

1. **Visibility**
2. **Detection**
3. **Mitigation**

Existing O-RAN Applications and Service Models

- Key Performance Indicator (KPI) monitor [ora23]
- RAN slicing management [ora24b]
- Traffic steering [ora24a]

Challenges and Opportunities

1. **Visibility**
2. **Detection**
3. **Mitigation**

Existing O-RAN Applications and Service Models

- Key Performance Indicator (KPI) monitor [ora23]
- RAN slicing management [ora24b]
- Traffic steering [ora24a]
- (Currently Absent) Security Applications
  - Attack / Anomaly monitoring and detection
  - Security mitigation and countermeasures
  - .....

Challenges and Opportunities

1. **Visibility**
2. **Detection**
3. **Mitigation**

Our Effort

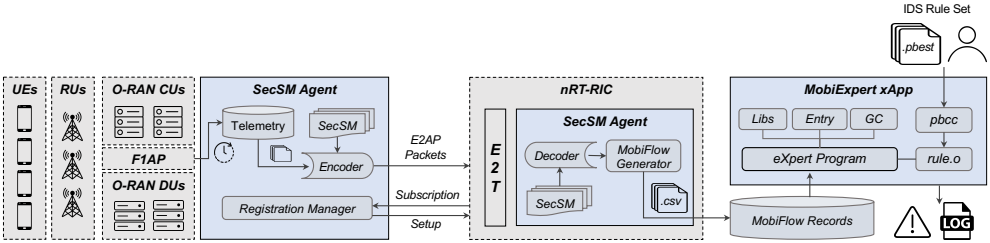
MobiFlow: A Fine-Grained Telemetry Stream for Security Services in 5G O-RAN networks [WPYL22] (CONEXT Emerging Topics in Wireless'22)

5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service [WPY+24] (NDSS'24)

6G-XSec: Explainable Edge Security for Emerging OpenRAN Architectures [WSP+24] (HotNets'24)

5G-Spector Overview

5G-Spector: The first O-RAN compliant IDS framework for comprehensive Layer-3 cellular attack detection



5G-Spector Overview

1. **Visibility**
2. **Detection**
3. **Mitigation**

Key Components of 5G-Spector

- **MobiFlow** [WPYL22] telemetry collecting UE state transitions and aggregated RAN statistics

5G-Spector Overview

1. **Visibility**
2. **Detection**
3. **Mitigation**

Key Components of 5G-Spector

- **MobiFlow** [WPYL22] telemetry collecting UE state transitions and aggregated RAN statistics
- Security xApp **MobieXpert** as a "plug-n-play" intrusion detection service on the nRT-RIC

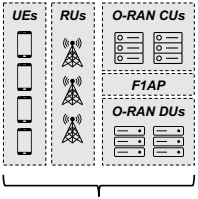
5G-Spector Overview

1. **Visibility**
2. **Detection**
3. **Mitigation**

Key Components of 5G-Spector

- **MobiFlow** [WPYL22] telemetry collecting UE state transitions and aggregated RAN statistics
- Security xApp **MobieXpert** as a "plug-n-play" intrusion detection service on the nRT-RIC
- **P-BEST** [LP99] w/ a decoupled architecture and efficient IDS programming language

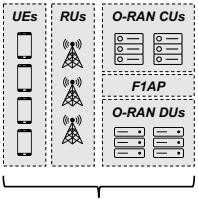
5G-Spector Design



RAN Data Plane

- Open-sourced UE and RAN implementations (LTE / 5G)
- Simulation or commodity SDRs

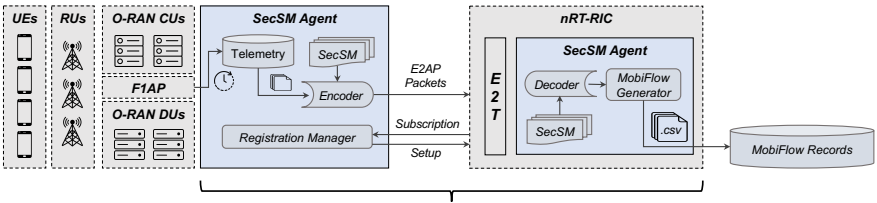
5G-Spector Design



RAN Data Plane

- Open-sourced UE and RAN implementations (LTE / 5G)
- Simulation or commodity SDRs

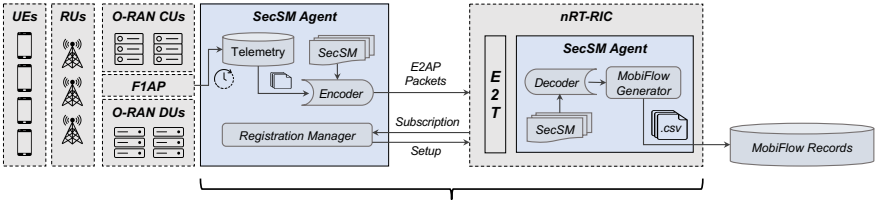
5G-Spector Design



5G-Spector Control Layer

- xApp Registration and Subscription management
- Telemetry Report & Collection (**MobiFlow**)

5G-Spector Design



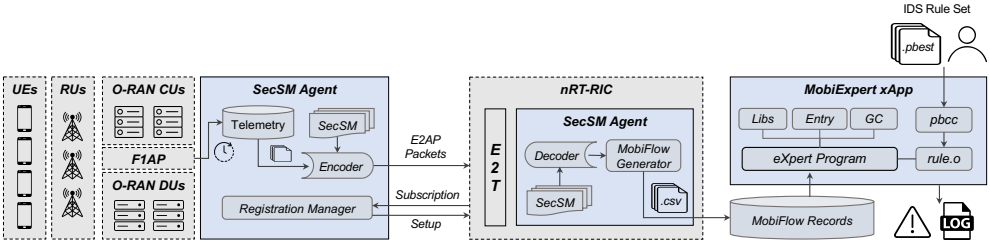
kubernetes

5G-Spector Control Layer

- xApp Registration and Subscription management
- Telemetry Report & Collection (**MobiFlow**)

SD-RAN

5G-Spector Design



5G-Spector xApp Layer

- P-Best programming framework
- Attack signatures / rules integration
- Real-time alert notifications

Evaluation w/ Simulated Attacks and Variants

Attack	Layer	Exploited L3 Message	New	Detected
BTS RC Depletion	RRC	ConnectionRequest *(Fabricated)*	○	✓
Blind DoS	RRC	ConnectionRequest *(Replayed TMSI)*	○	✓
Downlink DoS	NAS	AuthRequest ← AttachReject	○	✓
	NAS	SecModeCmd ← AttachReject	●	✓
	NAS	AttachAccept ← AttachReject	●	✓
	NAS	AuthRequest ← ServiceReject	●	✓
	NAS	SecModeCmd ← ServiceReject	●	✓
	NAS	AttachAccept ← ServiceReject	●	✓
Uplink DoS	NAS	AttachReq ← AttachReq *(Invalid IMSI)*	○	✓
	NAS	ServiceReq ← ServiceReq *(Invalid MAC)*	●	✓
Uplink IMSI Extractor	NAS	AttachReq ← AttachReq *(Unknown TMSI)*	○	✓
Downlink IMSI Extractor	NAS	AuthRequest ← IdentityRequest *(IMSI)*	○	✓
	NAS	AuthRequest ← IdentityRequest *(IMEI)*	●	✓
	NAS	AuthRequest ← IdentityRequest *(TMSI)*	●	✓
	NAS	SecModeCmd ← IdentityRequest *(IMSI)*	●	✓
	NAS	AttachAccept ← IdentityRequest *(IMSI)*	●	✓
Null Cipher & Integrity	RRC	SecModeComplete ← SecModeFailure	○	✓
	NAS	SecModeComplete ← SecModeReject	●	✓

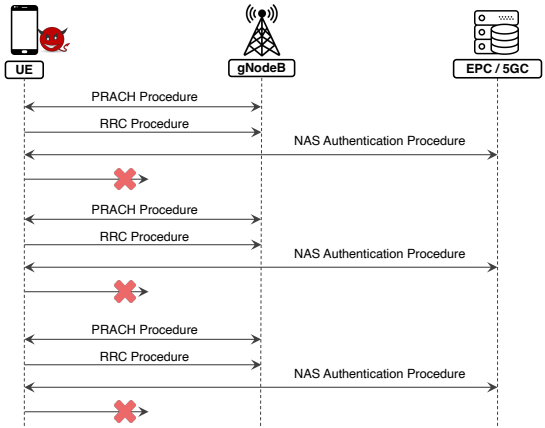
Table: All L3 cellular attacks and variants replicated and evaluated ($A \leftarrow B$ indicates message B overwrites A).

Evaluation w/ Simulated Attacks and Variants

Attack	Layer	Exploited L3 Message	New	Detected
BTS RC Depletion	RRC	ConnectionRequest *(Fabricated)*	○	✓
Blind DoS	RRC	ConnectionRequest *(Replayed TMSI)*	○	✓
Downlink DoS	NAS	AuthRequest ← AttachReject	○	✓
	NAS	SecModeCmd ← AttachReject	●	✓
	NAS	AttachAccept ← AttachReject	●	✓
	NAS	AuthRequest ← ServiceReject	●	✓
	NAS	SecModeCmd ← ServiceReject	●	✓
	NAS	AttachAccept ← ServiceReject	●	✓
Uplink DoS	NAS	AttachReq ← AttachReq *(Invalid IMSI)*	○	✓
	NAS	ServiceReq ← ServiceReq *(Invalid MAC)*	●	✓
Uplink IMSI Extractor	NAS	AttachReq ← AttachReq *(Unknown TMSI)*	○	✓
Downlink IMSI Extractor	NAS	AuthRequest ← IdentityRequest *(IMSI)*	○	✓
	NAS	AuthRequest ← IdentityRequest *(IMEI)*	●	✓
	NAS	AuthRequest ← IdentityRequest *(TMSI)*	●	✓
	NAS	SecModeCmd ← IdentityRequest *(IMSI)*	●	✓
	NAS	AttachAccept ← IdentityRequest *(IMSI)*	●	✓
Null Cipher & Integrity	RRC	SecModeComplete ← SecModeFailure	○	✓
	NAS	SecModeComplete ← SecModeReject	●	✓

Table: All L3 cellular attacks and variants replicated and evaluated ($A \leftarrow B$ indicates message B overwrites A).

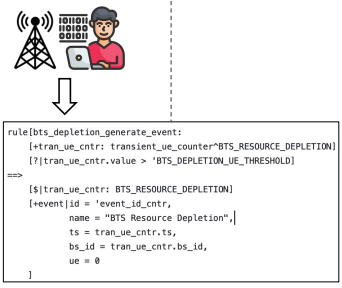
Evaluation w/ Simulated Attacks and Variants



BTS Resource Depletion Attack

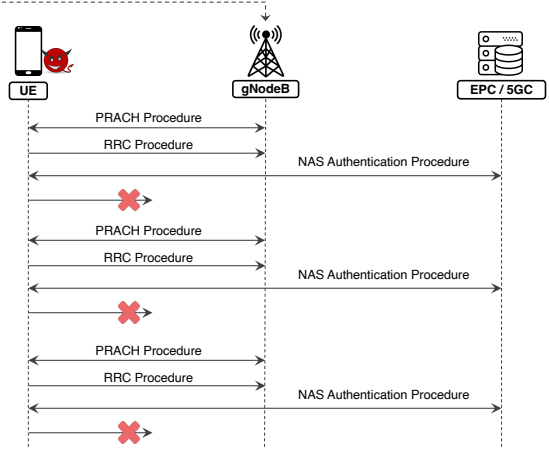
Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

Evaluation w/ Simulated Attacks and Variants



```
rule[bts_depletion_generate_event:
    [+tran_ue_cntr: transient_ue_counter^BTS_RESOURCE_DEPLETION]
    [?|tran_ue_cntr.value > 'BTS_DEPLETION_UE_THRESHOLD]
==>
    [$|tran_ue_cntr: BTS_RESOURCE_DEPLETION]
    [+event|id = 'event_id_cntr,
            name = "BTS Resource Depletion",
            ts = tran_ue_cntr.ts,
            bs_id = tran_ue_cntr.bs_id,
            ue = 0
    ]
```

P-BEST IDS Signature in 5G-Spector



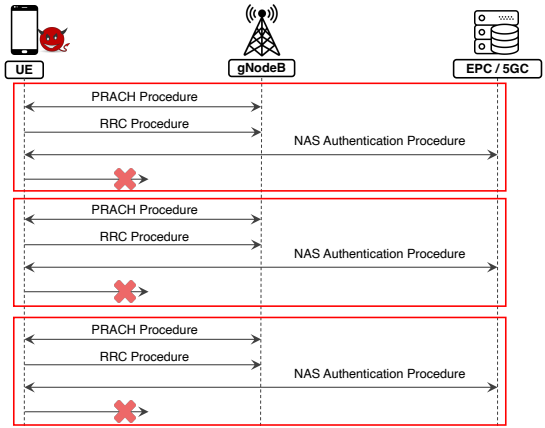
BTS Resource Depletion Attack

Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

Evaluation w/ Simulated Attacks and Variants

```
rule[bts_depletion_generate_event:
    [+tran_ue_cntr: transient_ue_counter^BTS_RESOURCE_DEPLETION]
    [?|tran_ue_cntr.value > 'BTS_DEPLETION_UE_THRESHOLD]
==>
    [$|tran_ue_cntr: BTS_RESOURCE_DEPLETION]
    [+event|id = 'event_id_cntr,
            name = "BTS Resource Depletion",
            ts = tran_ue_cntr.ts,
            bs_id = tran_ue_cntr.bs_id,
            ue = 0
    ]
```

P-BEST IDS Signature in 5G-Spector



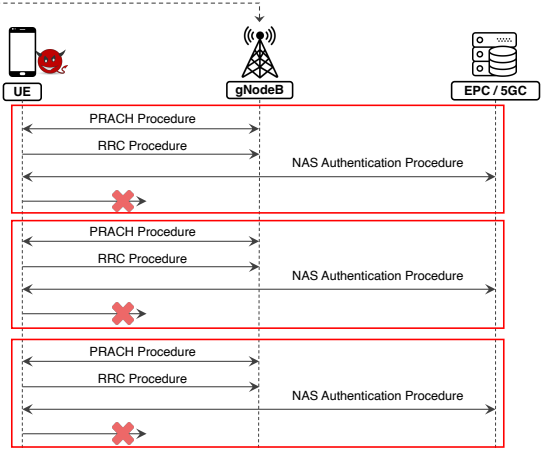
BTS Resource Depletion Attack

Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

Evaluation w/ Simulated Attacks and Variants

```
rule[bts_depletion_generate_event:
    [+tran_ue_cntr: transient_ue_counter^BTS_RESOURCE_DEPLETION]
    [?|tran_ue_cntr.value > 'BTS_DEPLETION_UE_THRESHOLD]
==>
    [$|tran_ue_cntr: BTS_RESOURCE_DEPLETION]
    [+event|id = 'event_id_cntr,
            name = "BTS Resource Depletion",
            ts = tran_ue_cntr.ts,
            bs_id = tran_ue_cntr.bs_id,
            ue = 0
    ]
```

P-BEST IDS Signature in 5G-Spector



BTS Resource Depletion Attack

Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

Evaluation w/ Simulated Attacks and Variants

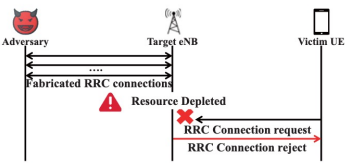
UE-Centric MobiFlow

```
type,id,ts,ver,gen,bsId,rnti,tmsi,imsi,imei,cipher,inter,cause,msg,rrc_state,nas_state,sec_state,emm_cause,timers
UE;0;1663091358252.3652;v1.0;SECSM;0;51265;0;208010272923905;0;0;0;3;RRCConnectionRequest;0;0;0;0;0;0;0
UE;1;1663091358252.803;v1.0;SECSM;0;51265;0;208010272923905;0;0;0;3;RRCConnectionSetup;2;0;0;1663091358164.0156;0;0;0
UE;2;1663091358253.2107;v1.0;SECSM;0;51265;0;208010272923905;0;0;0;3;RRCConnectionSetupComplete;2;1;0;1663091358164.0156;0;0;0
UE;3;1663091358253.7522;v1.0;SECSM;0;51265;0;208010272923905;0;0;0;3;AUTHENTICATION_REQUEST;2;1;0;1663091358164.0156;0;0;0
UE;4;1663091359177.4214;v1.0;SECSM;0;4840;0;208010272923905;0;0;0;3;RRCConnectionRequest;0;0;0;0;0;0;0
UE;5;1663091359177.9387;v1.0;SECSM;0;4840;0;208010272923905;0;0;0;3;RRCConnectionSetup;2;0;0;1663091359177.3555;0;0;0
UE;6;1663091359178.6028;v1.0;SECSM;0;4840;0;208010272923905;0;0;0;3;RRCConnectionSetupComplete;2;1;0;1663091359177.3555;0;0;0
UE;7;1663091359179.099;v1.0;SECSM;0;4840;0;208010272923905;0;0;0;3;AUTHENTICATION_REQUEST;2;1;0;1663091359177.3555;0;0;0
UE;8;1663091360164.5881;v1.0;SECSM;0;59853;0;208010272923905;0;0;0;3;RRCConnectionRequest;0;0;0;0;0;0;0
UE;9;1663091360164.7314;v1.0;SECSM;0;59853;0;208010272923905;0;0;0;3;RRCConnectionSetup;2;0;0;1663091360164.5225;0;0;0
UE;10;1663091360164.865;v1.0;SECSM;0;59853;0;208010272923905;0;0;0;3;RRCConnectionSetupComplete;2;1;0;1663091360164.5225;0;0;0
UE;11;1663091360164.9792;v1.0;SECSM;0;59853;0;208010272923905;0;0;0;3;AUTHENTICATION_REQUEST;2;1;0;1663091360164.5225;0;0;0
```

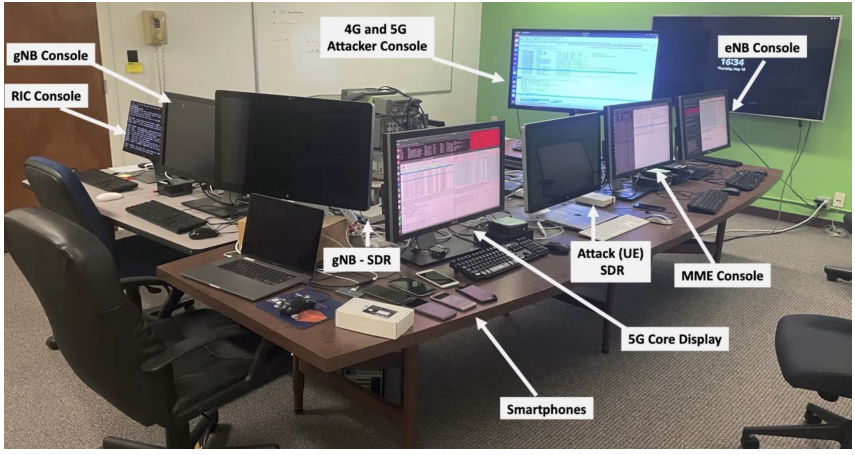
RAN-Centric MobiFlow

BTS Depletion Attack Detected

```
type,id,ts,ver,gen,bsId,mcc,mnc,tac,cellId,report_period,connected_ue_cnt,idle_ue_cnt,max_ue_cnt,timers
BS;0;1663091229100.6868;v1.0;SECSM;0;0;0;0;e0000;1000;0;0;0;1663091229100.5525;0
BS;1;1663091358253.047;v1.0;SECSM;0;0;0;0;e0000;1000;1;0;0;1663091229100.5525;0
BS;2;1663091358253.4182;v1.0;SECSM;0;0;0;0;e0000;1000;1;0;0;1663091229100.5525;0
BS;3;1663091359178.1868;v1.0;SECSM;0;0;0;0;e0000;1000;2;0;0;1663091229100.5525;0
BS;4;1663091359178.8777;v1.0;SECSM;0;0;0;0;e0000;1000;2;0;0;1663091229100.5525;0
BS;5;1663091360164.8127;v1.0;SECSM;0;0;0;0;e0000;1000;3;0;0;1663091229100.5525;0
BS;6;1663091360164.9314;v1.0;SECSM;0;0;0;0;e0000;1000;3;0;0;1663091229100.5525;0
BS;7;1663091361181.7952;v1.0;SECSM;0;0;0;0;e0000;1000;4;0;0;1663091229100.5525;0
BS;8;1663091361181.9158;v1.0;SECSM;0;0;0;0;e0000;1000;4;0;0;1663091229100.5525;0
BS;9;1663091362163.4292;v1.0;SECSM;0;0;0;0;e0000;1000;5;0;0;1663091229100.5525;0
BS;10;1663091363161.9412;v1.0;SECSM;0;0;0;0;e0000;1000;6;0;0;1663091229100.5525;0
```

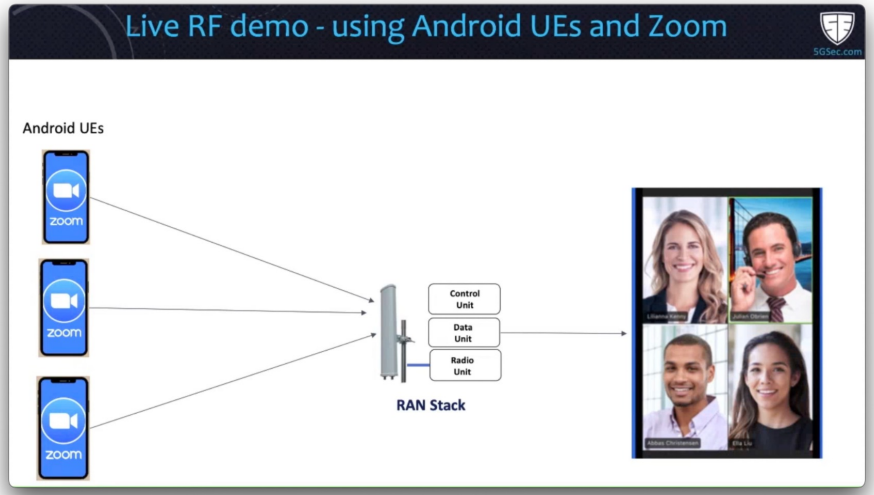


Evaluation w/ OTA Attacks

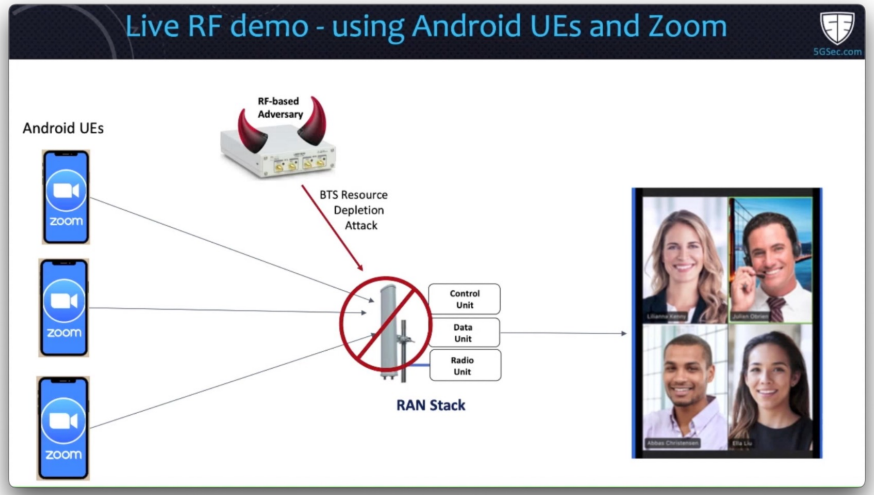


Our 5G Network Testbed at the Computer Science Lab of SRI International.

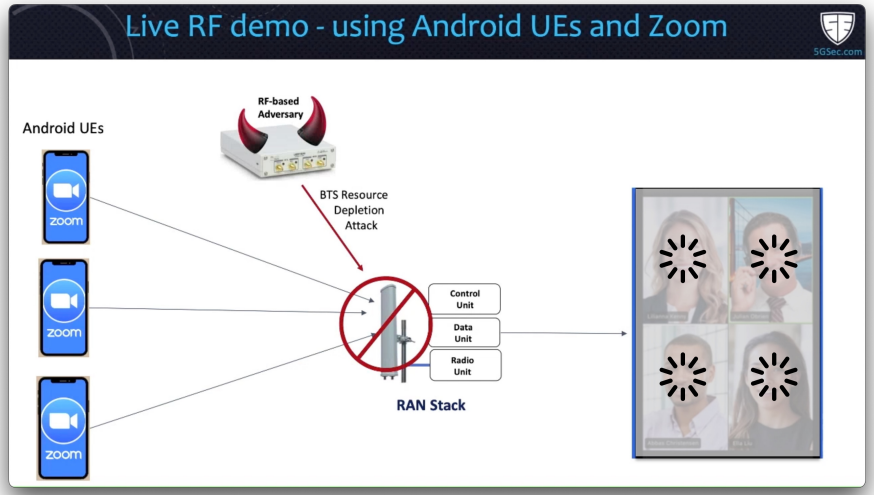
Evaluation w/ OTA Attacks



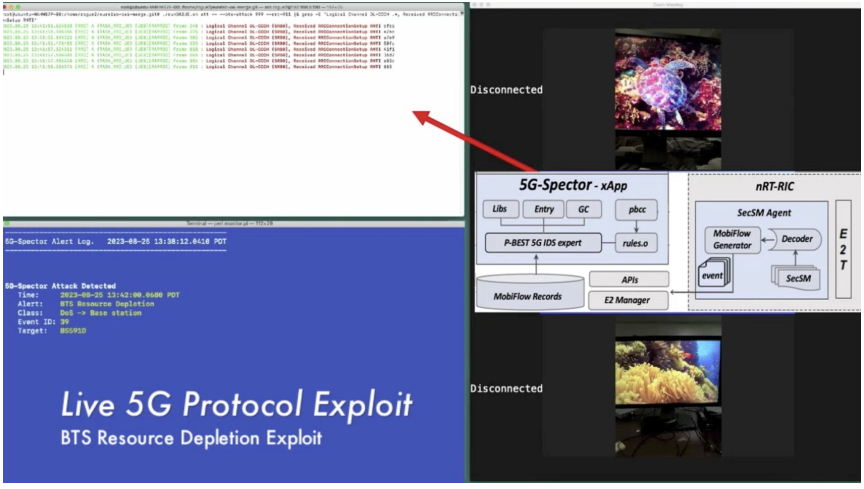
Evaluation w/ OTA Attacks



Evaluation w/ OTA Attacks

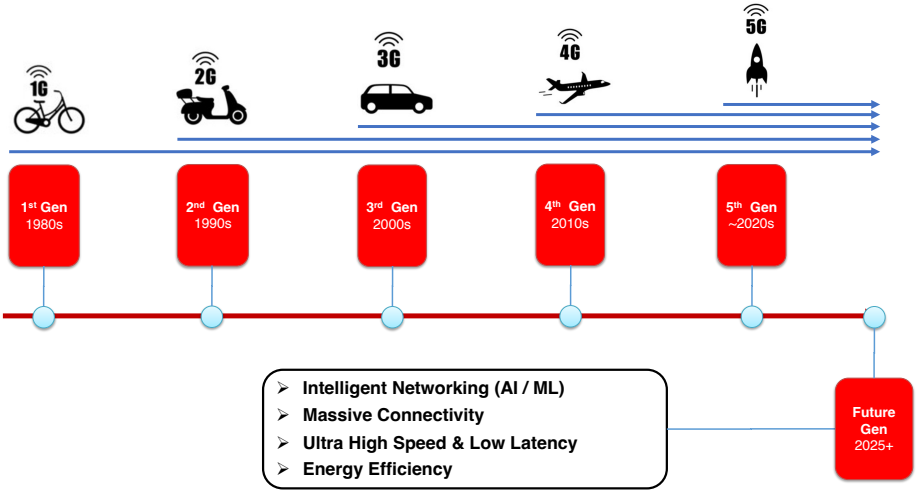


Evaluation w/ OTA Attacks

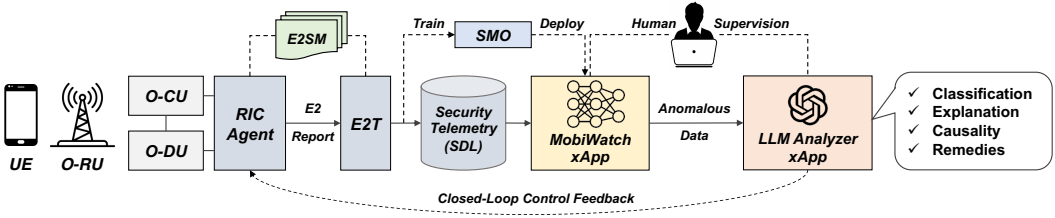


Demo video available at https://www.5gsec.com/post/5g-spector-demo

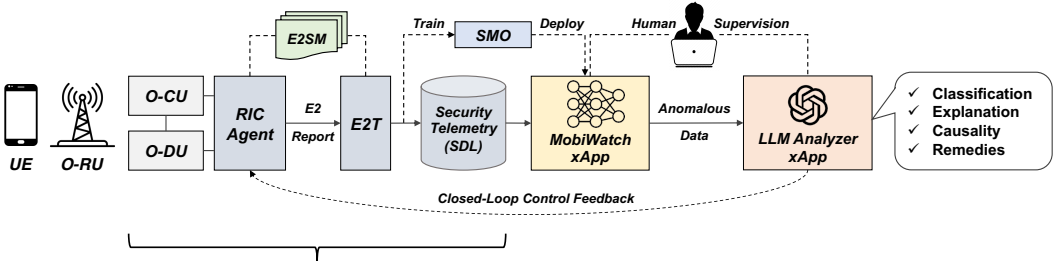
6GXsec Overview



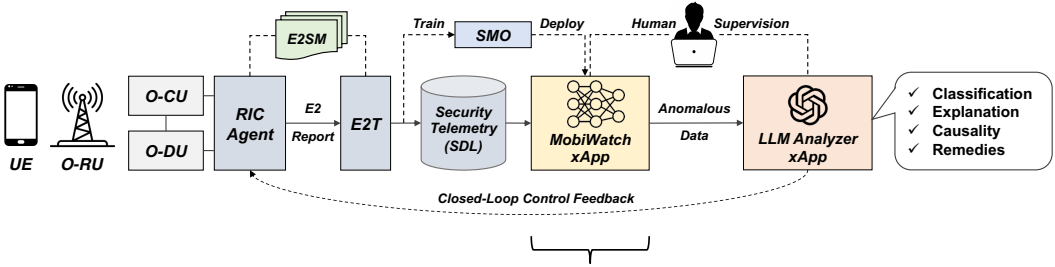
6GXsec Overview



6GXsec Overview



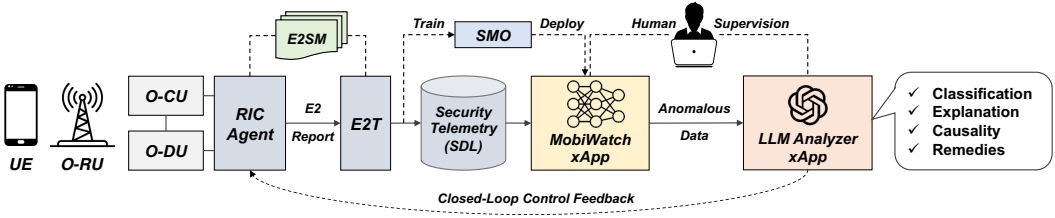
6GXsec Overview



O-RAN Control Plane: Threat Detection

- **MobiWatch**: xApp with unsupervised deep learning
- Trained on benign cellular control traffic datasets
- Detect unseen attack deviated from normal traffic patterns

6GXsec Overview

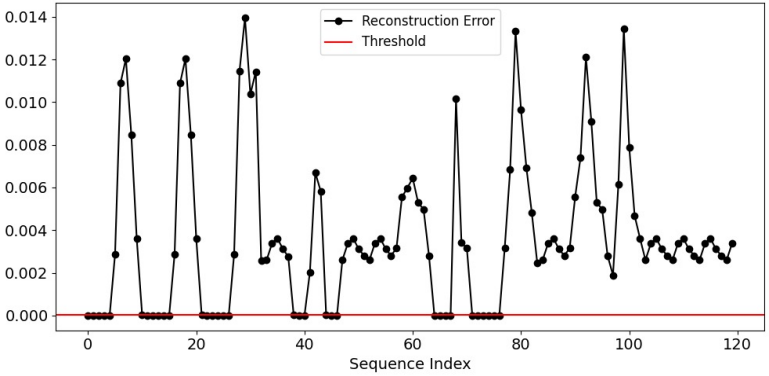


O-RAN Control Plane: Threat Explanation

- **LLM Analyzer**: Expert-Referencing xApp interfacing with LLM APIs
- Analyze / Explain complicated threat / anomaly patterns
- Propose potential mitigations for operators

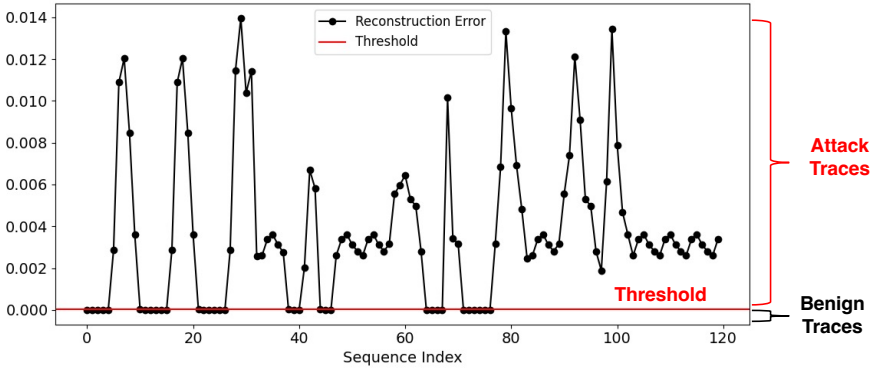
Preliminary Results

Unsupervised deep learning model for detecting layer-3 anomalies and attacks



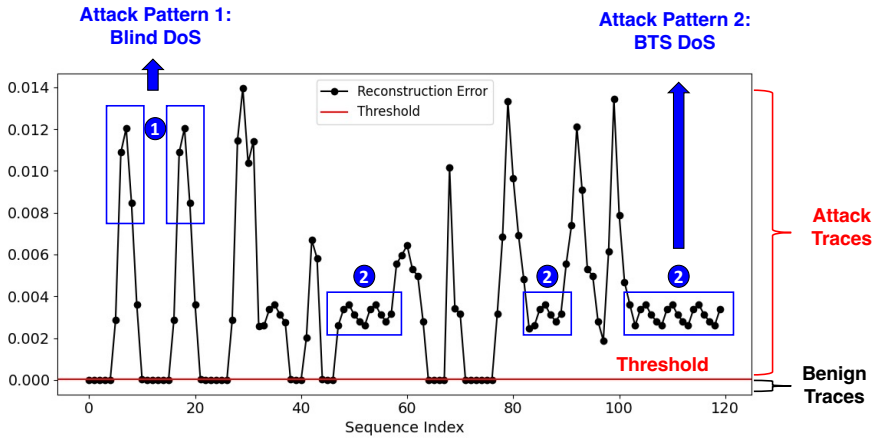
Preliminary Results

Unsupervised deep learning model for detecting layer-3 anomalies and attacks



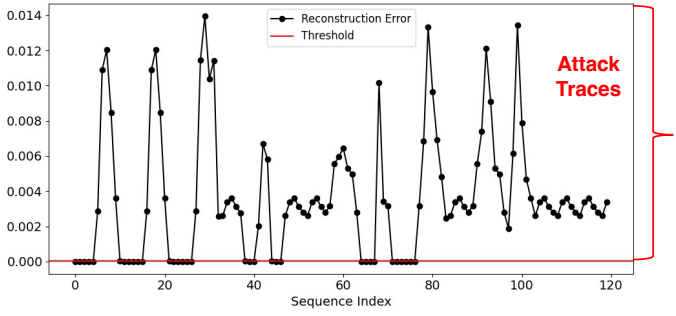
Preliminary Results

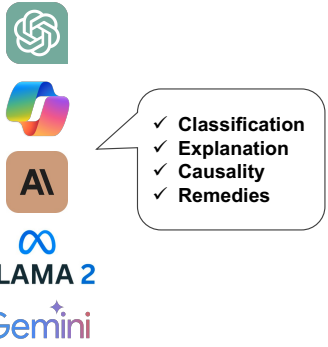
Unsupervised deep learning model for detecting layer-3 anomalies and attacks



Preliminary Results

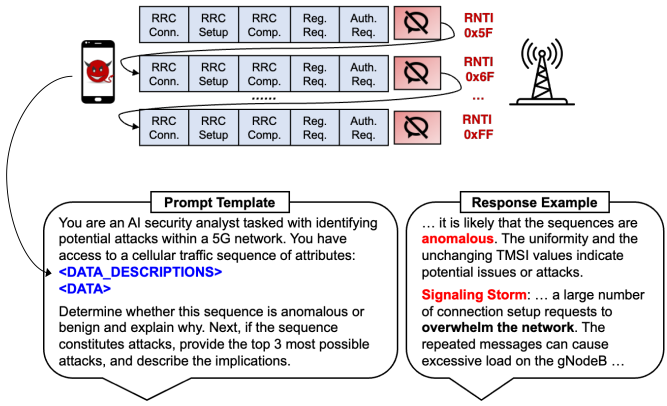
LLM Expert-Referencing xApp for explaining / classifying anomalous cellular traffic





Preliminary Results

LLM Expert-Referencing xApp for explaining / classifying anomalous cellular traffic

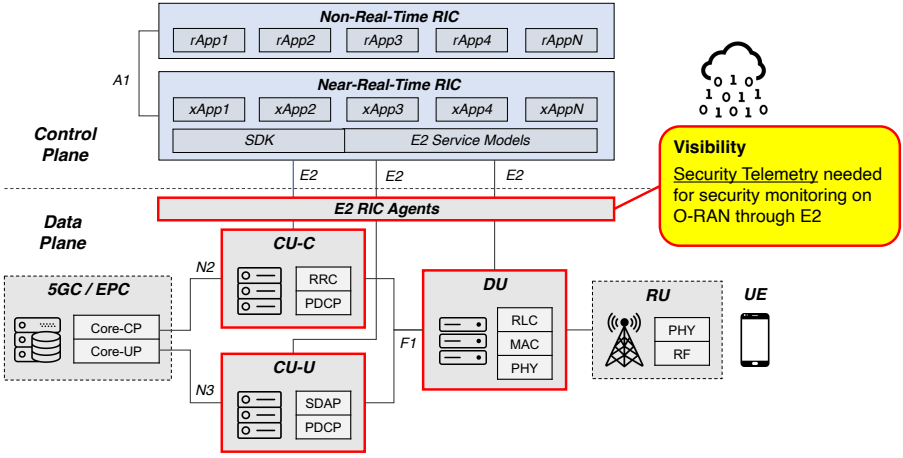


Preliminary Results

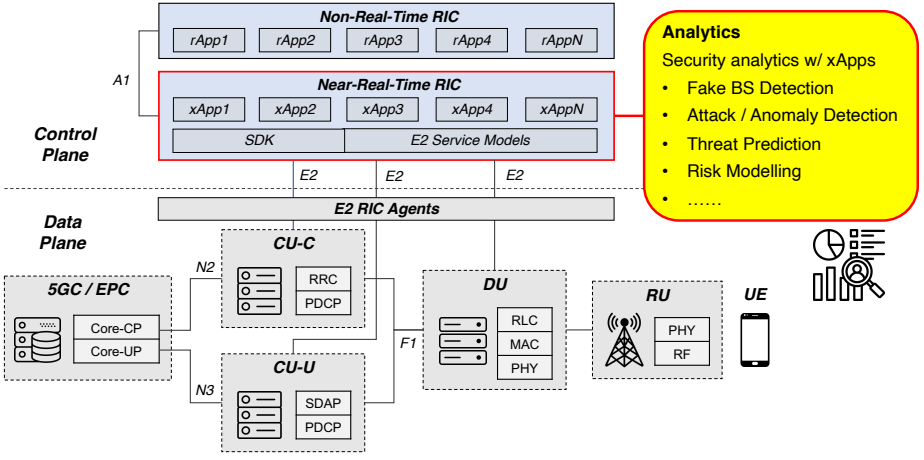
Attack / Trace	Baseline LLM Models				
	Chat GPT-4o	Gemini	Copilot	Llama3	Claude 3 Sonnet
BTS DoS [KLLK19]	✓	✓	✓	✗	✗
Blind DoS [KLLK19]	✓	✗	✗	✓	✗
Uplink ID Extr [EKL+22]	✗	✗	✗	✗	✓
Downlink ID Extr [KEL+22]	✓	✓	✗	✓	✓
Null Cipher & Int. [HEK+19]	✓	✓	✗	✓	✓
Benign Sequence 1	✓	✓	✓	✓	✓
Benign Sequence 2	✓	✓	✓	✓	✓

Table: Summary of attack classification results from different baseline LLMs. ✓ indicates the LLM correctly identifies the attack or benign cellular sequences. ✗ indicates wrong decisions.

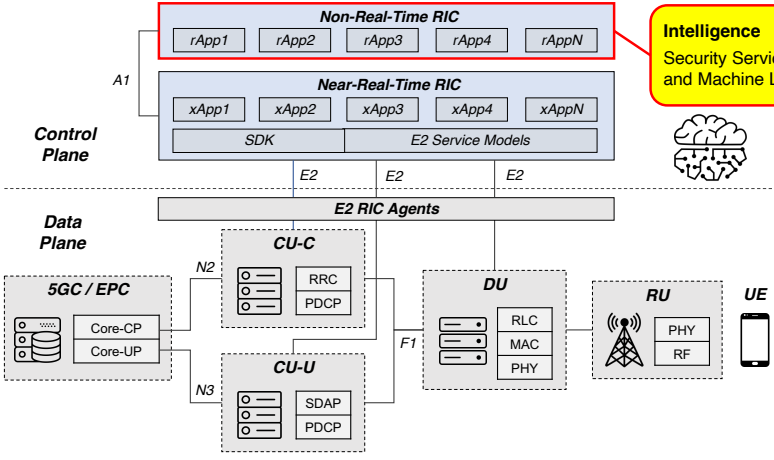
Our Vision on 5G / FutureG Security



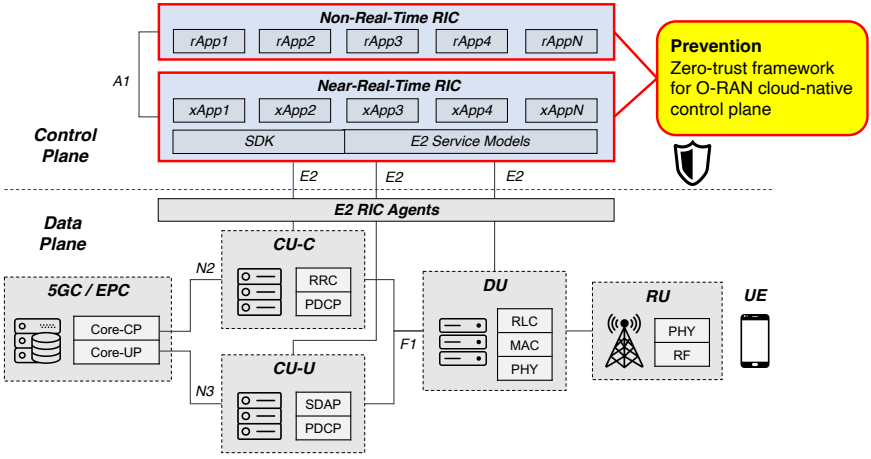
Our Vision on 5G / FutureG Security



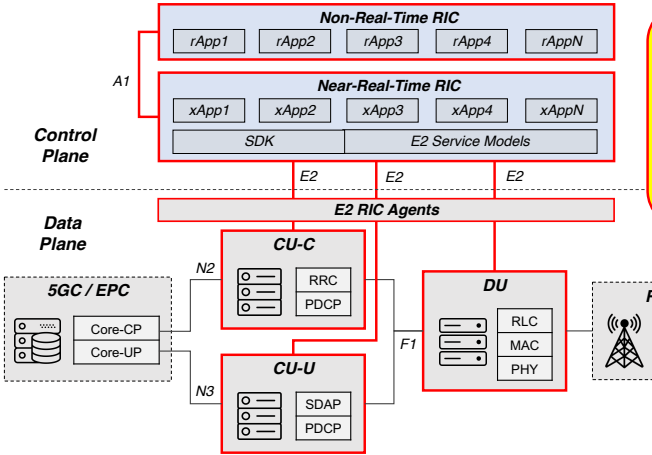
Our Vision on 5G / FutureG Security



Our Vision on 5G / FutureG Security



Our Vision on 5G / FutureG Security



Automation: AI-Ops

- Countermeasures
- Fault Recovery
- Dynamic Slicing
- Predative Management
- Self-Organizing Network (SON)

Project SE-RAN

sec.com

SE-RAN
Security Enhanced
Radio Access Network

Project SE-RAN

5Gsec.com

SE-RAN
Security Enhanced
Radio Access Network

Paper QR Code

Artifact Evaluated
NDSS SYMPOSIUM
Available
Functional
Reproduced


NDSS
SYMPOSIUM/2024

NETWORK & DISTRIBUTED SYSTEM SECURITY SYMPOSIUM

Distinguished Artifact Award

5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service

Haohuang Wen, Phillip Porras, Vinod Yegneswaran, Ashish Gehani, Zhiqiang Lin

Presented at the NDSS Symposium, February 26 – March 1, 2024, in San Diego, California

In recognition of an outstanding artifact
in the field of network and distributed system security research.

Cristina Nita-Rotaru
NDSS General Chair

Daniele Cono D'Elia
Artifact Evaluation Chair

FutureG Security Workshop

Workshop on Security and Privacy of Next-Generation Networks (FutureG)
(co-located with NDSS'25)

- Paper Submission Deadline: January 10, 2025
- Notification of Acceptance: January 31, 2025
- Camera-Ready Deadline: February 10, 2025
- Workshop Date: February 24, 2025

https://www.ndss-symposium.org/ndss2025/submissions/cfp-futureg/

Thank You

Security-Enhanced Radio Access Networks for 5G OpenRAN

Dr. Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

Joint work with Haohuang Wen, Prakhar Sharma, Phil Porras, Vinod Yegneswaran, and Ashish Gehani

11/21/2024

References I


Simon Erni, Martin Kotuliak, Patrick Leu, Marc Röschlin, and Srdjan Capkun, *Adaptover: adaptive overshadowing attacks in cellular networks*, Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, 2022, pp. 743–755.


Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino, *5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol*, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 669–684.


Martin Kotuliak, Simon Erni, Patrick Leu, Marc Roeschlin, and Srdjan Čapkun, *{LTrack}: Stealthy tracking of mobile phones in {LTE}*, 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 1291–1306.


Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim, *Touching the untouchables: Dynamic security analysis of the lte control plane*, 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 1153–1168.


Ulf Lindqvist and Phillip A Porras, *Detecting computer and network misuse through the production-based expert system toolset (p-best)*, Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344), IEEE, 1999, pp. 146–161.


O-ran alliance, `https://www.o-ran.org/`.


O-ran.wg3.e2sm-r003-v04.00: O-ran e2 service model (e2sm) kpm, October 2023.


O-ran software community, `https://wiki.o-ran-sc.org/display/ORAN`, May 2024.


O-ran.wg3.e2sm-rc-r003-v05.00: O-ran e2 service model (e2sm), ran control, February 2024.

References II

Michele Polese, Leonardo Bonati, Salvatore D'Oro, Stefano Basagni, and Tommaso Melodia, *Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges*, arXiv preprint arXiv:2202.01032 (2022).

Haohuang Wen, Phillip Porras, Vinod Yegneswaran, Ashish Gehani, and Zhiqiang Lin, *5g-spector: an o-ran compliant layer-3 cellular attack detection service*, Network and Distributed System Security (NDSS) Symposium, 2024.

Haohuang Wen, Phillip Porras, Vinod Yegneswaran, and Zhiqiang Lin, *A fine-grained telemetry stream for security services in 5g open radio access networks*, Proceedings of the 1st International Workshop on Emerging Topics in Wireless, 2022, pp. 18–23.

Haohuang Wen, Prakhar Sharma, Phillip Porras, Vinod Yegneswaran, Ashish Gehani, and Zhiqiang Lin, *6g-xsec: Explainable edge security for emerging openran architectures*, 23rd Workshop on Hot Topics in Networks (HotNets'24), 2024.