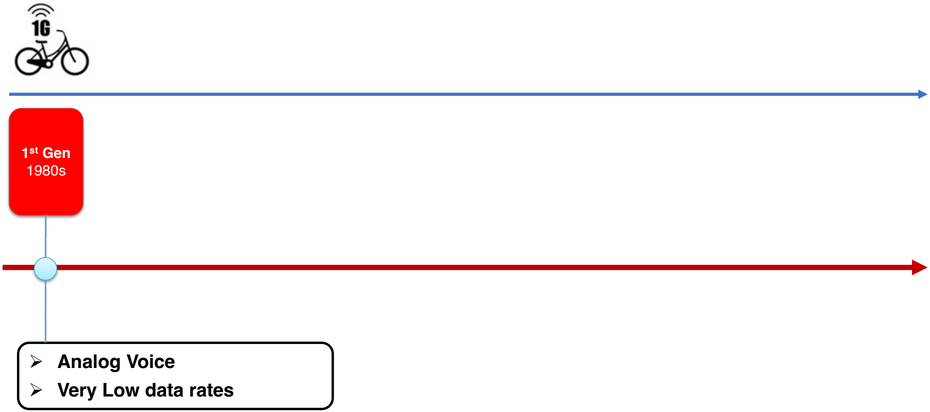
5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service

Haohuang Wen[1], Phillip Porras[2], Vinod Yegneswaran[2], Ashish Gehani[2], Zhiqiang Lin[1]

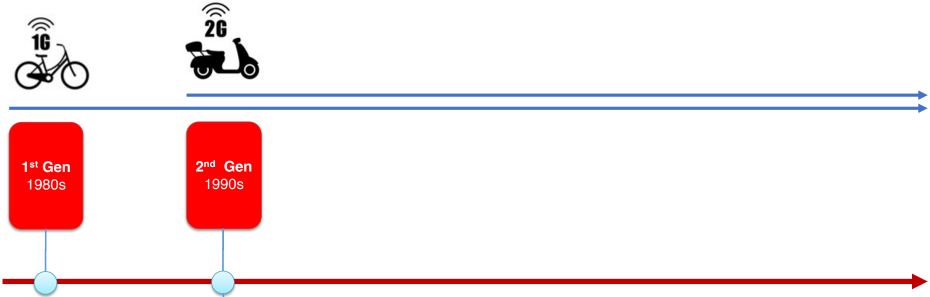
[1]The Ohio State University, [2]SRI International

Presented at the 31st ISOC Network and Distributed System Security Symposium (NDSS'24), San Diego, CA, February 28th 2024

Evolution of Cellular Network

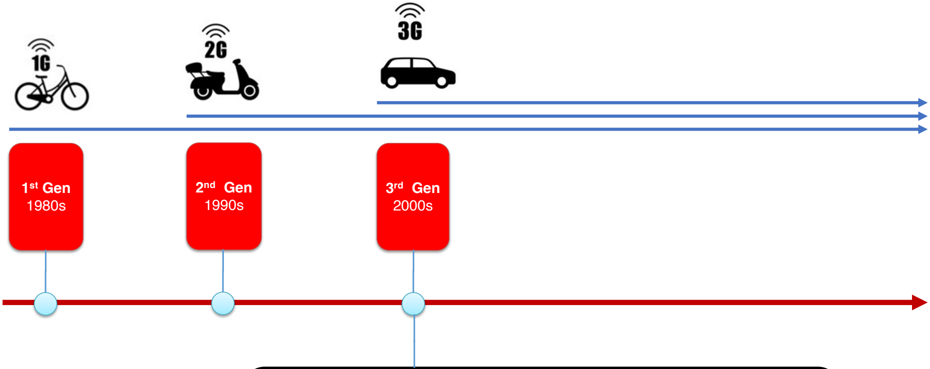


Evolution of Cellular Network



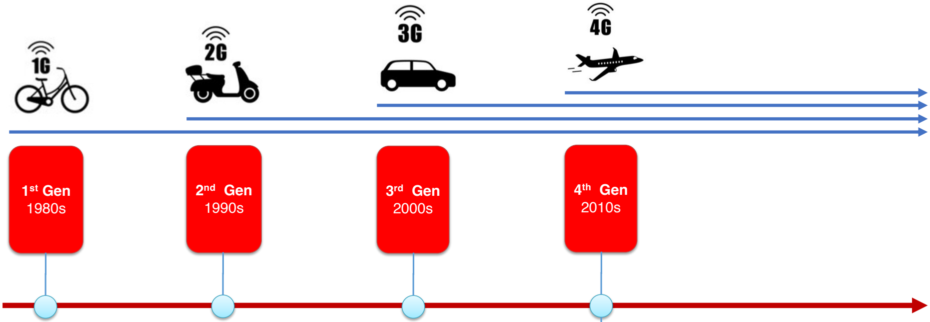
- Digital Communication
- SMS (Short Message Service)
- GSM (Global System for Mobile Communications)

Evolution of Cellular Network



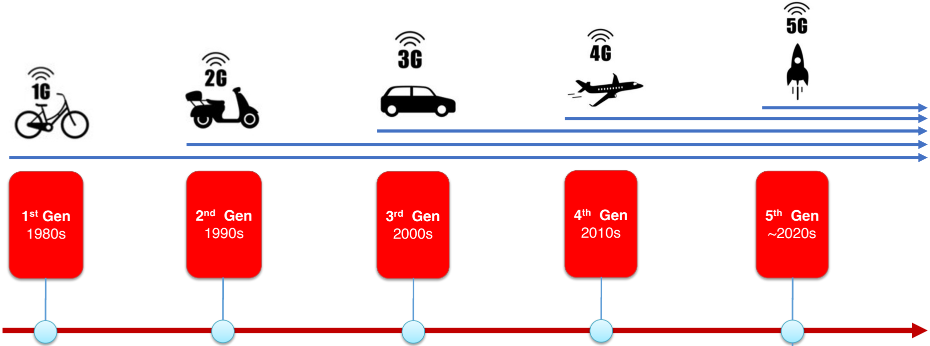
- **Mobile Internet (Kbps)**
- **Video Calls**
- **UMTS (Universal Mobile Telecommunications System)**

Evolution of Cellular Network



- **High-Speed Data (Mbps)**
- **LTE (Long-Term Evolution) Standard**
- **Mobile Broadband**

Evolution of Cellular Network



- Ultra High-Speed Data (Gbps)
- Massive Internet-of-Things (IoT)
- Extremely Low Latency (AR / VR)
- Network Slicing

Why 5G is not Secure

Why do we care about 5G Security and Privacy?

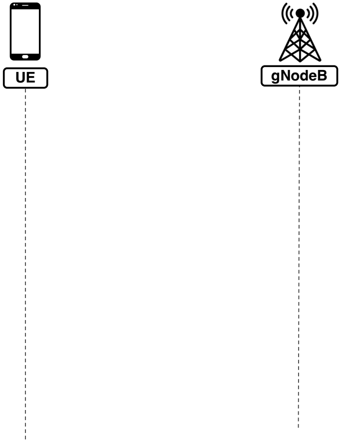
Why 5G is not Secure

Why do we care about 5G Security and Privacy?

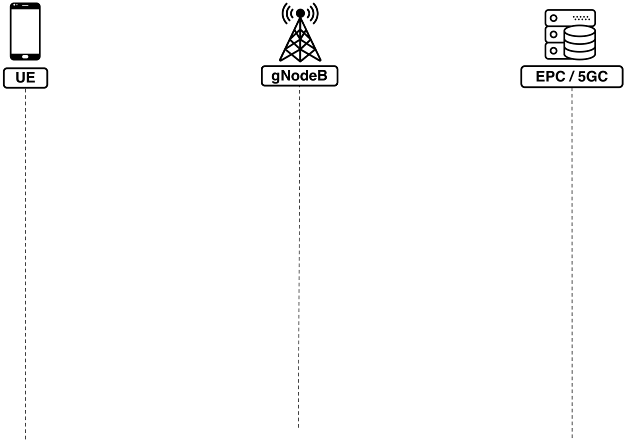
The vulnerable cellular network standard

Why 5G is not Secure

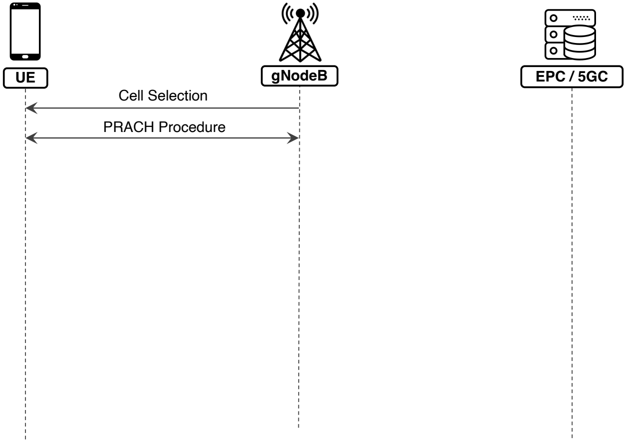
Why 5G is not Secure



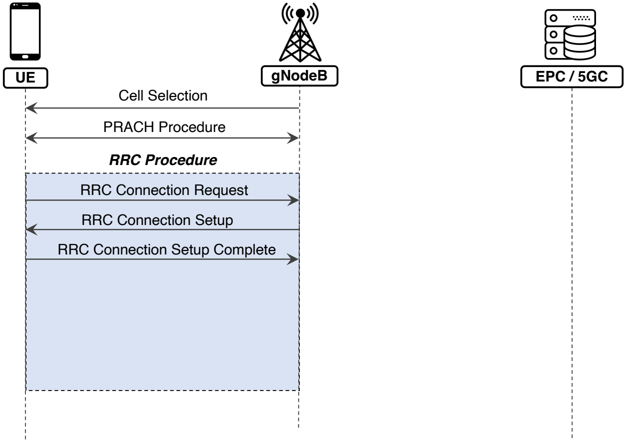
Why 5G is not Secure



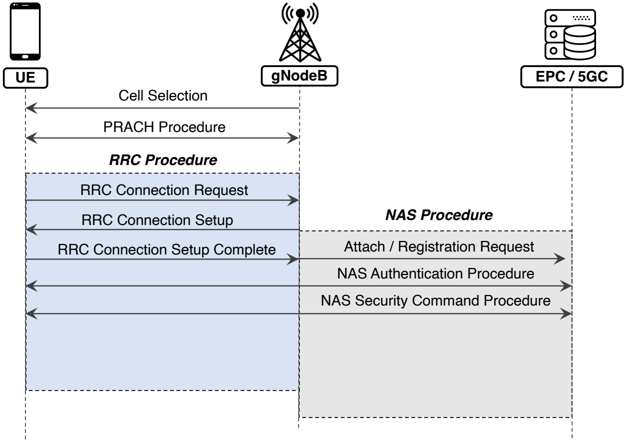
Why 5G is not Secure



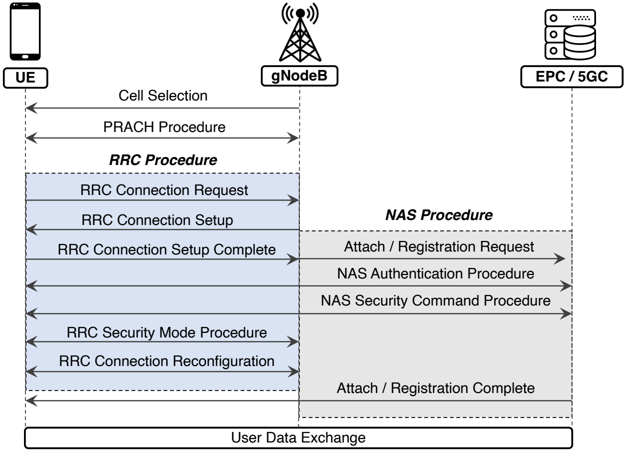
Why 5G is not Secure



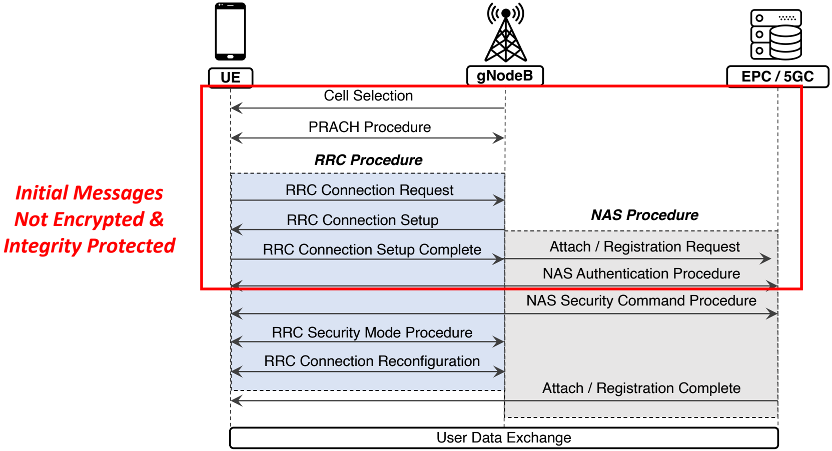
Why 5G is not Secure



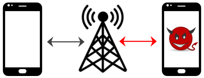
Why 5G is not Secure



Why 5G is not Secure

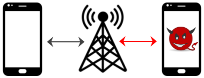


Threat Model

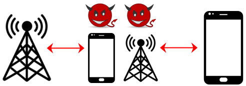


Adversary UEs

Threat Model

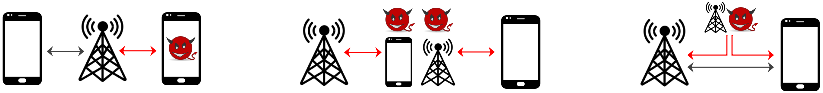


Adversary UEs



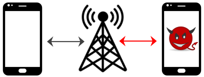
Man-In-the-Middle Attacker

Threat Model

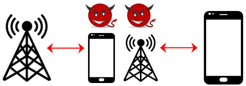


Adversary UEs *Man-In-the-Middle Attacker* *Signal Injector*

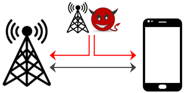
Threat Model



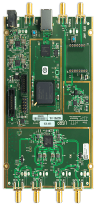
Adversary UEs



Man-In-the-Middle Attacker

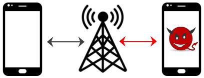


Signal Injector

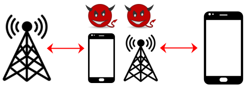


USRP B210
($2000)

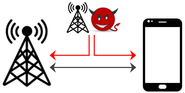
Threat Model



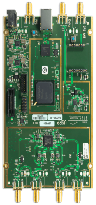
Adversary UEs



Man-In-the-Middle Attacker

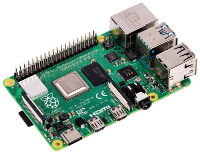


Signal Injector



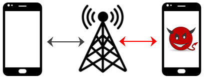
USRP B210
($2000)

+

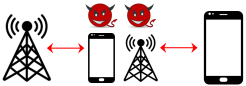


Raspberry Pi
($80)

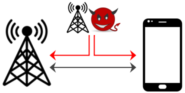
Threat Model



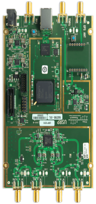
Adversary UEs



Man-In-the-Middle Attacker

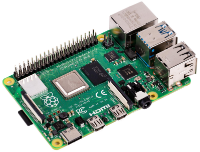


Signal Injector



USRP B210
($2000)

+



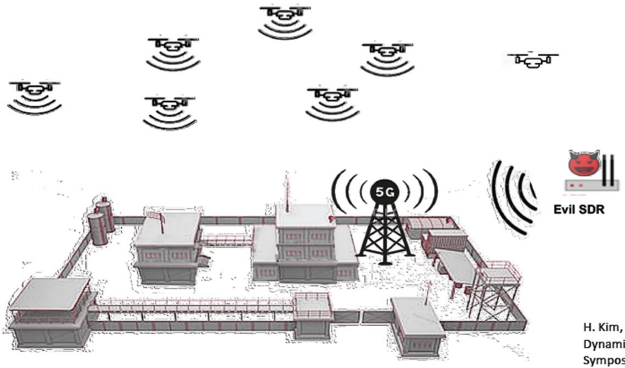
Raspberry Pi
($80)

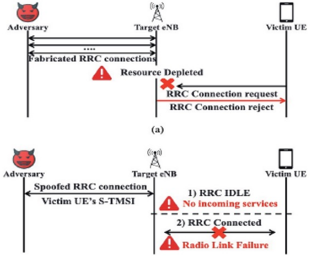
+

OpenAirInterface 5G
(Free)

Attack Scenarios

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

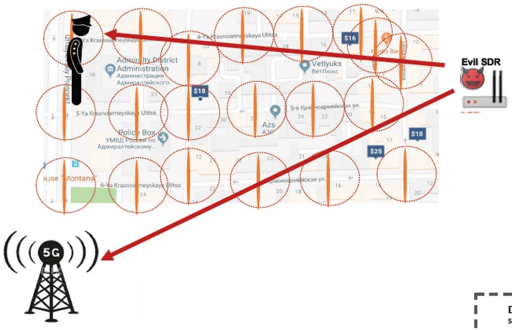




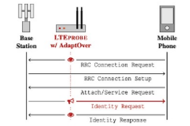
H. Kim, J. Lee, E. Lee and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," 2019 IEEE Symposium on Security and Privacy (SP), 2019.

Attack Scenarios

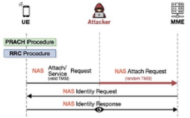
5G User Location Tracking Attack Scenario



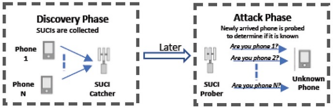
IMSI EXTRACTOR (DOWNLINK)



IMSI EXTRACTOR (UPLINK)



5G SUCI CATCHER



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
- ......

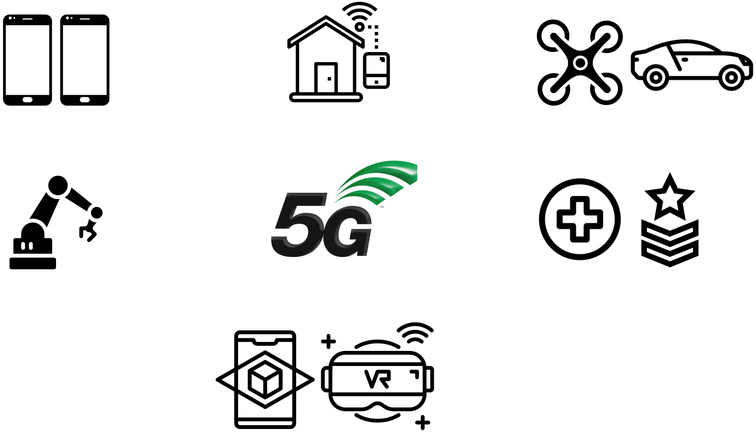
Attack Scenarios

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

~~Currently very challenging due to various concerns~~

How to defend against these attacks?

Our Key Insight: OpenRAN (O-RAN)



Our Key Insight: OpenRAN (O-RAN)

Our Key Insight: OpenRAN (O-RAN)

Our Key Insight: OpenRAN (O-RAN)

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

- Represent a new software-defined open cellular network architecture

Our Key Insight: OpenRAN (O-RAN)

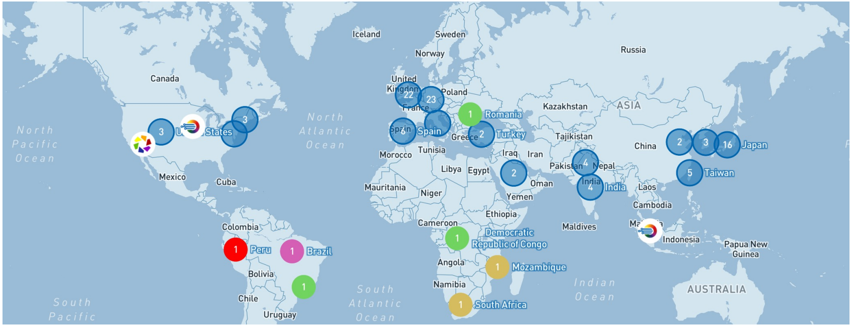
What is OpenRAN (O-RAN) [o-r]

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

Our Key Insight: OpenRAN (O-RAN)

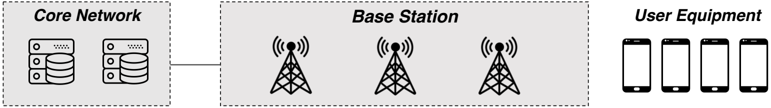
What is OpenRAN (O-RAN) [o-r]

- 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)



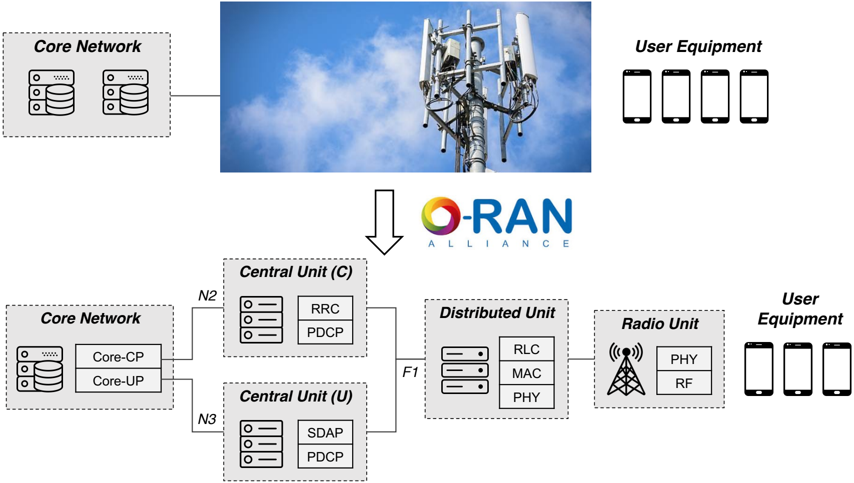
Deployments of O-RAN based technology and solutions from map.o-ran.org

Traditional RAN vs. Open RAN

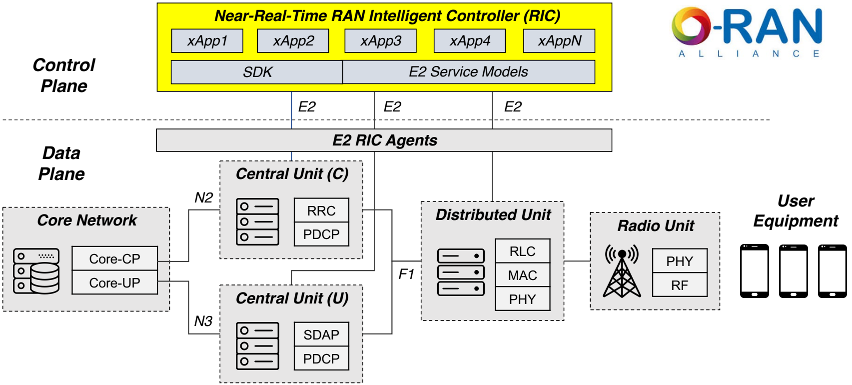


Traditional RAN vs. Open RAN

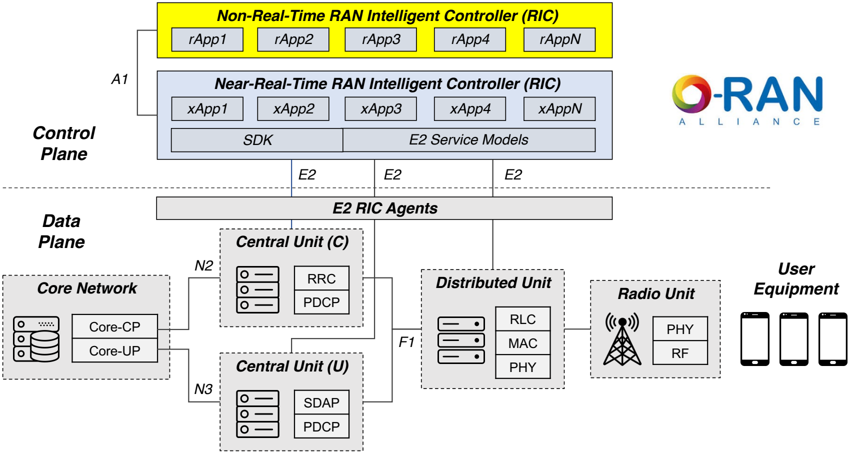
Traditional RAN vs. Open RAN



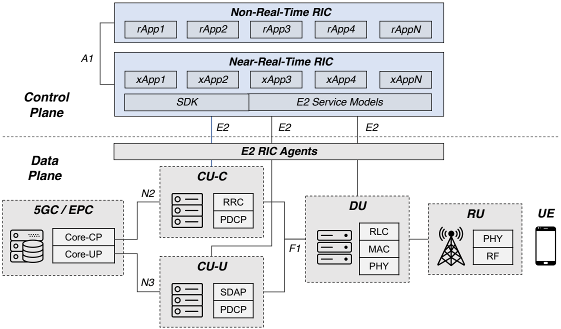
Traditional RAN vs. Open RAN



Traditional RAN vs. Open RAN



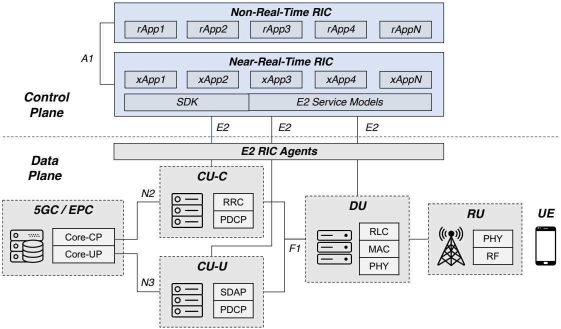
Traditional RAN vs. Open RAN



O-RAN's Key Capabilities

- Disaggregation

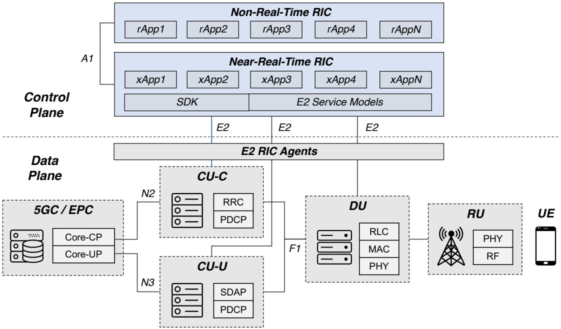
Traditional RAN vs. Open RAN



O-RAN's Key Capabilities

- Disaggregation
- Modularization (xApps / rApps)

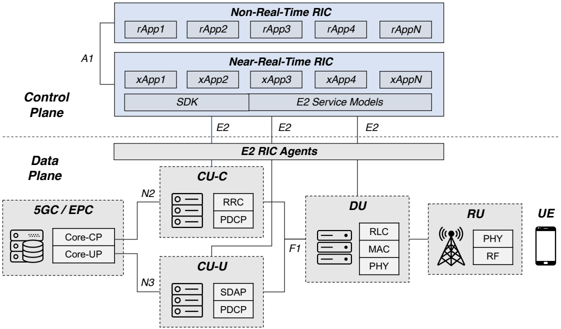
Traditional RAN vs. Open RAN



O-RAN's Key Capabilities

- Disaggregation
- Modularization (xApps / rApps)
- Interoperability

Traditional RAN vs. Open RAN



O-RAN's Key Capabilities

- Disaggregation
- Modularization (xApps / rApps)
- Interoperability
- Open Interfaces

Challenges and Solutions

Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security

Challenges and Solutions

Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security
- **Extensibility**: Extensible framework dealing with current and evolving attacks

Challenges and Solutions

Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security
- **Extensibility**: Extensible framework dealing with current and evolving attacks
- **Efficiency**: Capability to process data packets and produce alerts with low latency

Challenges and Solutions

Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security
- **Extensibility**: Extensible framework dealing with current and evolving attacks
- **Efficiency**: Capability to process data packets and produce alerts with low latency

5G-Spector Solutions

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

Challenges and Solutions

Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security
- **Extensibility**: Extensible framework dealing with current and evolving attacks
- **Efficiency**: Capability to process data packets and produce alerts with low latency

5G-Spector Solutions

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

Challenges and Solutions

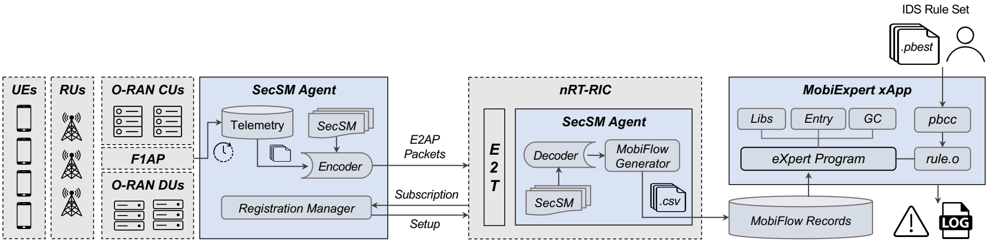
Challenges

- **Visibility**: Telemetry from existing O-RAN service models are insufficient for security
- **Extensibility**: Extensible framework dealing with current and evolving attacks
- **Efficiency**: Capability to process data packets and produce alerts with low latency

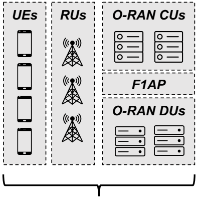
5G-Spector Solutions

- ✓ **MobiFlow** [WPYL22] 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



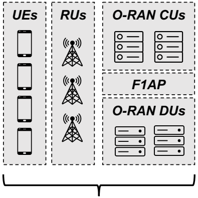
5G-Spector Design



RAN Data Plane

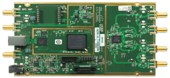
- Open-sourced UE and RAN implementations (LTE / 5G)
- Simulation or commodity SDRs

5G-Spector Design

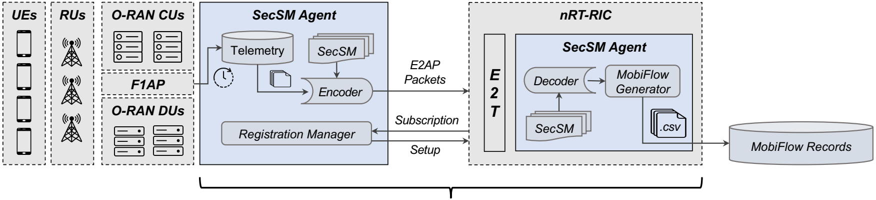


RAN Data Plane

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



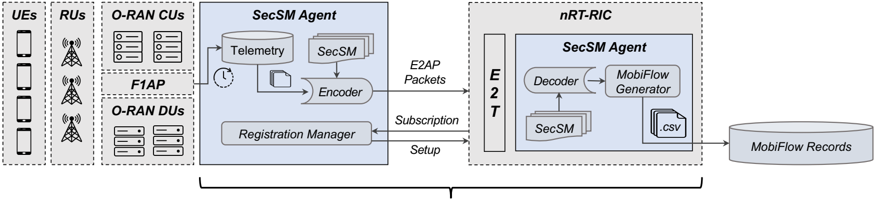
5G-Spector Design



5G-Spector Control Layer

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

5G-Spector Design



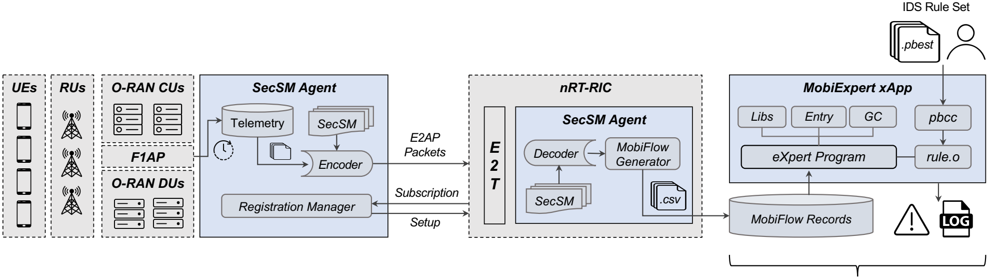
5G-Spector Control Layer

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

kubernetes

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	●	✓

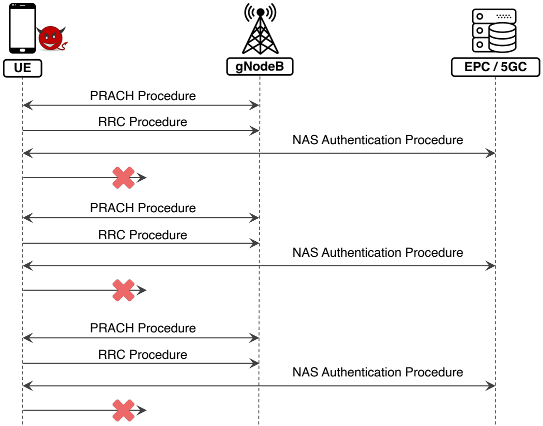
Table: All L3 cellular attacks and variants replicated and evaluated ($A \leftarrow B$ indicates message B overwrites A).

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).

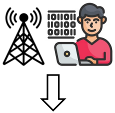
Evaluation w/ Simulated Attacks and Variants



BTS Resource Depletion Attack

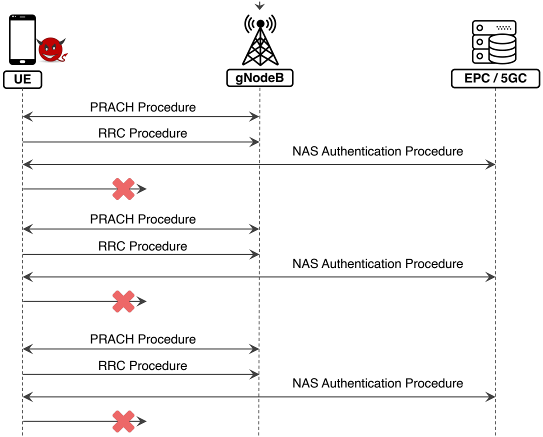
Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

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
    ]
```

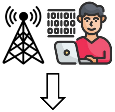
P-BEST IDS Signature in 5G-Spector



BTS Resource Depletion Attack

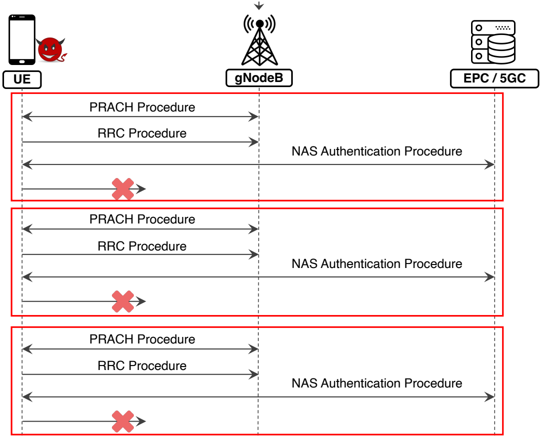
Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

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
    ]
```

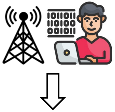
P-BEST IDS Signature in 5G-Spector



BTS Resource Depletion Attack

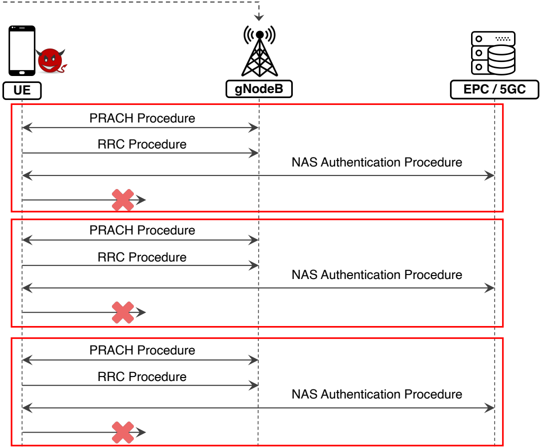
Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

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
    ]
```

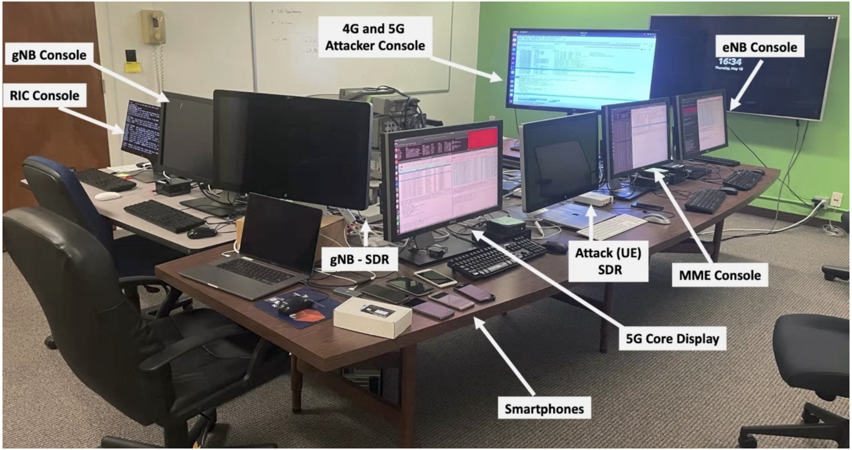
P-BEST IDS Signature in 5G-Spector



BTS Resource Depletion Attack

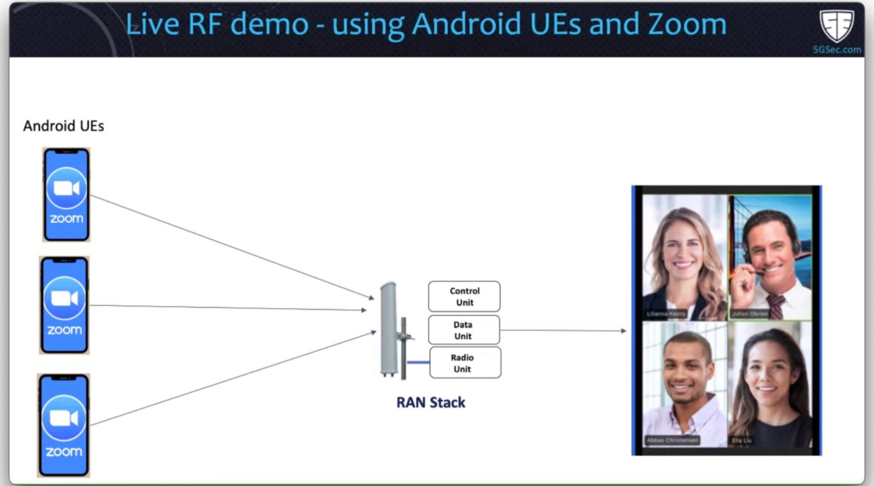
Kim et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane."

Evaluation w/ OTA Attacks

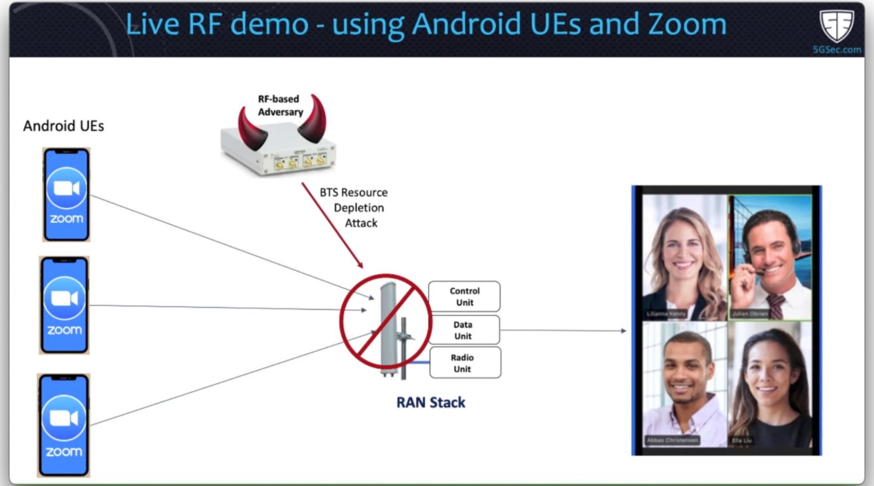


Our 5G Network Testbed at the Computer Science Lab of SRI International.

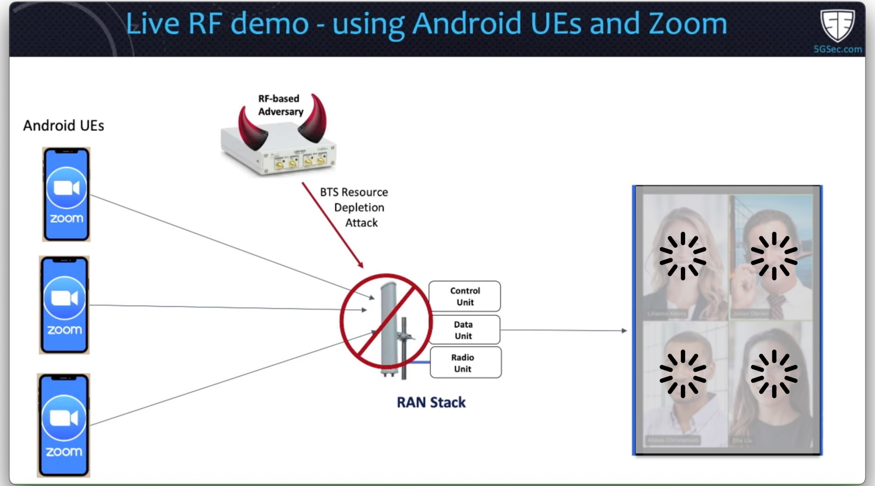
Evaluation w/ OTA Attacks



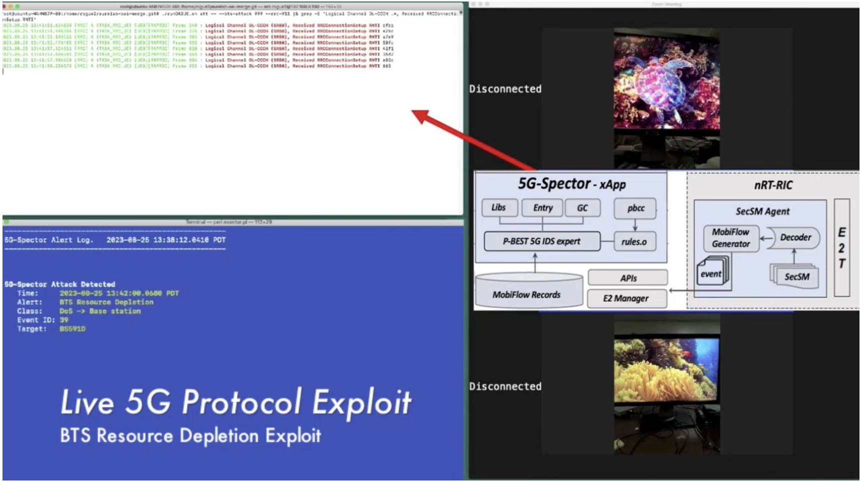
Evaluation w/ OTA Attacks



Evaluation w/ OTA Attacks



Evaluation w/ OTA Attacks



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

Evaluation w/ Real-World Datasets

Name	Ref	UE	Time(s)	#Pkt.	#MF	#Sess.	B	Event
BT-1	[LPY+16]	LG LS660	10,597	4,164	1,810	113	✓	0
BT-2	[LPY+16]	LG G3 VS985	514	3,803	173	15	✓	0
BT-3	[LPY+16]	LG G3 VS985	489	3,766	158	15	✓	0
BT-4	[LPY+16]	Galaxy S5	764	2,996	154	13	✓	0
BT-5	[LPY+16]	LG G3 VS985	16,324	26,548	1,217	114	✓	0
BT-6	[LPY+16]	Galaxy S5	1,459	2,803	97	13	✓	0
BT-7	[LPY+16]	Galaxy S5	2,053	4,794	448	27	✓	0
BT-8	[LPY+16]	Galaxy S5	6,387	2,839	1,435	113	✓	0
			......					
AT-1	[EAW+]	N/A	1	632	61	11	✗	0
AT-2	[EAW+]	N/A	1	482	53	8	✗	0
AT-3	[EAW+]	N/A	1	626	59	6	✗	0
			......					

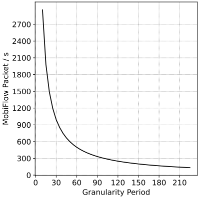
Table: Evaluation results using real-world benign cellular traffic.

Evaluation w/ Real-World Datasets

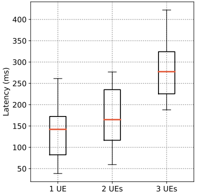
Name	Ref	UE	Time(s)	#Pkt.	#MF	#Sess.	B	Event
BT-1	[LPY+16]	LG LS660	10,597	4,164	1,810	113	✓	0
BT-2	[LPY+16]	LG G3 VS985	514	3,803	173	15	✓	0
BT-3	[LPY+16]	LG G3 VS985	489	3,766	158	15	✓	0
BT-4	[LPY+16]	Galaxy S5	764	2,996	154	13	✓	0
BT-5	[LPY+16]	LG G3 VS985	16,324	26,548	1,217	114	✓	0
BT-6	[LPY+16]	Galaxy S5	1,459	2,803	97	13	✓	0
BT-7	[LPY+16]	Galaxy S5	2,053	4,794	448	27	✓	0
BT-8	[LPY+16]	Galaxy S5	6,387	2,839	1,435	113	✓	0
			......					
AT-1	[EAW+]	N/A	1	632	61	11	✗	0
AT-2	[EAW+]	N/A	1	482	53	8	✗	0
AT-3	[EAW+]	N/A	1	626	59	6	✗	0
			......					

Table: Evaluation results using real-world benign cellular traffic.

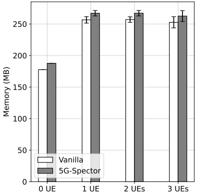
Evaluation of Performance and Overhead



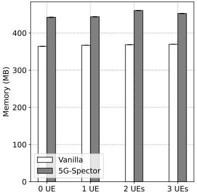
(a) Throughput.



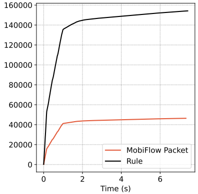
(b) Latency.



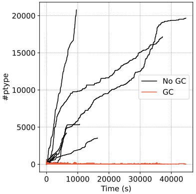
(a) RAN MEM.



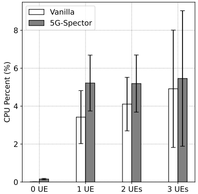
(b) RIC MEM.



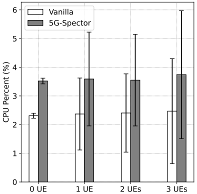
(c) Speed.



(d) GC Performance.

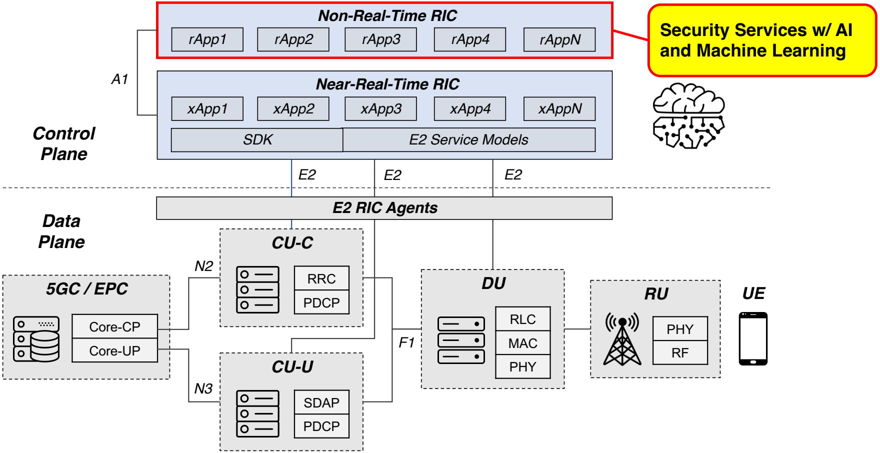


(c) RAN CPU.

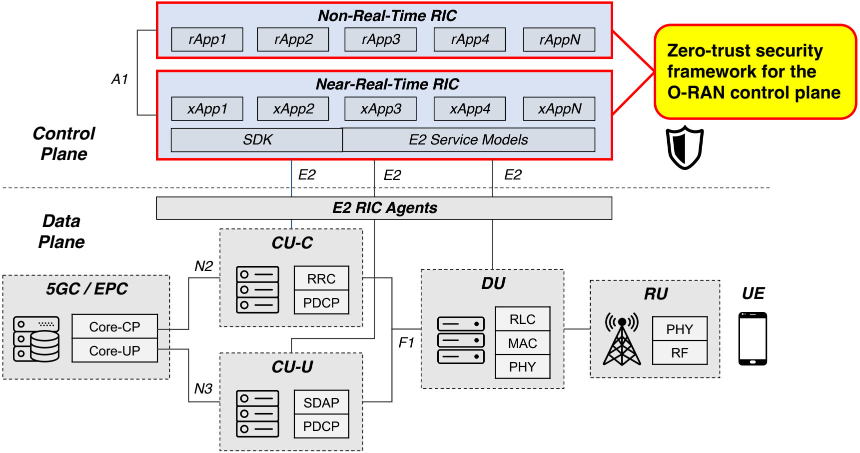


(d) RIC CPU.

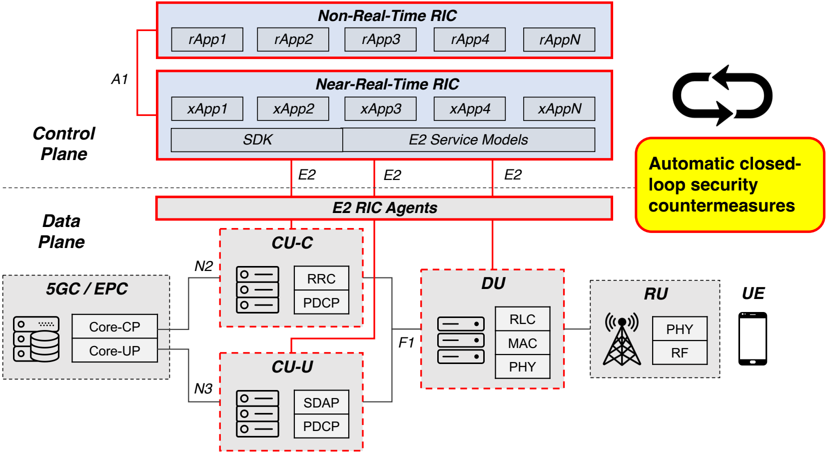
Future Work


Non-Real-Time RIC
rApp1
rApp2
rApp3
rApp4
rAppN
Security Services w/ AI and Machine Learning
A1
Near-Real-Time RIC
xApp1
xApp2
xApp3
xApp4
xAppN
SDK
E2 Service Models
Control Plane
E2
E2
E2
E2 RIC Agents
Data Plane
CU-C
RRC
PDCP
N2
5GC / EPC
Core-CP
Core-UP
N3
CU-U
SDAP
PDCP
F1
DU
RLC
MAC
PHY
RU
PHY
RF
UE

Future Work


Non-Real-Time RIC
rApp1
rApp2
rApp3
rApp4
rAppN
A1
Near-Real-Time RIC
xApp1
xApp2
xApp3
xApp4
xAppN
SDK
E2 Service Models
Zero-trust security framework for the O-RAN control plane
Control Plane
E2
E2
E2
E2 RIC Agents
Data Plane
CU-C
RRC
PDCP
N2
5GC / EPC
Core-CP
Core-UP
N3
CU-U
SDAP
PDCP
F1
DU
RLC
MAC
PHY
RU
PHY
RF
UE

Future Work


Non-Real-Time RIC
rApp1
rApp2
rApp3
rApp4
rAppN
A1
Near-Real-Time RIC
xApp1
xApp2
xApp3
xApp4
xAppN
SDK
E2 Service Models
Control Plane
E2
E2
E2
E2 RIC Agents
Data Plane
CU-C
RRC
PDCP
N2
5GC / EPC
Core-CP
Core-UP
N3
CU-U
SDAP
PDCP
F1
DU
RLC
MAC
PHY
RU
PHY
RF
UE
Automatic closed-loop security countermeasures

Thank You

5Gsec.com

SE-RAN

Security Enhanced Radio Access Network

Thank You

5Gsec.com

SE-RAN
Security Enhanced
Radio Access Network

Artifact Evaluated NDSS Symposium
Available
Functional
Reproduced

Paper QR Code

5G-Spector Full paper (NDSS'24): https://web.cse.ohio-state.edu/~wen.423/papers/5G-Spector-NDSS24.pdf

5G-Spector Source Code: https://github.com/5GSEC/5G-Spector

5G-Spector Demo Video: https://www.5gsec.com/post/5g-spector-demo

My personal homepage: https://web.cse.ohio-state.edu/~wen.423/

References I

- Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M Fareed Arif, Syed Rafiul Hussain, and Omar Chowdhury, *Phoenix: Device-centric cellular network protocol monitoring using runtime verification*.
- 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.
- Yuanjie Li, Chunyi Peng, Zengwen Yuan, Jiayao Li, Haotian Deng, and Tao Wang, *Mobileinsight: Extracting and analyzing cellular network information on smartphones*, Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, 2016, pp. 202–215.
- *O-ran alliance*, https://www.o-ran.org/.
- 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.