CENTER FOR
CYBER SECURITY

CSP-lab
Cyber Security and Privacy Lab

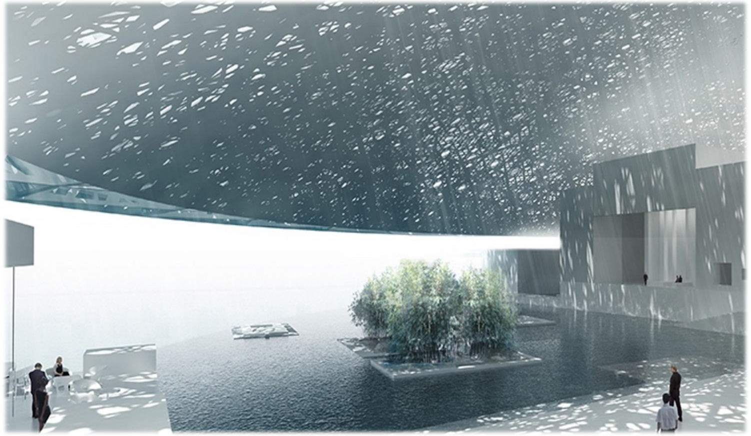
جامعة نيويورك أبوظبي
NYU | ABU DHABI

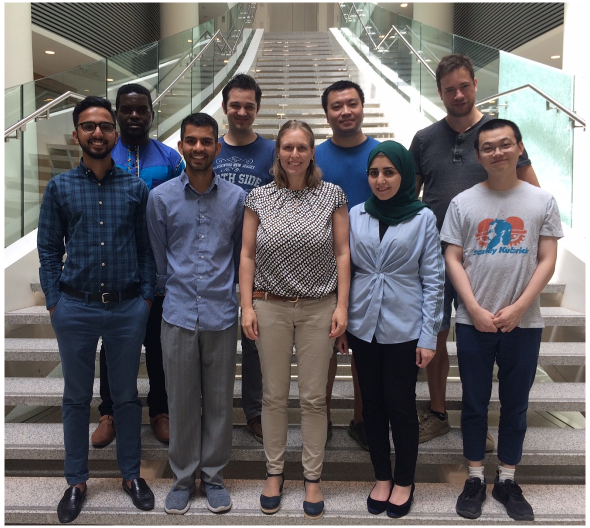
Securing Cellular Networks: Academic Challenges from 5G to Next-Generation Systems

Christina Pöpper, **New York University Abu Dhabi**

Dec 11, 2024

About





About

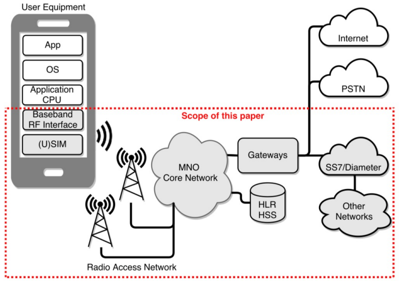
جامعة نيويورك أبوظبي
NYU ABU DHABI

CENTER FOR
CYBER SECURITY

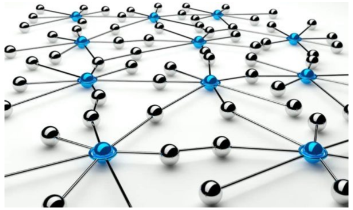
- Associate Professor of Computer Science at NYUAD, Ph.D. from ETH Zurich
  - Program Head of Computer Science at NYUAD since 2023
  - Director of Research at Center of Cybersecurity at NYUAD since 2019
  - Leading the Cyber Security & Privacy (CSP) Lab since 2016
- 18 years of research experience in **cyber security** and **wireless security**
  - ~10 years of in **mobile/cellular security**

CSP-lab
Cyber Security and Privacy Lab

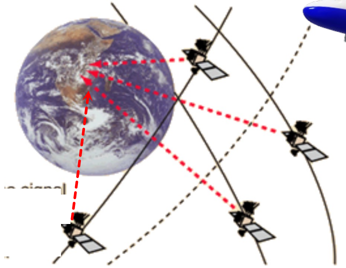
Mobile/Cellular Network Security



Anonymity & Privacy



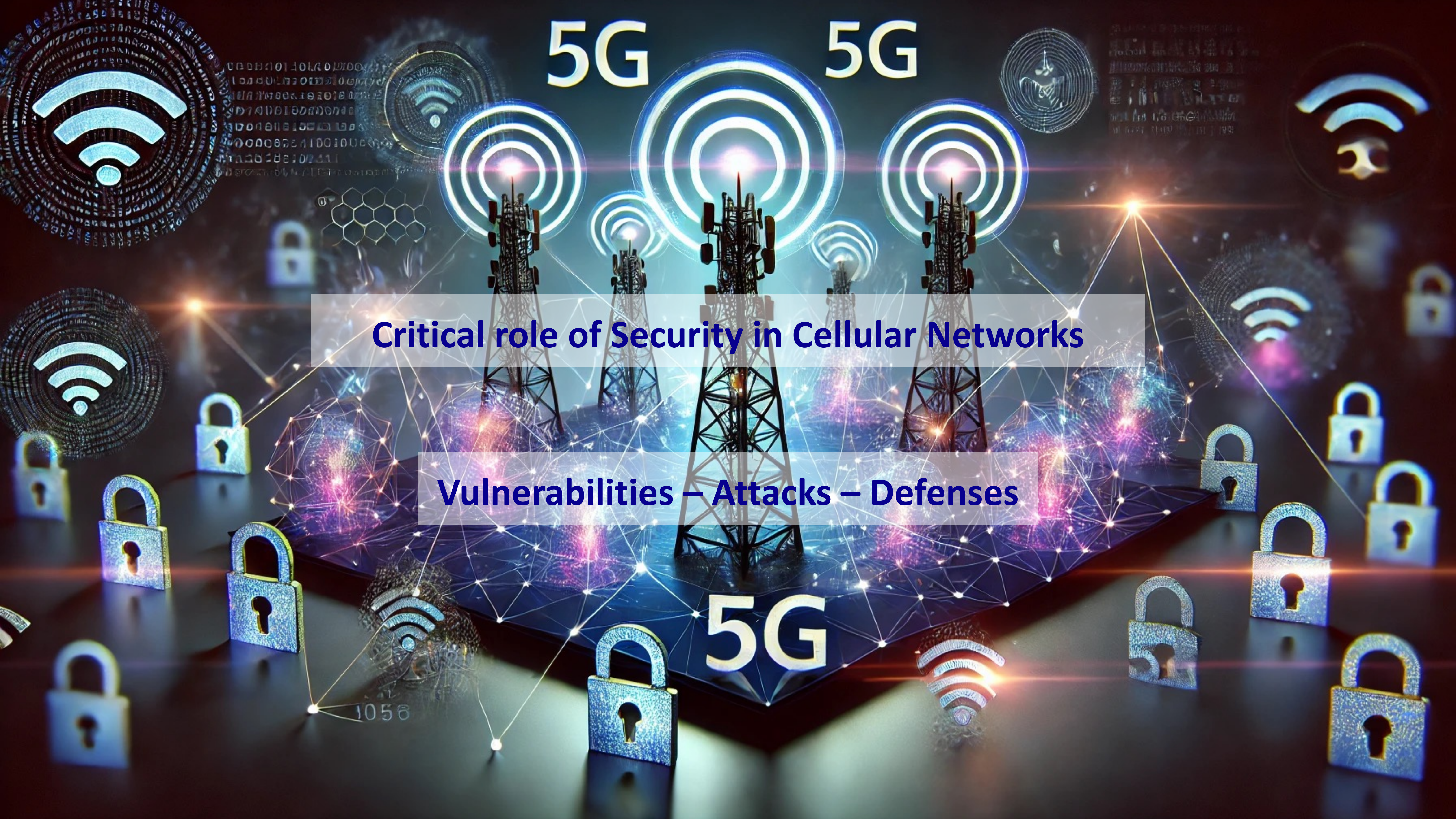
Secure Localization & Aviation



NextGEN ADS-B

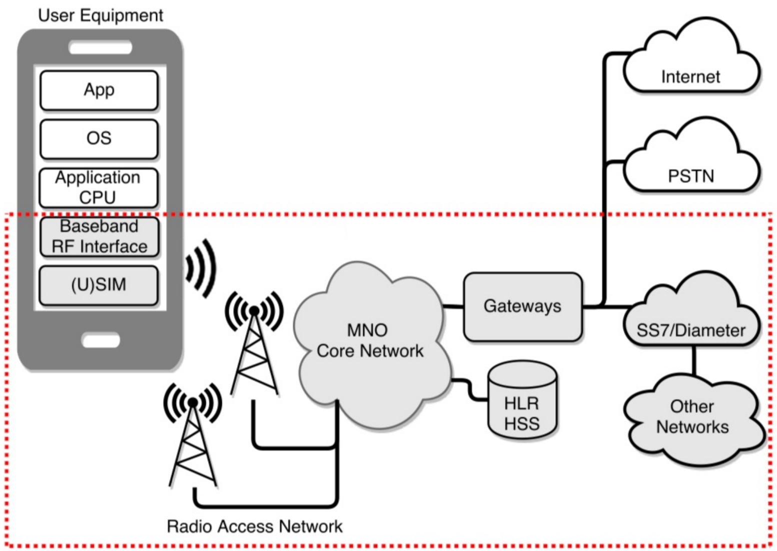
Critical role of Security in Cellular Networks

Vulnerabilities – Attacks – Defenses

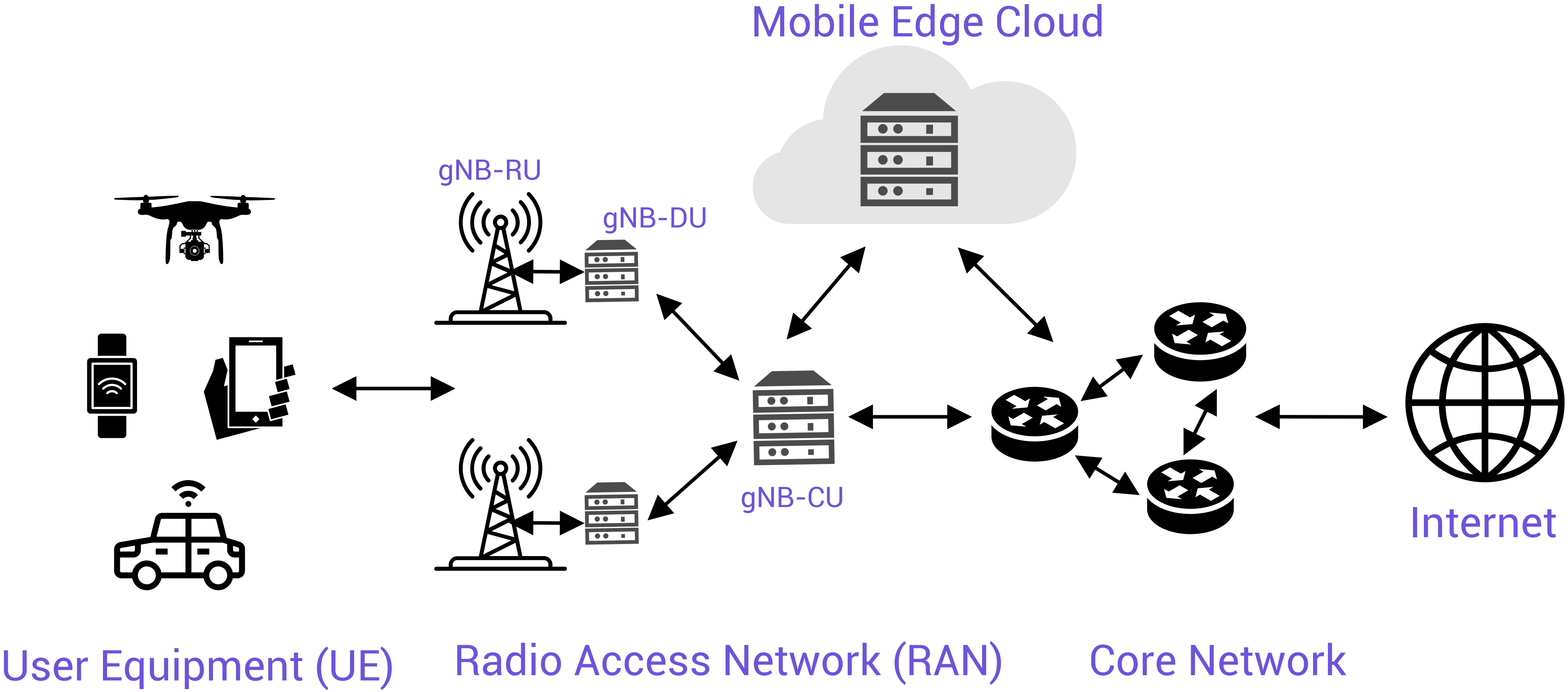


Cellular Network Security

Mobile/Cellular Network Security



Cellular Networks



Mobile Edge Cloud

gNB-RU

gNB-DU

gNB-CU

Internet

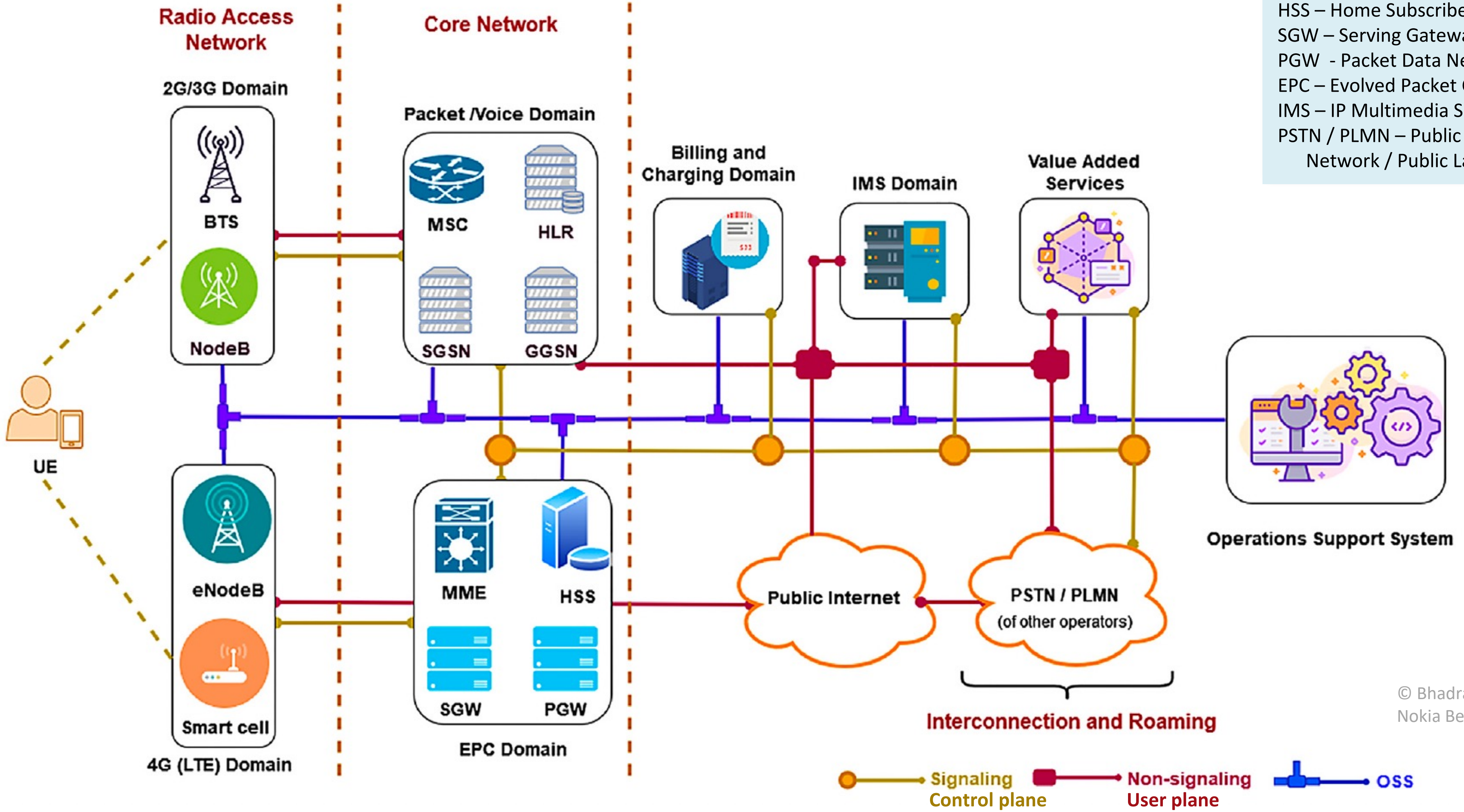
User Equipment (UE)

Radio Access Network (RAN)

Core Network

Cellular Network Topology

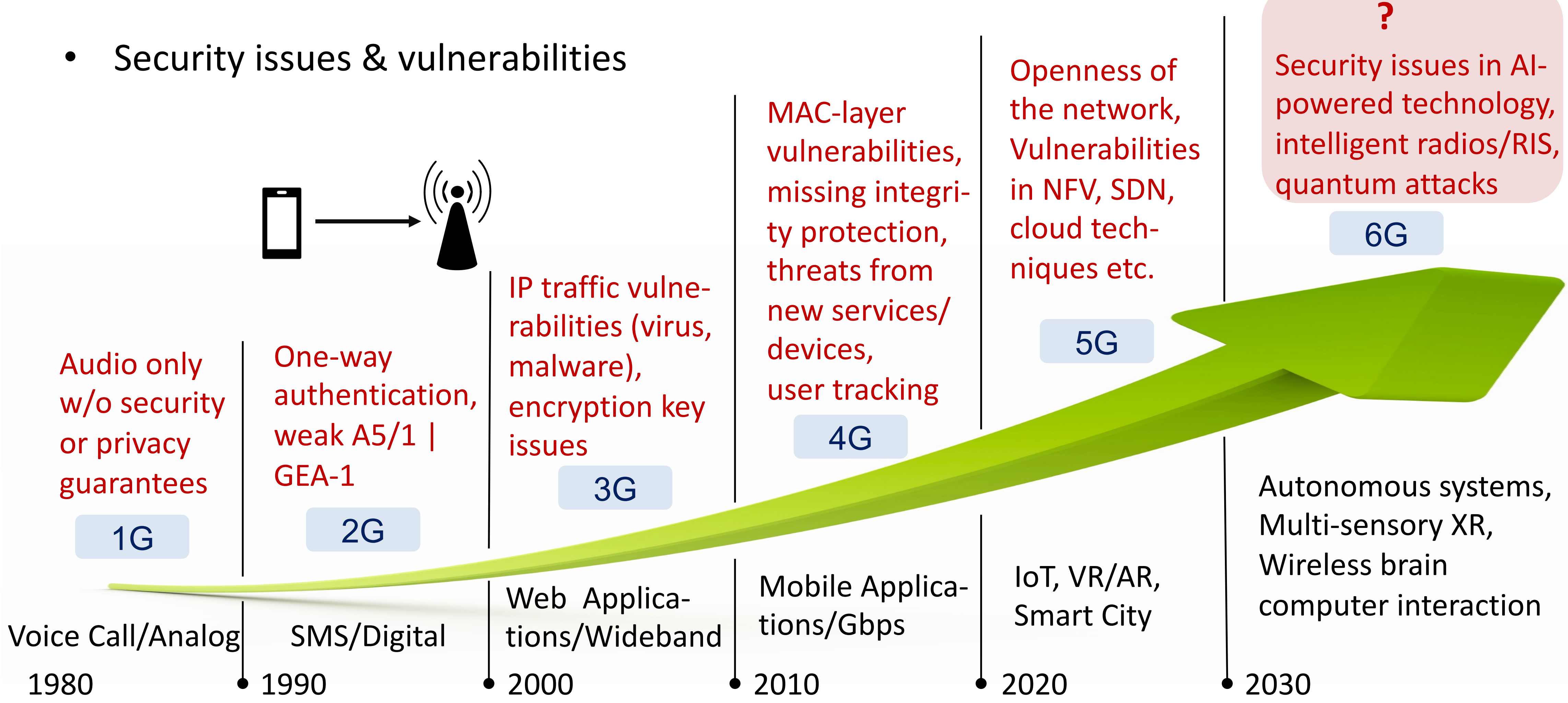
MSC – Mobile Switching Center
HLR – Home Location Register
SGSN – Serving GPRS Support Mode
GGSN – Gateway GPRS Support Mode
MME – Mobility Management Entity
HSS – Home Subscriber Server
SGW – Serving Gateway
PGW - Packet Data Network Gateway
EPC – Evolved Packet Core
IMS – IP Multimedia Subsystem
PSTN / PLMN – Public Switched Telephone Network / Public Land Mobile Network



© Bhadra Framework, Nokia Bell Labs 2022

Security in Cellular Networks – A Quick Pass through the Generations

- Security issues & vulnerabilities



1G

Audio only w/o security or privacy guarantees

Voice Call/Analog

1980

2G

One-way authentication, weak A5/1 | GEA-1

SMS/Digital

1990

3G

IP traffic vulnerabilities (virus, malware), encryption key issues

Web Applications/Wideband

2000

4G

MAC-layer vulnerabilities, missing integrity protection, threats from new services/ devices, user tracking

Mobile Applications/Gbps

2010

5G

Openness of the network, Vulnerabilities in NFV, SDN, cloud techniques etc.

IoT, VR/AR, Smart City

2020

6G

?

Security issues in AI-powered technology, intelligent radios/RIS, quantum attacks

Autonomous systems, Multi-sensory XR, Wireless brain computer interaction

2030

Security Requirements (5G)

Mitigation of downgrading attacks

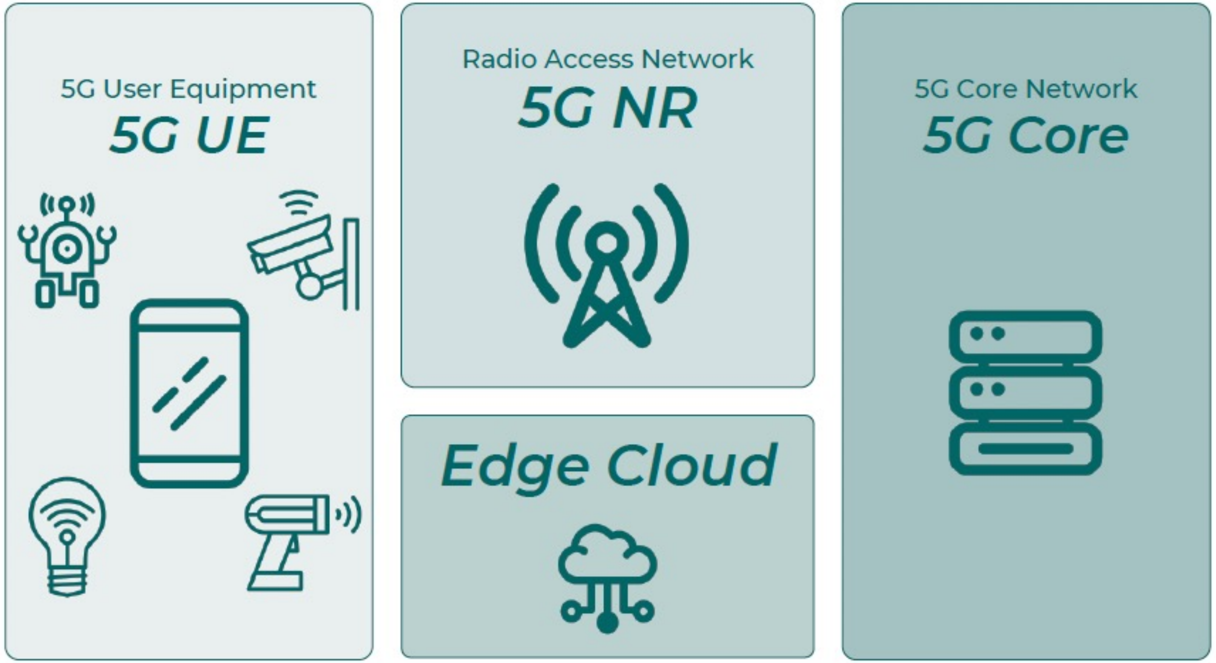
4G → 3G

Mutual Authentications

Traffic Confidentiality

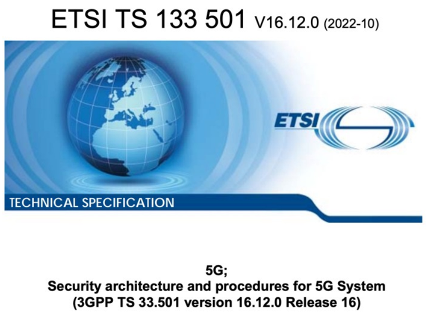
Signaling Integrity

Identity & Location Privacy



Source: wenovator

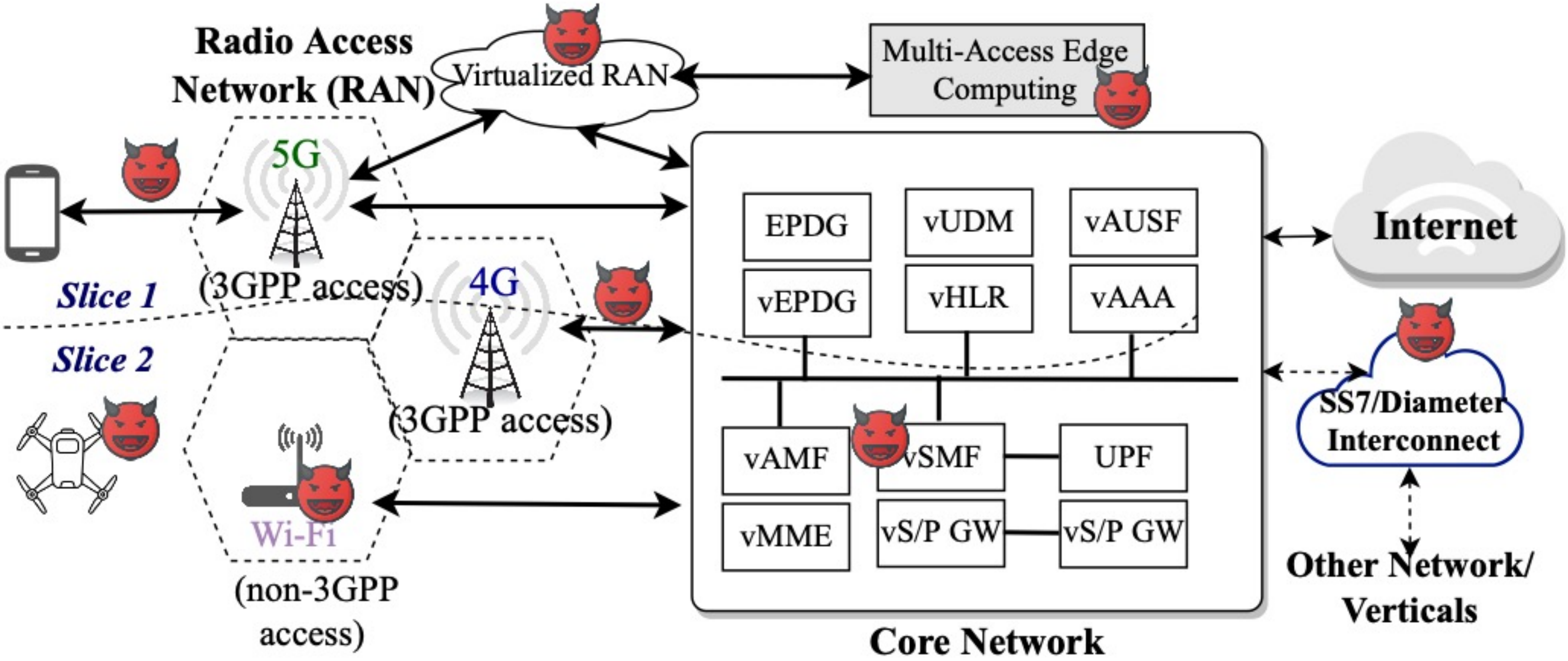
Secure storage & processing of subscription credentials


ETSI TS 133 501 V16.12.0 (2022-10)

TECHNICAL SPECIFICATION

5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 16.12.0 Release 16)

Threat Landscape on Cellular Networks

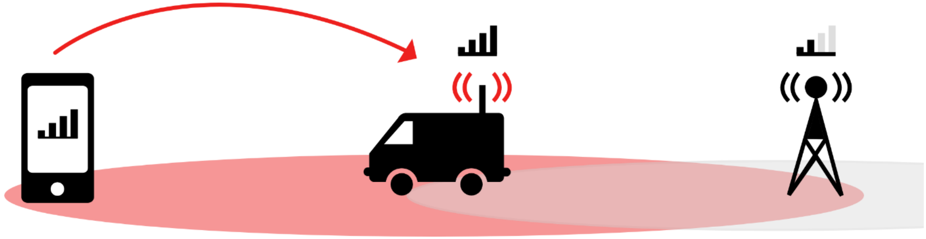


© Syed Rafiul Hussein

Attacks on Cellular Networks

Radio-layer Attacks on Cellular Networks

- Jamming | DoS | Downgrading
- IMSI catchers | Stingrays | False Base Stations | Cell Site Simulators



Categories of attacks:

- Denial of service & Service downgrading
- Presence testing & Location tracking
- Communication interception (2G/3G)

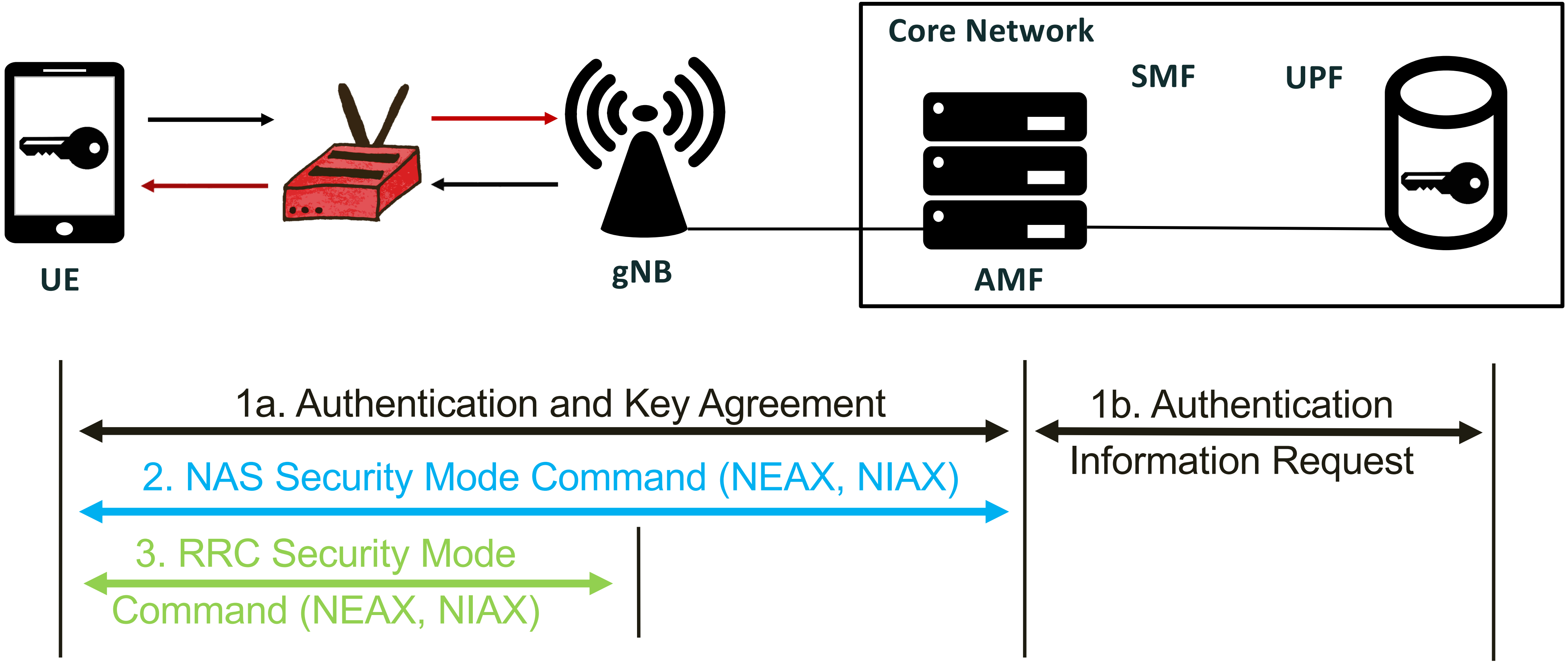
Higher-layer Attacks on Cellular Networks

- Phishing, Smishing, Spamming
- RoboCalls, Silent SMS
- Malware (Simjacker, WibAttack), Viruses (Flubot)
- Potential of AI/ML attacks

Categories of attacks:

- Targeting mobile users
- Targeting mobile apps
- Targeting mobile devices
- Targeting network/core/ operator

Types of MITM/Relay Cellular Attackers



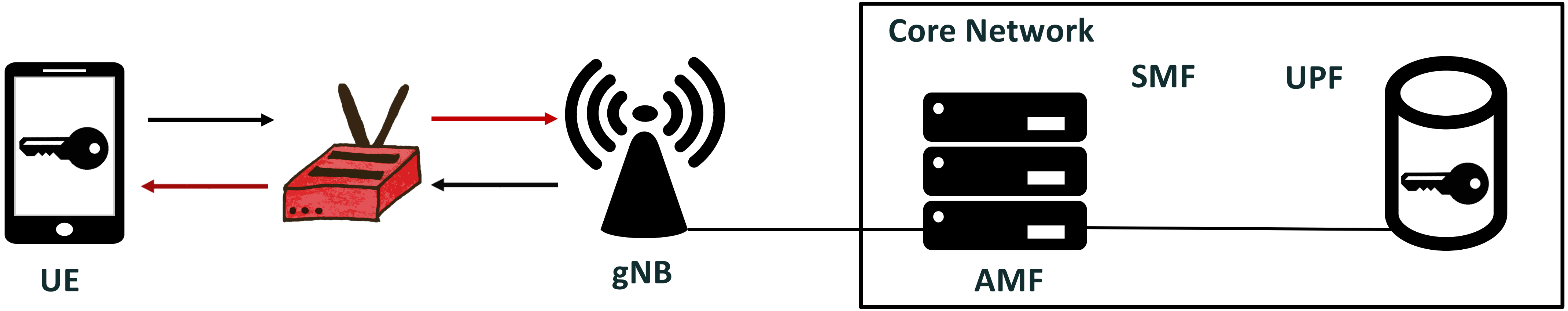
1a. Authentication and Key Agreement

1b. Authentication Information Request

2. NAS Security Mode Command (NEAX, NIAX)

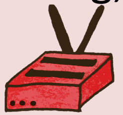
3. RRC Security Mode Command (NEAX, NIAX)

Types of MITM/Relay Cellular Attackers



1) Repeater/Forwarder
(on the PHY-layer)
→ boosting signal strength

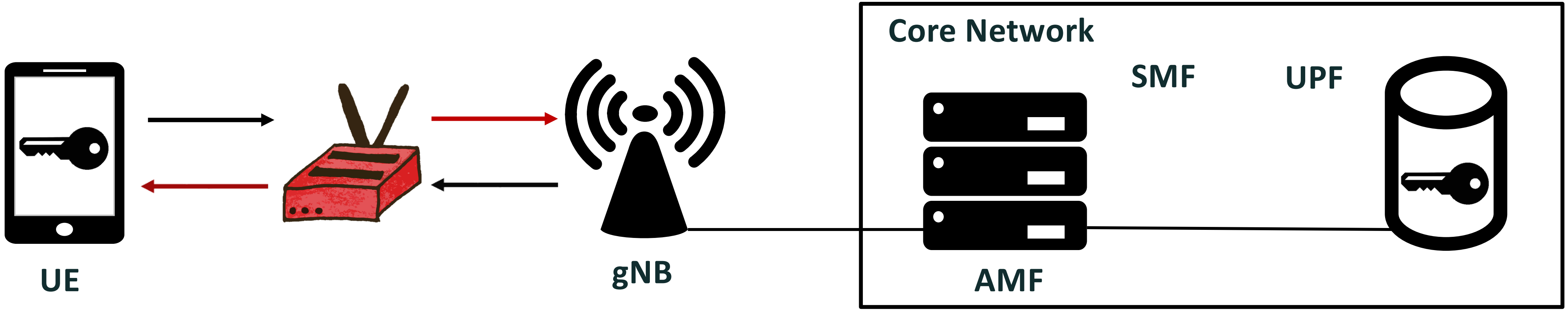
- Leaking plaintext identities, payload (2G-3G)
- Fingerprinting of user activities (browsing, videos)

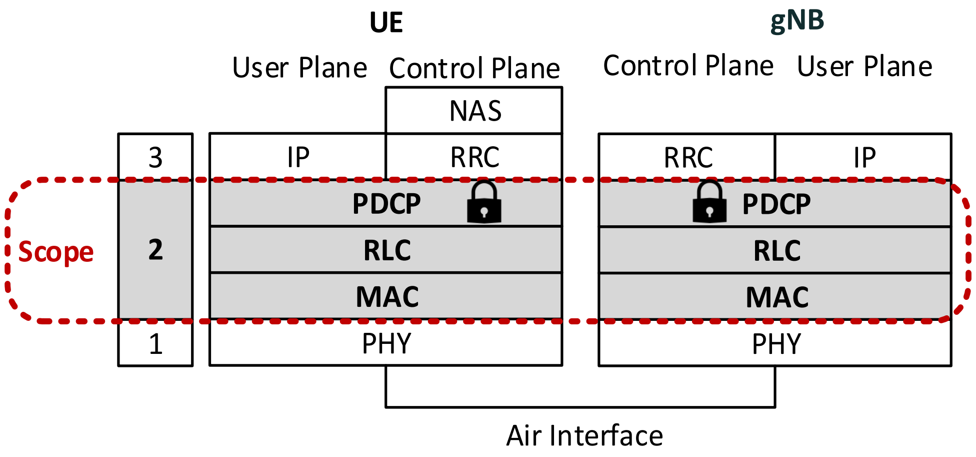


Rupprecht, Kohls, Holz, Pöpper: **Breaking LTE on Layer Two** IEEE S&P, 2019 (**aLTEr**)

Rupprecht, Kohls, Holz, Pöpper: **IMP4GT: IMPersonation Attacks in 4G NeTworks,** NDSS, 2020

Types of MITM/Relay Cellular Attackers





1) Repeater/Forwarder (on the PHY-layer)
   → boosting signal strength

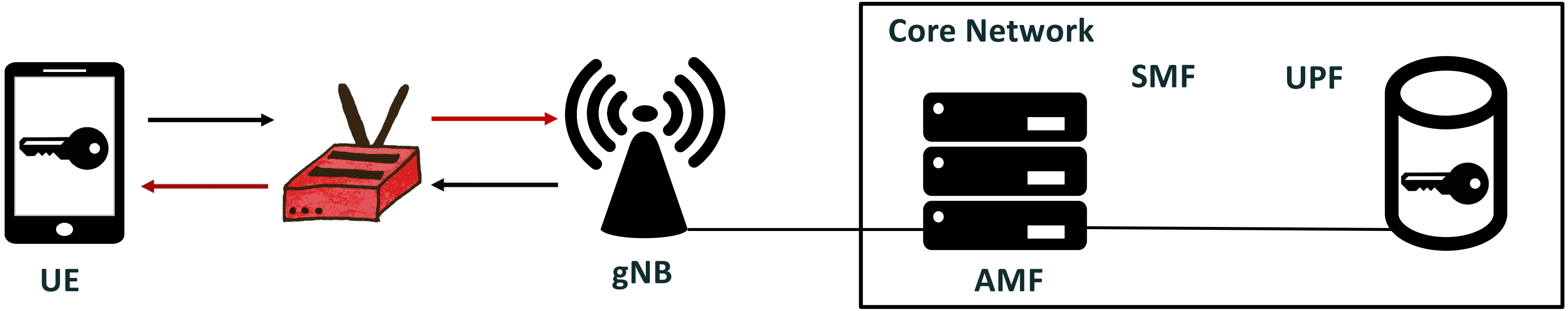
2) Relay (on the MAC-layer)
   → signals to bits, (de)modulation, connections, forwarding on PDCP/RRC layers

- Tampering with packets, recover data
- Impersonate users (in 4G or if user-plane traffic is not integrity-protected)

Types of MITM/Relay Cellular Attackers

Rupprecht, Kohls, Holz, Pöpper: **Breaking LTE on Layer Two**
IEEE S&P, 2019 (**aLTEr**)

Rupprecht, Kohls, Holz, Pöpper: **IMP4GT: IMPersonation Attacks in 4G NeTworks,** NDSS, 2020



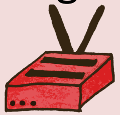
AdaptOver (LTE & 5G-NSA, 2022):

- decode, overshadow & inject arbitrary messages over the air in up- and downlink direction between network and UE

1) Repeater/Forwarder (on the PHY-layer)
→ boosting signal strength

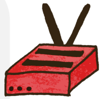
2) Relay (on the MAC-layer)
→ signals to bits, (de)modulation, connections, forwarding on PDCP/RRC layers

- Tampering with packets, recover data
- Impersonate users (in 4G or if user-plane traffic is not integrity-protected)



Exemplary Security Enhancements from 4G to 5G

Issue	4G	5G Enhancement	Mitigated Threat
Confidentiality & Integrity Protect.	*Control Layer*: Encryption & Integrity Protection *User Plane*: Encryption	+ Mandatory support for User Plane Integrity Protection	If used: Prevention of tampering with user data (aLTEr/IMP4GT-like attacks)
Subscriber Privacy	SUPI sent in plaintext No guidelines for updating temp. identities (GUTI)	SUPI → SUCI concealment Well defined timing of 5G-GUTI redistribution	Large-scale IMSI-catchers, location exposure, user tracking
NAS Security	Initial NAS messages are sent in plaintext	Confidentiality protection of initial NAS messages	Network spoofing, message hijacking, DoS attacks

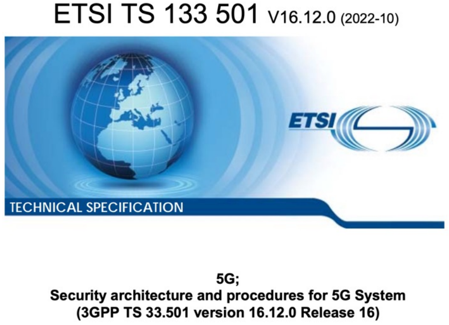


https://www.gsma.com/security/securing-the-5g-era/

Cellular Network Entities and Development Phases

Specification → Implementation → Deployment

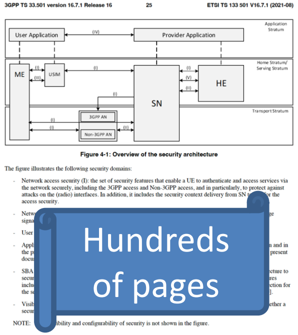
Specification & Standarization Bodies



ETSI TS 133 501 V16.12.0 (2022-10)

TECHNICAL SPECIFICATION

5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 16.12.0 Release 16)



3GPP TS 33.501 version 16.7.1 Release 16 25 ETSI TS 133 501 V16.7.1 (2021-08)

Figure 4-1: Overview of the security architecture

The figure illustrates the following security domains:

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN t for the access security.

NOTE: ibility and configurability of security is not shown in the figure.

Hundreds of pages

Vendors

NOKIA

HUAWEI

CISCO

Qualcomm

ERICSSON

Network Operators

T · ·

GSMA

Telefónica | O₂

etisalat

vodafone

du

Our Research Contributions

Specification → **Implementation** → **Deployment**

aLTEr-Attacks: Breaking LTE on Layer Two IEEE S&P'19

IMP4GT: IMPersonation Attacks in 4G NeTworks NDSS'20

Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE USENIX Sec'20

LTE Security Disabled – Misconfiguration in Commercial Networks ACM WiSec'19

Freaky Leaky SMS: FREAKYLEAKS Extracting User Locations by Analyzing SMS Timings USENIX-Sec'23 + WOOT'24

4G/LTE

5G/NR

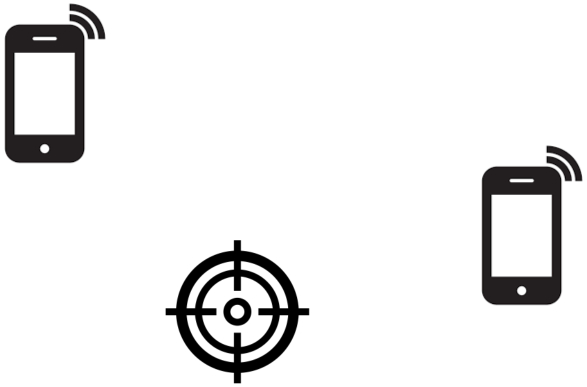
Don't hand it Over: Vulnerabilities in 5G Handover Procedures ACSAC'21

ASTRA-5G: Automated OtA Security Testing for 5G UEs ACM WiSec'23+24

5G SUCI-Catchers: Still catching them all? ACM WiSec'21

Abusing 5G's Warning and Emergency Systems ACSAC'22

Logos: © Katharina Kohls

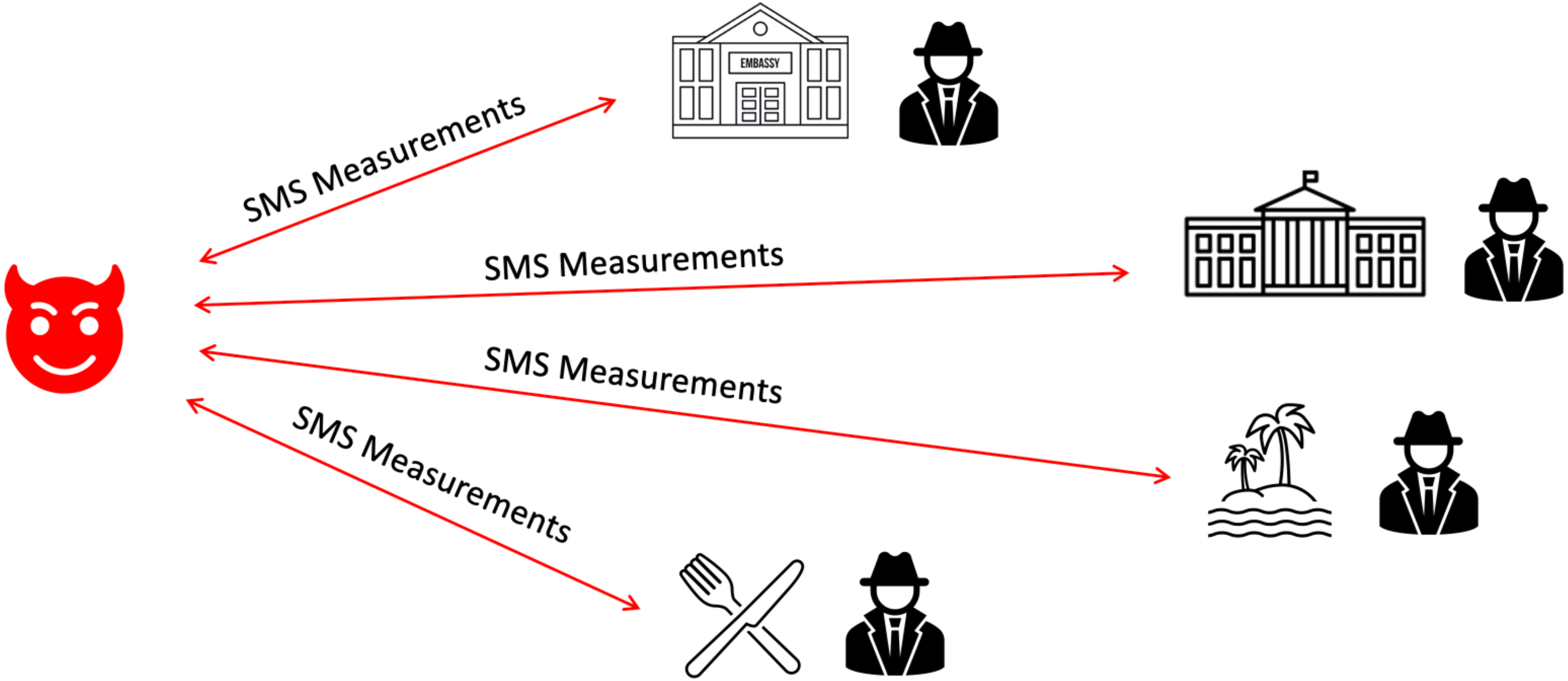


Freaky Leaky SMS –
An Attack on Location Privacy

Collaboration with Evangelos Bitsikas, Theodor Schnitzler, & Aanjhan Ranganathan

Let’s Consider the Following Scenario

Tracking the diplomat to routinely locations



Let’s Consider the Following Scenario

Can we infer the location of a victim by simply sending SMS messages?

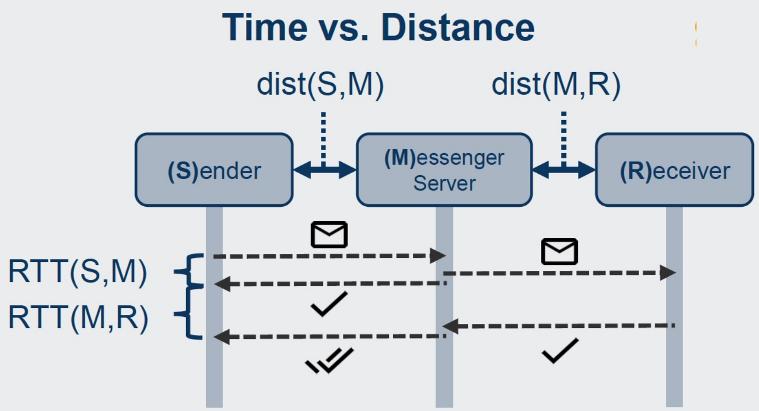
Steps of the attack:

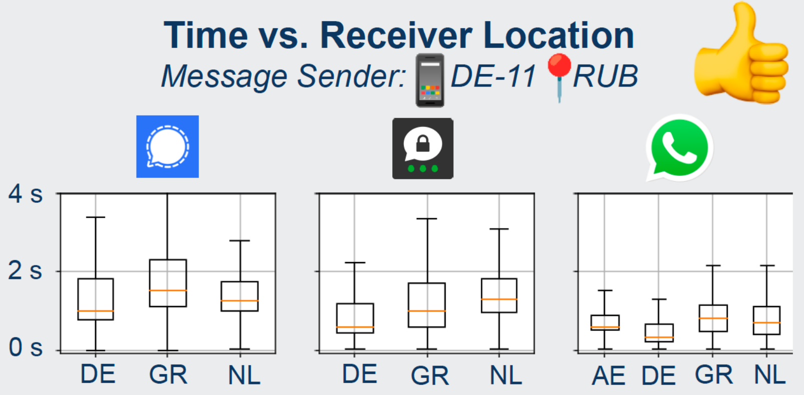
1. Know routine locations and mobile number of the victim.
2. Send silent SMSs and receive acknowledgements and delivery reports.
3. Use the SMS timings to generate fingerprints per location.
4. Use the fingerprints to predict the location of the victim using ML.

Localizing Users based on 5G SMS Delivery Reports

NDSS'23

Hope of delivery: Extracting User Locations from Mobile Instant Messengers. Theodor Schnitzler et al.


Time vs. Distance


Time vs. Receiver Location

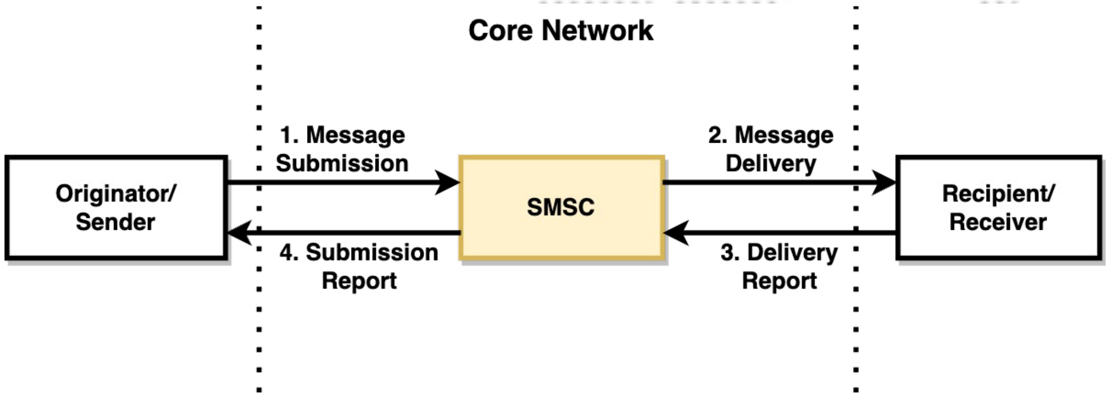
Message Sender: DE-11 RUB

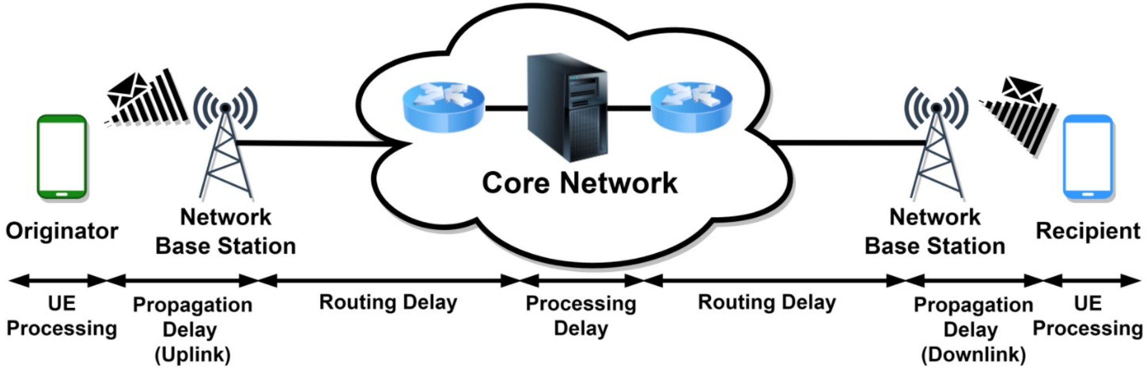
Our Contributions:

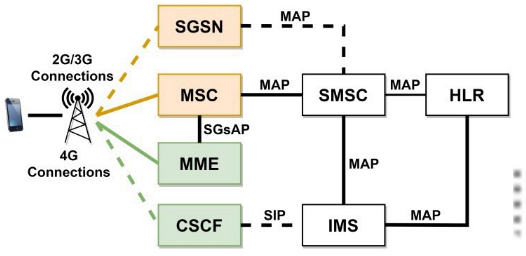
1. Unique and stealthy location identification attack based on the SMS infrastructure
2. Large-scale evaluation: 3 continents, 9 countries, 10 operators, 16 devices
3. The attack can achieve up to 96% accuracy for international classifications, and over 70% more for many national/regional classifications.
4. Countermeasures against the SMS location inference attack

Localizing Users based on 5G SMS Delivery Reports

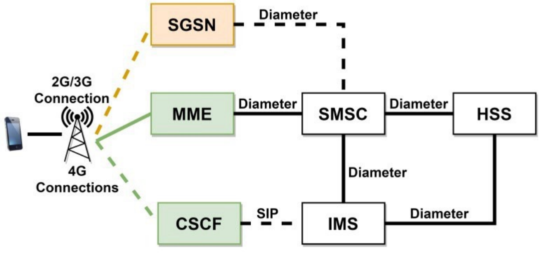
Usenix Sec'23
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings. Evangelos Bitsikas et al.



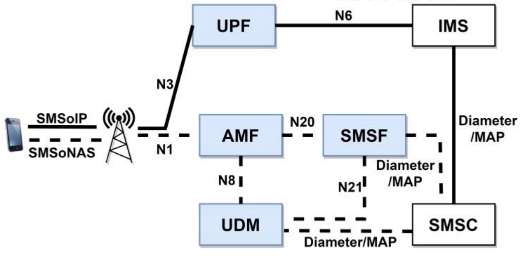




(a) 2G/3G/4G with MAP and IMS



(b) 2G/3G/4G with Diameter and IMS



(c) 5G Standalone with IMS and NAS

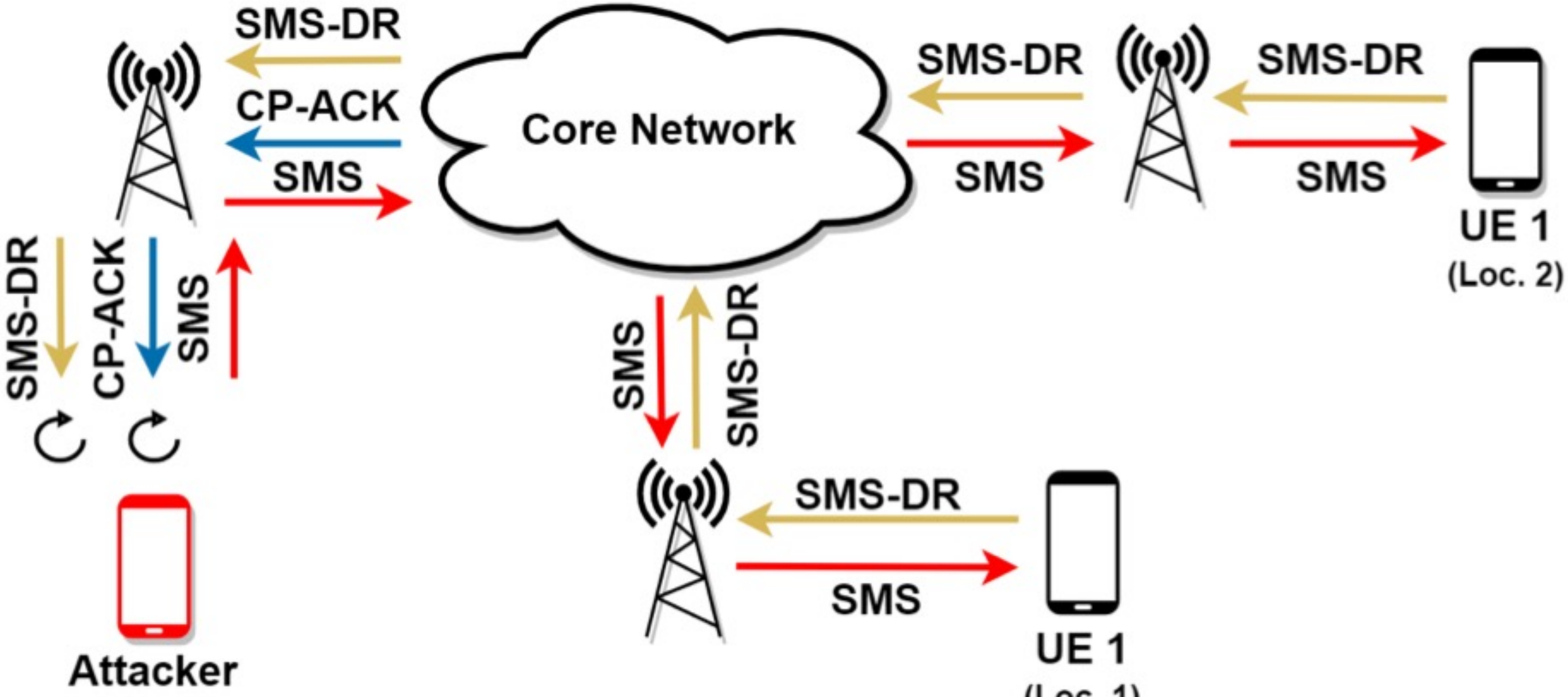
Northeastern University
Khoury College of Computer Sciences

technische universität dortmund

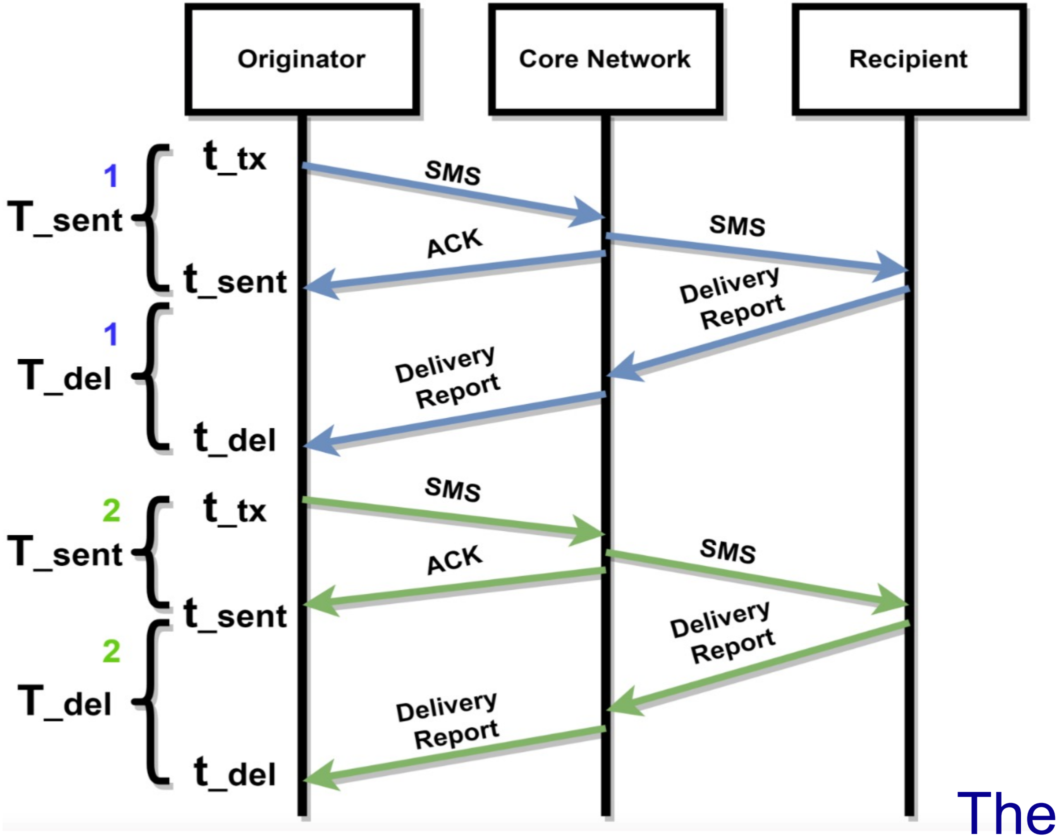
جامعة نيويورك ابوظبي
NYU ABU DHABI

Network Architectures

Localizing Users based on 5G SMS Delivery Reports



Localizing Users based on 5G SMS Delivery Reports – Location Fingerprints

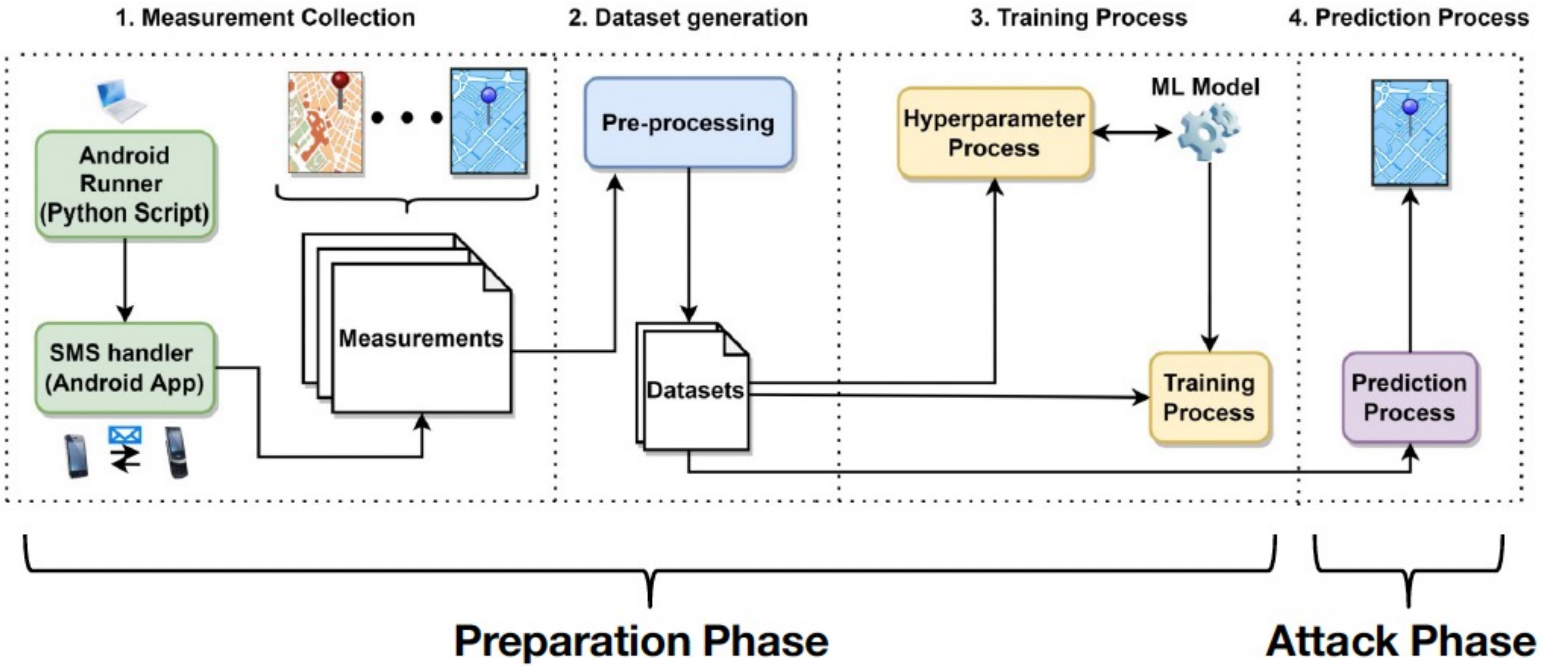


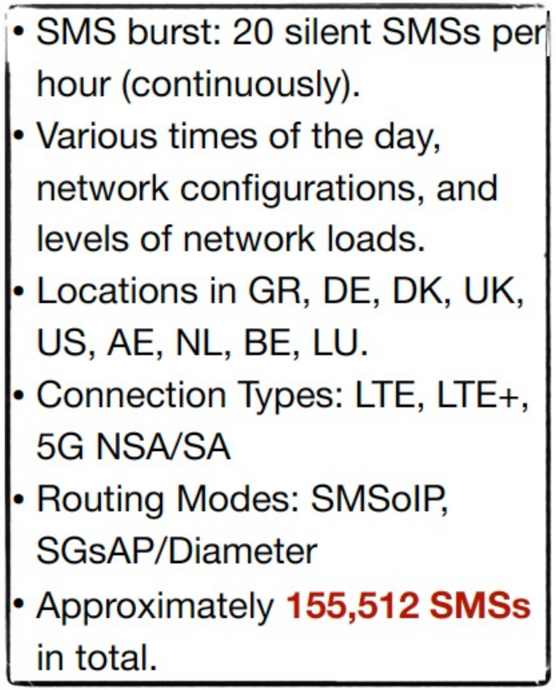
$$\left.\begin{aligned}
T_{sent} &= t_{sent} - t_{tx} && (1)\\
T_{del} &= t_{del} - t_{sent} && (2)\\
T_{tot} &= T_{del} + T_{sent} && (3)\\
P &= \frac{T_{del}}{T_{tot}} = \frac{t_{del} - t_{sent}}{t_{del} - t_{tx}} && (4)
\end{aligned}\right\} \text{Individual SMS}$$

$$\left.\begin{aligned}
T_{\Delta sent} &= (T^{i}_{sent} - T^{i-1}_{sent})/T^{i-1}_{sent} && (5)\\
T_{\Delta del} &= (T^{i}_{del} - T^{i-1}_{del})/T^{i-1}_{del} && (6)
\end{aligned}\right\} \text{Consecutive SMS}$$

The ***location fingerprint*** is a combination of 6 features: (T_{sent}, T_{del}, T_{tot}, P, $T_{\Delta sent}$, $T_{\Delta del}$)

Localizing Users based on 5G SMS Delivery Reports – Measurement Setup





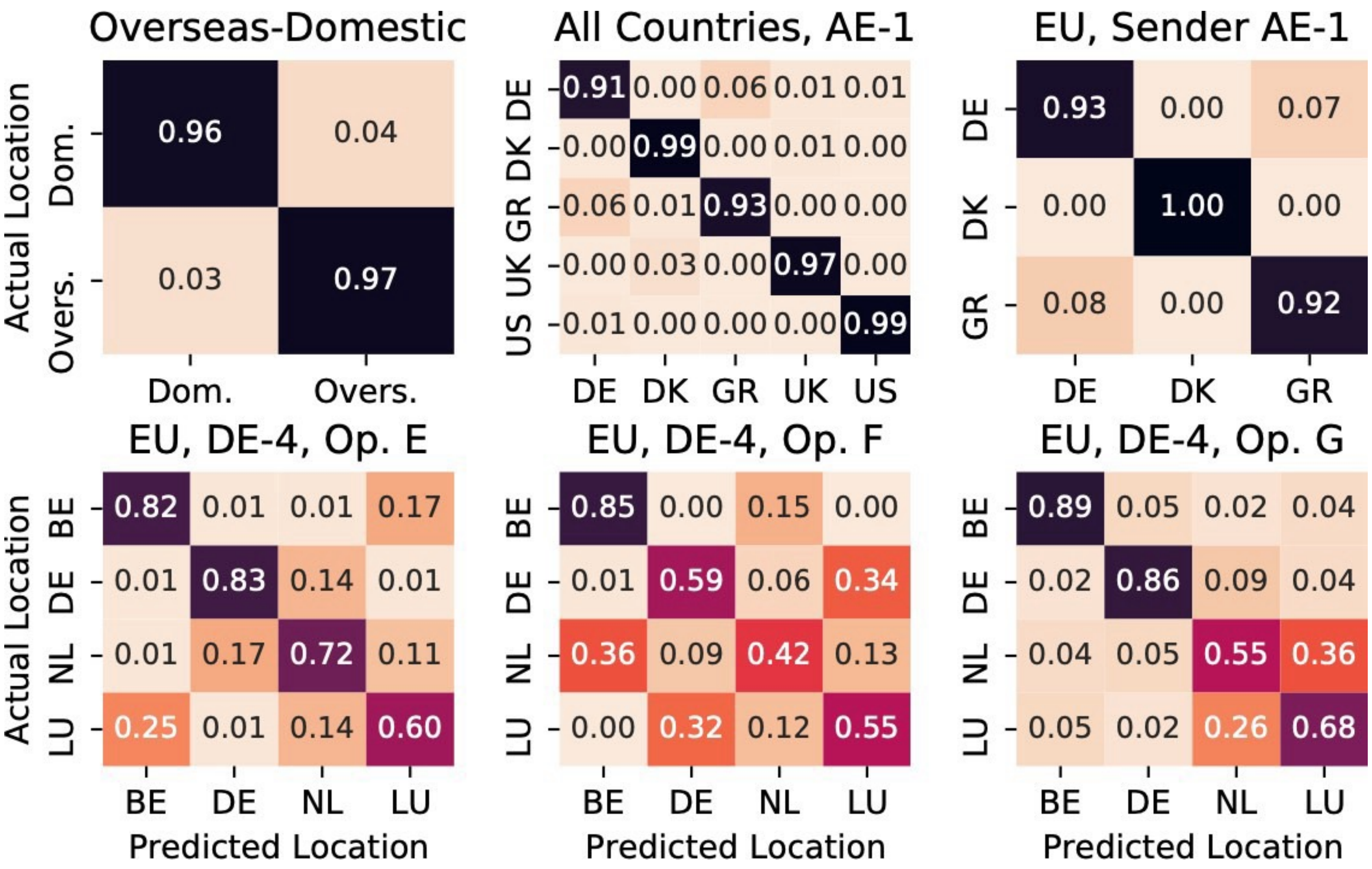
- SMS burst: 20 silent SMSs per hour (continuously).
- Various times of the day, network configurations, and levels of network loads.
- Locations in GR, DE, DK, UK, US, AE, NL, BE, LU.
- Connection Types: LTE, LTE+, 5G NSA/SA
- Routing Modes: SMSoIP, SGsAP/Diameter
- Approximately **155,512 SMSs** in total.

Localizing Users based on 5G SMS Delivery Reports – ML Parameter Tuning

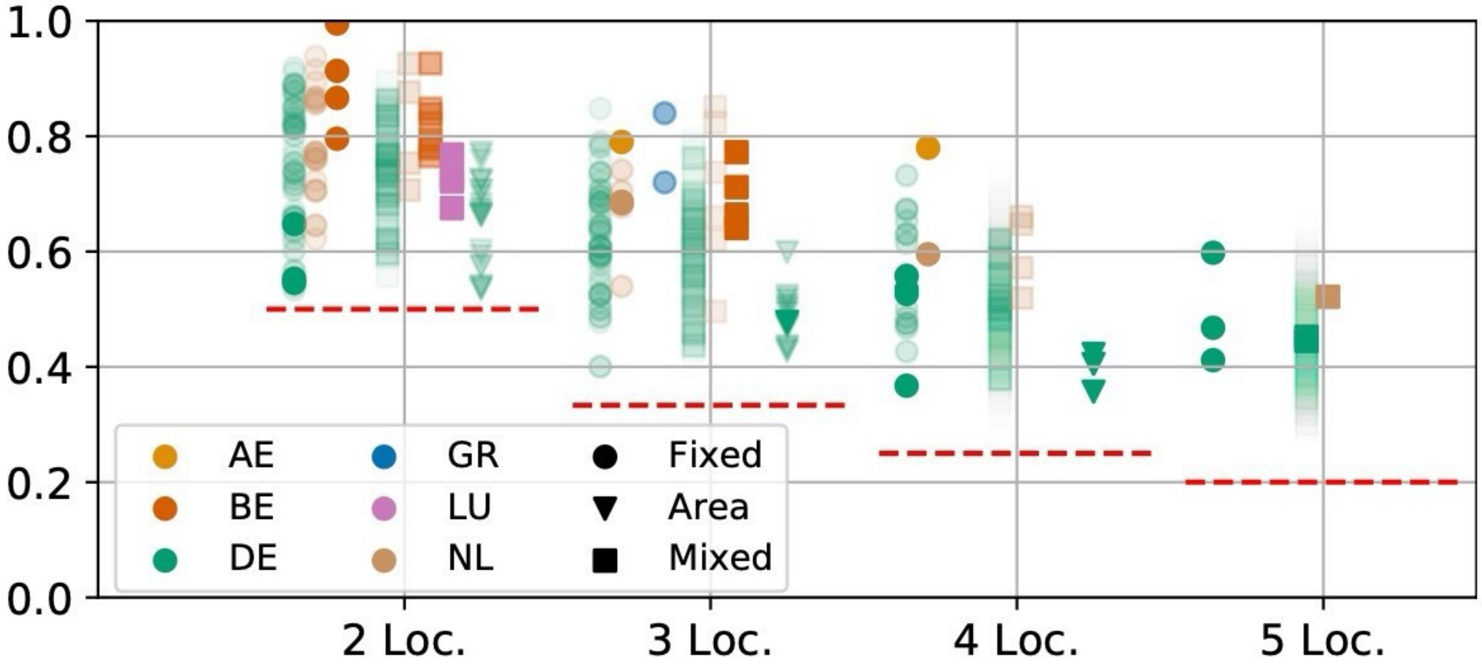
Multi Layer Perceptron (MLP) Neural Network

- Manual & Automatic Hyperparameter tuning
- Stochastic gradient descent solver
- SoftMax and Sigmoid activations
- Three layers of 10, 40, 10
- Maximum iterations: 5000
- Constant learning rate
- Batch size: 32
- Alpha: 0.0001

Results: International Classification



Results: Regional Classification



Receiver Locations	**Accuracy**
Sender Location: DE-4, Operator E	
BE-1, BE-2	83 %
BE-1, BE-3	80 %
BE-2, BE-3	74 %
LU-1, LU-3	64 %
Sender Location: DE-4, Operator F	
BE-1, BE-2	95 %
BE-1, BE-3	72 %
BE-2, BE-3	80 %
LU-1, LU-3	66 %
Sender Location: DE-4, Operator G	
BE-1, BE-2	86 %
BE-1, BE-3	84 %
BE-2, BE-3	84 %
LU-1, LU-3	72 %

Pros and Cons

- Low attacker resources (e.g., no need for false base stations)
- Stealthy (silent SMS), no need for infrastructure access (e.g., network insider)
- Existing SMS infrastructure available across generations of cellular networks
- GSMA Mobile Security Research Acknowledgement: CVD-2023-072 https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements

- Less accurate than other sophisticated location inference attacks (such as:) especially for multiple classes

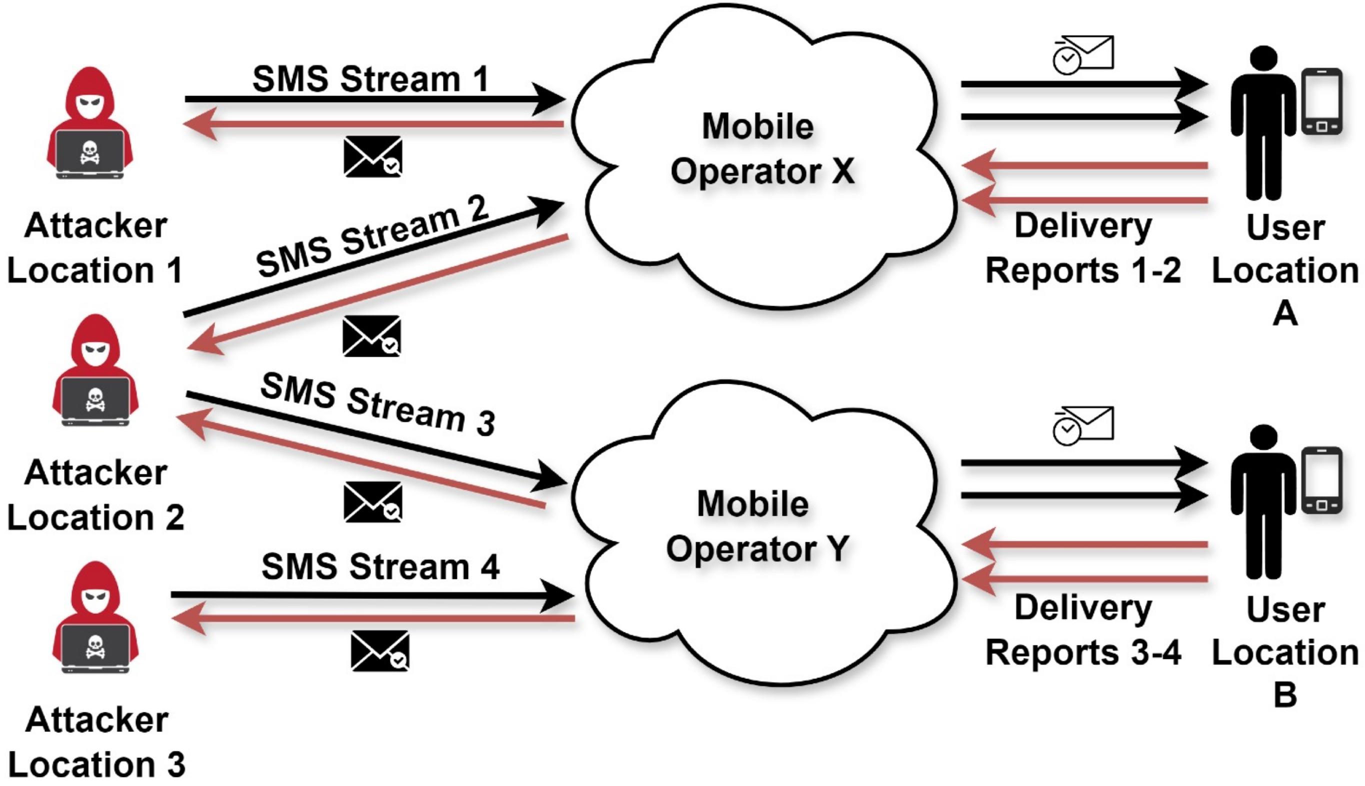
MobiCom '24
Physical Localization of Uncooperative Cellular Devices. *Taekkyung Oh* et al.

- Hard to adapt top an open-world setting
- **Provider might block that single sender**

Leveraging Multiple Senders to Improve the Limitations

WOOT'24

The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks
Ev. Bitsikas et al.



- Synchronous transmissions of silent SMSs
- Recording of timing characteristics with timestamps
- Combination and statistical fusion of sender data
- ML training and prediction
- Reduces the sample sizes -> Less SMS transmissions

Leveraging Multiple Senders to Improve the Limitations

Initial Features:

$$T_{sent} = t_{sent} - t_{tx}$$

$$T_{del} = t_{del} - t_{sent}$$

$$T_{tot} = T_{del} + T_{sent}$$

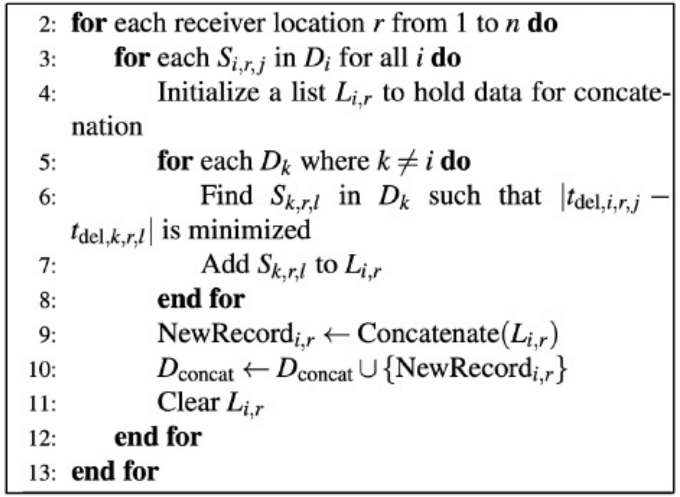
$$P = \frac{T_{del}}{T_{tot}} = \frac{t_{del} - t_{sent}}{t_{del} - t_{tx}}$$

On single transmissions

$$T_{\Delta sent} = (T^{j}_{sent} - T^{j-1}_{sent})/T^{j-1}_{sent}$$

$$T_{\Delta del} = (T^{j}_{del} - T^{j-1}_{del})/T^{j-1}_{del}$$

On consecutive transmissions



```
for each receiver location $r$ from 1 to $n$ do
    for each $S_{i,r,j}$ in $D_i$ for all $i$ do
        Initialize a list $L_{i,r}$ to hold data for concatenation
        for each $D_k$ where $k \neq i$ do
            Find $S_{k,r,l}$ in $D_k$ such that $|t_{\text{del},i,r,j} - t_{\text{del},k,r,l}|$ is minimized
            Add $S_{k,r,l}$ to $L_{i,r}$
        end for
        $\text{NewRecord}_{i,r} \leftarrow \text{Concatenate}(L_{i,r})$
        $D_{\text{concat}} \leftarrow D_{\text{concat}} \cup \{\text{NewRecord}_{i,r}\}$
        Clear $L_{i,r}$
    end for
end for
```

Expanded Features:

$$\mu^{(s,r)} = \frac{1}{z}\sum_{i=1}^{z} t^{(s,r)}_{\text{del},i}$$

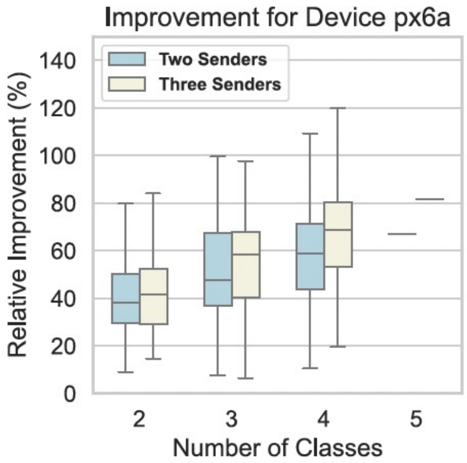
$$\text{Median}^{(s,r)} = \text{Median}\{t^{(s,r)}_{\text{del},1}, t^{(s,r)}_{\text{del},2}, \ldots, t^{(s,r)}_{\text{del},z}\}$$

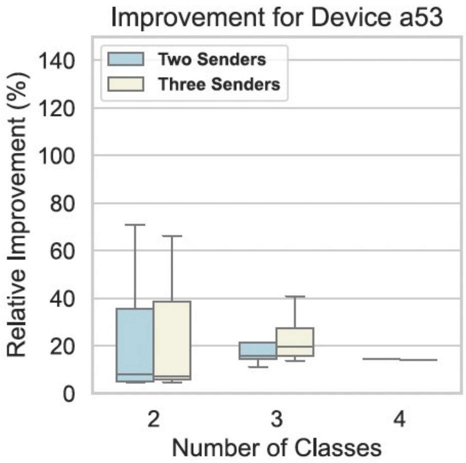
$$\sigma^{(s,r)} = \sqrt{\frac{1}{z-1}\sum_{i=1}^{z}(t^{(s,r)}_{\text{del},i} - \mu^{(s,r)})^2}$$

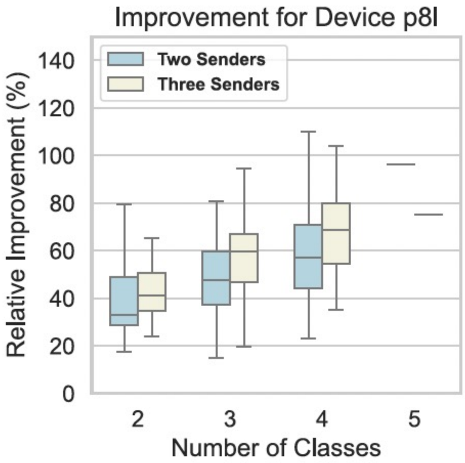
$$\Delta\mu^{(s_1,s_2,r)} = \mu^{(s_1,r)} - \mu^{(s_2,r)}$$

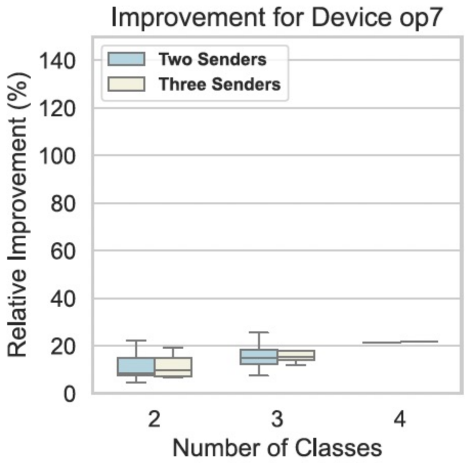
Mean, Median and Standard Deviation per two sender locations

Results for Multiple Senders









Countermeasures

- ✓ Rejecting/Dropping Silent SMS at the Core Network
- ✓ More Robust Spamming/Flooding Filters
- ✓ Artificial Random Delays for the Delivery Report
- ✓ Total Elimination of the Delivery Reports

GSMA Mobile Security Research Acknowledgements* under *CVD-2023-0072

GitHub

Longer Version

ASTRA-5G – A UE security testing framework

Collaboration with Syed Khandker, Evangelos Bitsikas, Michele Guerra, Aanjhan Ranganathan, Roger Piqueras Jover

5G SA User Equipment (UE) Security

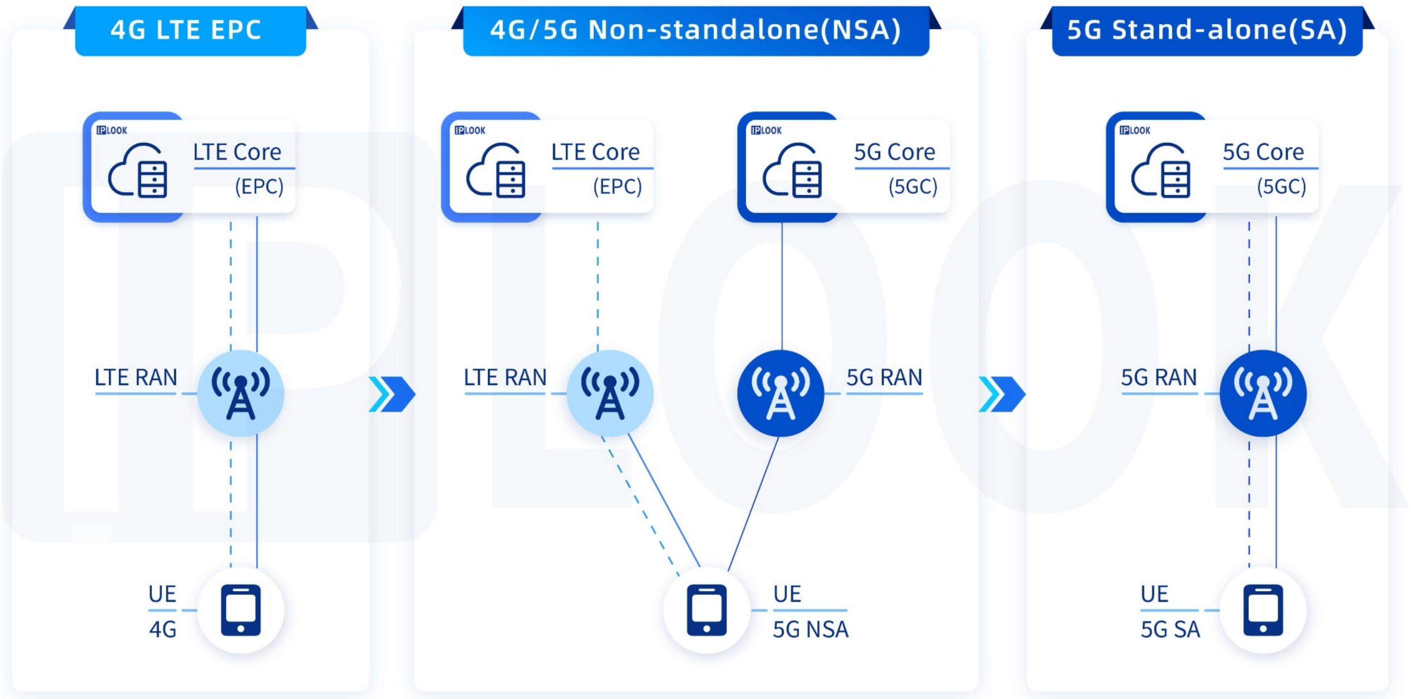
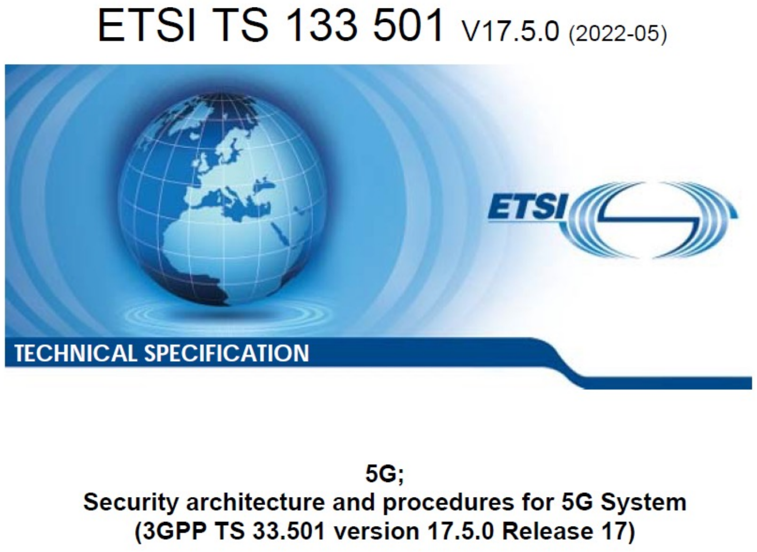


Image source: IPLook/GSMA


ETSI TS 133 501 V17.5.0 (2022-05)

TECHNICAL SPECIFICATION

5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 17.5.0 Release 17)

- Do the implementations of the UE following the specifications?

- An over-the-air test may reveal the real scenario

5G SA User Equipment (UE) Security

Need for frameworks verifying the security of implementations, specifically 5G SA UE devices

Paper	Venue	Generation	Topic
DoLTEest	Usenix Sec’21	4G	Negative UE security testing
Noncompliance as Deviant Behavior	CCS’21	4G	UE security
Never Let Me Down Again	WiSec’23	4G/5G	Bidding down attacks on UE
UE Security Reloaded	WiSec’23	5G	UE security
ASTRA-5G	**WiSec’24**	**5G**	**UE security**

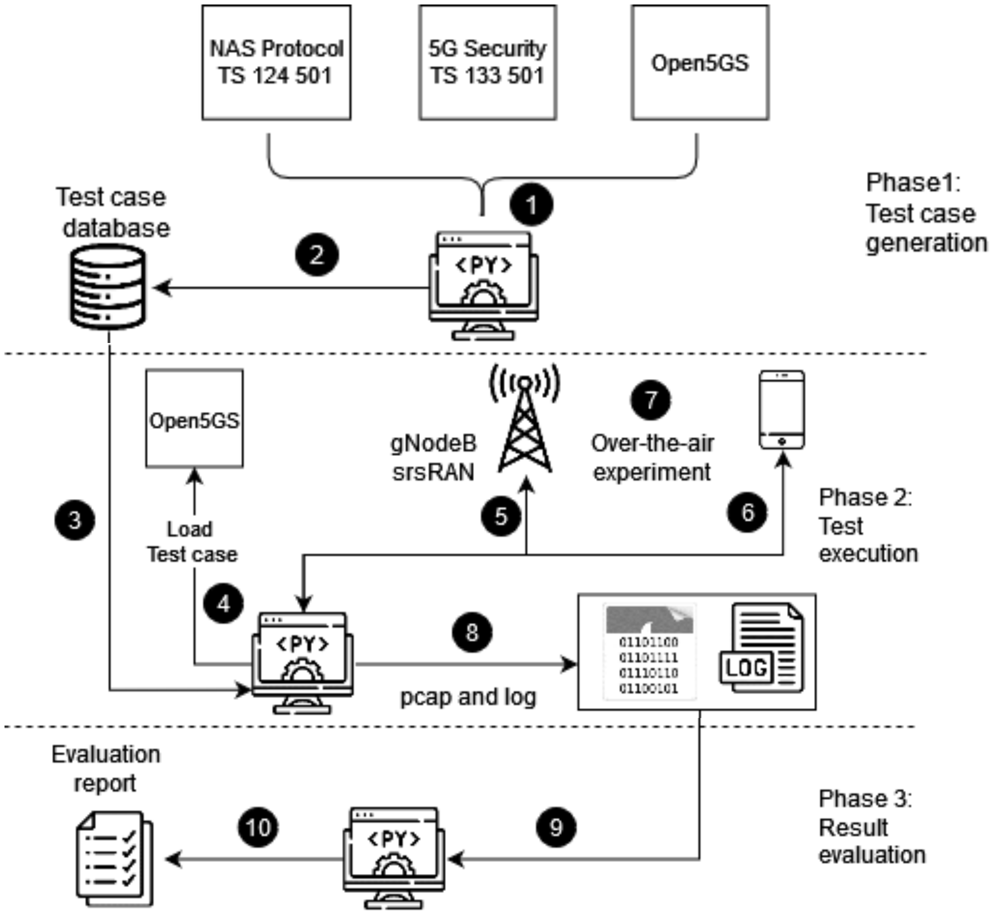
ASTRA-5G

WiSec'24
ASTRA-5G: Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices. Syed Khandker et al.

Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices

- Users can generate variety of test cases
- Tests can be executed automatically one after another (e.g., 4 tests/minute)
- Evaluation reports are generated, eliminating time-consuming & labor-intensive manual checks
- Users do not need deep knowledge in this domains to conduct the tests

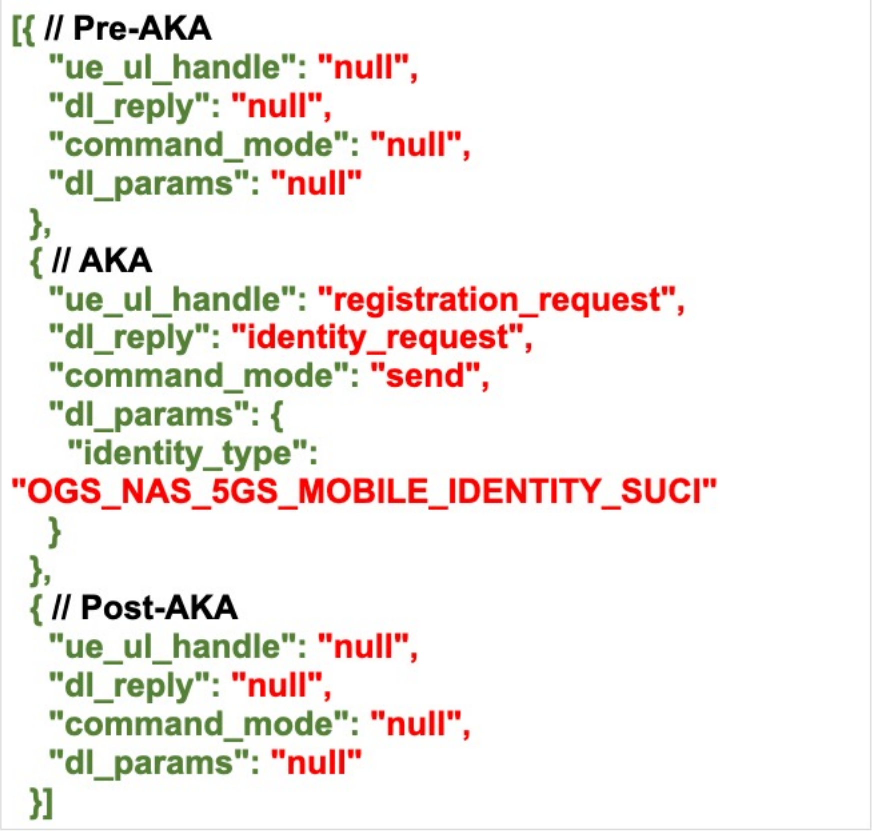
ASTRA-5G – Automation Process



Striving for as much automation as possible

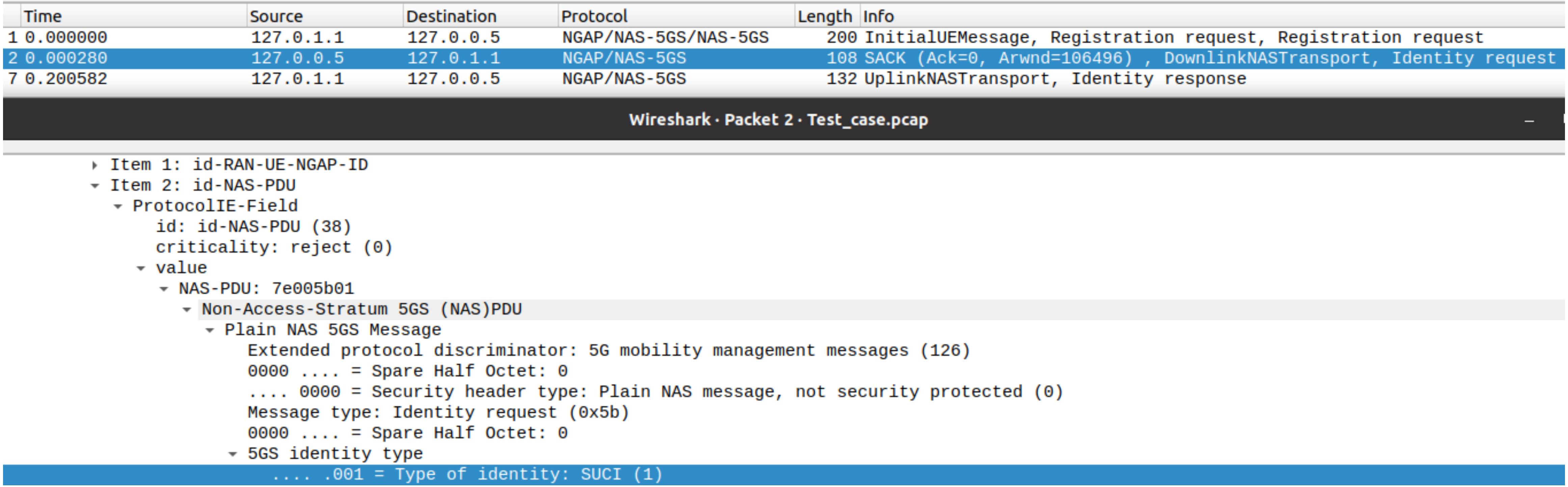
ASTRA-5G – Test Cases

- A **test case** is a set of instructions to be executed in the core network to send a fabricated signal to the UE via RAN.
- The follow-up uplink message reveals the UE's response to the test.
- A test case can be formulated in a way that either follows the protocol or violates it.
- Therefore, the follow-up uplink message reveals whether UE adheres to the protocol or not.



```
[{ // Pre-AKA
   "ue_ul_handle": "null",
   "dl_reply": "null",
   "command_mode": "null",
   "dl_params": "null"
 },
 { // AKA
   "ue_ul_handle": "registration_request",
   "dl_reply": "identity_request",
   "command_mode": "send",
   "dl_params": {
     "identity_type":
"OGS_NAS_5GS_MOBILE_IDENTITY_SUCI"
   }
 },
 { // Post-AKA
   "ue_ul_handle": "null",
   "dl_reply": "null",
   "command_mode": "null",
   "dl_params": "null"
 }]
```

ASTRA-5G – UE Response

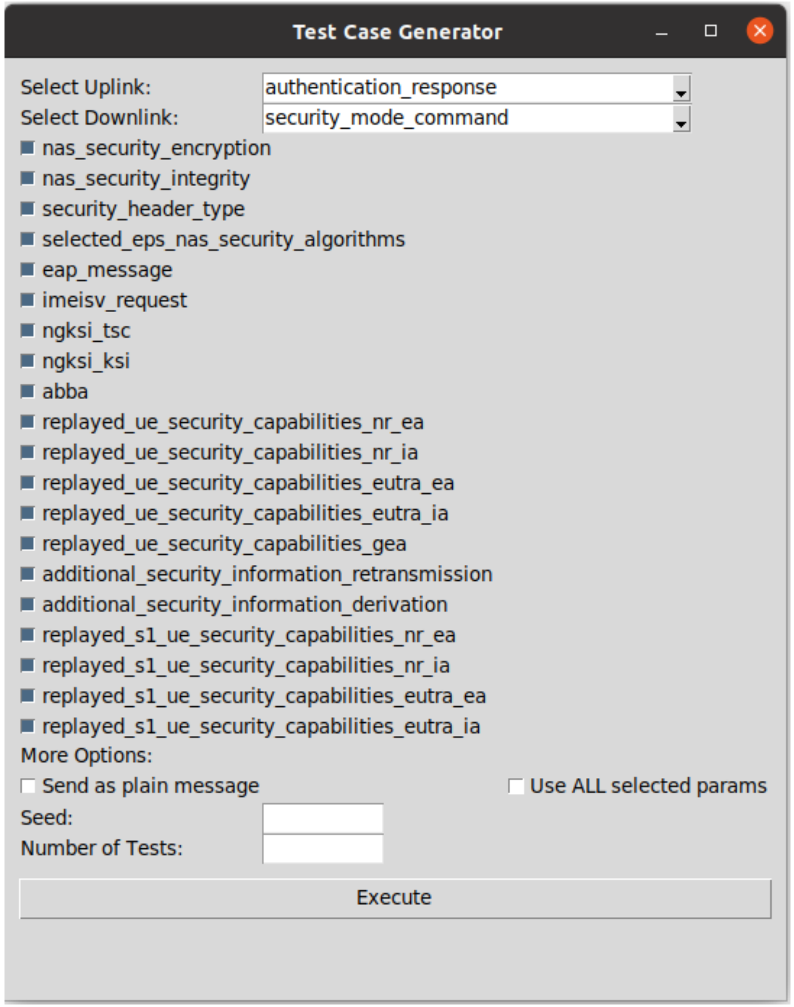


```
  Time        Source      Destination  Protocol               Length Info
1 0.000000    127.0.1.1   127.0.0.5    NGAP/NAS-5GS/NAS-5GS      200 InitialUEMessage, Registration request, Registration request
2 0.000280    127.0.0.5   127.0.1.1    NGAP/NAS-5GS              108 SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request
7 0.200582    127.0.1.1   127.0.0.5    NGAP/NAS-5GS              132 UplinkNASTransport, Identity response
```

```
  ▸ Item 1: id-RAN-UE-NGAP-ID
  ▾ Item 2: id-NAS-PDU
    ▾ ProtocolIE-Field
        id: id-NAS-PDU (38)
        criticality: reject (0)
      ▾ value
        ▾ NAS-PDU: 7e005b01
          ▾ Non-Access-Stratum 5GS (NAS)PDU
            ▾ Plain NAS 5GS Message
                Extended protocol discriminator: 5G mobility management messages (126)
                0000 .... = Spare Half Octet: 0
                .... 0000 = Security header type: Plain NAS message, not security protected (0)
                Message type: Identity request (0x5b)
                0000 .... = Spare Half Octet: 0
              ▾ 5GS identity type
                  .... .001 = Type of identity: SUCI (1)
```

ASTRA-5G – Possible Test Cases

- Requesting IMEI before 5G-AKA completion
- Request to accept null integrity / cipher algorithm
- Sending a security-protected message as a plain message
- Using an inappropriate security header type
- Sending a message out of sequence
- Parameter violation: ABBA, RAND, AUTN, ngKSI tsc, ksi, GMM cause, etc.



Test Case Generator

Select Uplink: authentication_response

Select Downlink: security_mode_command

■ nas_security_encryption
■ nas_security_integrity
■ security_header_type
■ selected_eps_nas_security_algorithms
■ eap_message
■ imeisv_request
■ ngksi_tsc
■ ngksi_ksi
■ abba
■ replayed_ue_security_capabilities_nr_ea
■ replayed_ue_security_capabilities_nr_ia
■ replayed_ue_security_capabilities_eutra_ea
■ replayed_ue_security_capabilities_eutra_ia
■ replayed_ue_security_capabilities_gea
■ additional_security_information_retransmission
■ additional_security_information_derivation
■ replayed_s1_ue_security_capabilities_nr_ea
■ replayed_s1_ue_security_capabilities_nr_ia
■ replayed_s1_ue_security_capabilities_eutra_ea
■ replayed_s1_ue_security_capabilities_eutra_ia

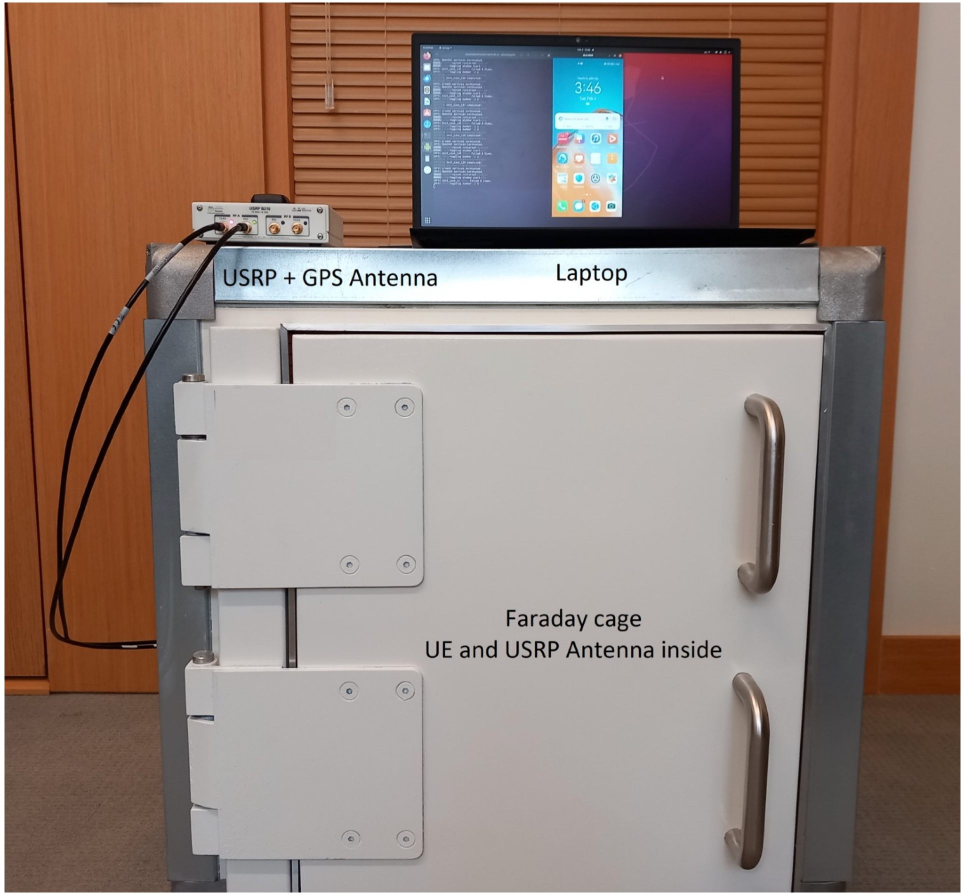
More Options:

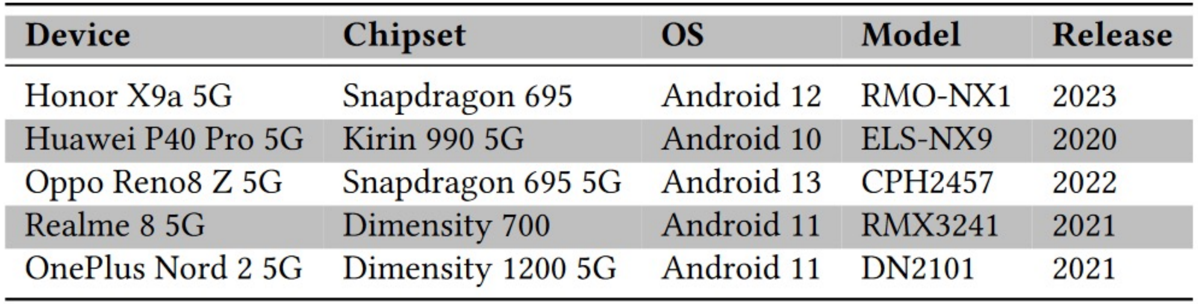
☐ Send as plain message ☐ Use ALL selected params

Seed:

Number of Tests:

ASTRA-5G – Experiment Setup and Verification



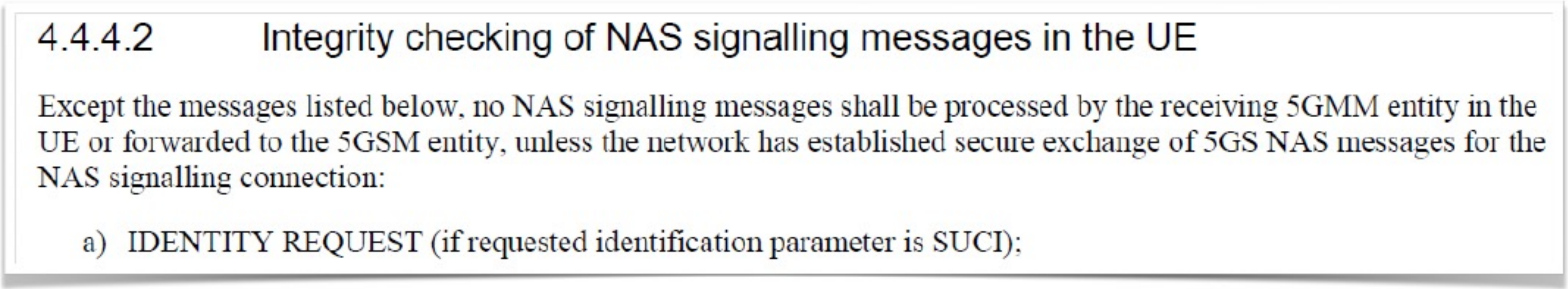


Device	Chipset	OS	Model	Release
Honor X9a 5G	Snapdragon 695	Android 12	RMO-NX1	2023
Huawei P40 Pro 5G	Kirin 990 5G	Android 10	ELS-NX9	2020
Oppo Reno8 Z 5G	Snapdragon 695 5G	Android 13	CPH2457	2022
Realme 8 5G	Dimensity 700	Android 11	RMX3241	2021
OnePlus Nord 2 5G	Dimensity 1200 5G	Android 11	DN2101	2021

Test Evaluation

- Checking the hooking point, DL message, and parameters from the test case
- Identify the same from the pcap file
- Retrieving the UE response for the test case
- Evaluate whether the UE response aligns with the state and parameters according to the protocol

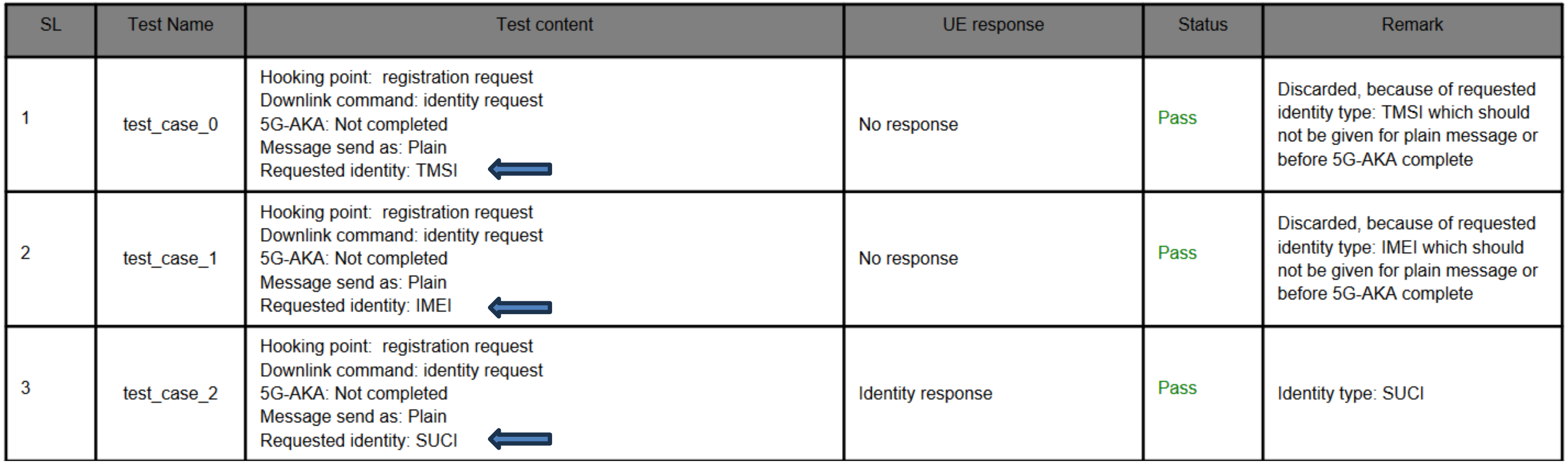
ASTRA-5G – Example Test Case 1: Identity Report



4.4.4.2 Integrity checking of NAS signalling messages in the UE

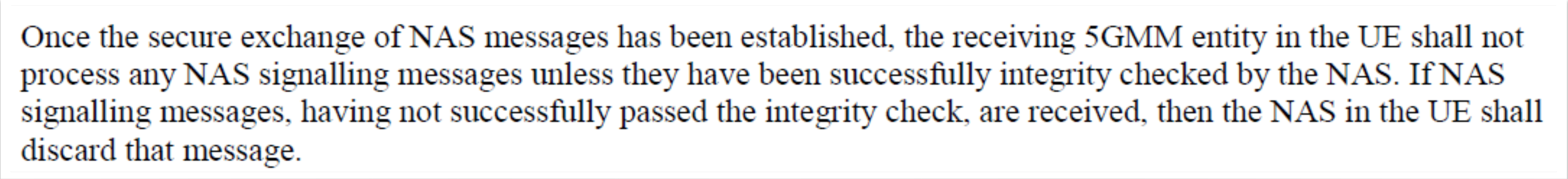
Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

a) IDENTITY REQUEST (if requested identification parameter is SUCI);

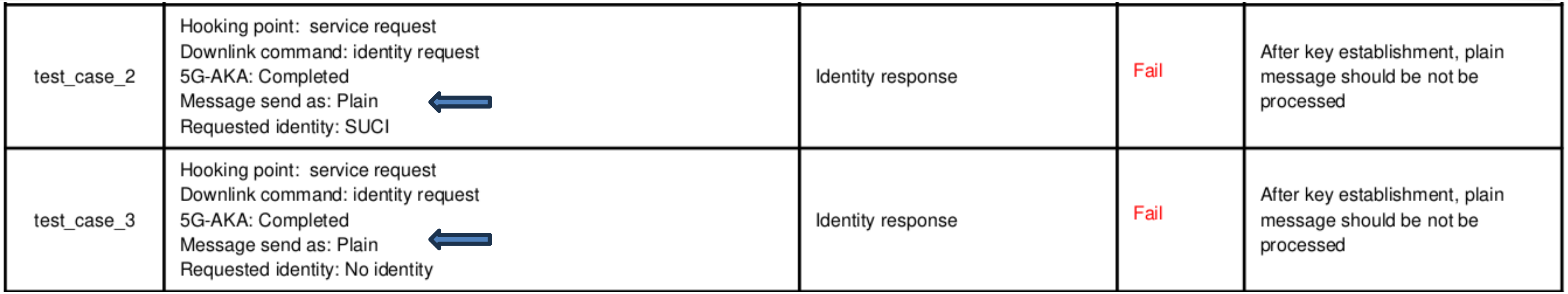


SL	Test Name	Test content	UE response	Status	Remark
1	test_case_0	Hooking point: registration request Downlink command: identity request 5G-AKA: Not completed Message send as: Plain Requested identity: TMSI ⬅	No response	Pass	Discarded, because of requested identity type: TMSI which should not be given for plain message or before 5G-AKA complete
2	test_case_1	Hooking point: registration request Downlink command: identity request 5G-AKA: Not completed Message send as: Plain Requested identity: IMEI ⬅	No response	Pass	Discarded, because of requested identity type: IMEI which should not be given for plain message or before 5G-AKA complete
3	test_case_2	Hooking point: registration request Downlink command: identity request 5G-AKA: Not completed Message send as: Plain Requested identity: SUCI ⬅	Identity response	Pass	Identity type: SUCI

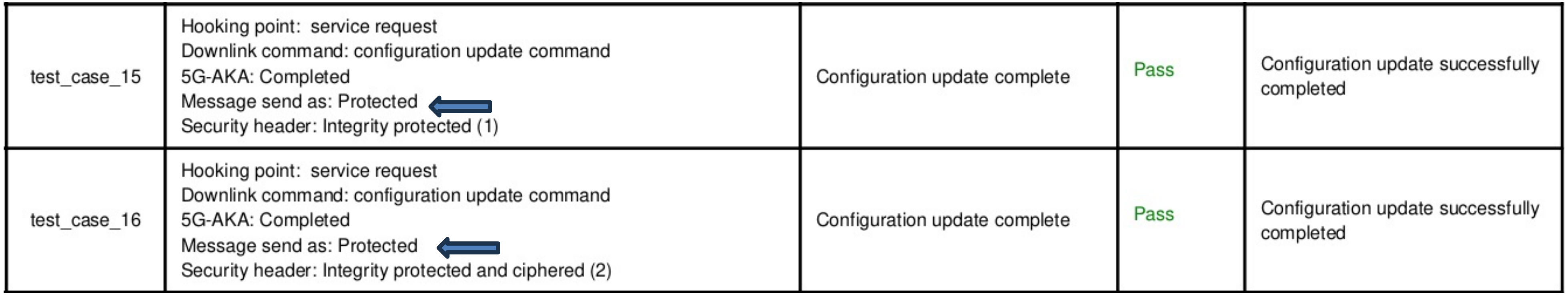
ASTRA-5G – Example Test Case 2: Plain Messages and Protected Messages



Once the secure exchange of NAS messages has been established, the receiving 5GMM entity in the UE shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS in the UE shall discard that message.



test_case_2	Hooking point: service request Downlink command: identity request 5G-AKA: Completed Message send as: Plain Requested identity: SUCI	Identity response	Fail	After key establishment, plain message should be not be processed
test_case_3	Hooking point: service request Downlink command: identity request 5G-AKA: Completed Message send as: Plain Requested identity: No identity	Identity response	Fail	After key establishment, plain message should be not be processed



test_case_15	Hooking point: service request Downlink command: configuration update command 5G-AKA: Completed Message send as: Protected Security header: Integrity protected (1)	Configuration update complete	Pass	Configuration update successfully completed
test_case_16	Hooking point: service request Downlink command: configuration update command 5G-AKA: Completed Message send as: Protected Security header: Integrity protected and ciphered (2)	Configuration update complete	Pass	Configuration update successfully completed

ASTRA-5G – Summary of Results

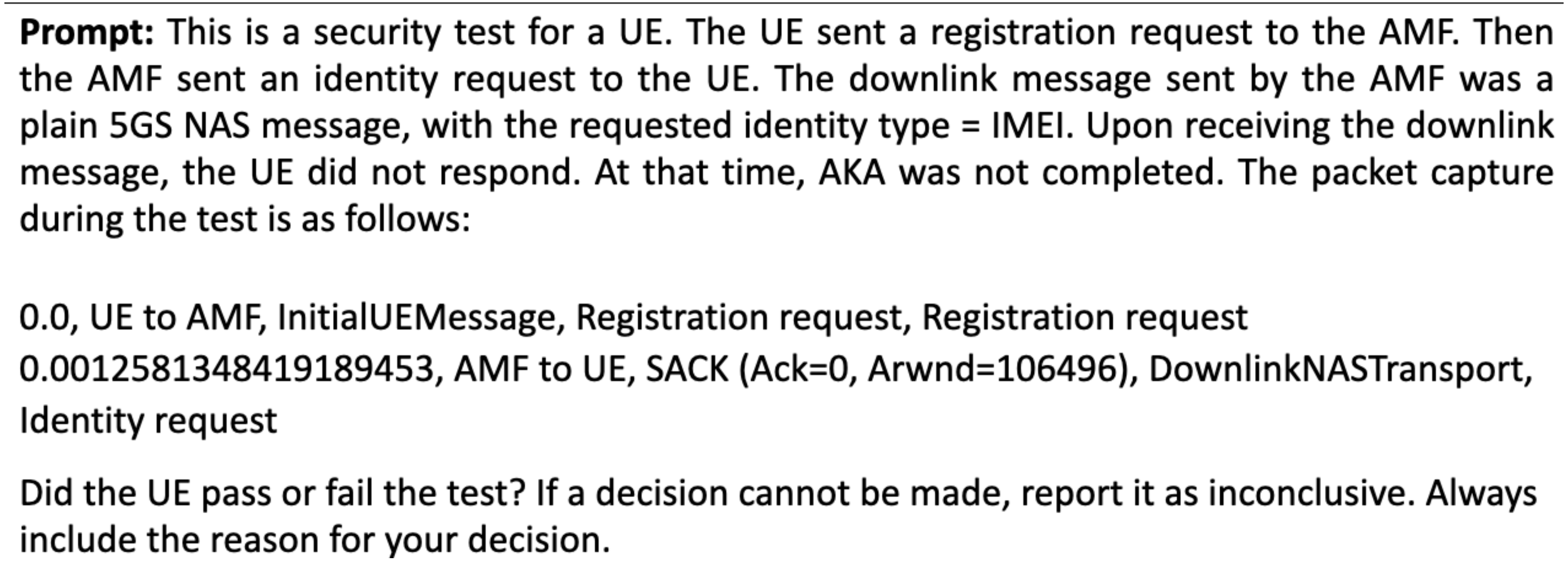
Test	Huawei	Oneplus	Honor	Oppo	Realme
Identity request other than SUCI in plain message	✓	✓	✓	✓	✓
Identity requested in plain message after 5G-AKA completed	✗	✓	✗	✗	✓
Security header type mismatch	✓	✓	✓	✓	✓
Non-zero ABBA	⦸	⦸	⦸	⦸	⦸
Deregistration accept before registration complete	✓	✓	✓	✓	✓
Identity request for unlisted identity type	✓	✗	✗	✗	✗
Parameter violation (RAND, AUTN, ngKSI, GMM cause etc.,)	✓	✓	✓	✓	✓
Null-Cipher / integrity algorithm acceptance	✓	✓	✓	✓	✓
Protected message as plain message	✓	✓	✓	✓	✓
Message out of sequence or state	✓	✓	✓	✓	✓

Note:

- ✓= Pass ✗ = Fail ⦸ = some violation / inconclusive
- We have reported our findings to relevant manufacturer

ASTRA-5G – LLM Based Evaluation

- Manual Verification takes a lot of time – Can LLMs help us?
- ChatGPT • Google Bard • LLAMA-2 • TelecomGPT



Prompt: This is a security test for a UE. The UE sent a registration request to the AMF. Then the AMF sent an identity request to the UE. The downlink message sent by the AMF was a plain 5GS NAS message, with the requested identity type = IMEI. Upon receiving the downlink message, the UE did not respond. At that time, AKA was not completed. The packet capture during the test is as follows:

0.0, UE to AMF, InitialUEMessage, Registration request, Registration request
0.001258134819189453, AMF to UE, SACK (Ack=0, Arwnd=106496), DownlinkNASTransport, Identity request

Did the UE pass or fail the test? If a decision cannot be made, report it as inconclusive. Always include the reason for your decision.

ChatGPT Answer: *Based on the provided informayion, the UE behavior appears to be secure. The UE did not respond to the identity request from the AMF because the AKA (Authentication and Key Agreement) was not completed. This is a security measure to prevent unauthorized access or manipulation of the UE's identity. The UE is correctly waiting for the completion of the AKA before responding to the identity request, which is a good practice in maintaining the security of the UE. Therefore, the UE passes the test.*

ASTRA-5G – Summary

- 5G SA testing is not straightforward, requires handling all the network components e.g., core, RAN, and UE.
- Automation significantly reduces testing complexity and broadens the testing scope (e.g., order of multiple minutes to ≈15 seconds).
- Such open source tools can ensuring transparency and independence in testing.
- In the future, LLMs will likely play a crucial role in the cellular security domain.

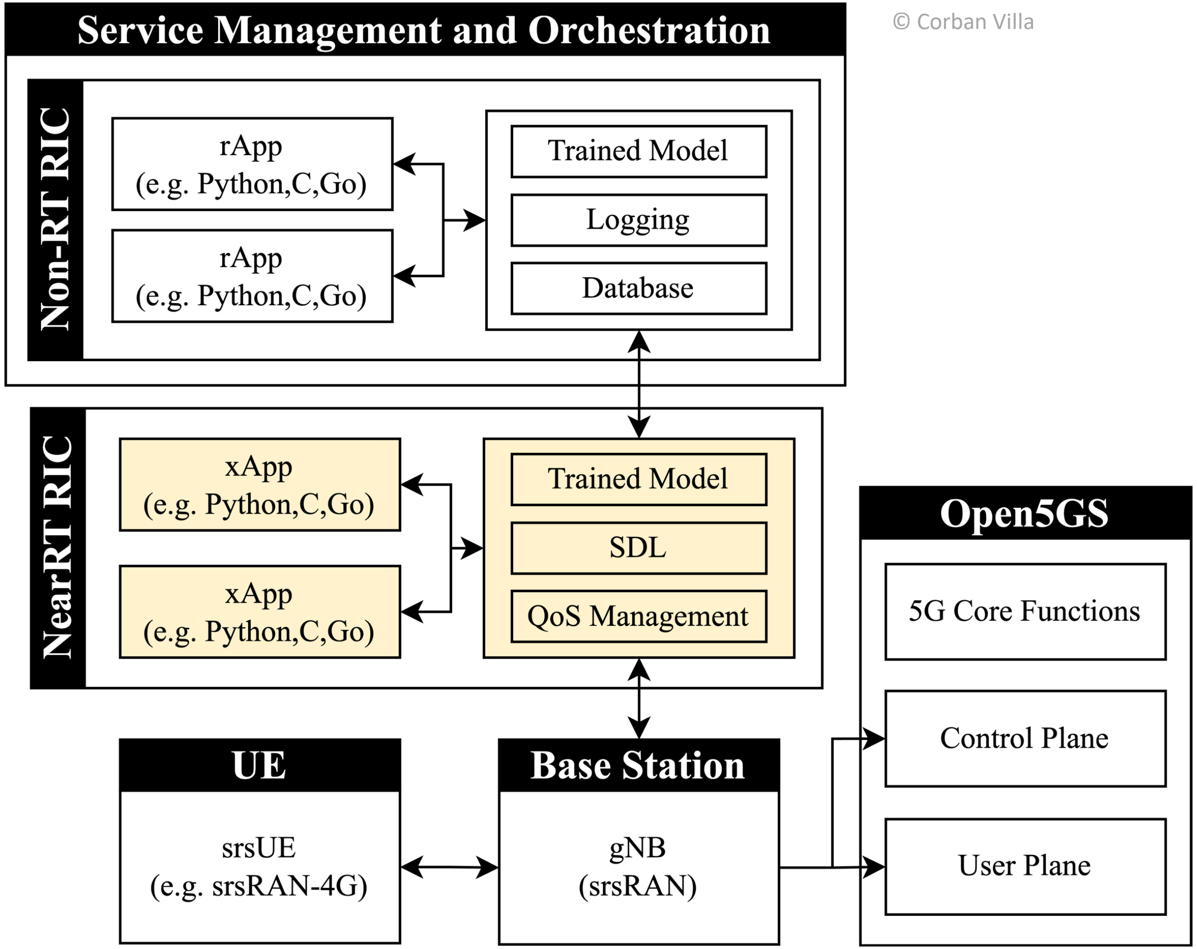
Github Repo

ORAN Security

Open Radio Access Network (ORAN)

A new wireless communication architecture

- Open standards for 5G and 6G network deployments
- Softwarization of infrastructure: Software-defined networking (SDN).
- AI and machine learning pipelines
- Multi-vendor support
- Cloud Radio Access Networks (C-RAN) inspired

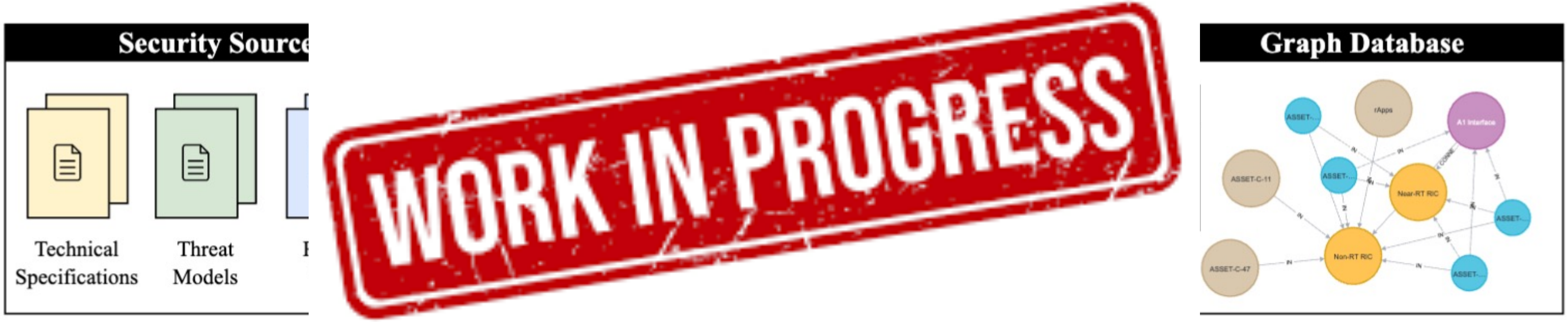


© Corban Villa

Open Radio Access Network (ORAN)

What are the new attack vectors, threats and vulnerabilities specific to ORAN?

A first step: A graph-based ORAN threat mapping



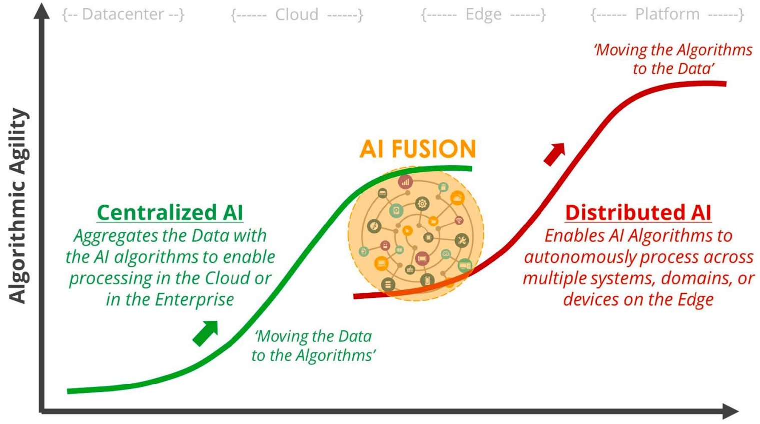
© Corban Villa

Conclusion & Outlook

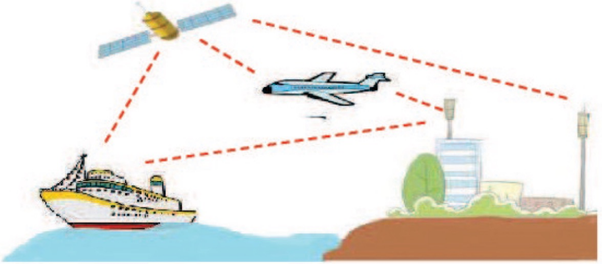
Towards 6G Security Research

Distributed AI & Intelligent Radios

- Protection against ML attacks: backdoors, injection, model pollution

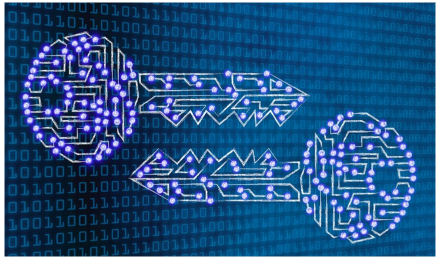


© CMU



Global Coverage

- Securely Connecting & Integrating Vertical Applications as diverse as Satellite, UAV, Maritime, Terrestrial
- Not introducing new vulnerabilities at their boundaries



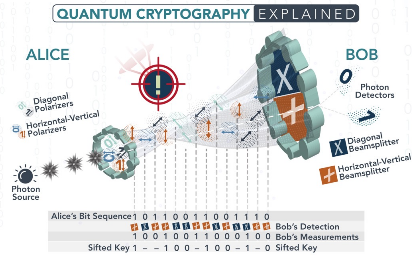
Post-Quantum Cryptography (PQC)

Hash-Based Signatures

Code-Based Cryptography

Multivariate Cryptography

Lattice-Based Cryptography


QUANTUMXCHANGE
QUANTUM CRYPTOGRAPHY EXPLAINED
ALICE
BOB
Diagonal Polarizers
Horizontal-Vertical Polarizers
Photon Source
Photon Detectors
Diagonal Beamsplitter
Horizontal-Vertical Beamsplitter
Alice's Bit Sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's Detection
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's Measurements
Sifted Key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted Key

Post-Quantum Crypto/Algorithms

- Integration of PQ mechanisms
- Realization of quantum exchange

Conclusion

- Our Research Focus:
  - Mobile/Cellular Network Security
  - Mis-/Disinformation Campaigns
  - Secure Localization & Aviation
  - LLM/ML Security & Privacy
  - Anonymous Communication

- Interested in collaborations – Please reach out to me if you'd like to know more or would like to collaborate

Thank You for Your Attention!

Christina Pöpper

christina.poepper@nyu.edu

Cyber Security & Privacy Lab (CSP-lab)

https://www.poepper.net