Evolving Security in Cellular Networks:

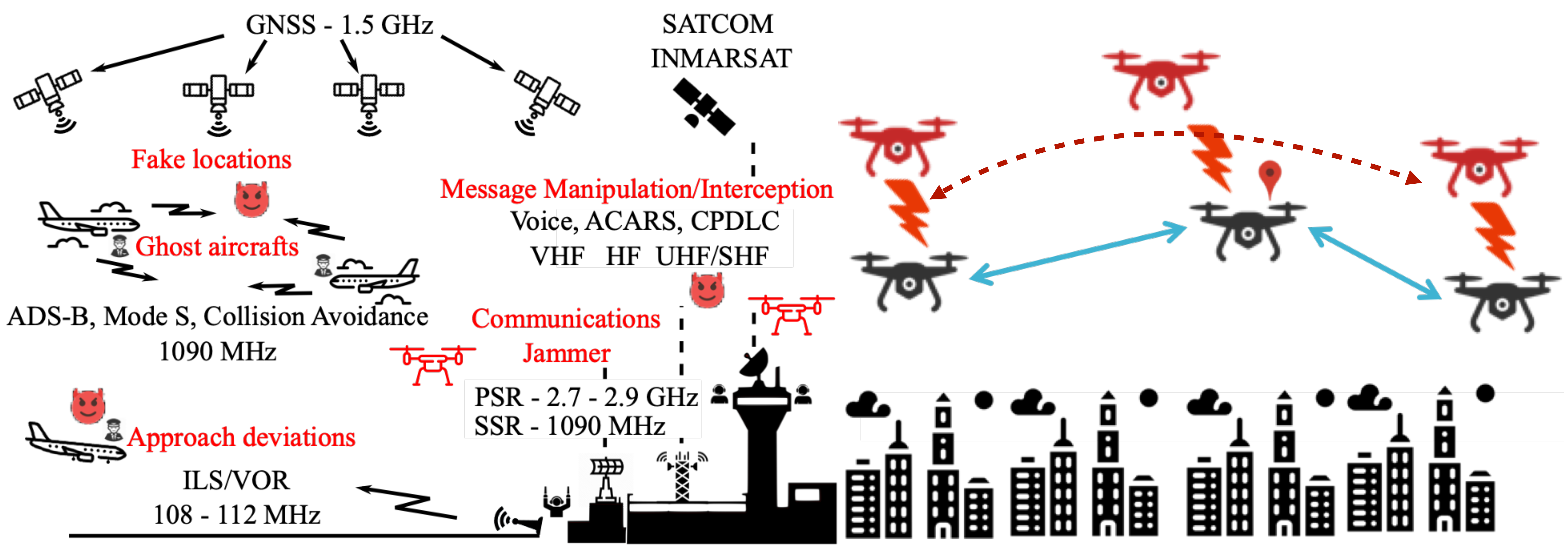
Privacy Challenges, Device-Level Testing, and Autonomous Swarm Networking

Aanjhan Ranganathan

Signal Intelligence Lab @ Northeastern

Security and privacy of wireless networks with a focus on *autonomous cyber-physical systems and smart ecosystems*.

Secure and Private Wide-area Positioning



Aviation and Aerospace Security

Security and Privacy of xIoT

Faculty

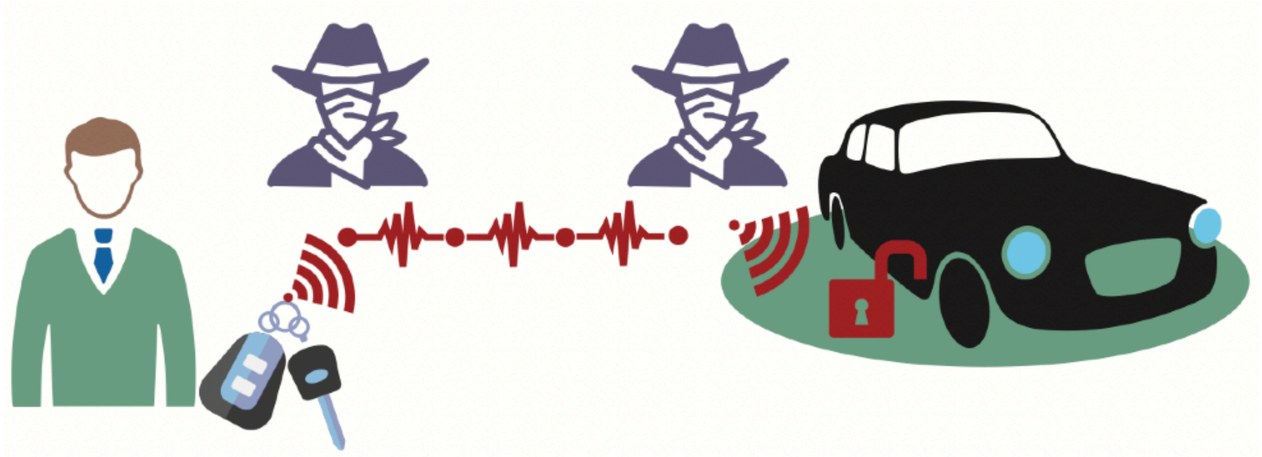
Aanjhan Ranganathan
Assistant Professor
www.aanjhan.com

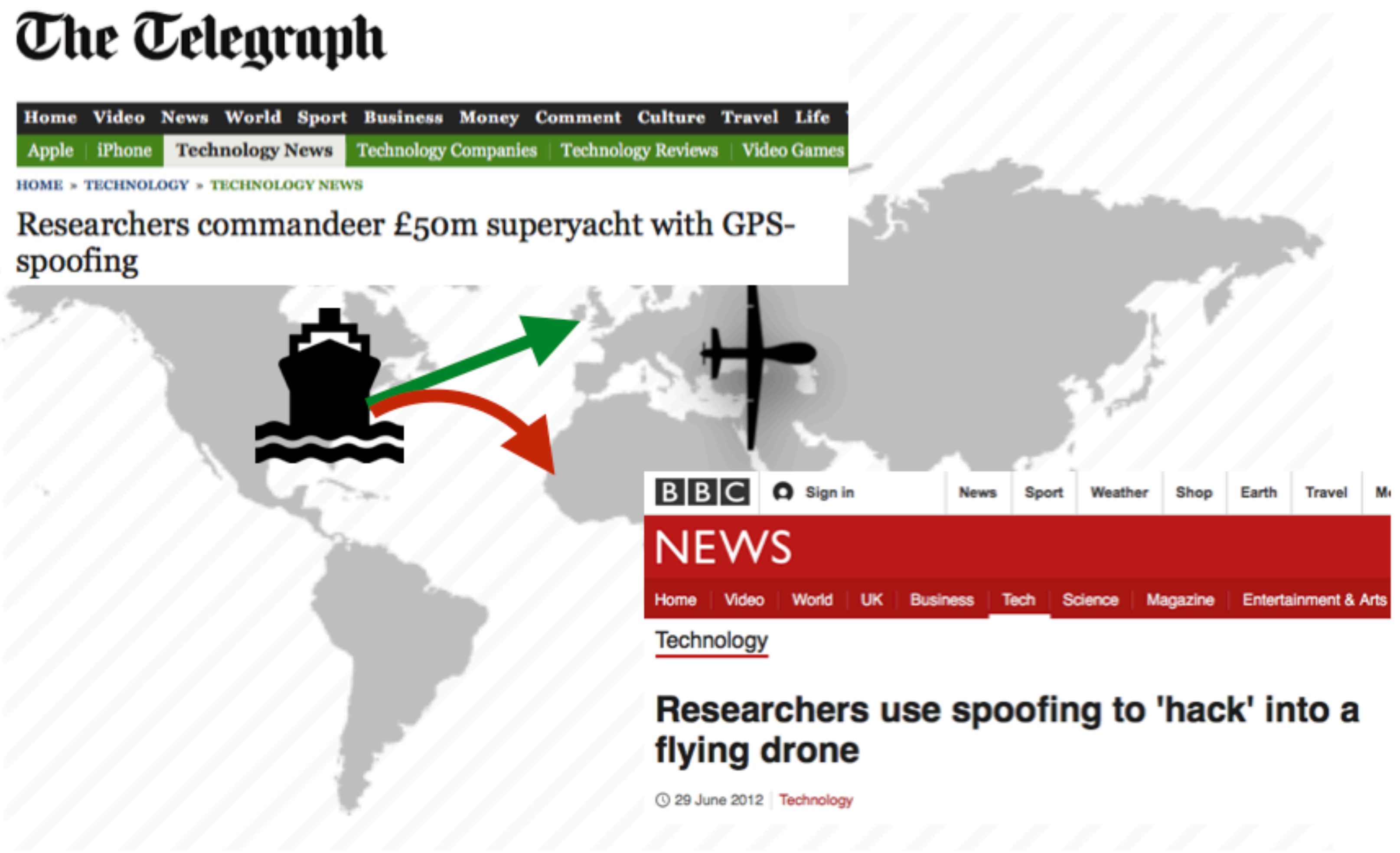
Group Members

Secure Proximity and Location Verification

Towards Secure and Private Wide-area Positioning

Attacks on Location




The Telegraph
Home Video News World Sport Business Money Comment Culture Travel Life
Apple iPhone Technology News Technology Companies Technology Reviews Video Games
HOME » TECHNOLOGY » TECHNOLOGY NEWS

Researchers commandeer £50m superyacht with GPS-spoofing

BBC Sign in News Sport Weather Shop Earth Travel
NEWS
Home Video World UK Business Tech Science Magazine Entertainment & Arts
Technology

Researchers use spoofing to 'hack' into a flying drone

29 June 2012 | Technology

Selected Research

Breaking the Formation: The Impact of GNSS Spoofing on UAV Swarms, Aanjhan Ranganathan, Adam Belfki, Pau Closas (InsideGNSS Magazine 2024)

An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs, Harshad Sathaye, Martin Strohmeier, Vincent Lenders, Aanjhan Ranganathan (USENIX Security 2022)

VRange: Enabling Secure Ranging in 5G-NR Wireless Networks, Mridula Singh, Marc Roeschlin, Aanjhan Ranganathan, Srdjan Capkun (NDSS 2022)

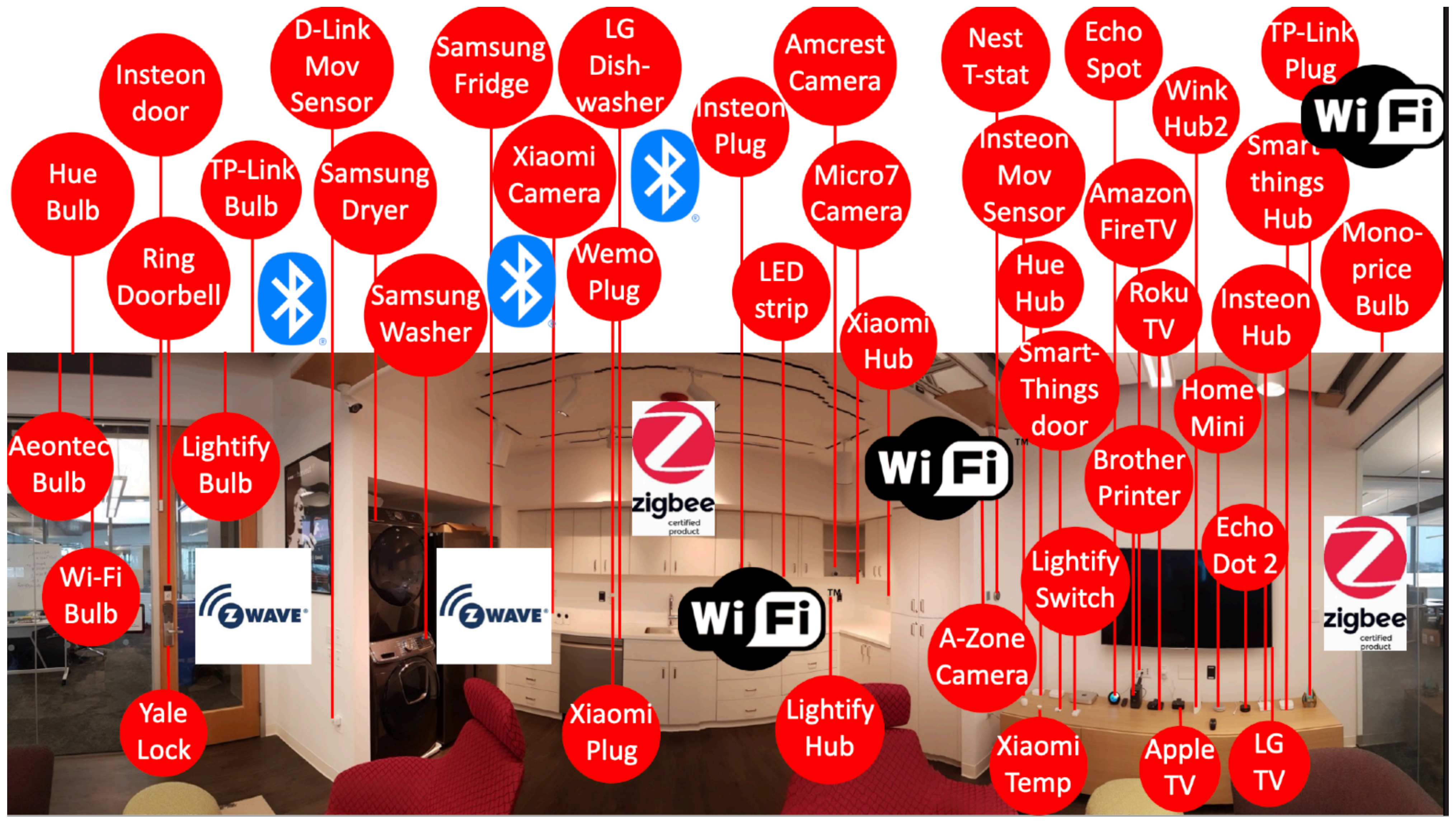
SemperFi: Anti-spoofing GPS receiver for UAVs, Harshad Sathaye, Gerald LaMountain, Pau Closas, Aanjhan Ranganathan (NDSS 2022)

Swarm Takeover through GPS Spoofing

Swarm Takeover through GPS Spoofing

Security and Privacy in xIoT

Validating and Building Trustworthy Smart Ecosystems



Mon(Iot)Or Lab at Northeastern University

Selected Research

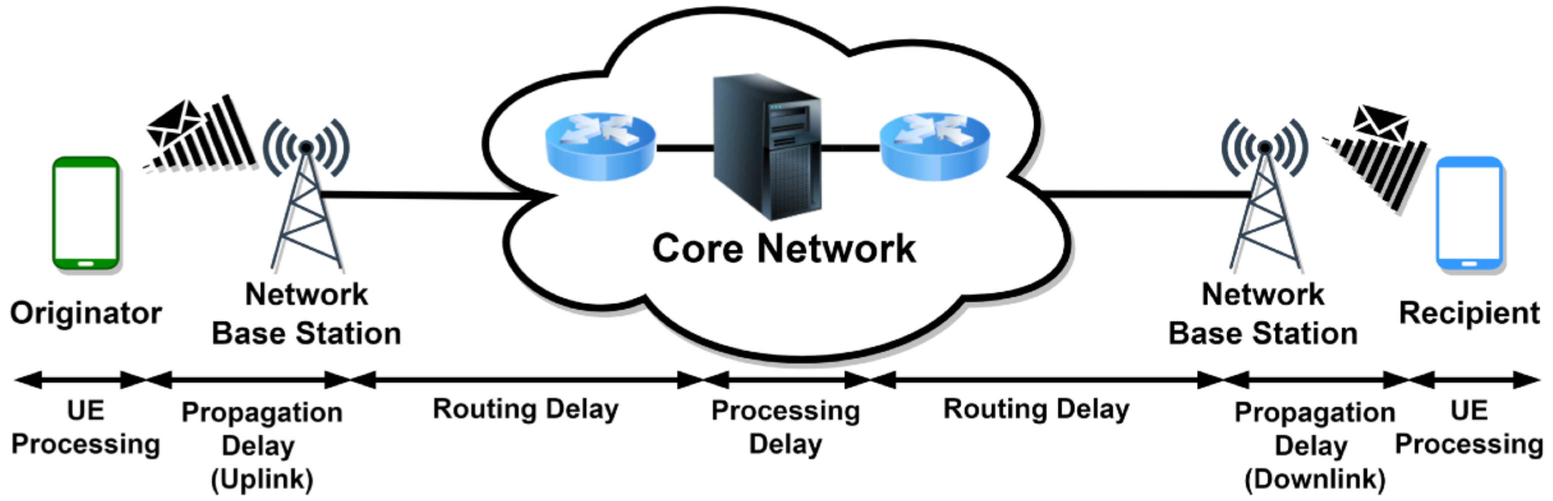
MakeShift: Security Analysis of <redacted> Wireless Gear Shifting in Bicycles, Maryam Motallebighomi, Earlence Fernandes, Aanjhan Ranganathan (Usenix WOOT 2024)

Track You: A Deep Dive into Safety Alerts for Apple AirTags, Narmeen Shafqat, Nicole Gerzon, Maggie Von Nortwick, Victor Sun, Alan Mislove, Aanjhan Ranganathan (PETS 2023)

ZLeaks: Passive Inference Attacks on Zigbee based Smart Homes, Narmeen Shafqat, Daniel Dubois, Dave Choffnes, Aaron Schulman, Dinesh Bharadia, Aanjhan Ranganathan (ACNS 2022, *Best Student Paper Award*)

Privacy-Preserving Positioning in Wi-Fi Fine Timing Measurements, Domien Schepers, Aanjhan Ranganathan (PETS 2022)

Wi-Fi and Cellular Security



Selected Research

Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues
Domien Schepers, Aanjhan Ranganathan, Mathy Vanhoef (USENIX Security 2023)

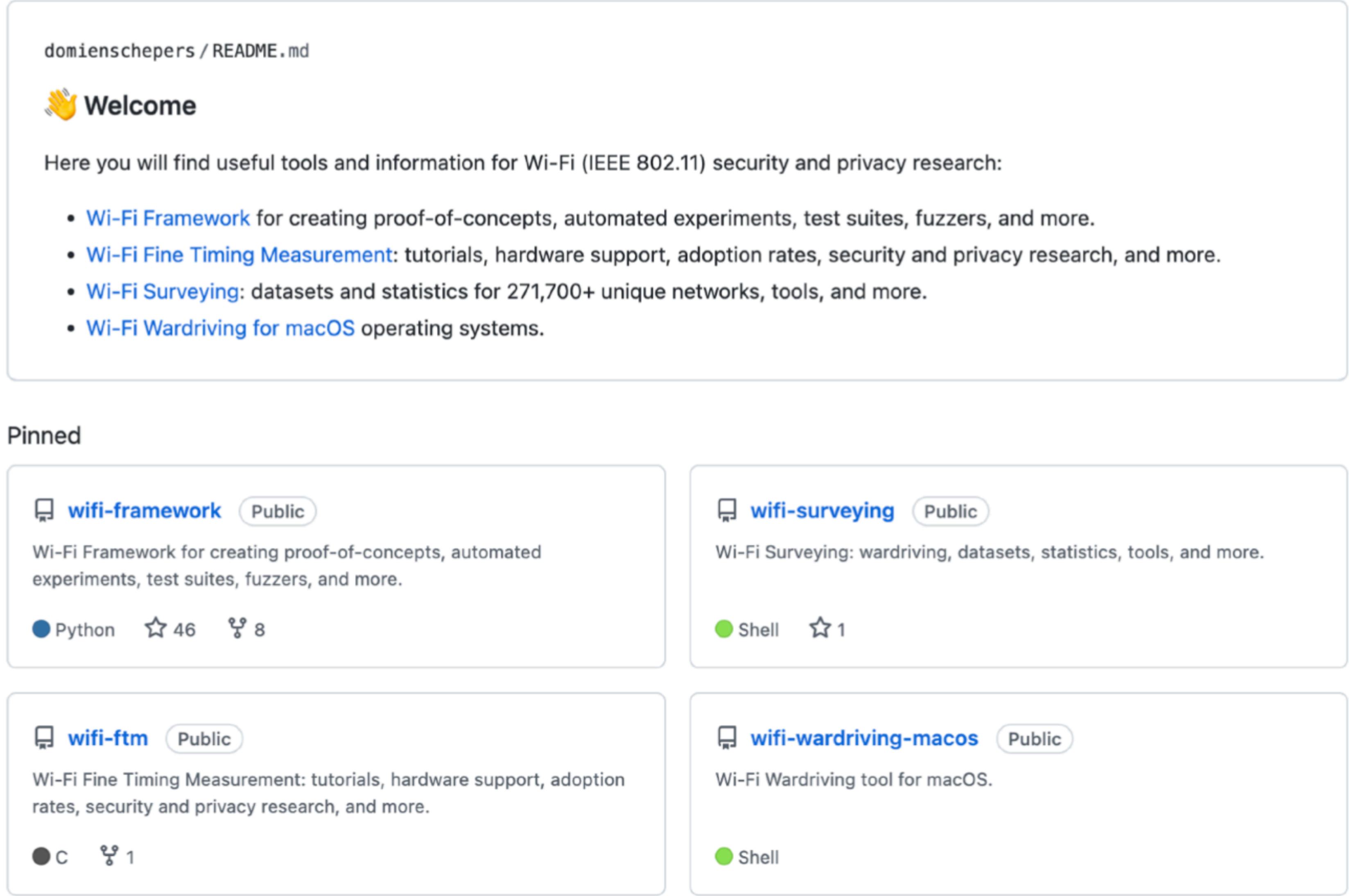
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings

Evangelos Bitsikas, Theo Schnitzler, Christina Poepper, Aanjhan Ranganathan (USENIX Security 2023)

On the Robustness of Wi-Fi Deauthentication Countermeasures, Domien Schepers, *Aanjhan Ranganathan*, Mathy Vanhoef (Wisec 2022)

Broader Impact

Repositories



domienschepers / README.md

👋 **Welcome**

Here you will find useful tools and information for Wi-Fi (IEEE 802.11) security and privacy research:

- Wi-Fi Framework for creating proof-of-concepts, automated experiments, test suites, fuzzers, and more.
- Wi-Fi Fine Timing Measurement: tutorials, hardware support, adoption rates, security and privacy research, and more.
- Wi-Fi Surveying: datasets and statistics for 271,700+ unique networks, tools, and more.
- Wi-Fi Wardriving for macOS operating systems.

Pinned

wifi-framework Public
Wi-Fi Framework for creating proof-of-concepts, automated experiments, test suites, fuzzers, and more.
● Python ☆ 46 8

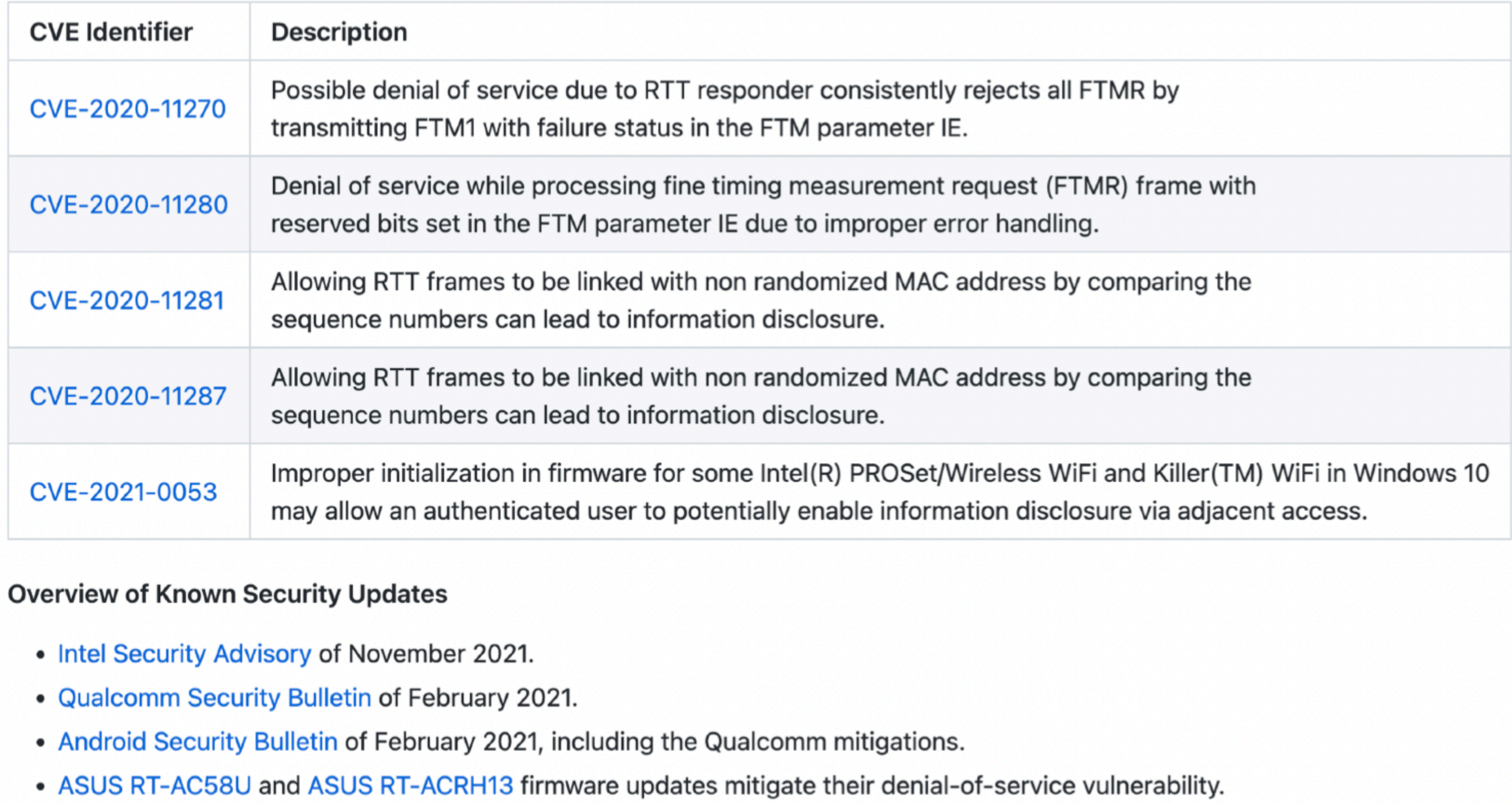
wifi-surveying Public
Wi-Fi Surveying: wardriving, datasets, statistics, tools, and more.
● Shell ☆ 1

wifi-ftm Public
Wi-Fi Fine Timing Measurement: tutorials, hardware support, adoption rates, security and privacy research, and more.
● C 1

wifi-wardriving-macos Public
Wi-Fi Wardriving tool for macOS.
● Shell

Github

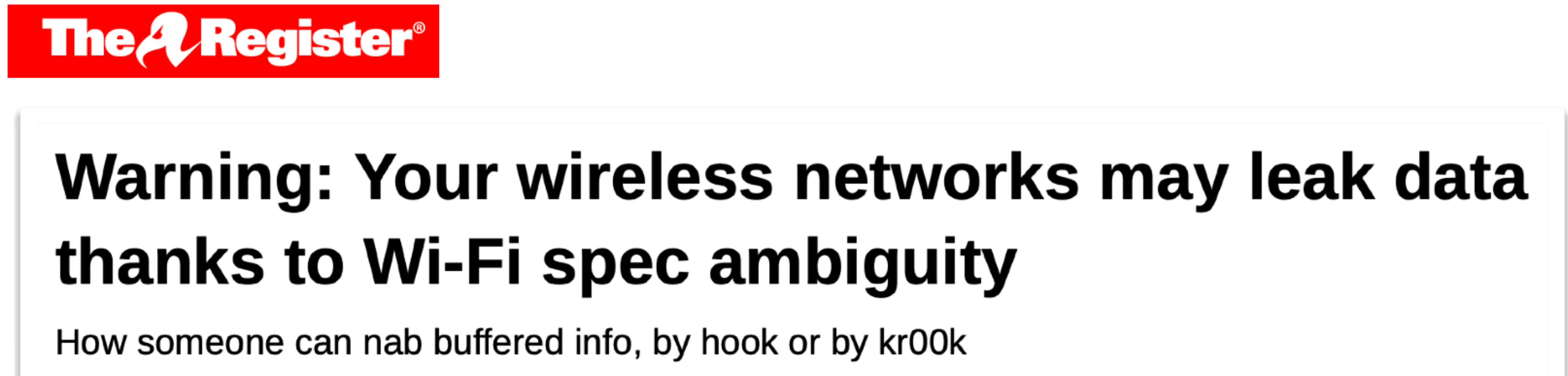
CVE Identifiers



CVE Identifier	Description
CVE-2020-11270	Possible denial of service due to RTT responder consistently rejects all FTMR by transmitting FTM1 with failure status in the FTM parameter IE.
CVE-2020-11280	Denial of service while processing fine timing measurement request (FTMR) frame with reserved bits set in the FTM parameter IE due to improper error handling.
CVE-2020-11281	Allowing RTT frames to be linked with non randomized MAC address by comparing the sequence numbers can lead to information disclosure.
CVE-2020-11287	Allowing RTT frames to be linked with non randomized MAC address by comparing the sequence numbers can lead to information disclosure.
CVE-2021-0053	Improper initialization in firmware for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi in Windows 10 may allow an authenticated user to potentially enable information disclosure via adjacent access.

Overview of Known Security Updates

- Intel Security Advisory of November 2021.
- Qualcomm Security Bulletin of February 2021.
- Android Security Bulletin of February 2021, including the Qualcomm mitigations.
- ASUS RT-AC58U and ASUS RT-ACRH13 firmware updates mitigate their denial-of-service vulnerability.

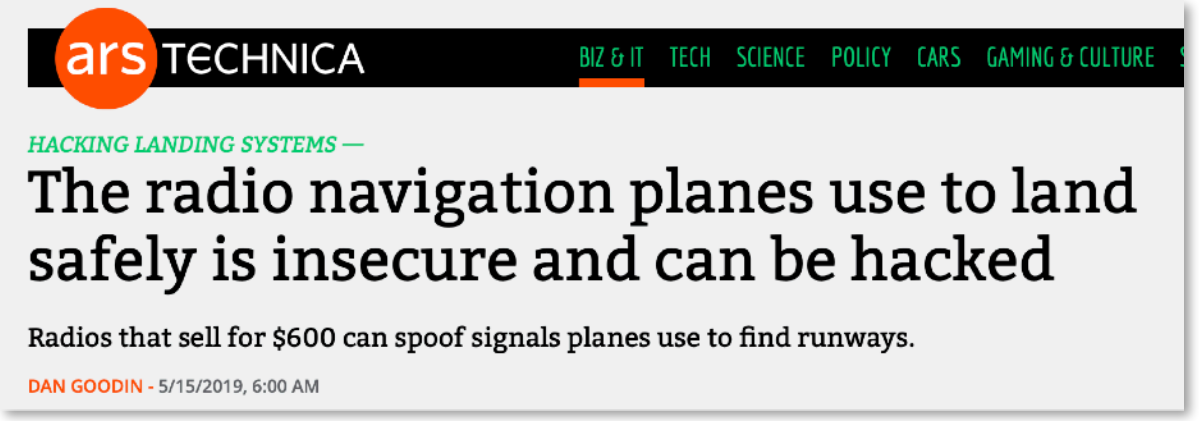


The Register®

Warning: Your wireless networks may leak data thanks to Wi-Fi spec ambiguity

How someone can nab buffered info, by hook or by kr00k

Thomas Claburn

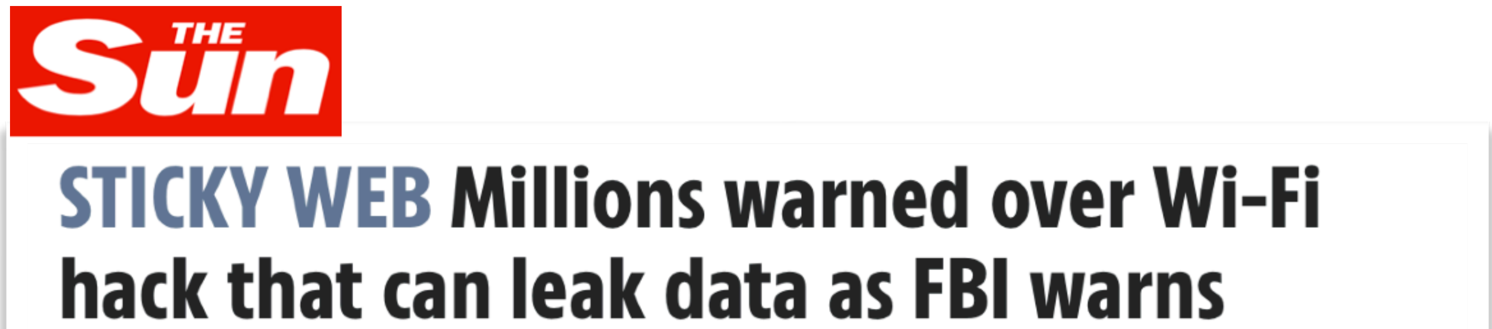


HACKING LANDING SYSTEMS —

The radio navigation planes use to land safely is insecure and can be hacked

Radios that sell for $600 can spoof signals planes use to find runways.

DAN GOODIN - 5/15/2019, 6:00 AM

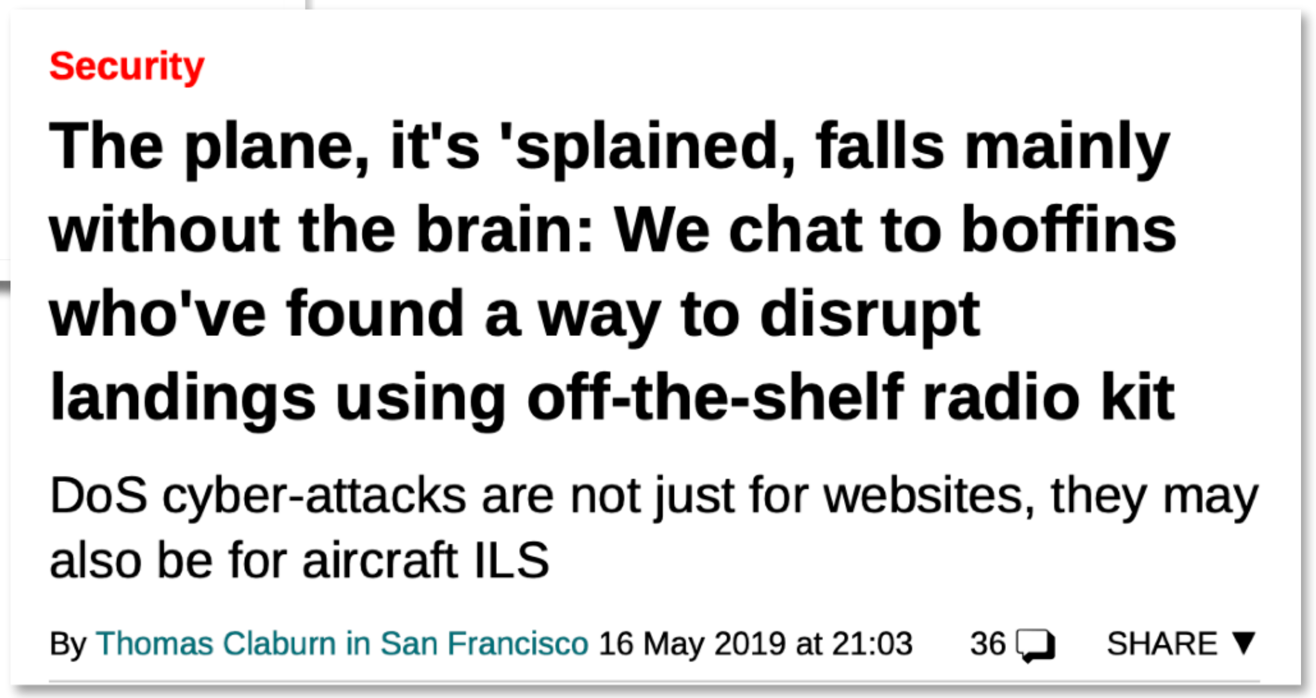


The Sun

STICKY WEB Millions warned over Wi-Fi hack that can leak data as FBI warns against using public networks

Millie Turner

Published: 12:13, 13 Apr 2023 | Updated: 12:13, 13 Apr 2023



Security

The plane, it's 'splained, falls mainly without the brain: We chat to boffins who've found a way to disrupt landings using off-the-shelf radio kit

DoS cyber-attacks are not just for websites, they may also be for aircraft ILS

By Thomas Claburn in San Francisco 16 May 2019 at 21:03 36 SHARE ▼

Evolution of Cellular Networks

From Analog to 5G

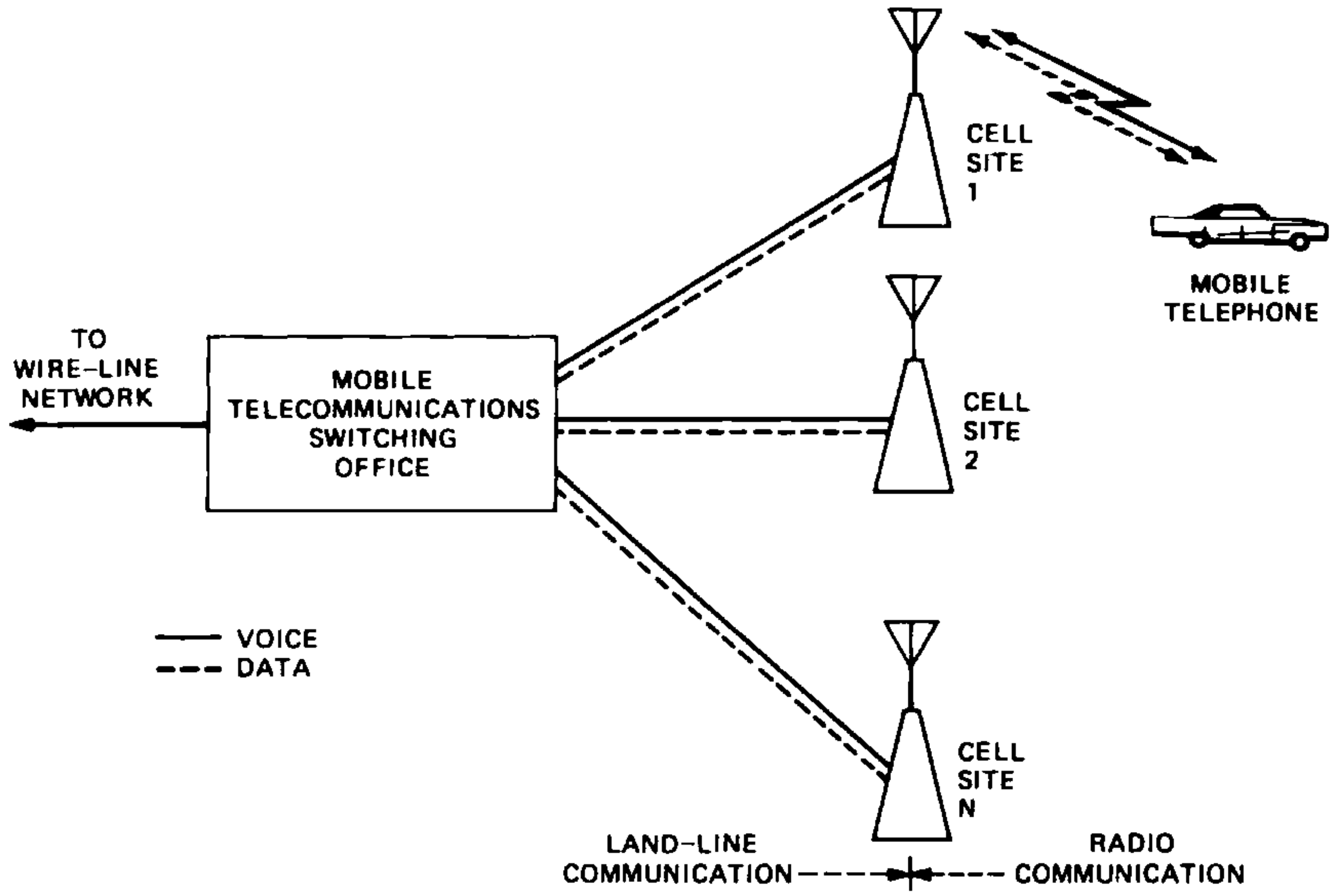
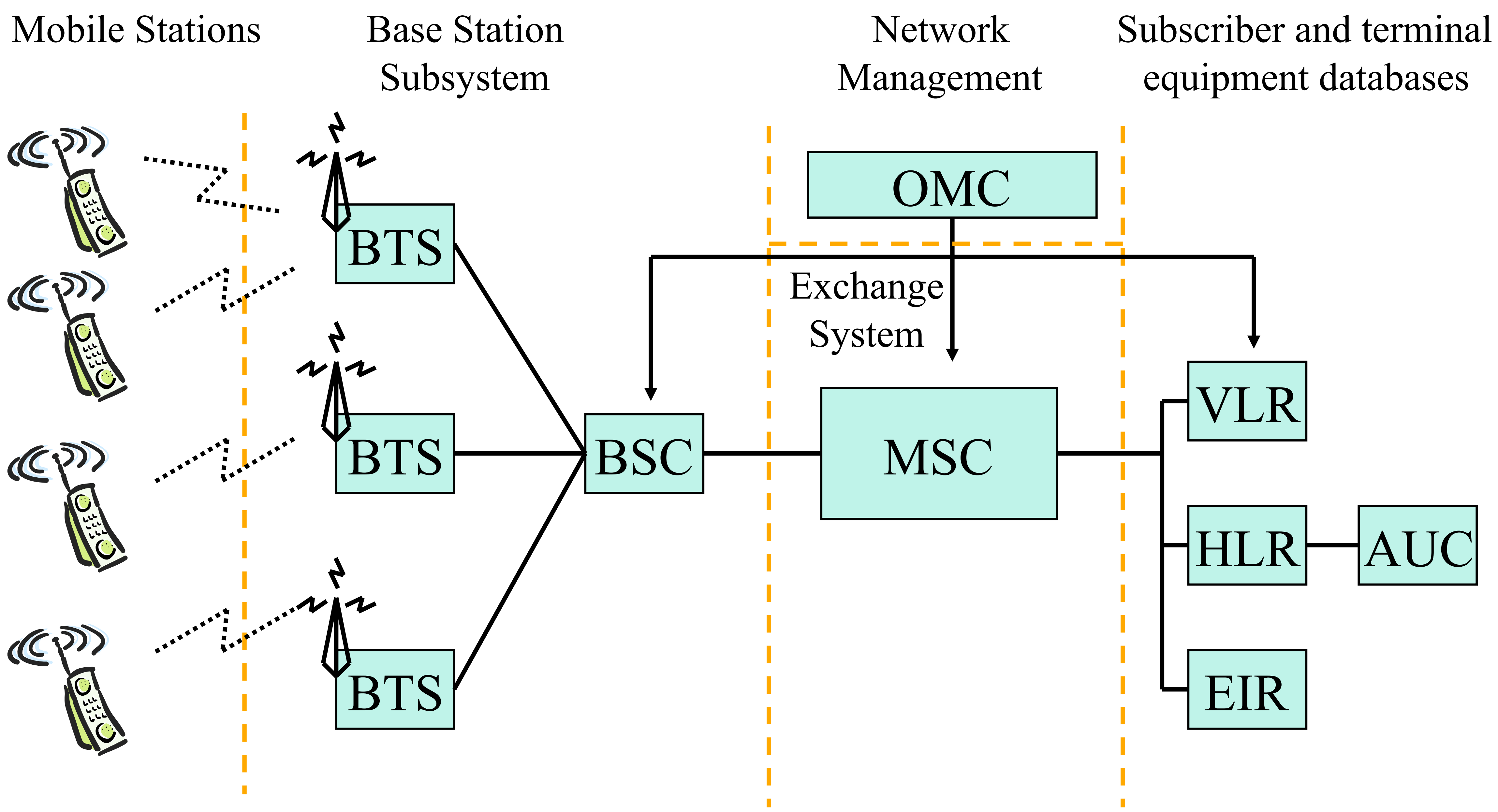


Fig. 3—AMPS system control elements.

46 THE BELL SYSTEM TECHNICAL JOURNAL, JANUARY 1979



HLR = Home Location Register

AC = Authentication center

VLR = Visitor Location Register

EIR - Equipment Identity Register

Today's 5G networks..

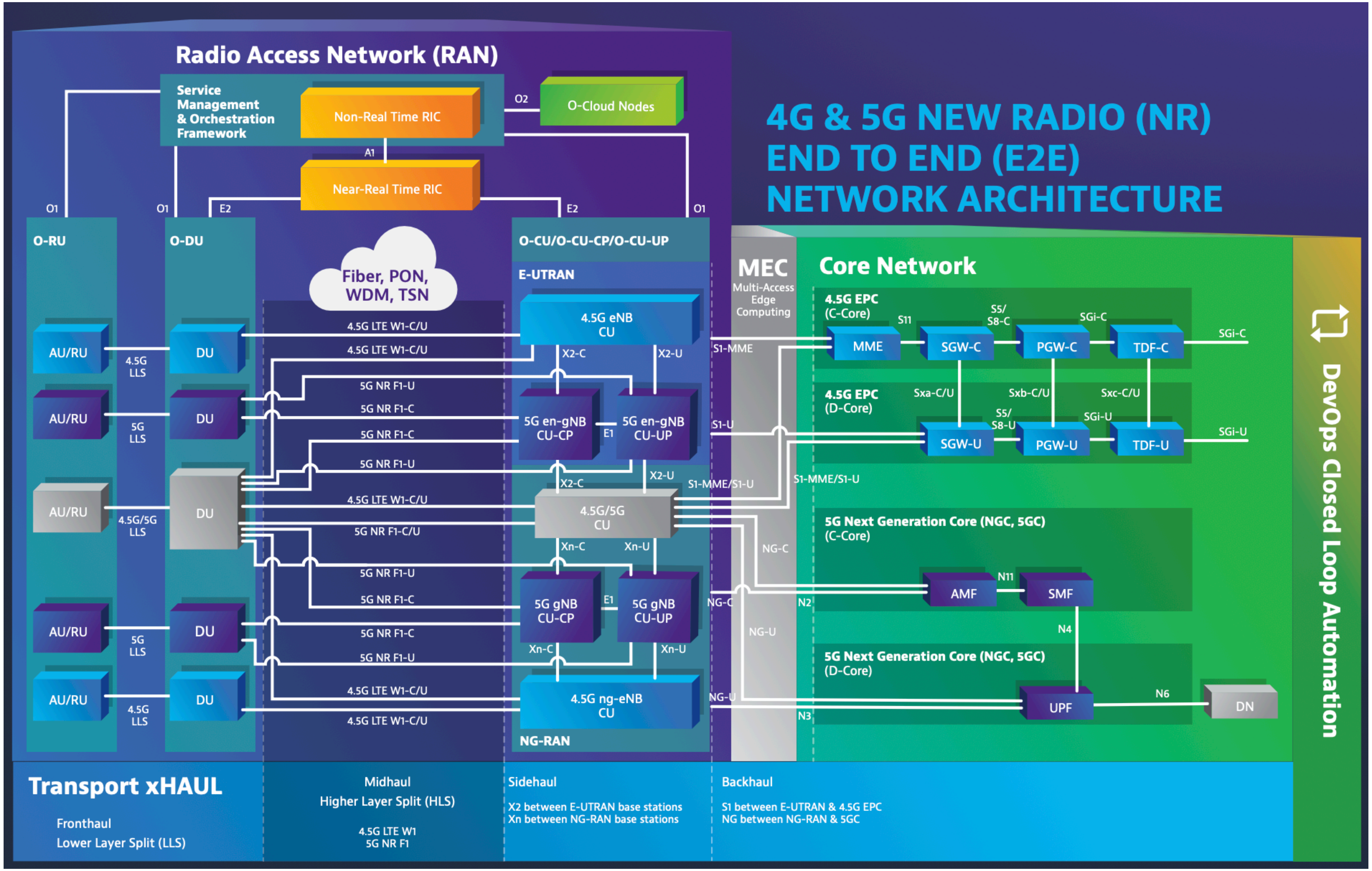
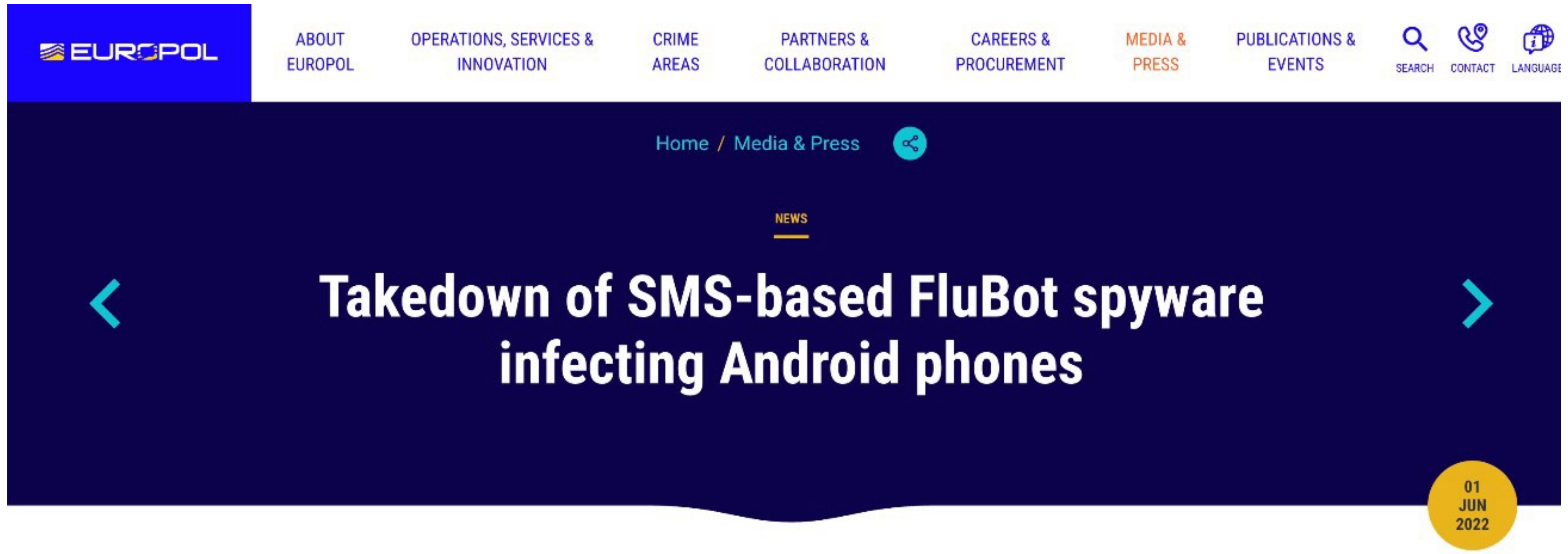


Image source: VIAVI

SMS-based Location Inference

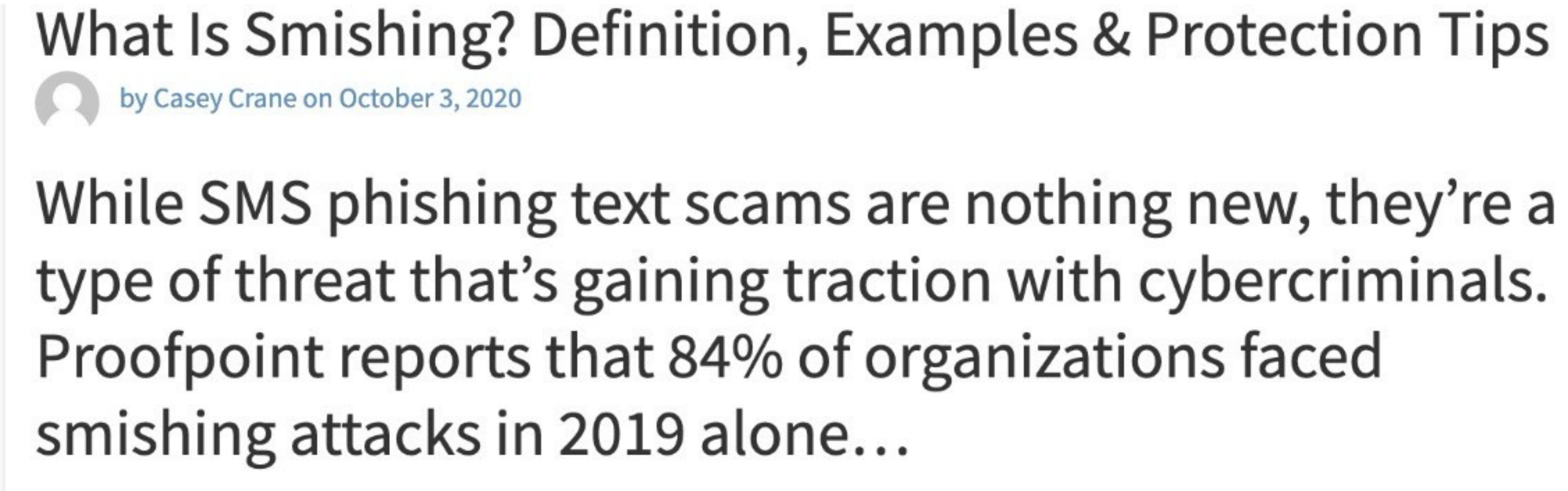
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings
Evangelos Bitsikas, Theodor Schnitzler, Christina Pöpper, Aanjhan Ranganathan (Usenix Security 2023)

SMS Insecurity



Takedown of SMS-based FluBot spyware infecting Android phones

01 JUN 2022

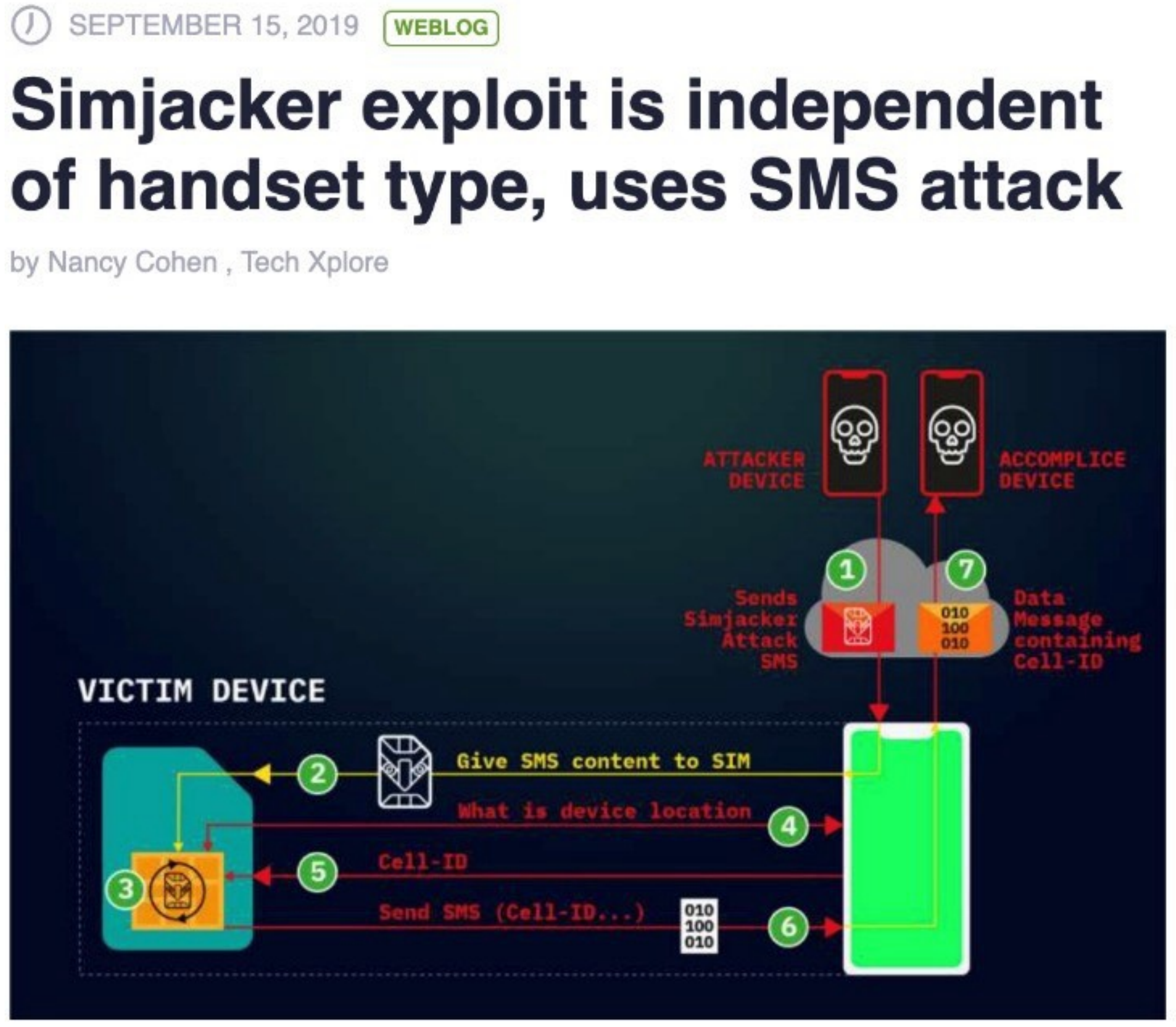


What Is Smishing? Definition, Examples & Protection Tips

by Casey Crane on October 3, 2020

While SMS phishing text scams are nothing new, they're a type of threat that's gaining traction with cybercriminals. Proofpoint reports that 84% of organizations faced smishing attacks in 2019 alone…

ETSI TS 123 040 V17.3.0 (2023-07)

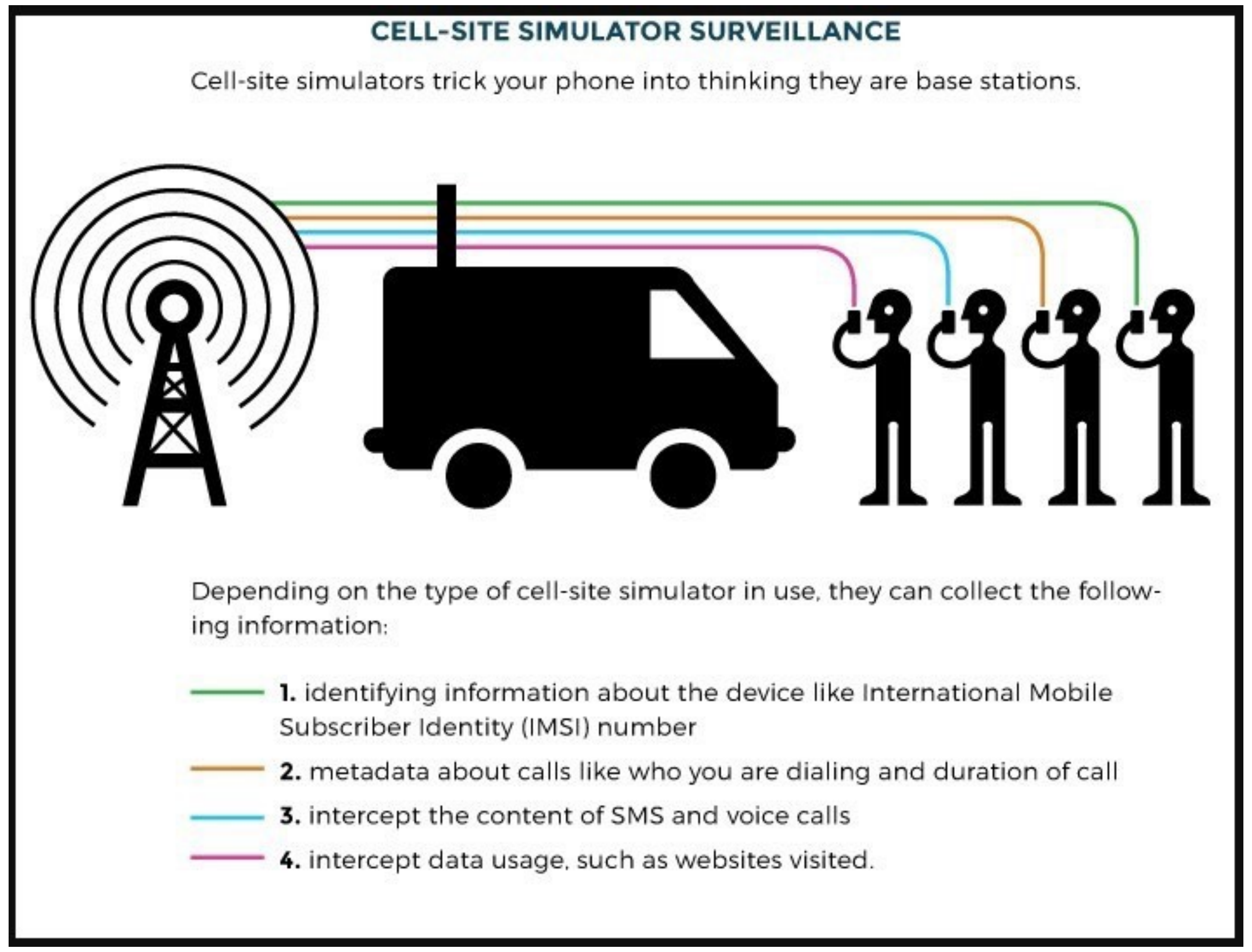


SEPTEMBER 15, 2019 WEBLOG

Simjacker exploit is independent of handset type, uses SMS attack

by Nancy Cohen , Tech Xplore

Credit: AdaptiveMobile Security



CELL-SITE SIMULATOR SURVEILLANCE

Cell-site simulators trick your phone into thinking they are base stations.

Depending on the type of cell-site simulator in use, they can collect the following information:

1. identifying information about the device like International Mobile Subscriber Identity (IMSI) number
2. metadata about calls like who you are dialing and duration of call
3. intercept the content of SMS and voice calls
4. intercept data usage, such as websites visited.

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Technical realization of the Short Message Service (SMS)
(3GPP TS 23.040 version 17.3.0 Release 17)

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

Attack Overview

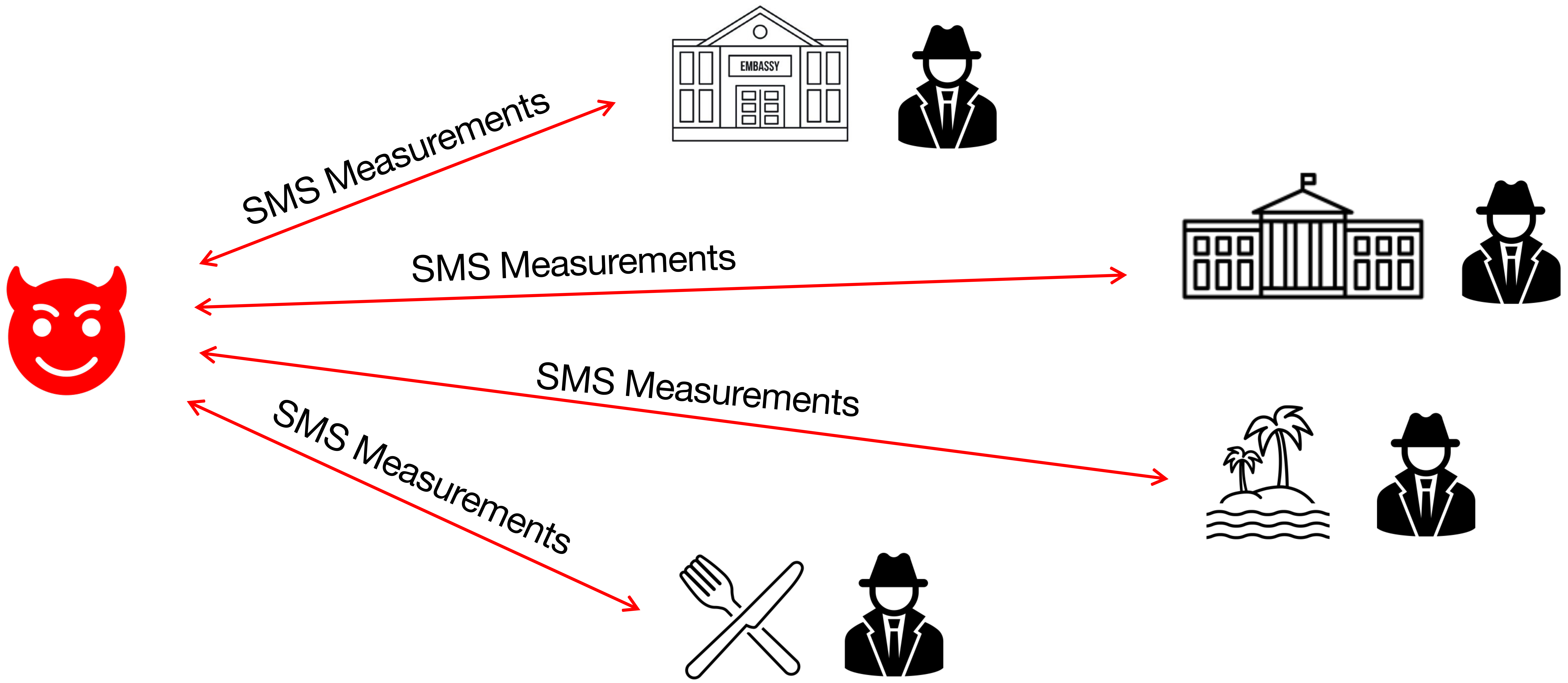
Goal: Identify the location of the SMS recipient-victim

Steps:

1. Know the 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 techniques.

Example Scenario

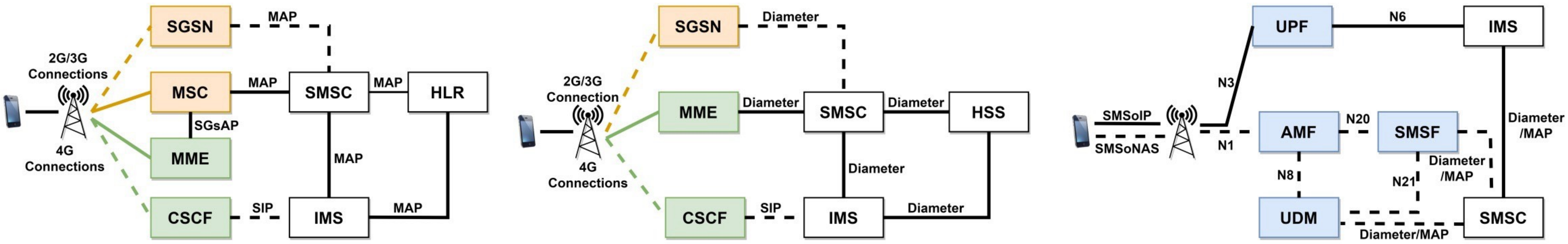
Tracking a diplomat to routine locations



Our Contributions

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

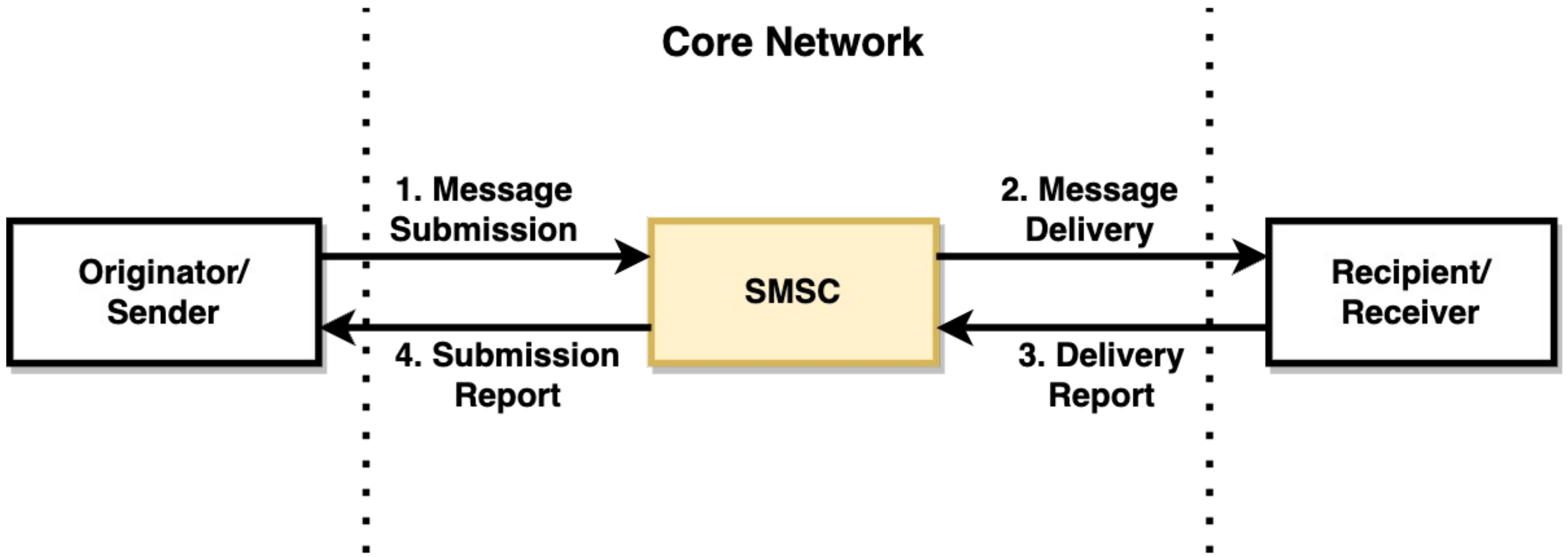
SMS Network Architecture



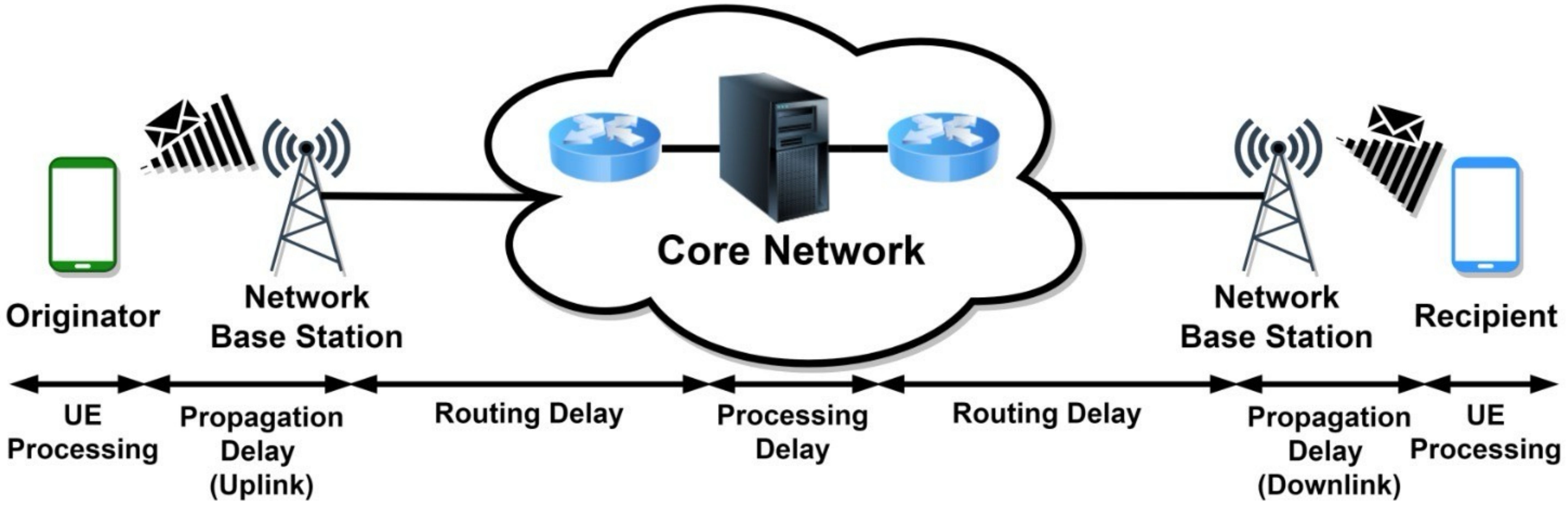
(a) 2G/3G/4G with MAP and IMS

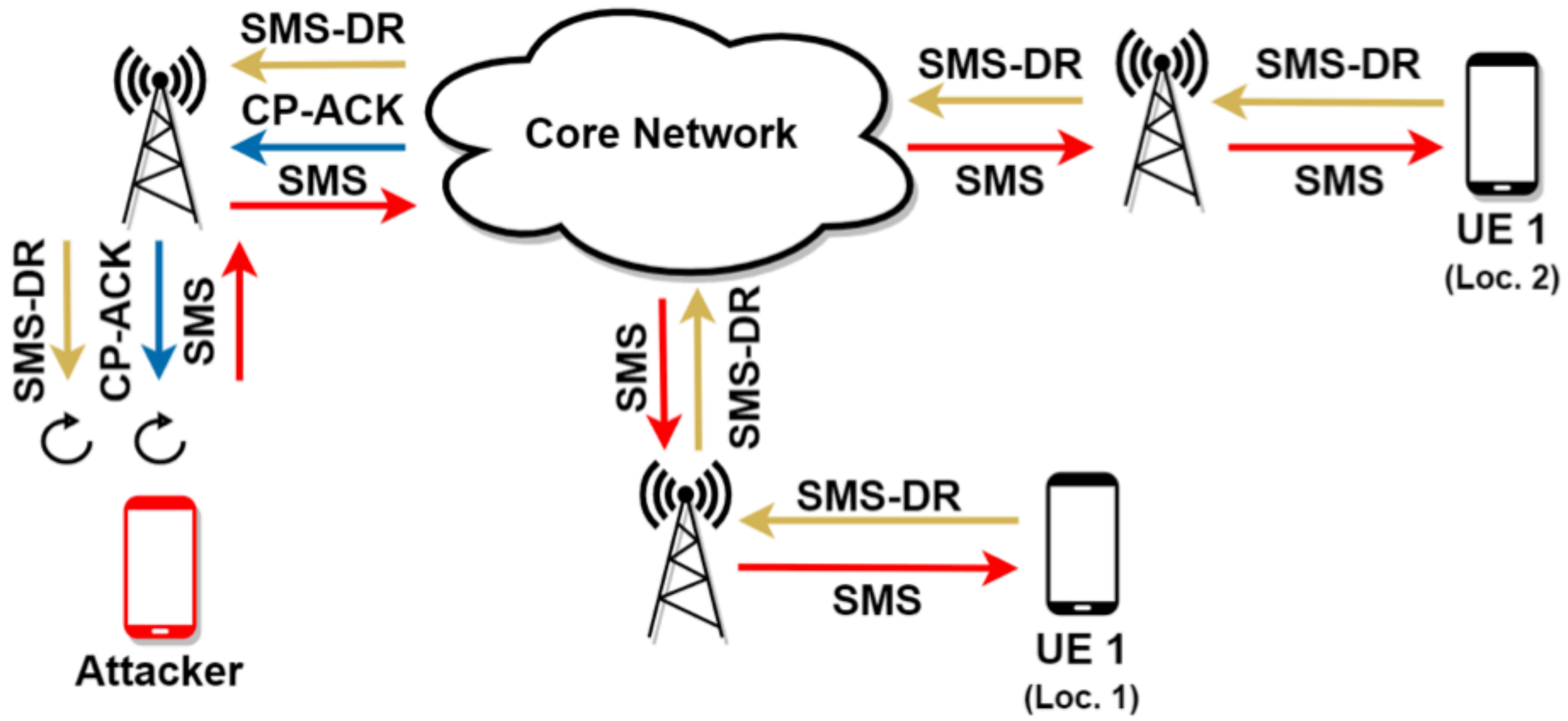
(b) 2G/3G/4G with Diameter and IMS

(c) 5G Standalone with IMS and NAS

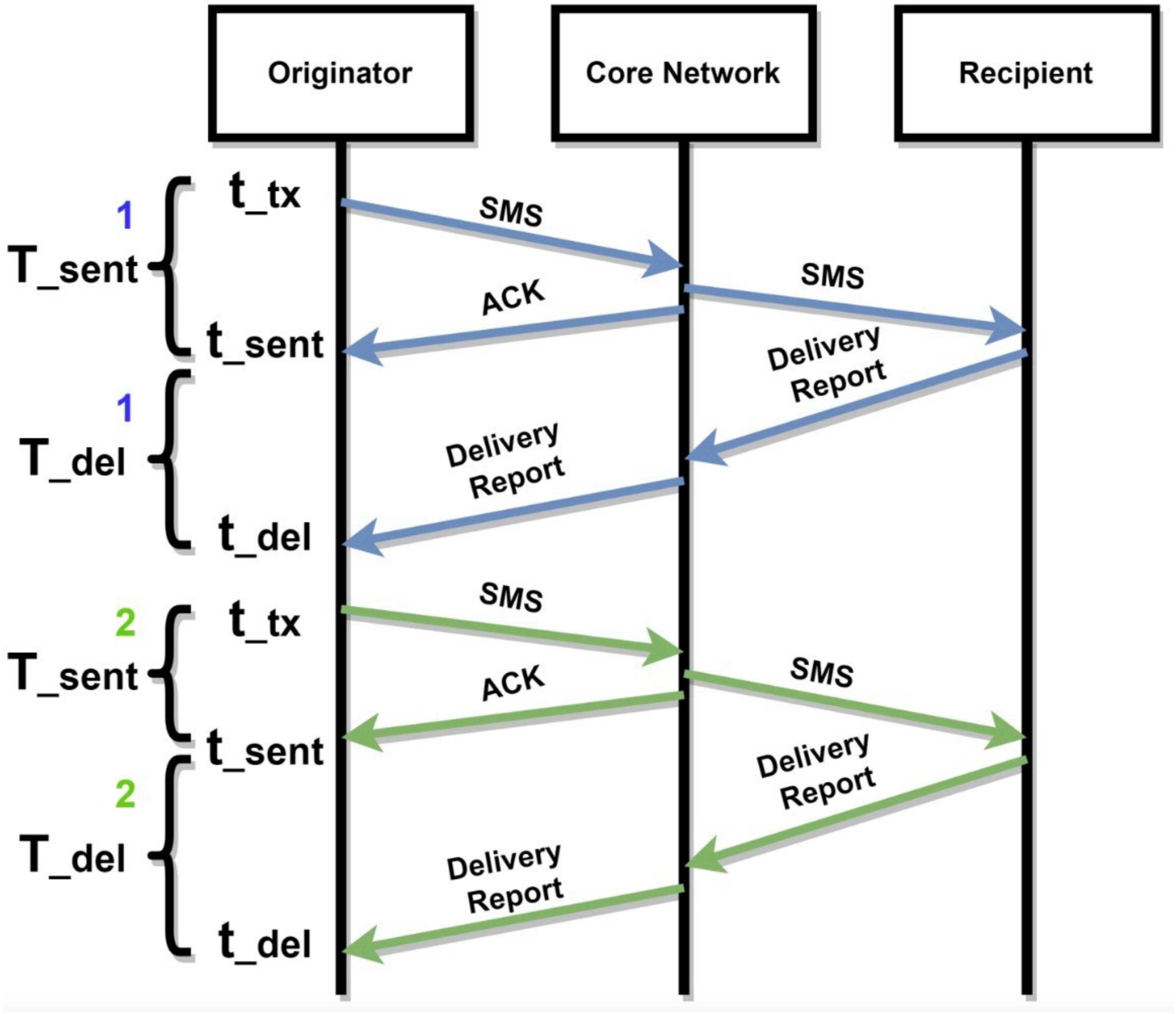


SMS Timing Delays and Flow





SMS Timing Features



$$T_{sent} = t_{sent} - t_{tx} \tag{1}$$

$$T_{del} = t_{del} - t_{sent} \tag{2}$$

$$T_{tot} = T_{del} + T_{sent} \tag{3}$$

$$P = \frac{T_{del}}{T_{tot}} = \frac{t_{del} - t_{sent}}{t_{del} - t_{tx}} \tag{4}$$

Individual SMS

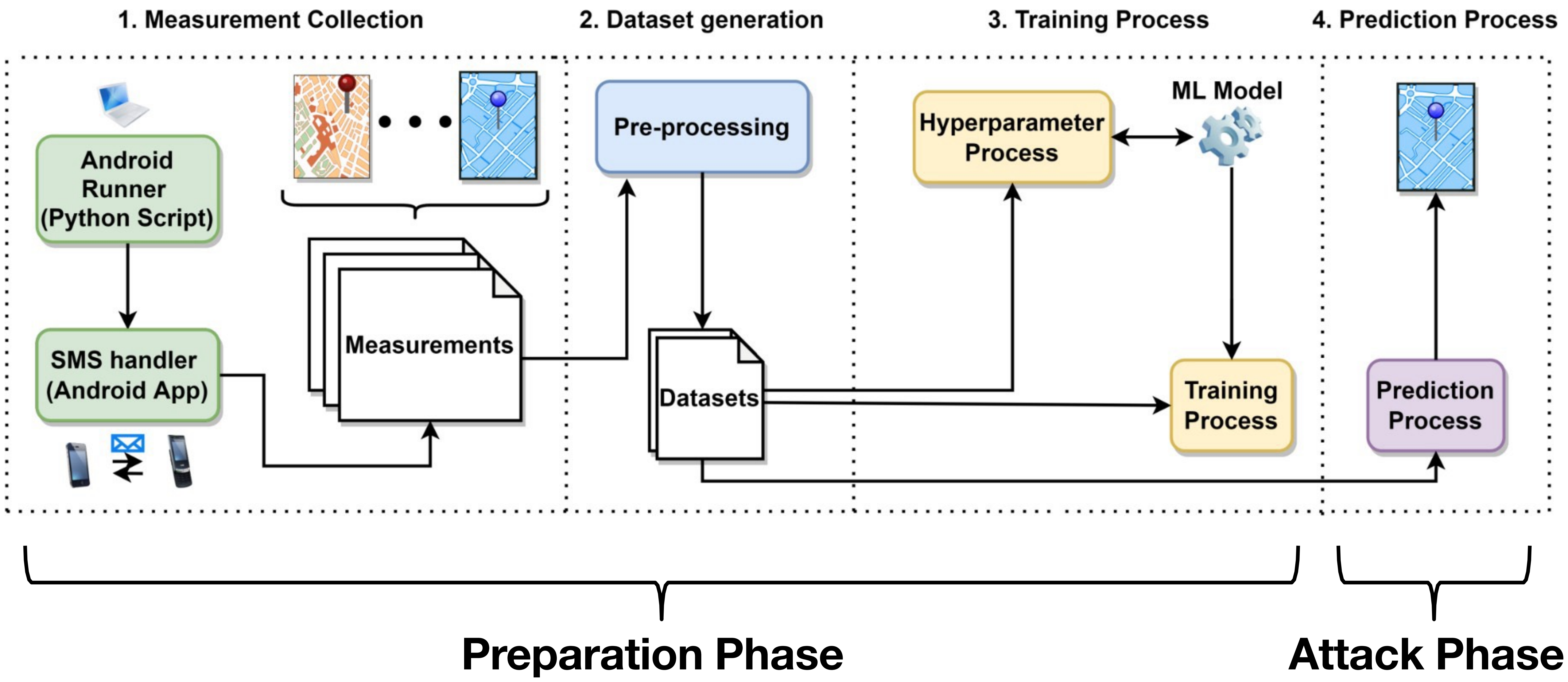
$$T_{\Delta sent} = (T^{i}_{sent} - T^{i-1}_{sent})/T^{i-1}_{sent} \tag{5}$$

$$T_{\Delta del} = (T^{i}_{del} - T^{i-1}_{del})/T^{i-1}_{del} \tag{6}$$

Consecutive SMS

The location signature/fingerprint is a combination of these six features:
(T_{sent}, T_{del}, T_{tot}, P, $T_{\Delta sent}$, $T_{\Delta del}$)

Evaluation Method and 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.

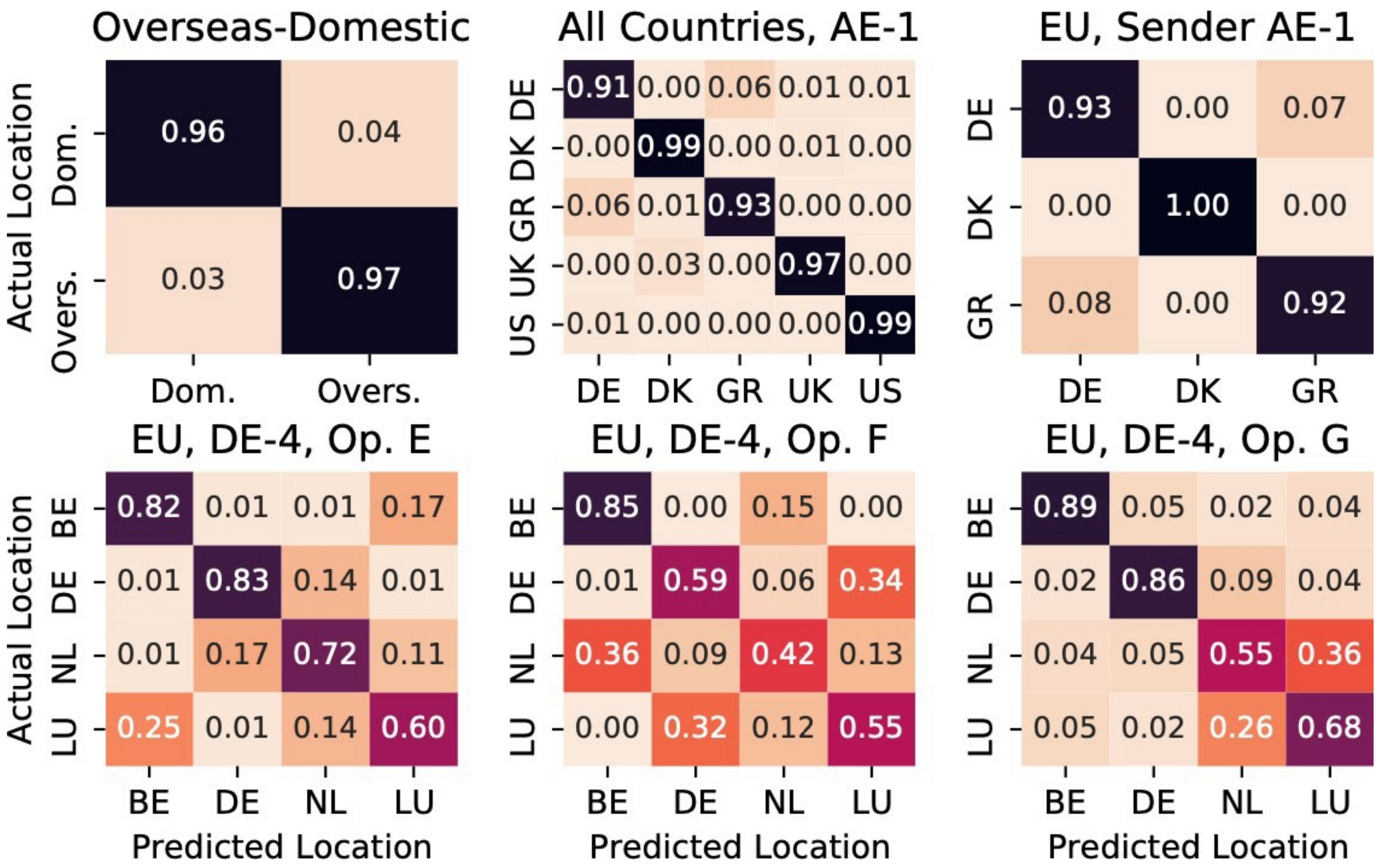
ML Parameter Tuning

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



Overseas-Domestic

	Dom.	Overs.
Dom.	0.96	0.04
Overs.	0.03	0.97

All Countries, AE-1

	DE	DK	GR	UK	US
DE	0.91	0.00	0.06	0.01	0.01
DK	0.00	0.99	0.00	0.01	0.00
GR	0.06	0.01	0.93	0.00	0.00
UK	0.00	0.03	0.00	0.97	0.00
US	0.01	0.00	0.00	0.00	0.99

EU, Sender AE-1

	DE	DK	GR
DE	0.93	0.00	0.07
DK	0.00	1.00	0.00
GR	0.08	0.00	0.92

EU, DE-4, Op. E

	BE	DE	NL	LU
BE	0.82	0.01	0.01	0.17
DE	0.01	0.83	0.14	0.01
NL	0.01	0.17	0.72	0.11
LU	0.25	0.01	0.14	0.60

EU, DE-4, Op. F

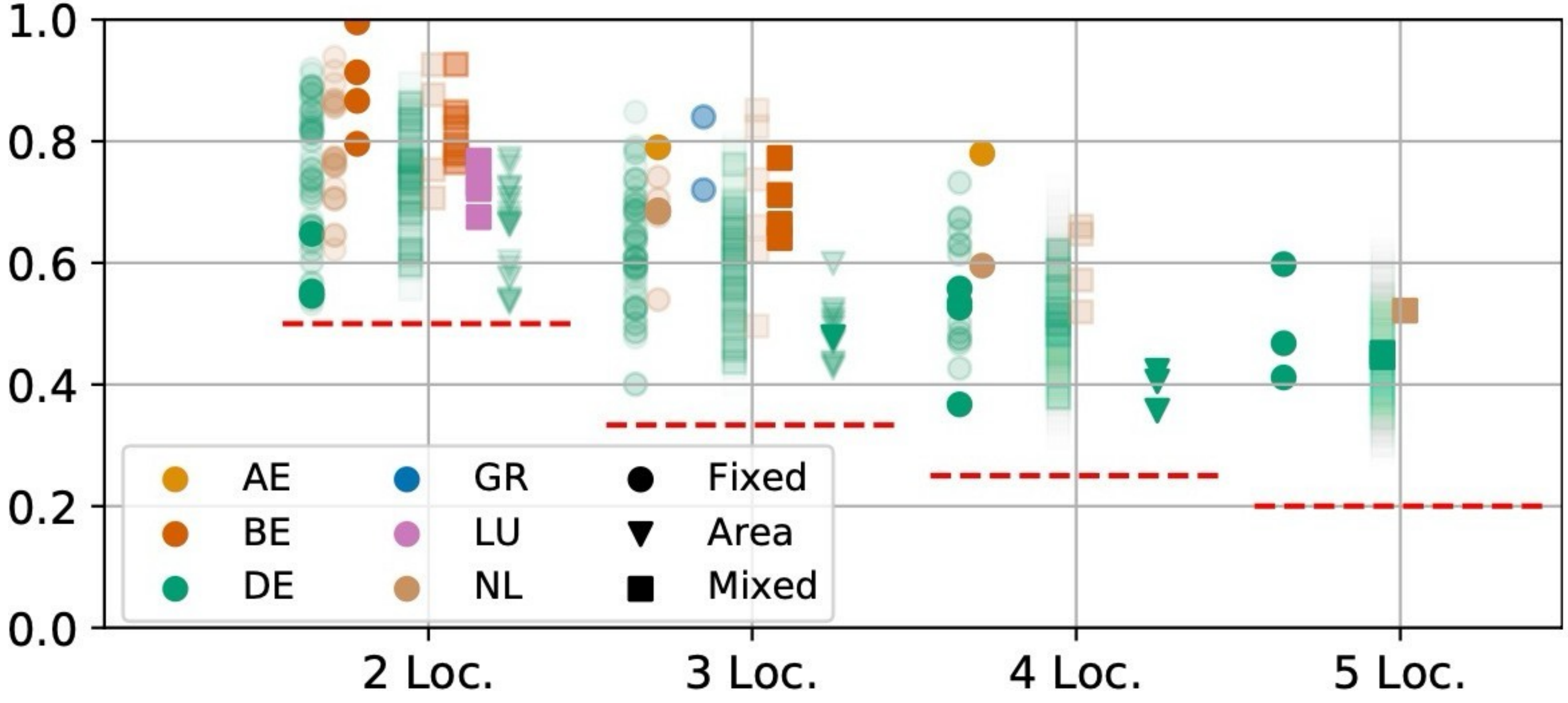
	BE	DE	NL	LU
BE	0.85	0.00	0.15	0.00
DE	0.01	0.59	0.06	0.34
NL	0.36	0.09	0.42	0.13
LU	0.00	0.32	0.12	0.55

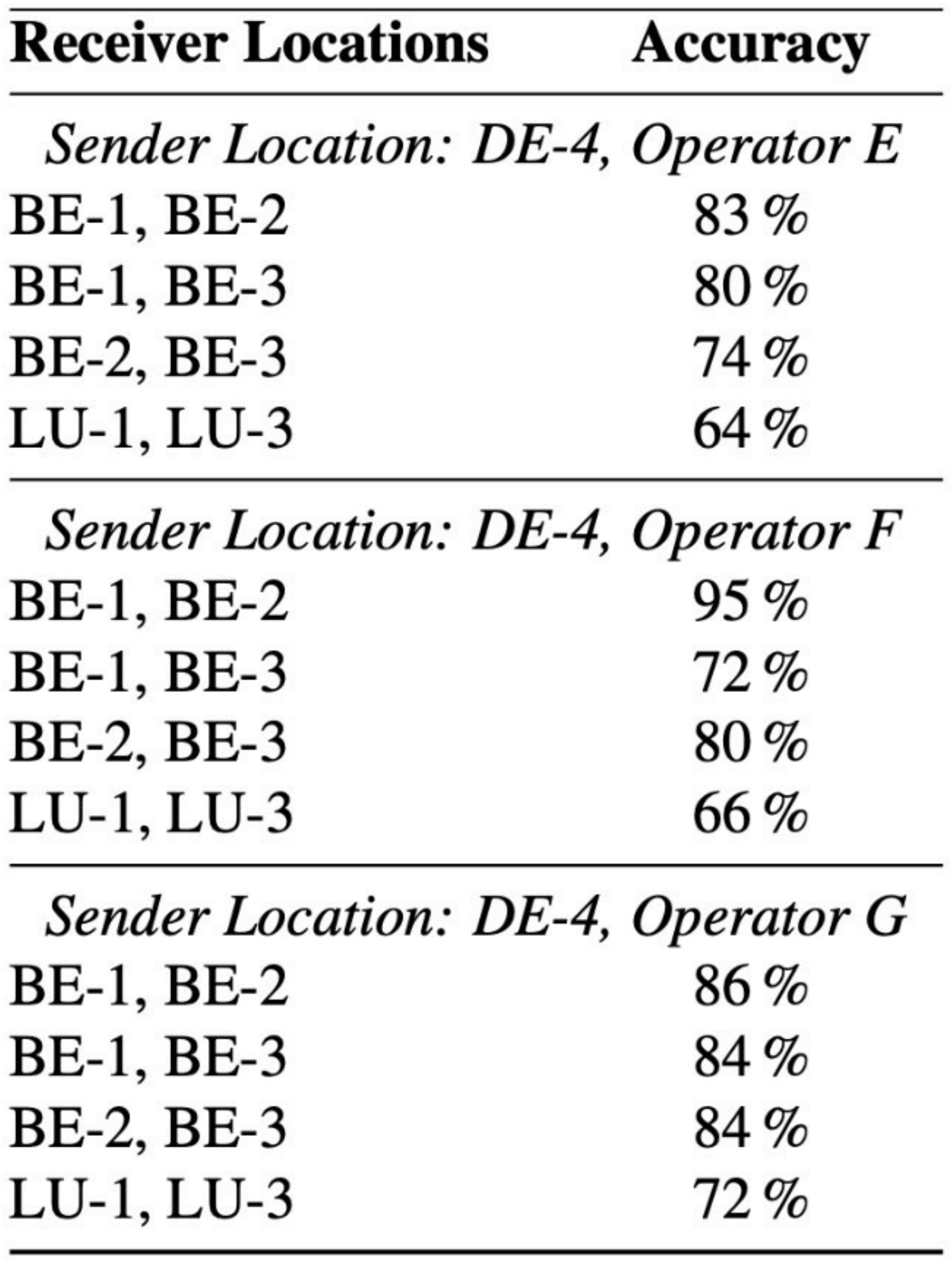
EU, DE-4, Op. G

	BE	DE	NL	LU
BE	0.89	0.05	0.02	0.04
DE	0.02	0.86	0.09	0.04
NL	0.04	0.05	0.55	0.36
LU	0.05	0.02	0.26	0.68

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

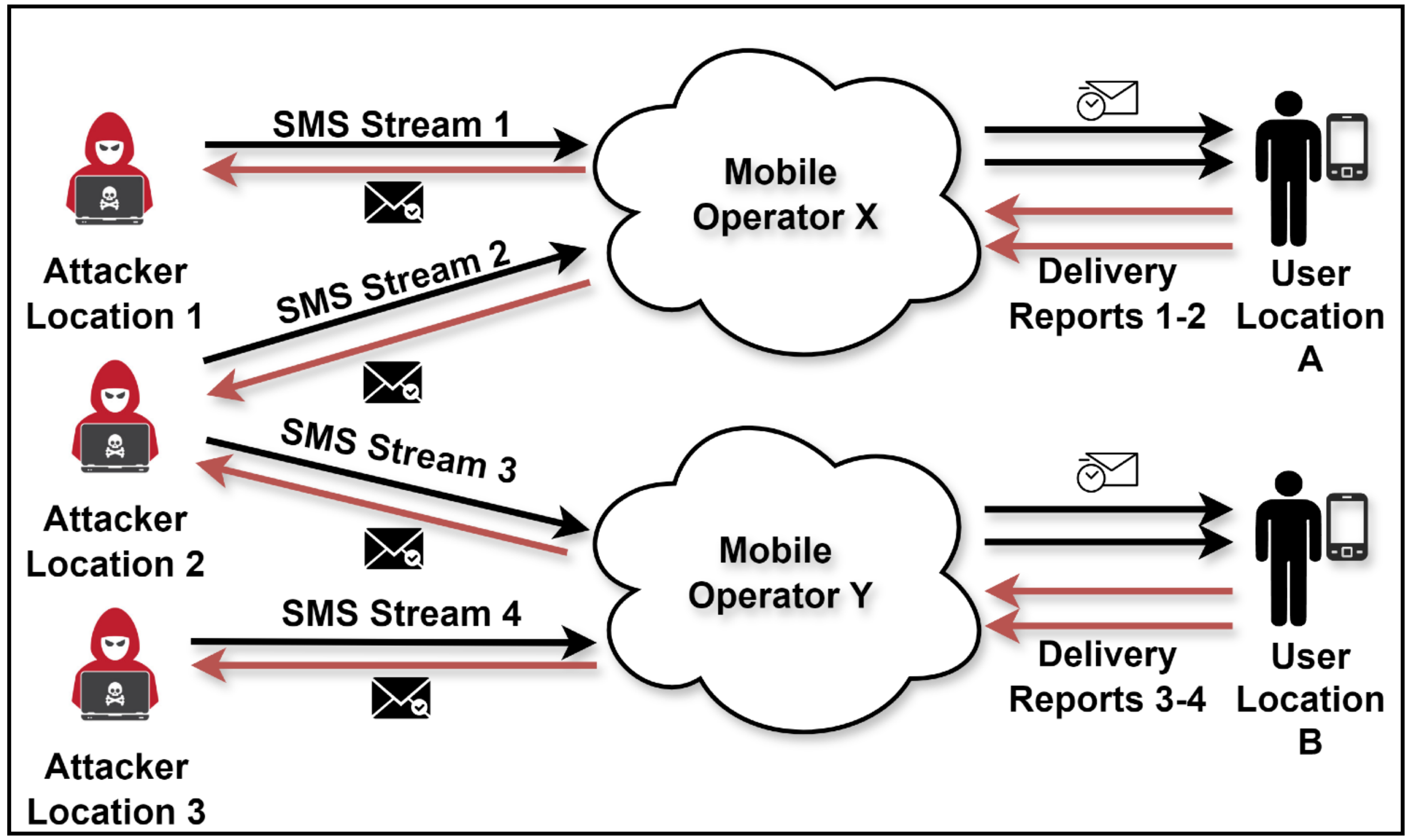
- Low attacker resources (e.g., no need for false base stations)
- Stealthy (silent SMS), no need for infrastructure access (e.g., network insider)
- Existing SMS infrastructure available across generations of cellular networks
- Well, its machine learning :)
- ***Less accurate than other sophisticated location inference attacks especially for multiple classes***
- Hard to adapt top an open-world setting
- ***Provider might block that single sender***

Can we leverage multiple senders to improve on the limitations?

Amplifying Threats:
The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks
Evangelos Bitsikas, Theodor Schnitzler, Christina Poepper, Aanjhan Ranganathan **(Usenix WOOT'24)**

Role of Multi-sender Co-ordination in Location Inference

- Significantly improve the accuracy of the model
- Combine multiple sender locations for “multilateration”
- Statistically fuse synchronized features to create robust fingerprints
- Reduce the sample sizes -> Less SMS transmissions



- Synchronous transmissions of silent SMSs
- Recording of the timing characteristics with the timestamps
- Combination and statistical fusion of sender data
- ML training and prediction

Expanded Feature Set and Fusion

Initial Features:

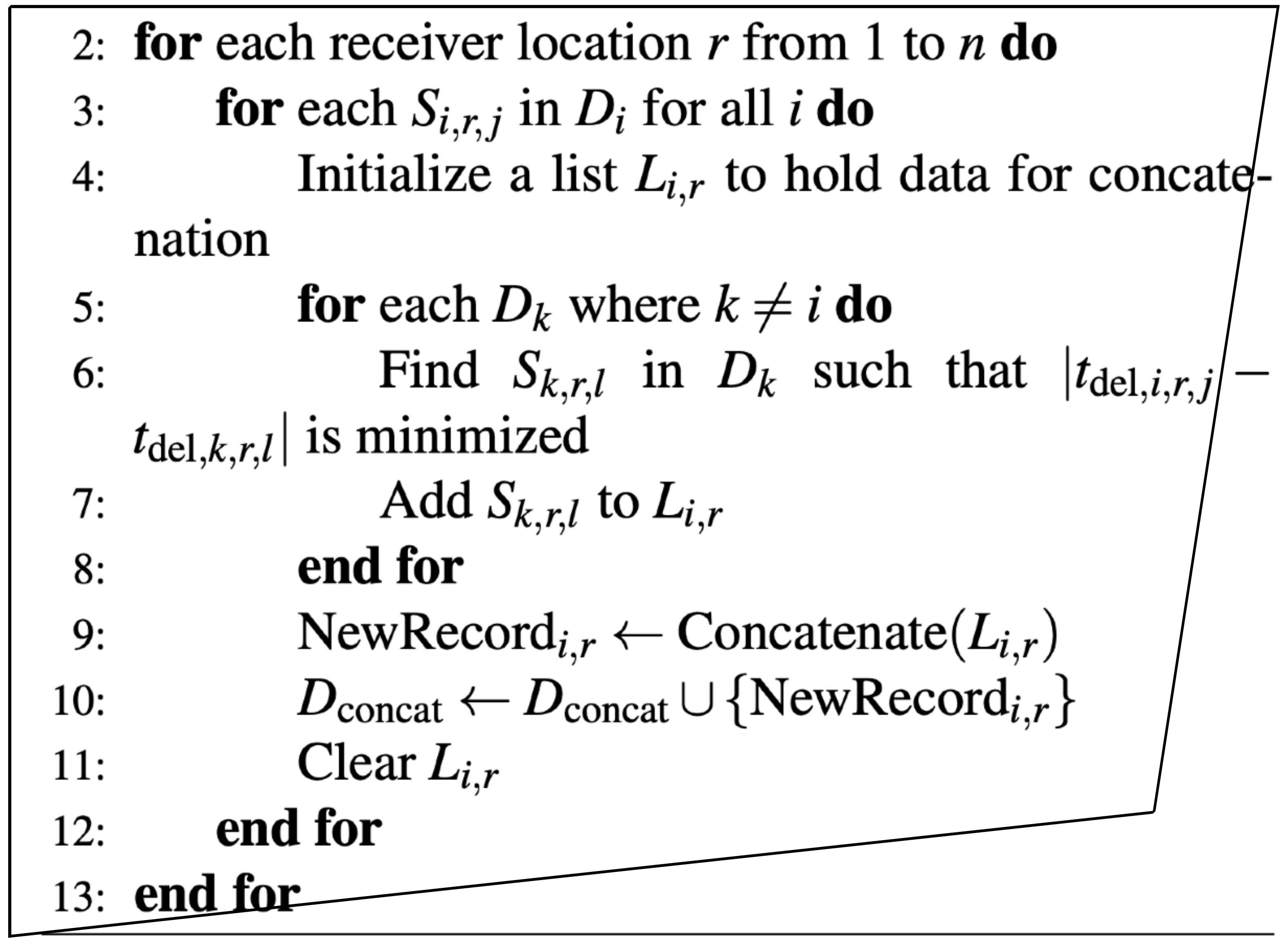
$$T_{sent} = t_{sent} - t_{tx}$$

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

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

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

On single transmissions



```
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:

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

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

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

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

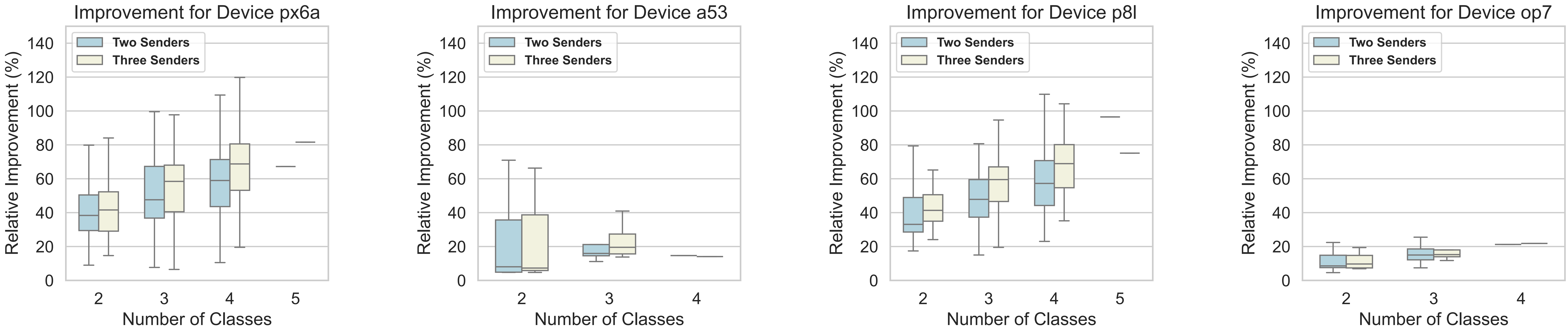
Mean, Median and Standard Deviation per two sender locations

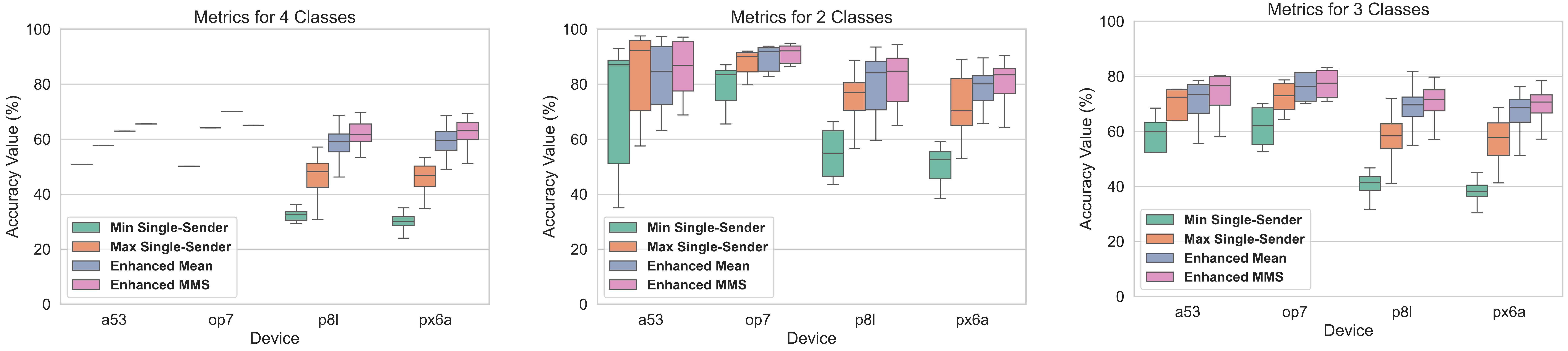
$$T_{\Delta sent} = (T_{sent}^{j} - T_{sent}^{j-1}) / T_{sent}^{j-1}$$

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

On consecutive transmissions

Results for Multi-sender





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

From threats to building frameworks and networks…

4G to 5G transition

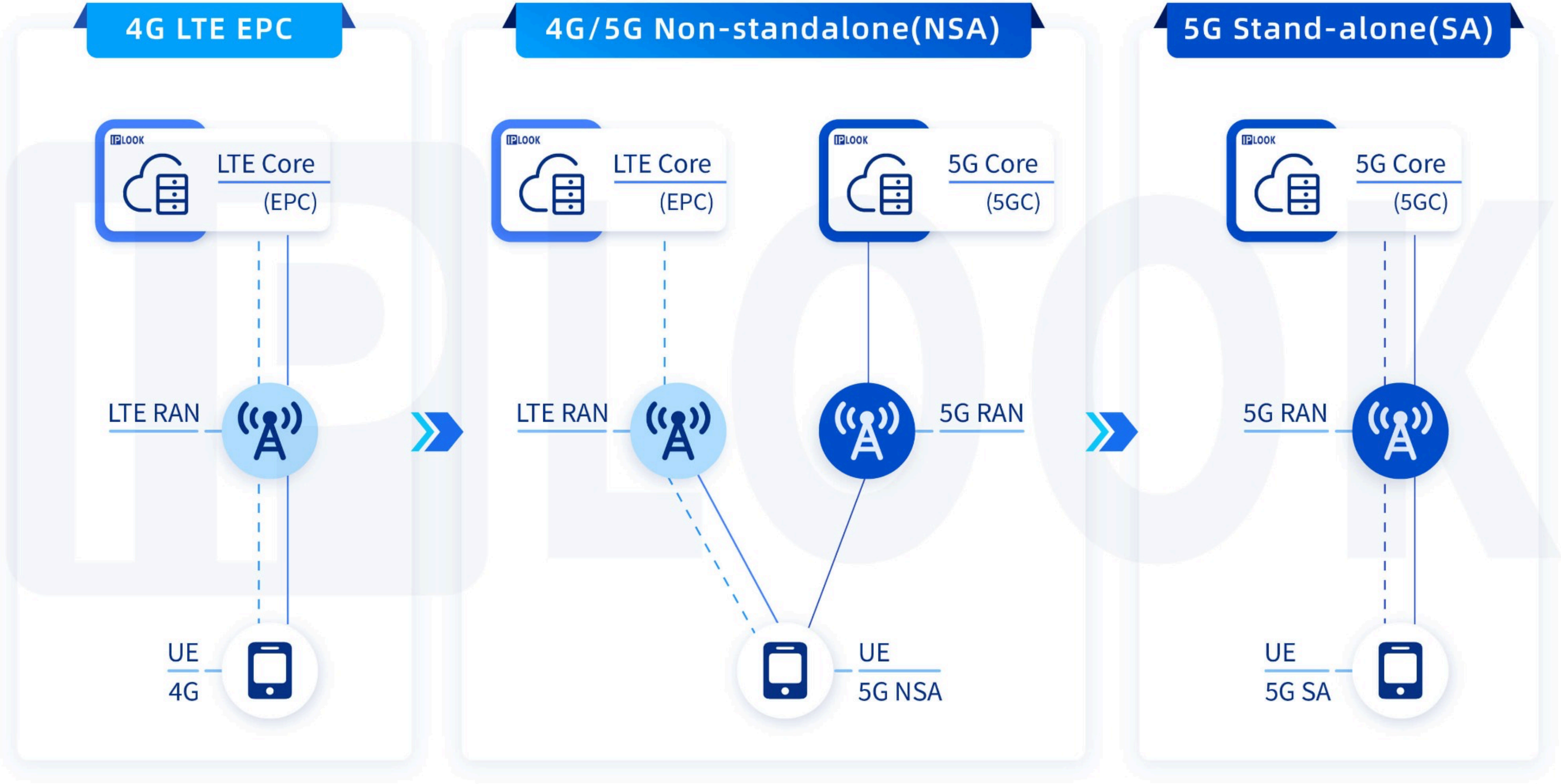


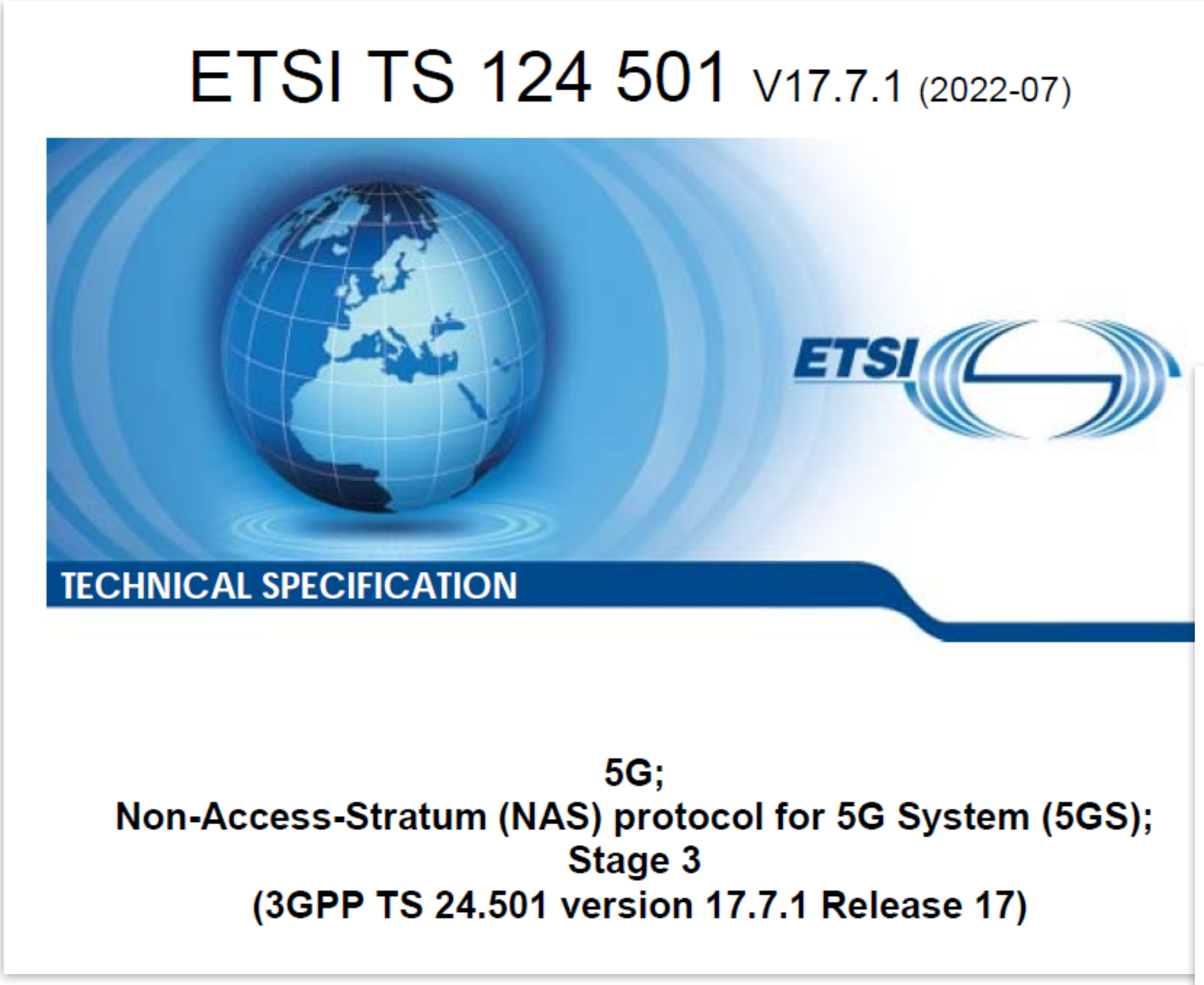
Image source: IPLook/GSMA

5G Standalone (SA)

The Real 5G

- Increasing complexity across the board even from 4G
- Network slicing, ultra-low latency, massive machine-machine communications, and so on..
- Interesting facts (in theory of course): **5G SA can support up to 1 million devices per square kilometer, ultra-low latency of 1 ms (~50 ms in 4G LTE) and is almost always used alongside technology jargons such as autonomous vehicles, mixed reality, remote surgery, etc.**

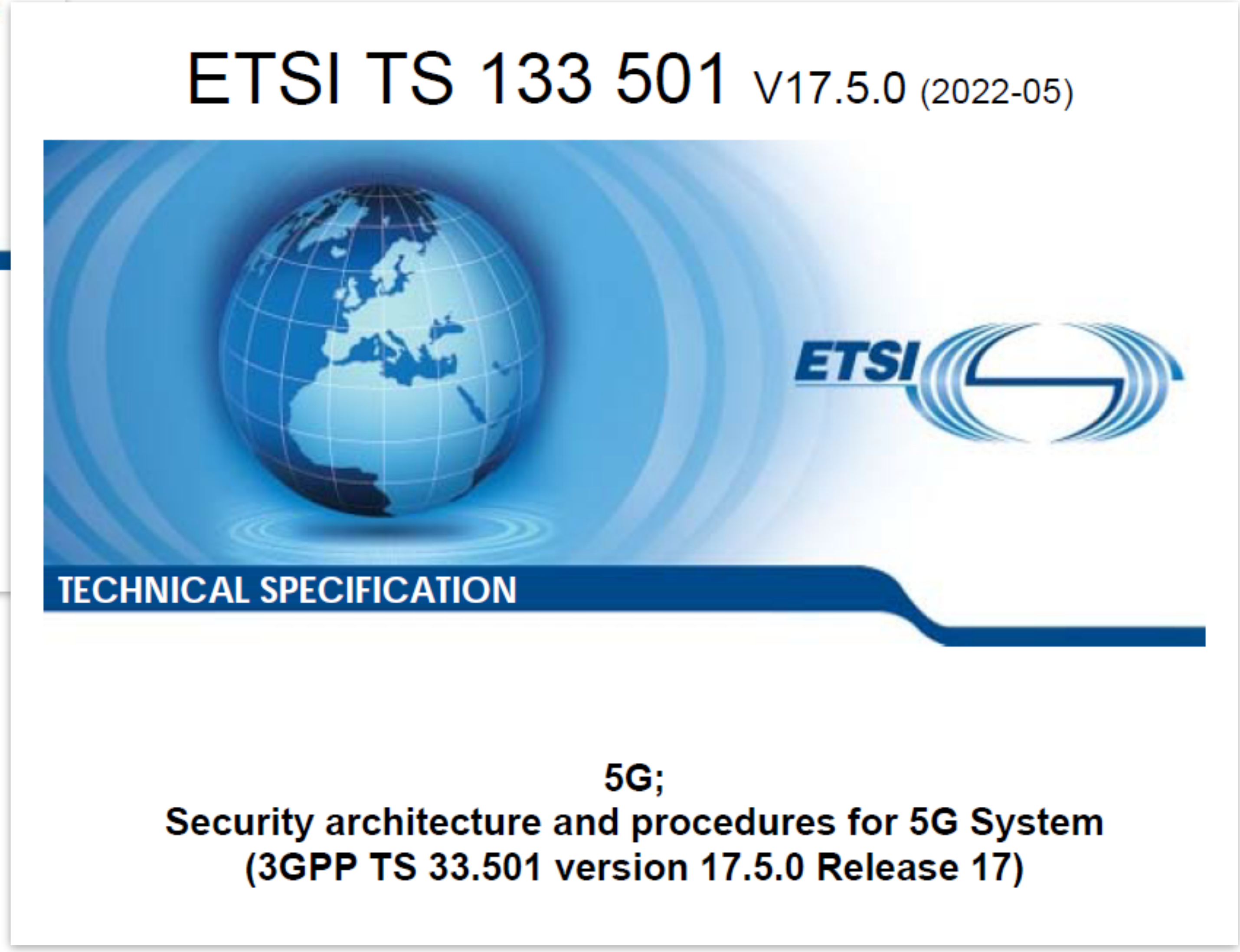
5G SA User Equipment (UE) Security



ETSI TS 124 501 V17.7.1 (2022-07)

TECHNICAL SPECIFICATION

5G;
Non-Access-Stratum (NAS) protocol for 5G System (5GS);
Stage 3
(3GPP TS 24.501 version 17.7.1 Release 17)



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)

- Are they implemented in the UE?
- Are they following the specifications?
- An over-the-air test may reveal the real scenario

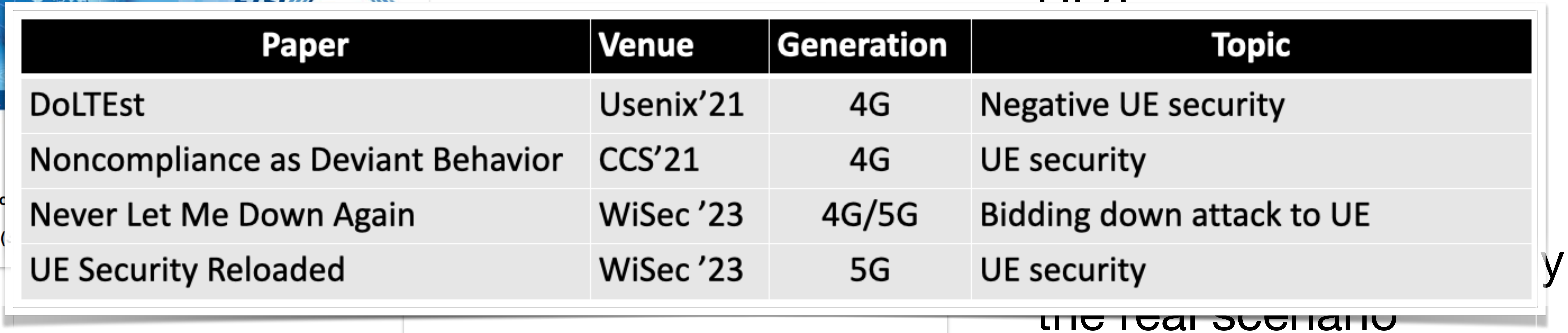
5G SA User Equipment (UE) Security

ETSI TS 124 501 V17.7.1 (2022-07)

TECHNICAL

Non-Acc

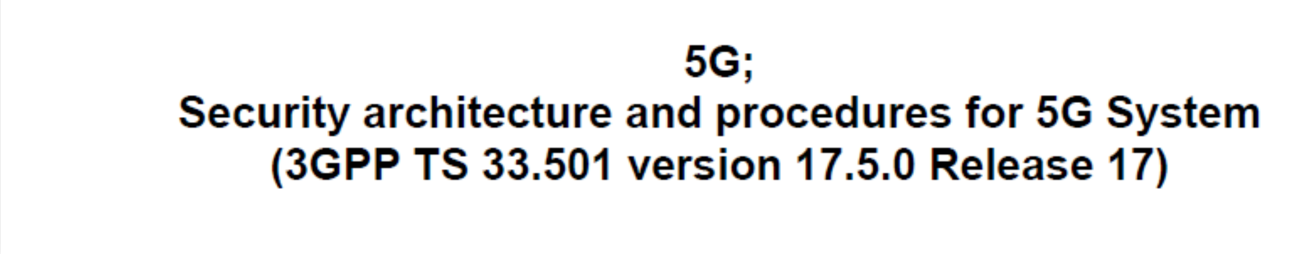
- Are they implemented in the



Paper	Venue	Generation	Topic
DoLTEst	Usenix'21	4G	Negative UE security
Noncompliance as Deviant Behavior	CCS'21	4G	UE security
Never Let Me Down Again	WiSec '23	4G/5G	Bidding down attack to UE
UE Security Reloaded	WiSec '23	5G	UE security

y reveal

the real scenario



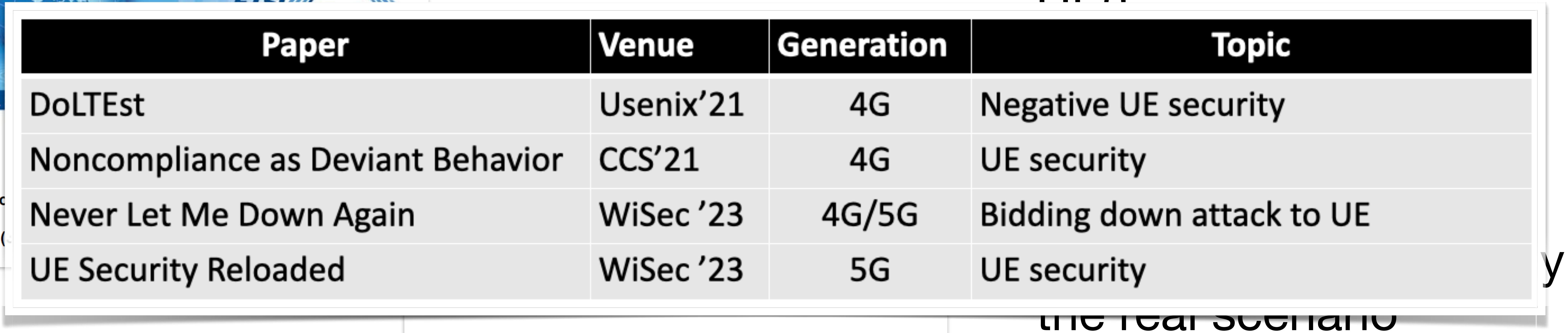
5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 17.5.0 Release 17)

5G SA User Equipment (UE) Security

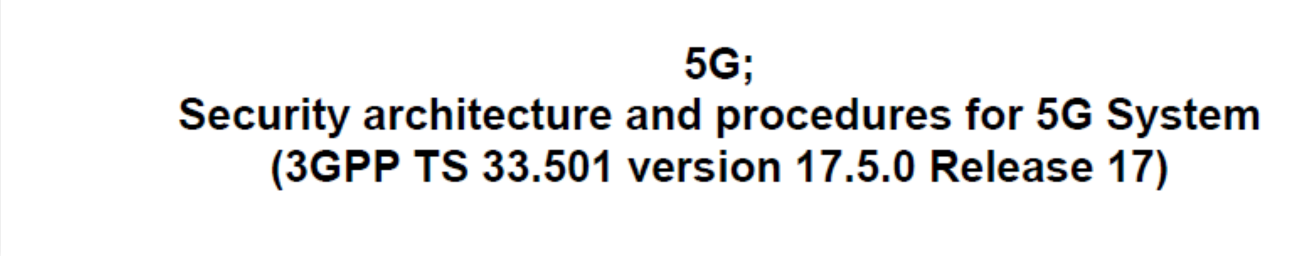
ETSI TS 124 501 V17.7.1 (2022-07)

TECHNICAL

Non-Acc



Paper	Venue	Generation	Topic
DoLTEst	Usenix'21	4G	Negative UE security
Noncompliance as Deviant Behavior	CCS'21	4G	UE security
Never Let Me Down Again	WiSec '23	4G/5G	Bidding down attack to UE
UE Security Reloaded	WiSec '23	5G	UE security


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

- Are they implemented in the UE?

y reveal
the real scenario

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

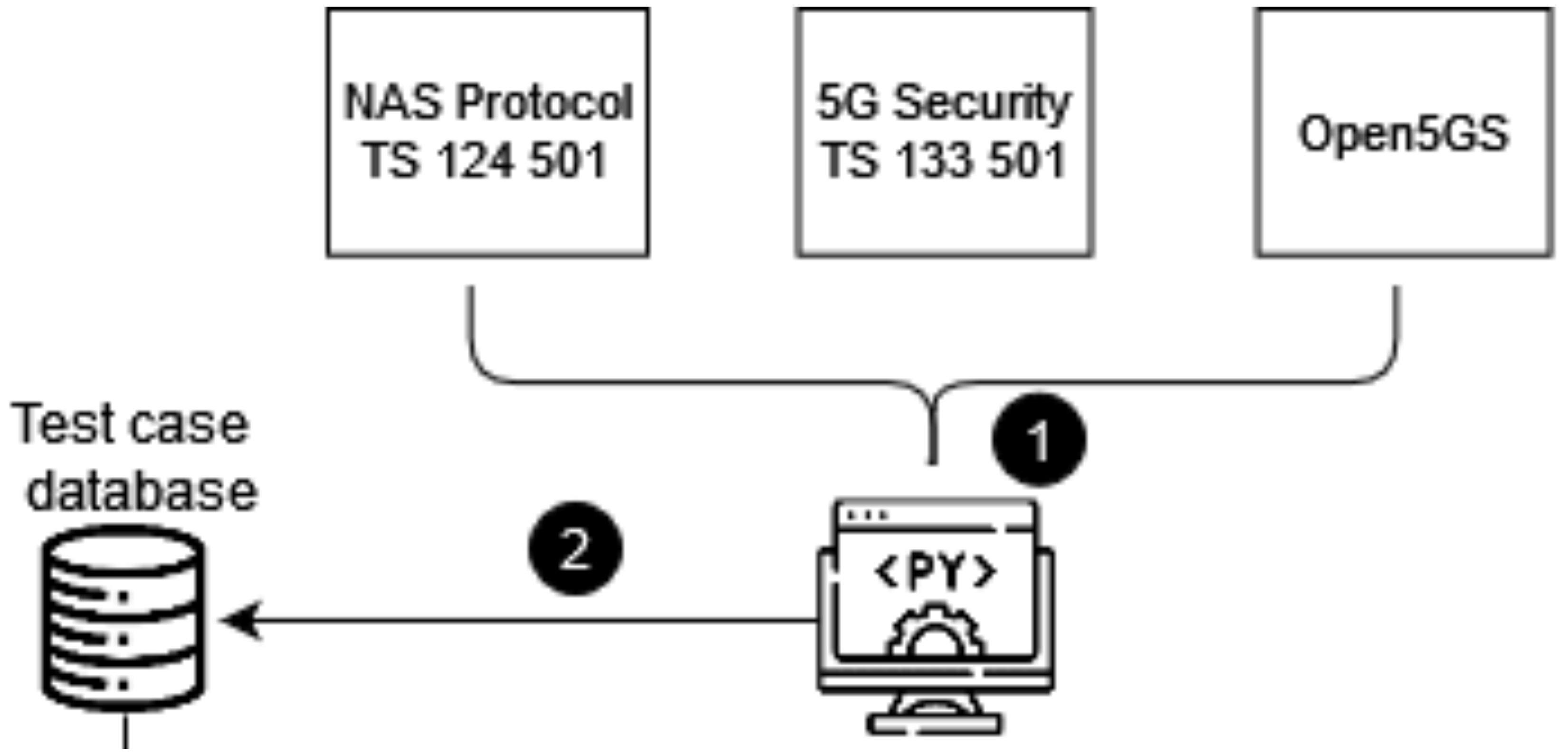
ASTRA-5G

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

- Users can generate verity of test cases
- Tests can be executed automatically one after another at a high speed (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

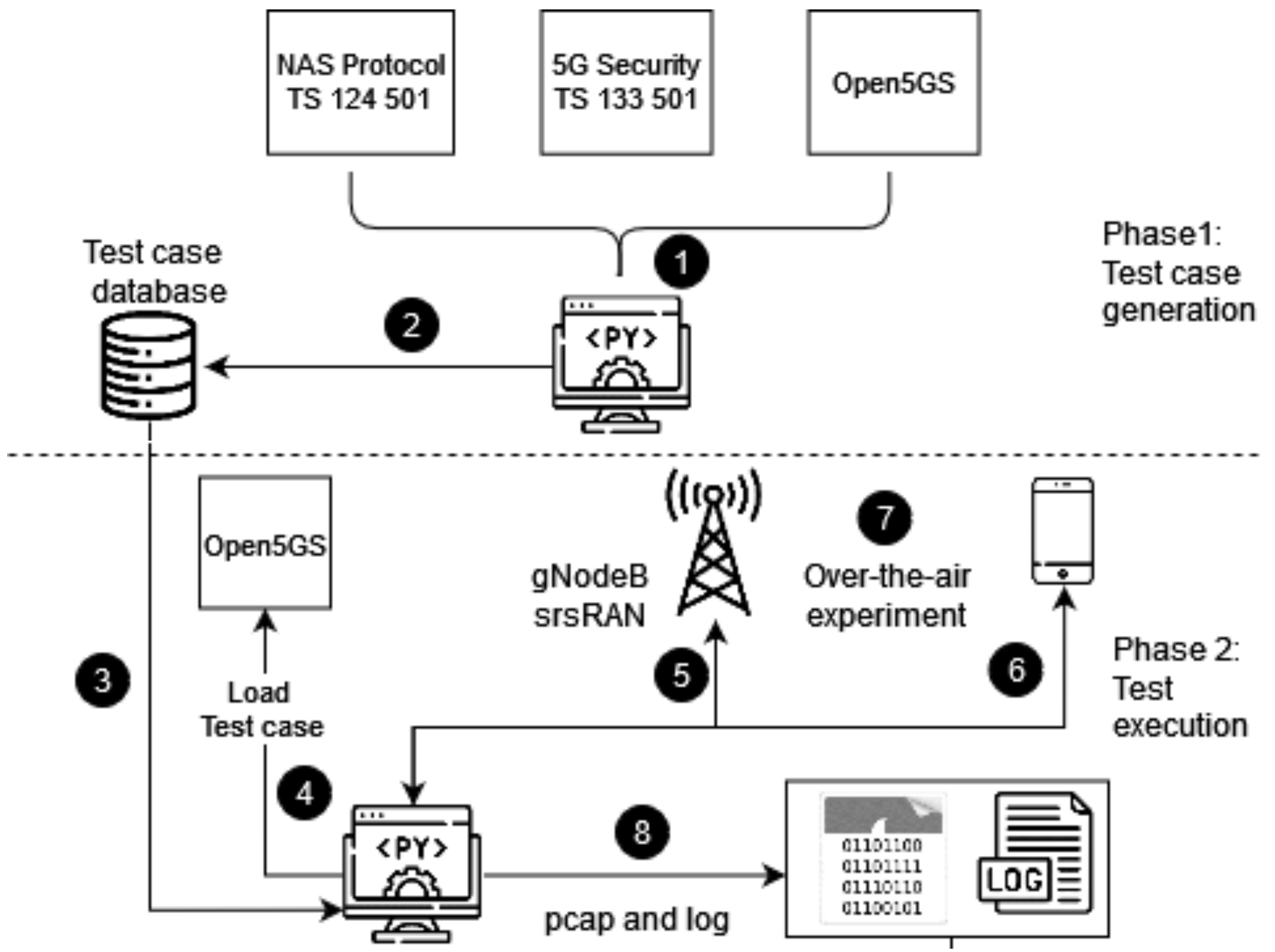
ASTRA-5G: Automated Over-the-Air Security Testing and Research Architecture for 5G SA Devices
Syed Khandker, Michele Guerra, Evangelos Bitsikas, Roger Piqueras Jover, Aanjhan Ranganathan, Christina Poepper (**ACM WiSec 2024)**

Automation Process

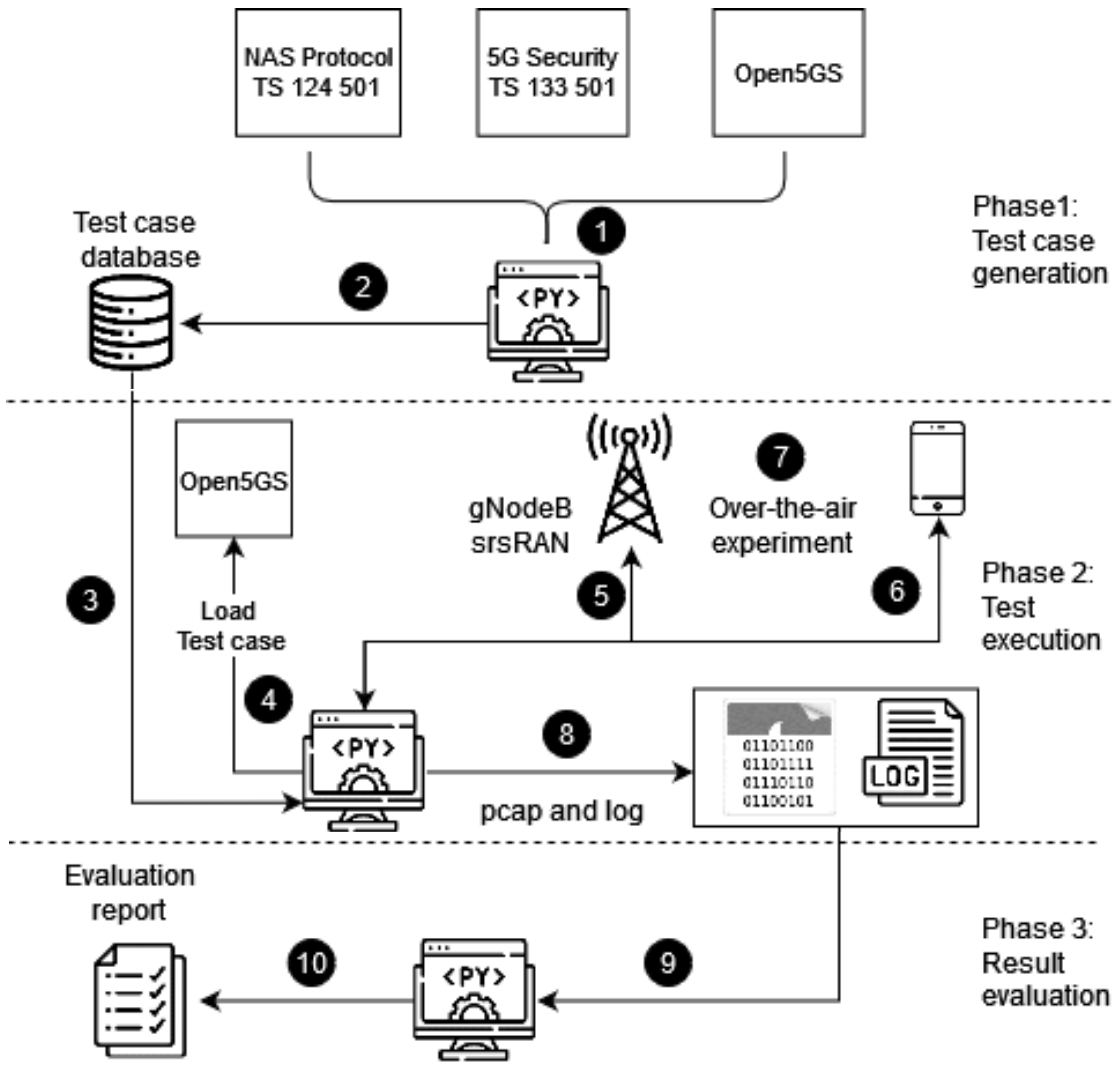


Phase1:
Test case
generation

Automation Process

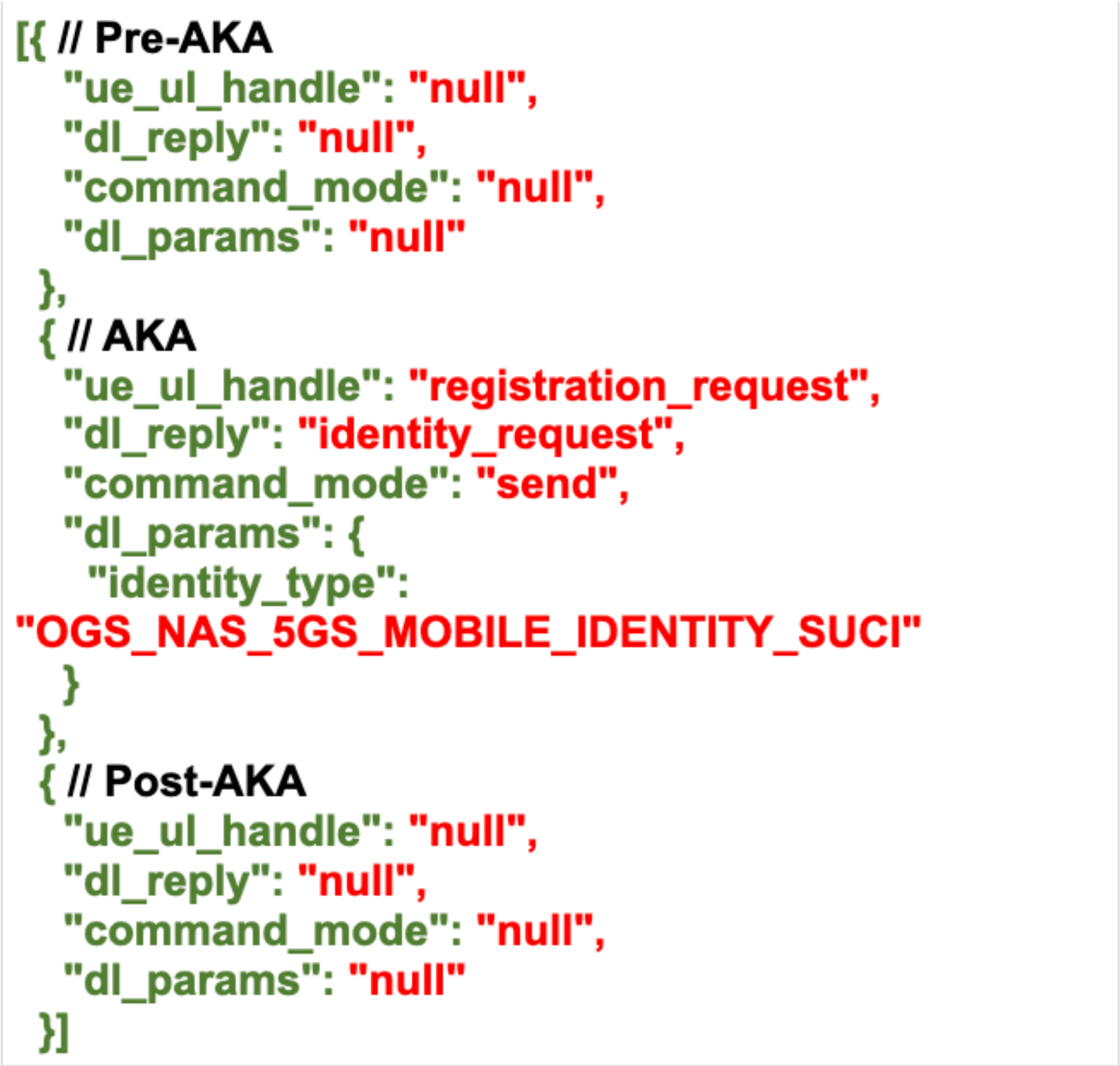


Automation Process



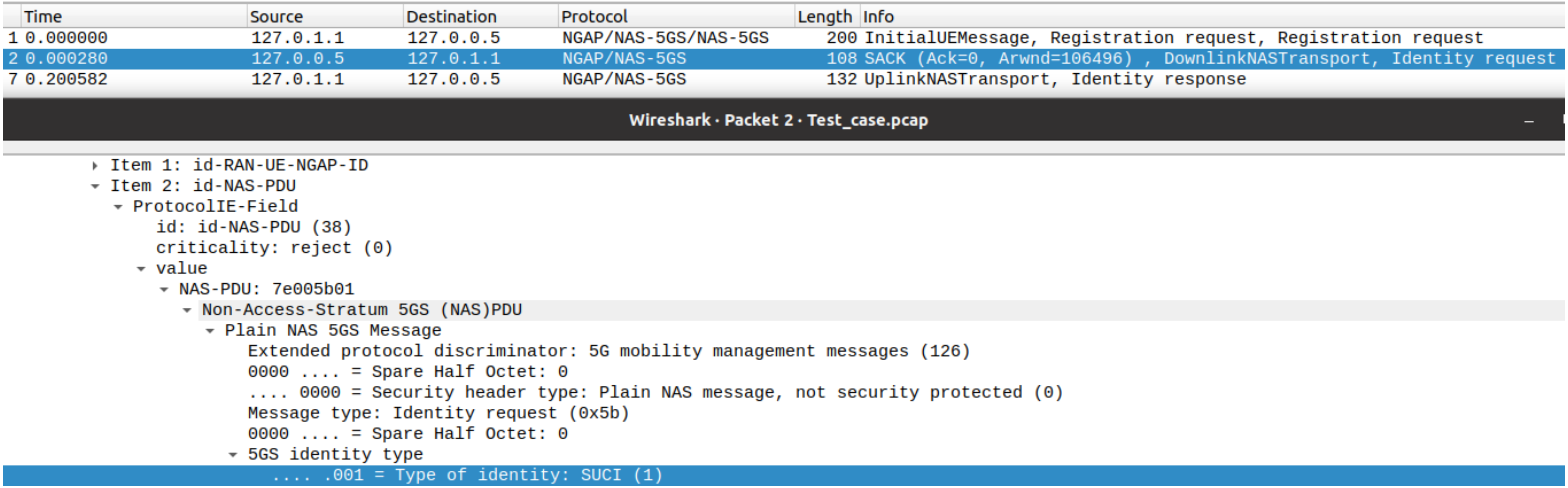
Test Case

- 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"
 }]
```

UE Response

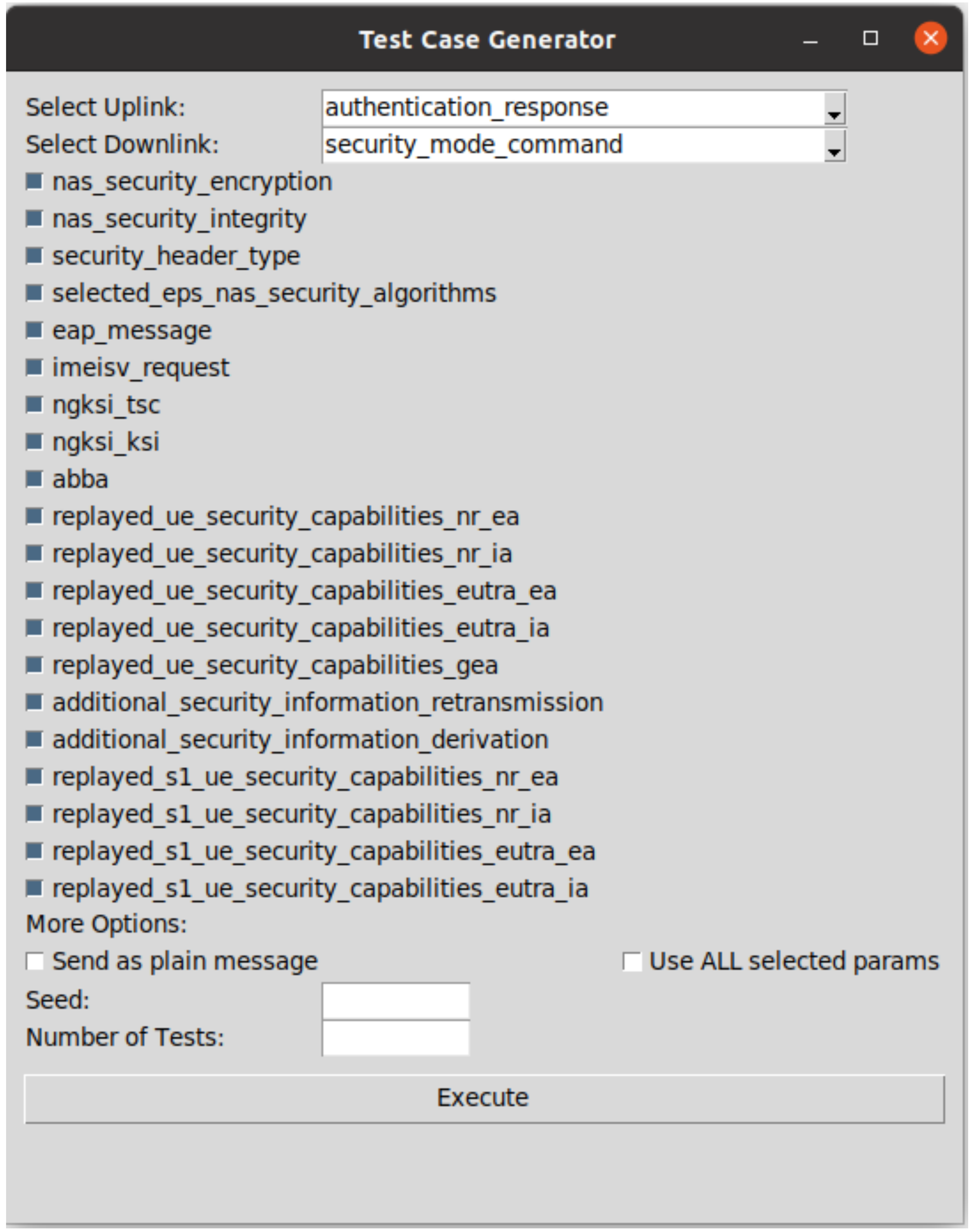


```
  Time              Source        Destination   Protocol             Length Info
1 0.000000          127.0.1.1     127.0.0.5     NGAP/NAS-5GS/NAS-5GS    200 InitialUEMessage, Registration request, Registration request
2 0.000280          127.0.0.5     127.0.1.1     NGAP/NAS-5GS            108 SACK (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)
```

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.



Select Uplink: authentication_response
Select Downlink: security_mode_command

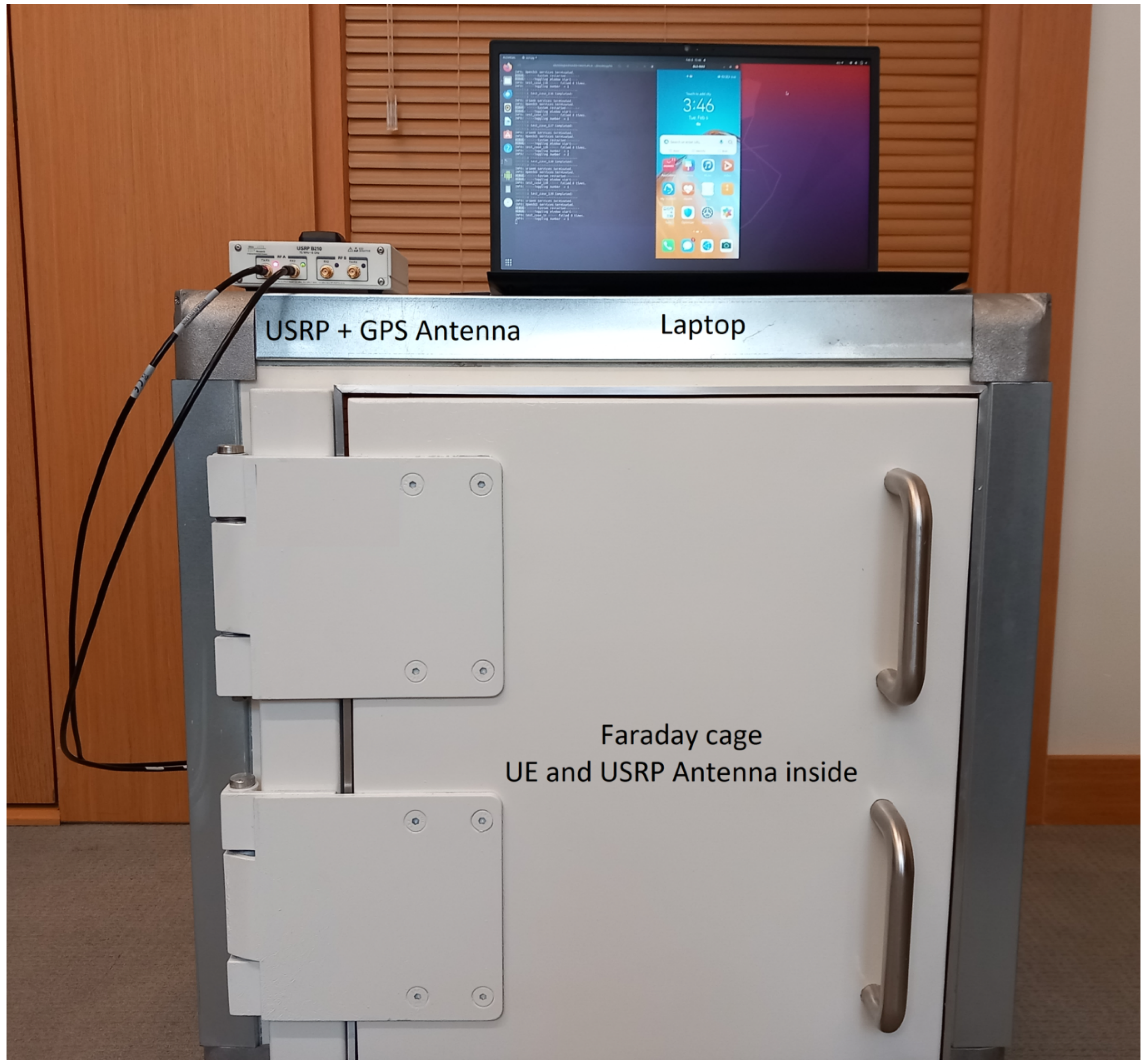
☑ nas_security_encryption
☑ nas_security_integrity
☑ security_header_type
☑ selected_eps_nas_security_algorithms
☑ eap_message
☑ imeisv_request
☑ ngksi_tsc
☑ ngksi_ksi
☑ abba
☑ replayed_ue_security_capabilities_nr_ea
☑ replayed_ue_security_capabilities_nr_ia
☑ replayed_ue_security_capabilities_eutra_ea
☑ 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:

Experiment Setup and Verification

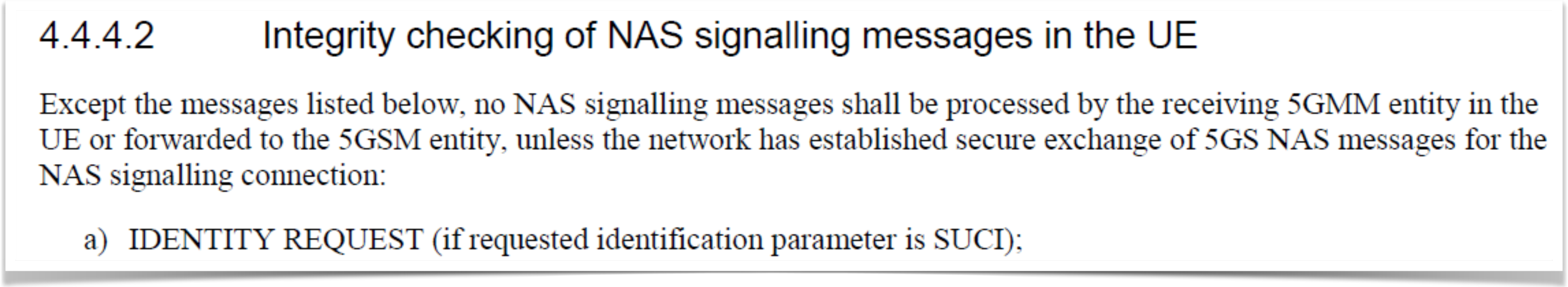


Device	Chipset	OS	Model	Release
Honor X9a 5G	Snapdragon 695	Android 12	RMO-NX1	2023
Huawei P40 Pro 5G	Kirin 990 5G	Android 10	ELS-NX9	2020
Oppo Reno8 Z 5G	Snapdragon 695 5G	Android 13	CPH2457	2022
Realme 8 5G	Dimensity 700	Android 11	RMX3241	2021
OnePlus Nord 2 5G	Dimensity 1200 5G	Android 11	DN2101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

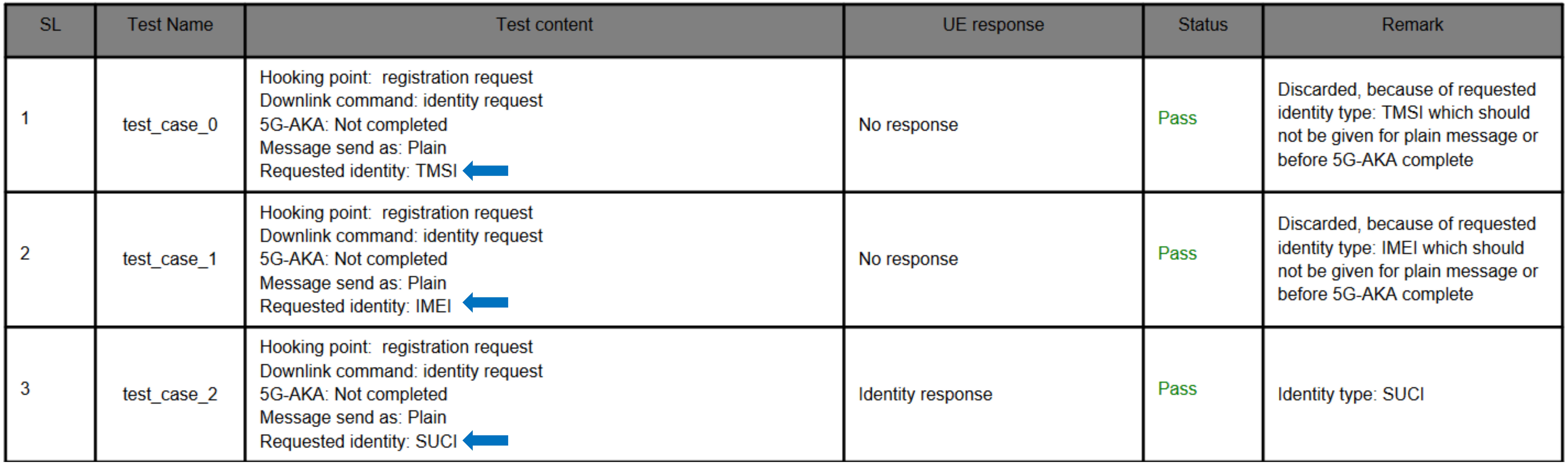
Example Test Case: Identity Request



4.4.4.2 Integrity checking of NAS signalling messages in the UE

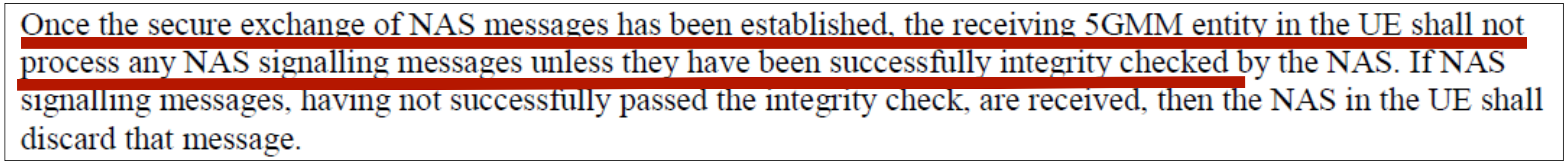
Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

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

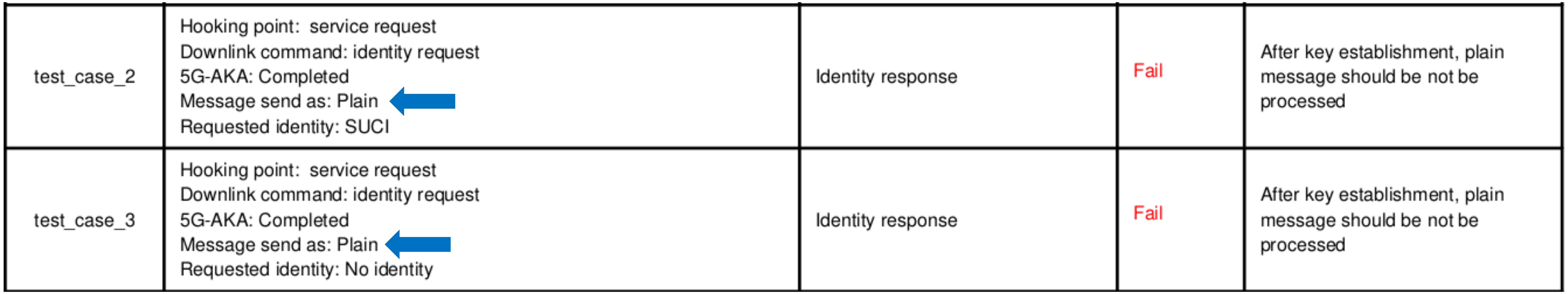


SL	Test Name	Test content	UE response	Status	Remark
1	test_case_0	Hooking point: registration request Downlink command: identity request 5G-AKA: Not completed Message send as: Plain Requested identity: TMSI ⬅	No response	Pass	Discarded, because of requested identity type: TMSI which should not be given 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

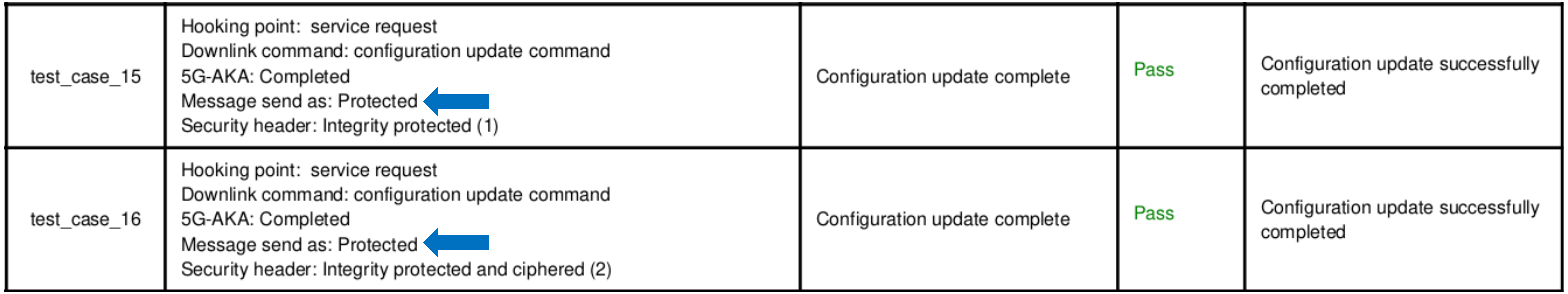
Example 2: Plain and Protected Message



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

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	✓	✓	✓	✓	✓

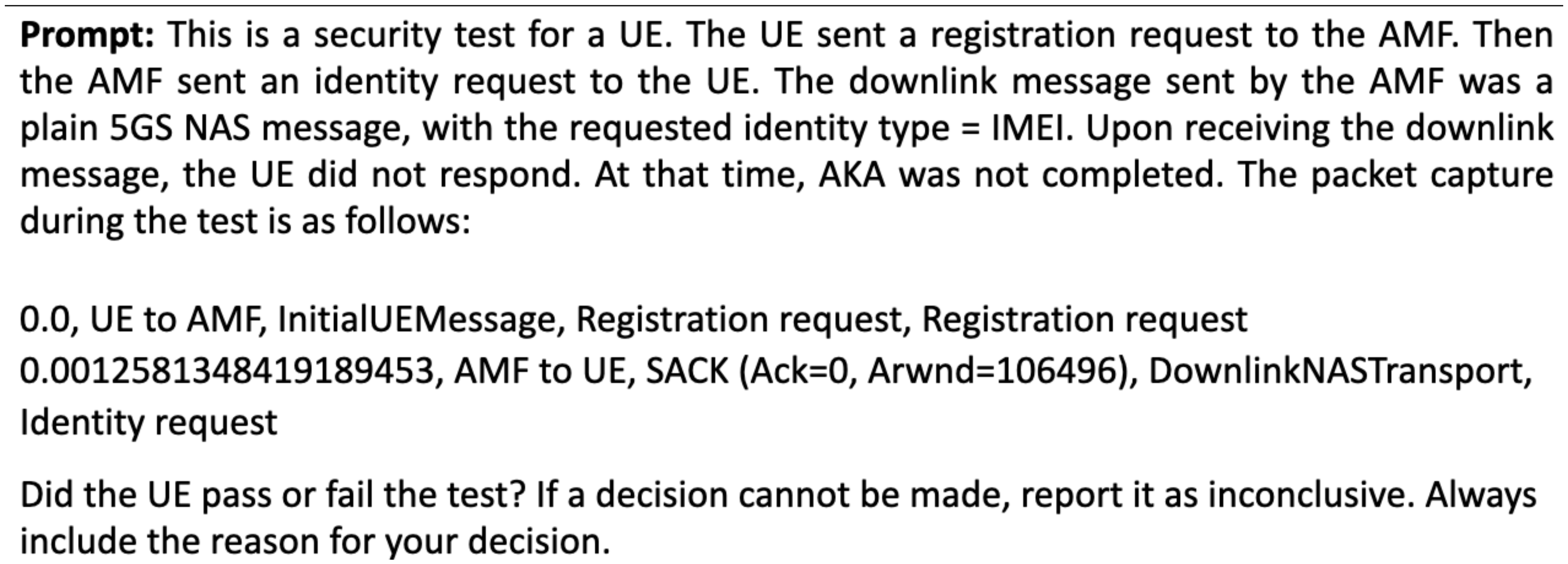
Note:

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

LLM-based Evaluation

Of-course, why not?

- ChatGPT
- Google Bard
- LLAMA-2



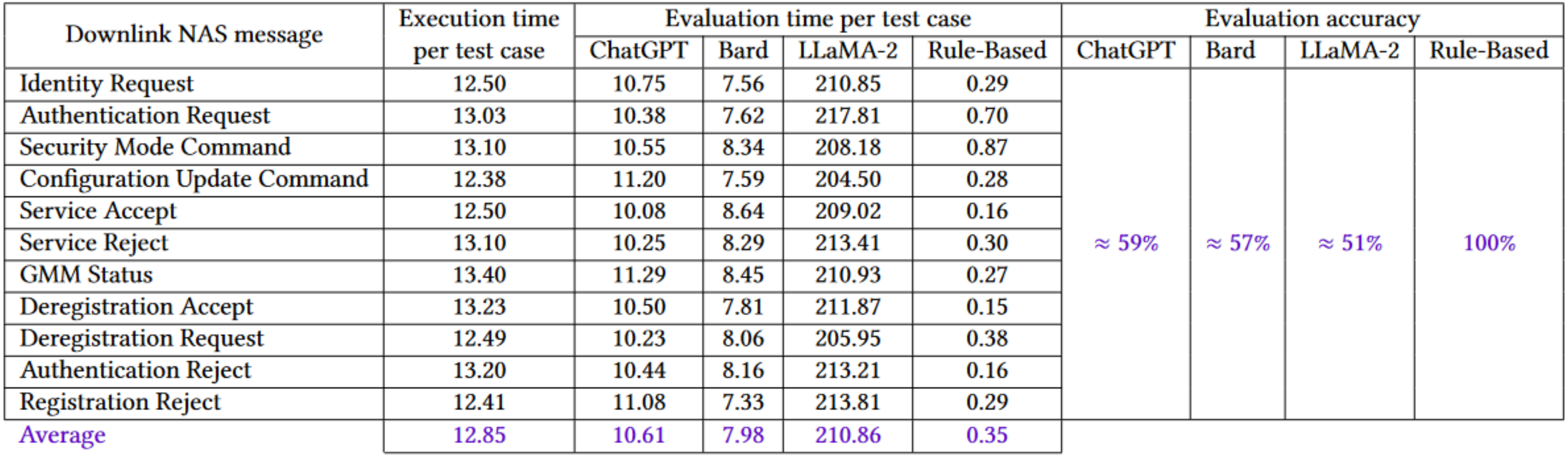
Prompt: This is a security test for a UE. The UE sent a registration request to the AMF. Then the AMF sent an identity request to the UE. The downlink message sent by the AMF was a plain 5GS NAS message, with the requested identity type = IMEI. Upon receiving the downlink message, the UE did not respond. 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
0.0012581348419189453, 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 information, 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.*

LLM-based Evaluation



Downlink NAS message	Execution time per test case	Evaluation time per test case				Evaluation accuracy			
		ChatGPT	Bard	LLaMA-2	Rule-Based	ChatGPT	Bard	LLaMA-2	Rule-Based
Identity Request	12.50	10.75	7.56	210.85	0.29	≈ 59%	≈ 57%	≈ 51%	100%
Authentication Request	13.03	10.38	7.62	217.81	0.70				
Security Mode Command	13.10	10.55	8.34	208.18	0.87				
Configuration Update Command	12.38	11.20	7.59	204.50	0.28				
Service Accept	12.50	10.08	8.64	209.02	0.16				
Service Reject	13.10	10.25	8.29	213.41	0.30				
GMM Status	13.40	11.29	8.45	210.93	0.27				
Deregistration Accept	13.23	10.50	7.81	211.87	0.15				
Deregistration Request	12.49	10.23	8.06	205.95	0.38				
Authentication Reject	13.20	10.44	8.16	213.21	0.16				
Registration Reject	12.41	11.08	7.33	213.81	0.29				
Average	12.85	10.61	7.98	210.86	0.35				

*All times in seconds

Summary

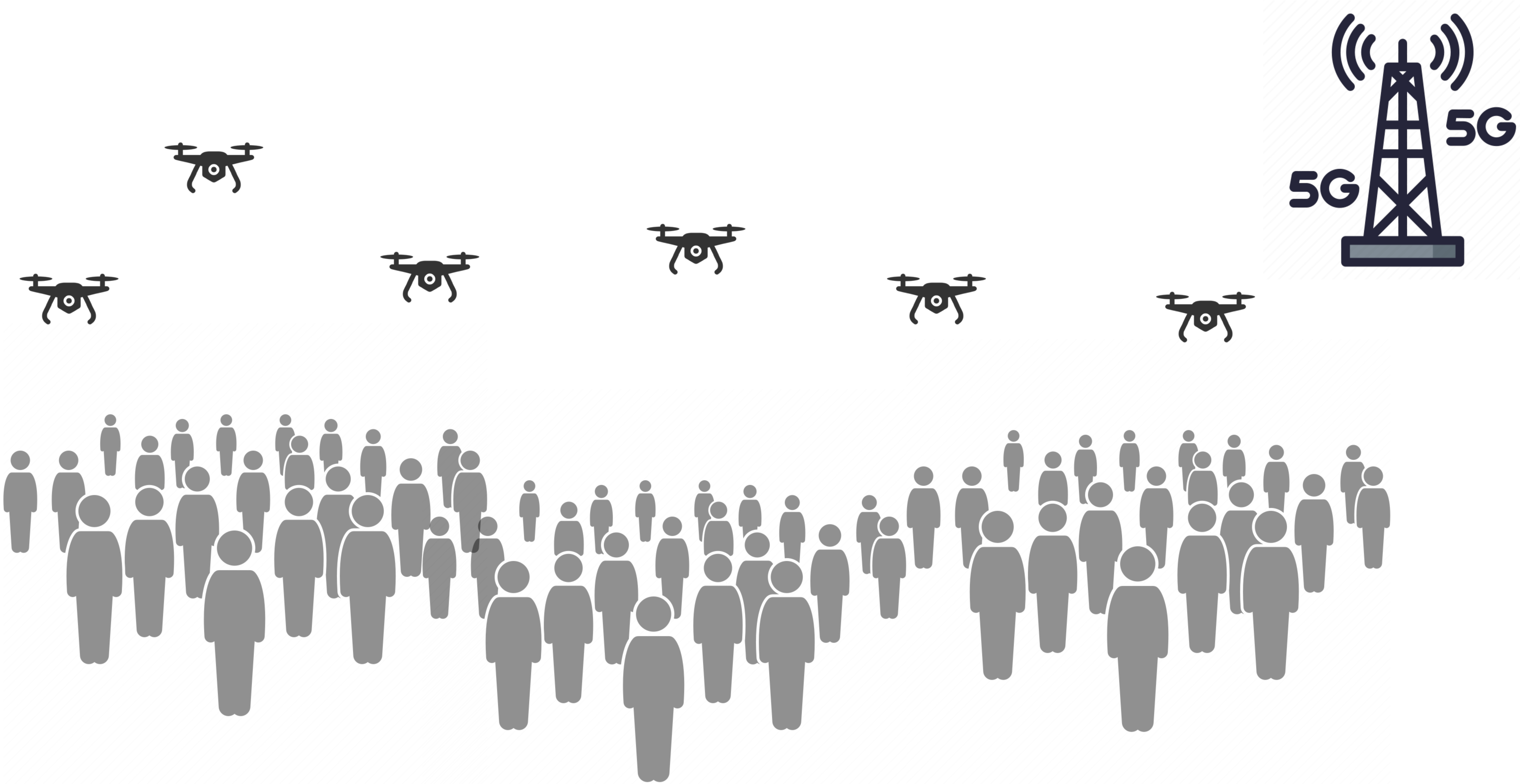
- 5G SA testing is not straightforward, requires handling all the network components e.g., core, RAN, and UE
- Automation significantly reduces testing complexity and broadens the testing scope (e.g., order of multiple minutes to ≈15 seconds)
- Such open source tool can ensuring transparency and independence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

Github Repo

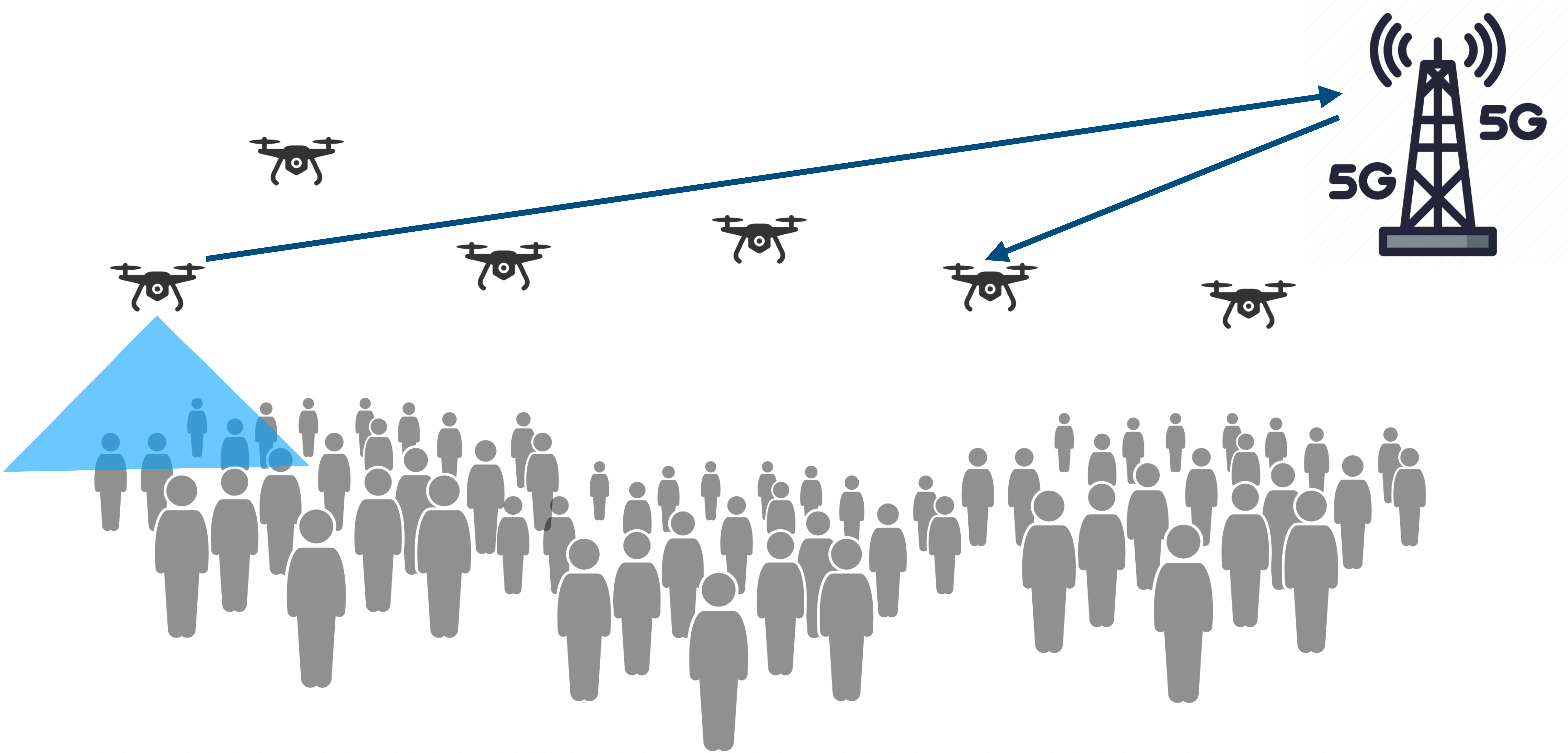
Do you remember this statement?

- Interesting facts (in theory of course): **5G SA can support up to 1 million devices per square kilometer, ultra-low latency of 1 ms (~50 ms in 4G LTE) and is almost always used alongside technology jargons such as autonomous vehicles, mixed reality, remote surgery, etc.**

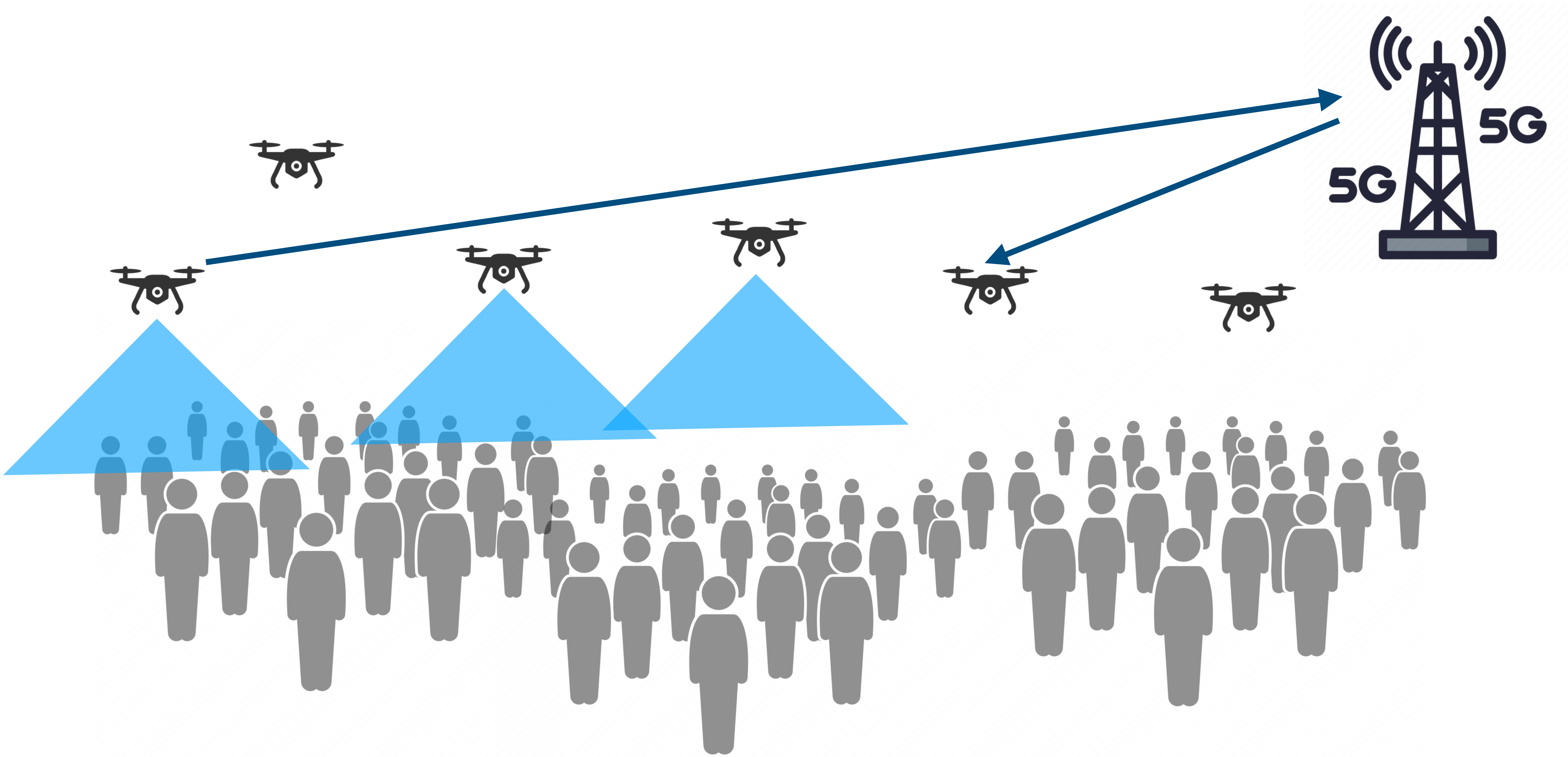
Drone Swarms — Crowd Monitoring



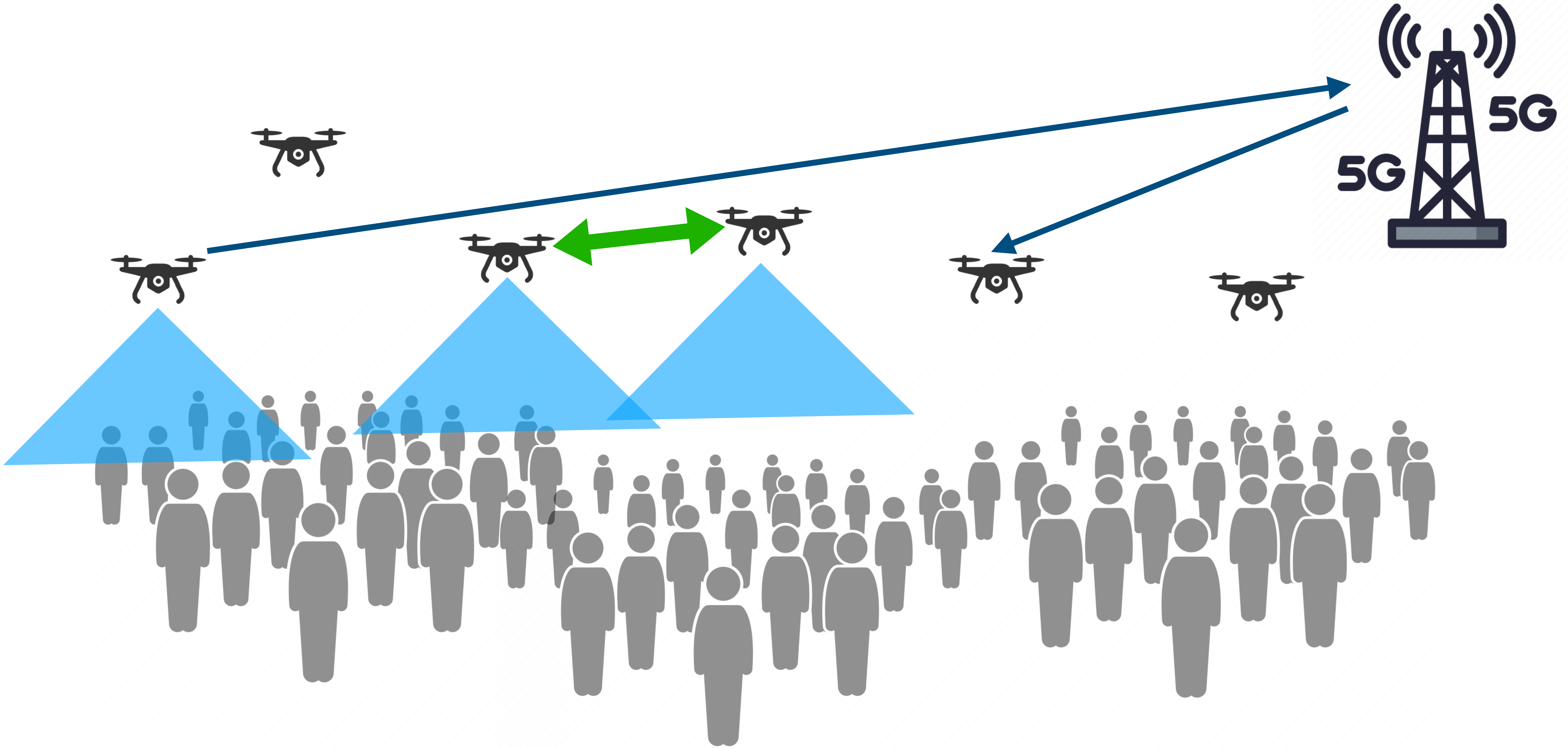
Drone Swarms — Crowd Monitoring



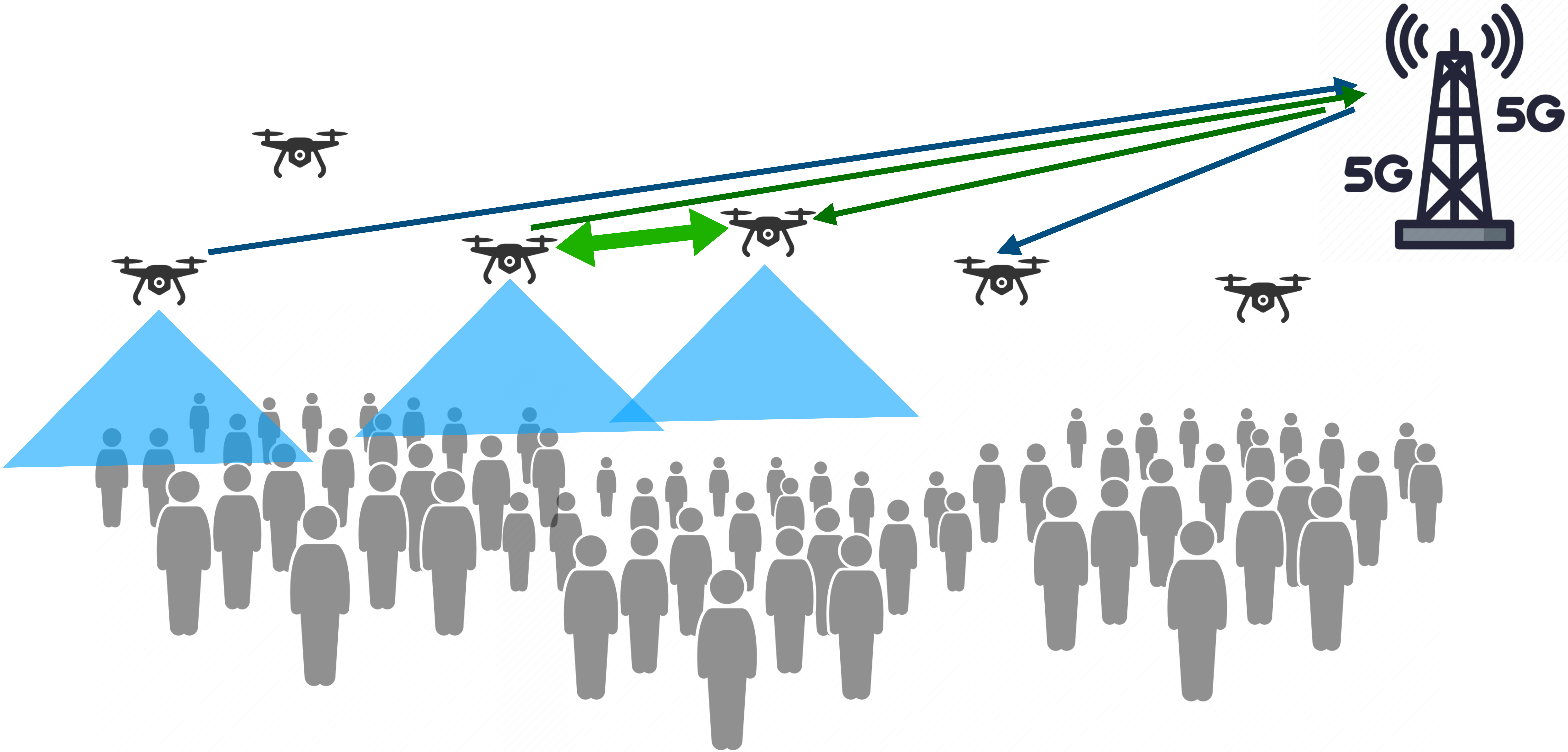
Drone Swarms — Crowd Monitoring



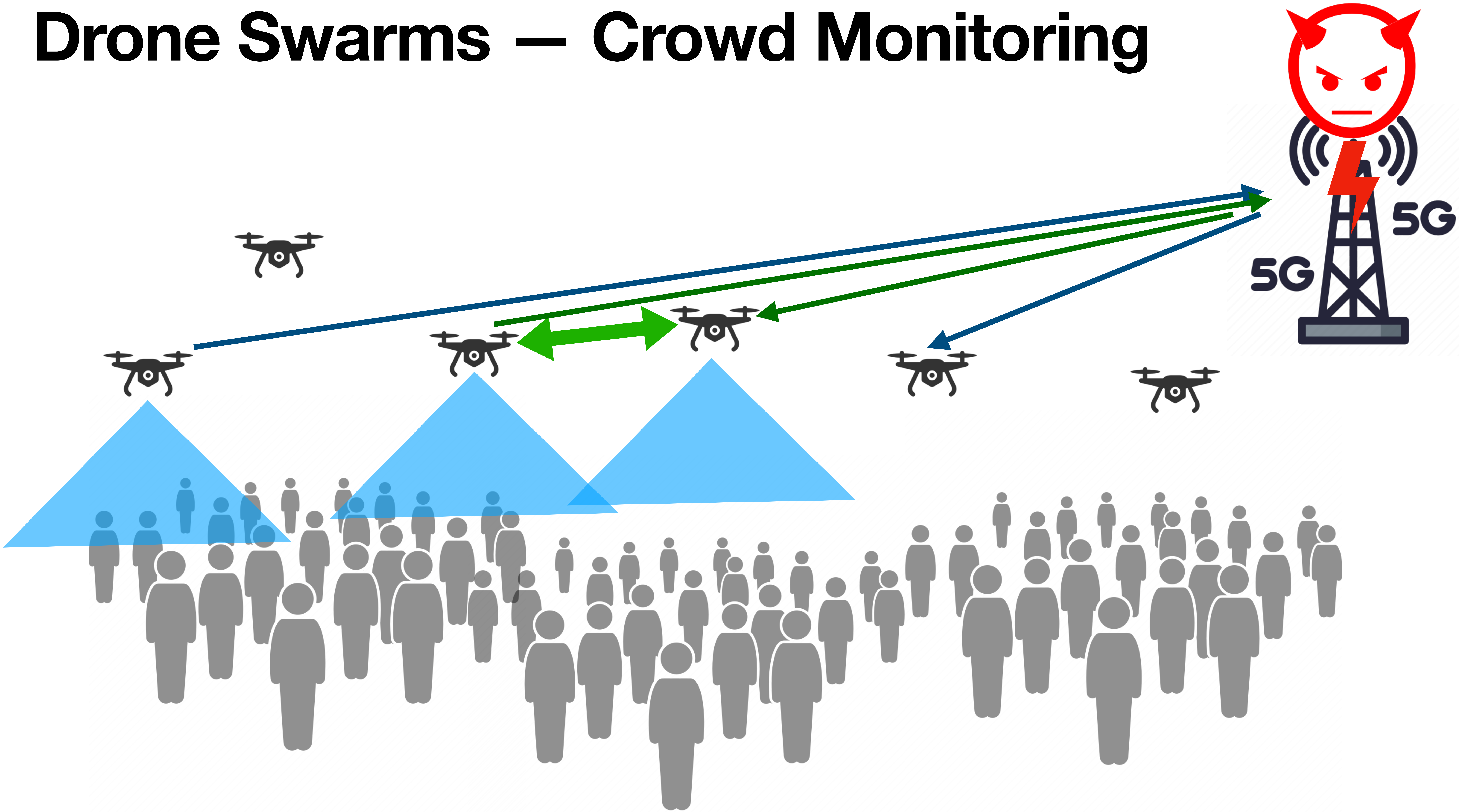
Drone Swarms — Crowd Monitoring



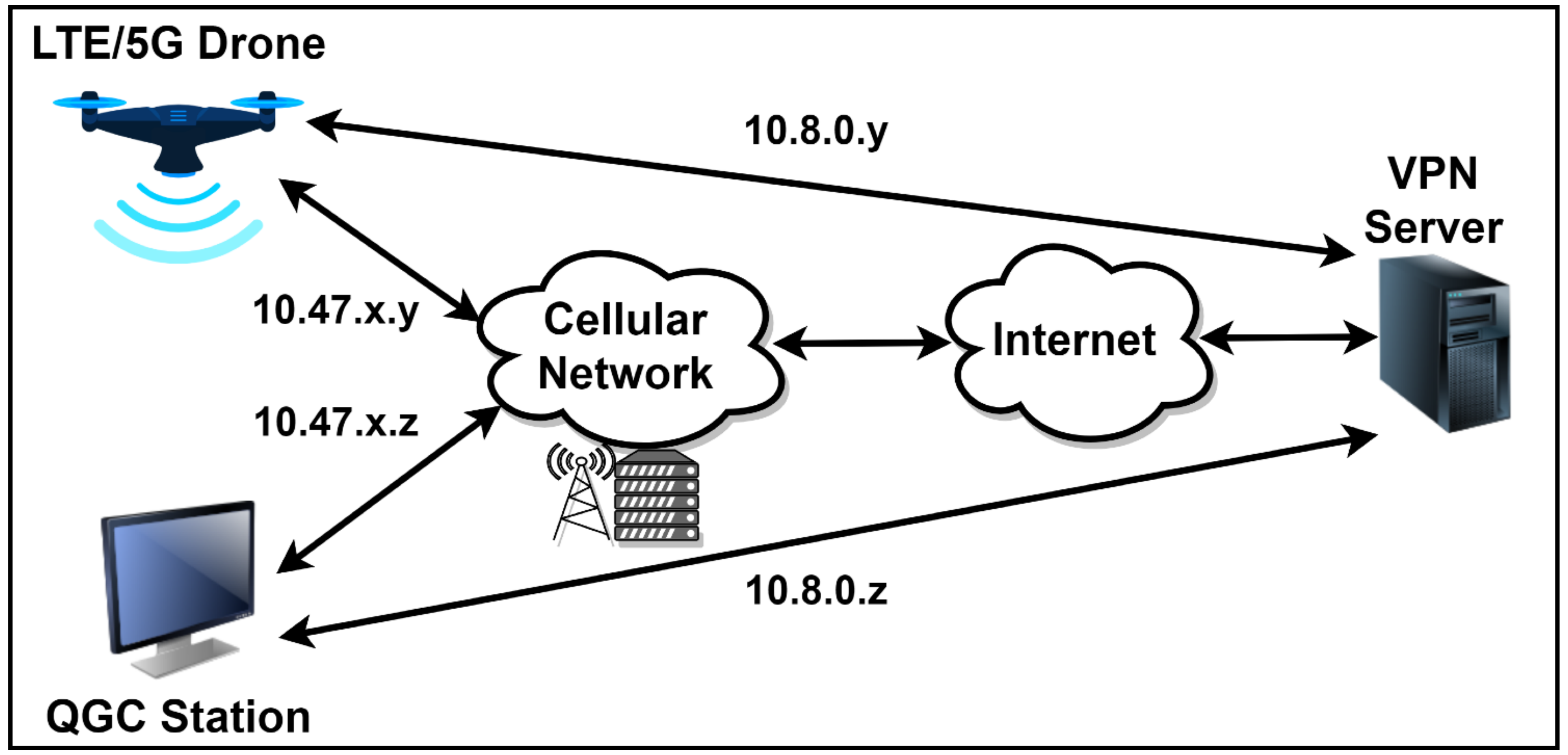
Drone Swarms — Crowd Monitoring



Drone Swarms — Crowd Monitoring



Many limitations…



- Conventional cellular networks
- Single points of failures
- Slow M2M communications
- Deficient failure recovery mechanisms

{
- Rigid
- Static
- Immobile
- Not fully suitable for dynamic applications and devices

Can 5G really support massive M2M applications in its true sense?

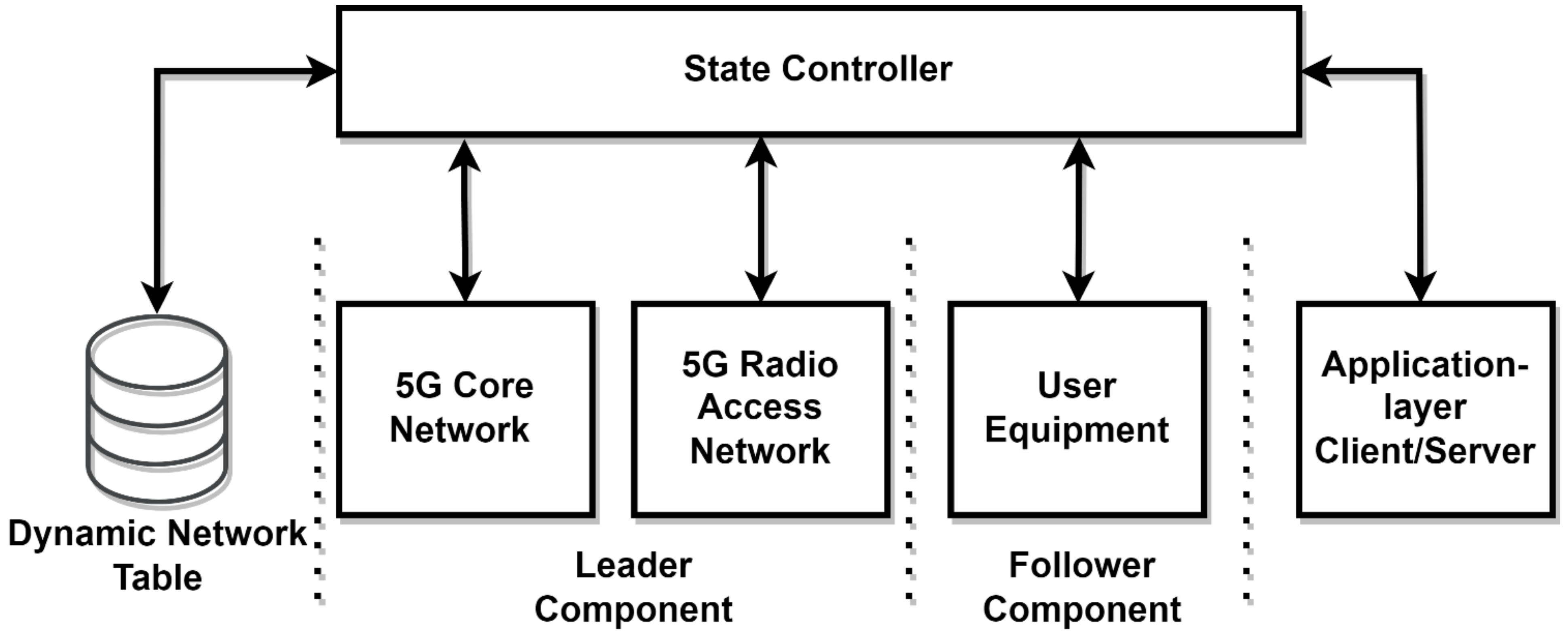
Dyna-5G

Dynamic 5G standalone deployment tailored specifically for massive M2M

- Every node in the network can act as UE or RAN/Core Network
- No single point of failure
- Dynamic reconfiguration of the network
- Failure recovery mechanisms

Network Requirements & Structure

System structure per device



State Controller

Dynamic Network Table

5G Core Network

5G Radio Access Network

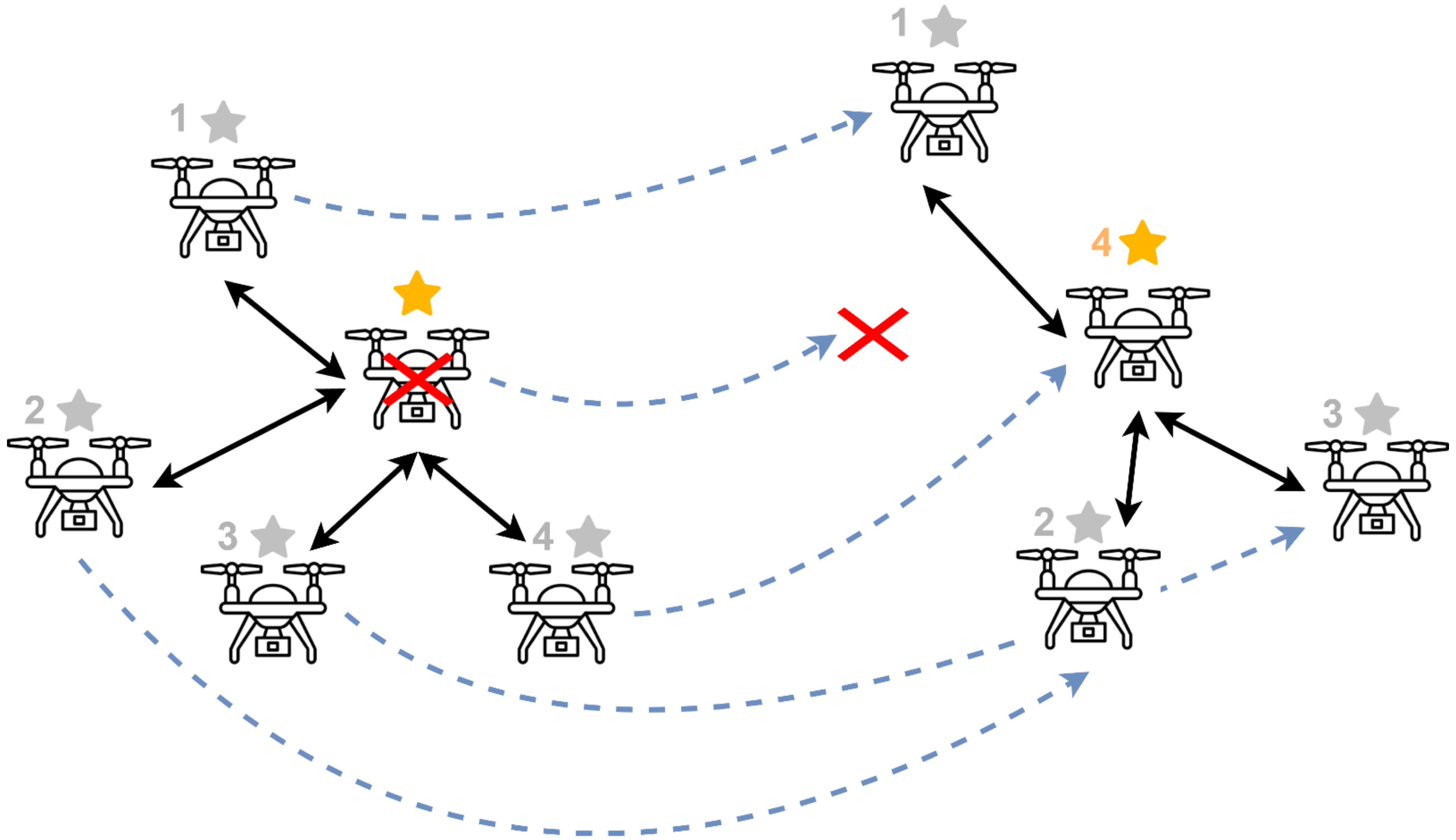
User Equipment

Application-layer Client/Server

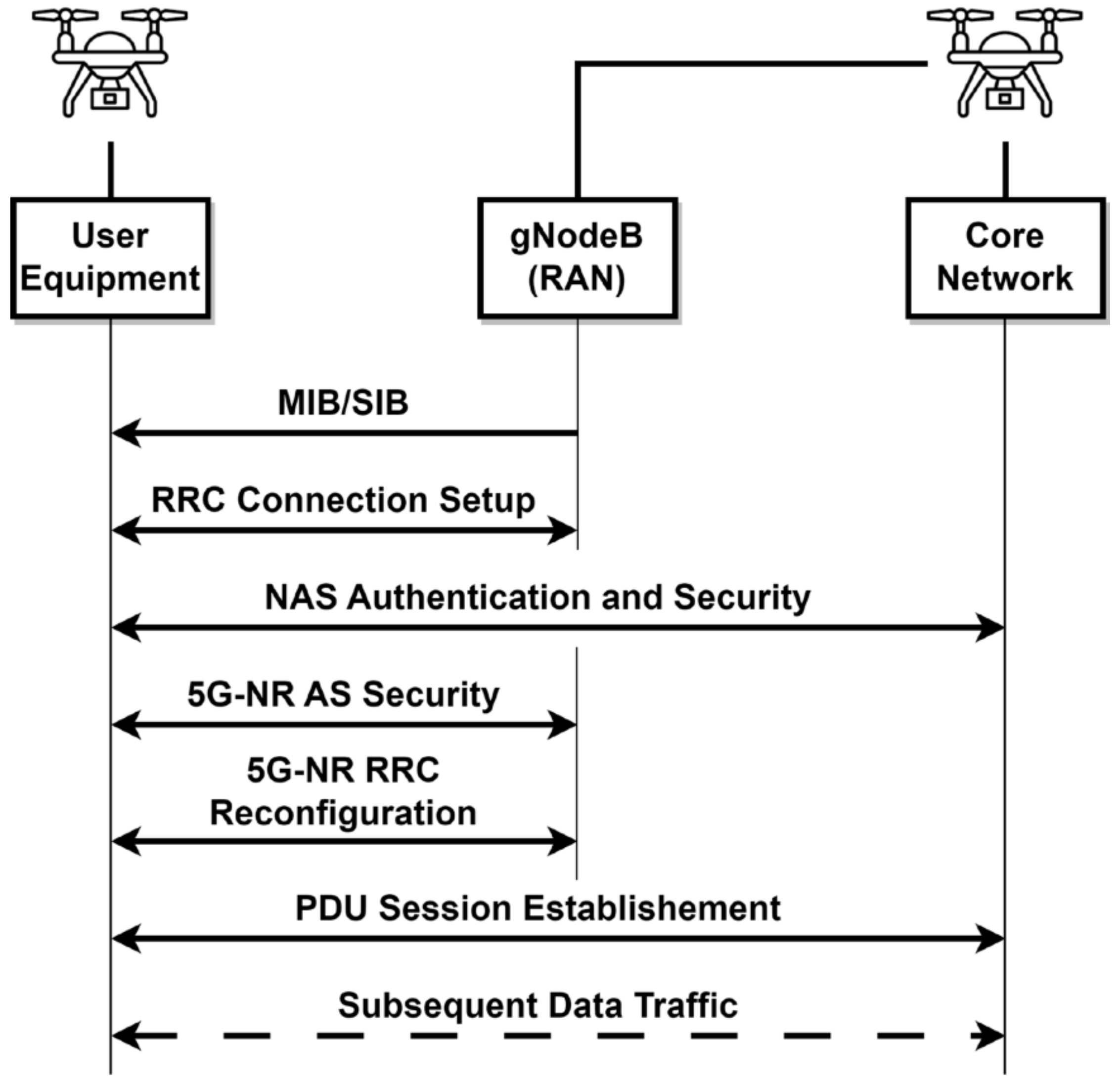
Leader Component

Follower Component

Drone network transition during the mission



Cellular protocol integration



User Equipment

gNodeB (RAN)

Core Network

MIB/SIB

RRC Connection Setup

NAS Authentication and Security

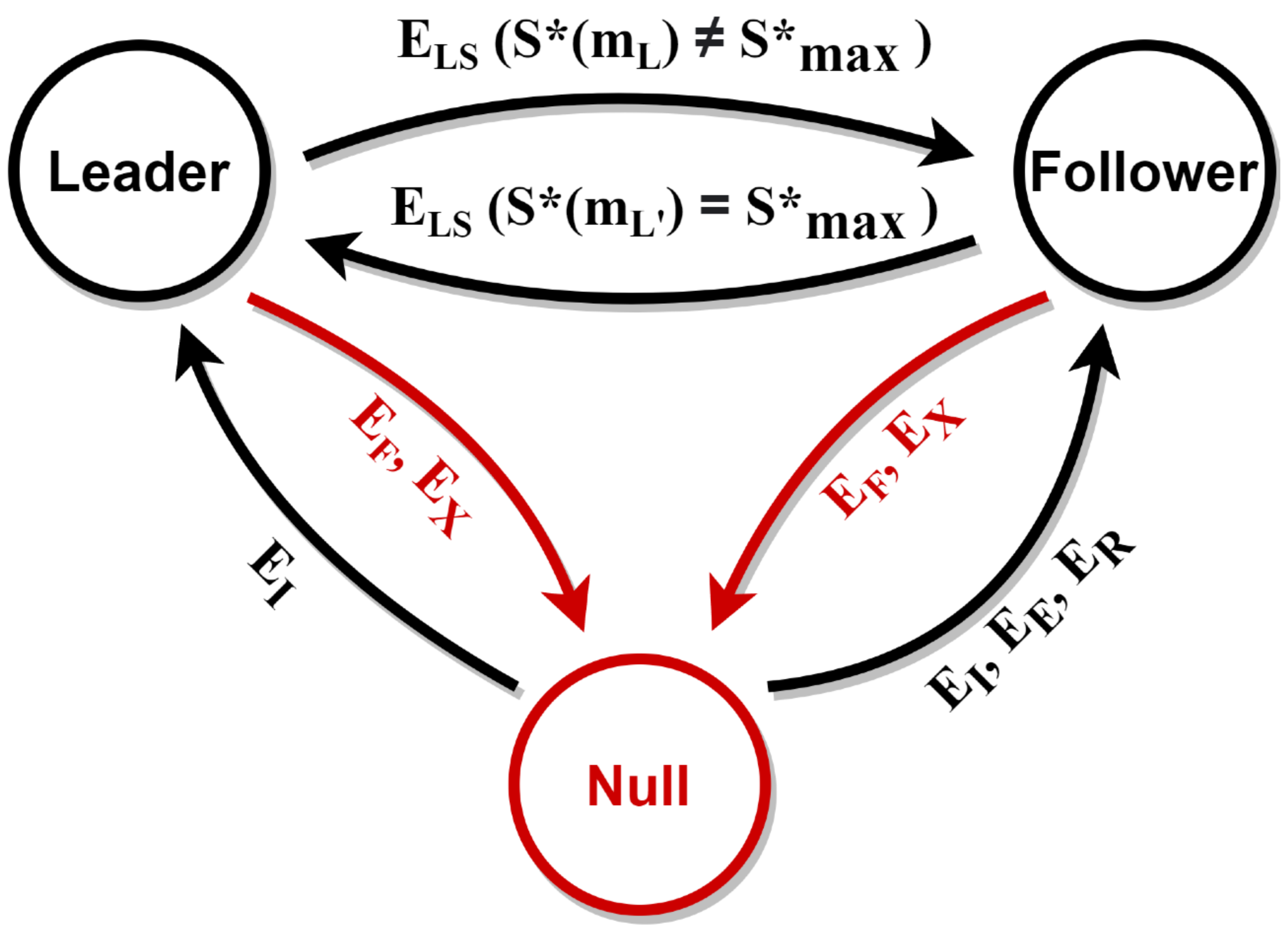
5G-NR AS Security

5G-NR RRC Reconfiguration

PDU Session Establishement

Subsequent Data Traffic

Finite State Machine & Performance Calculation


E_{LS} ($S^*(m_L) \neq S^*_{max}$)
Leader
Follower
E_{LS} ($S^*(m_{L'}) = S^*_{max}$)
E_F, E_X
E_F, E_X
E_I
E_I, E_E, E_R
Null

Initialization: E_I

Entering: E_E

Leader Selection: E_{LS}

Exiting: E_X

Failure: E_F

Recovery: E_R

Performance Score Calculation:

1. $Cc(i) = (M+B+P)/3$
2. $Sp(i) = 100/1+a \cdot dist(P(i), COMx,y,z)$
3. $S(i) = (Sp(i)+Cc(i))/2$

Main implementation components:

- State Controller
- Network State Table
- Operational Timers (e.g., leader selection timer)

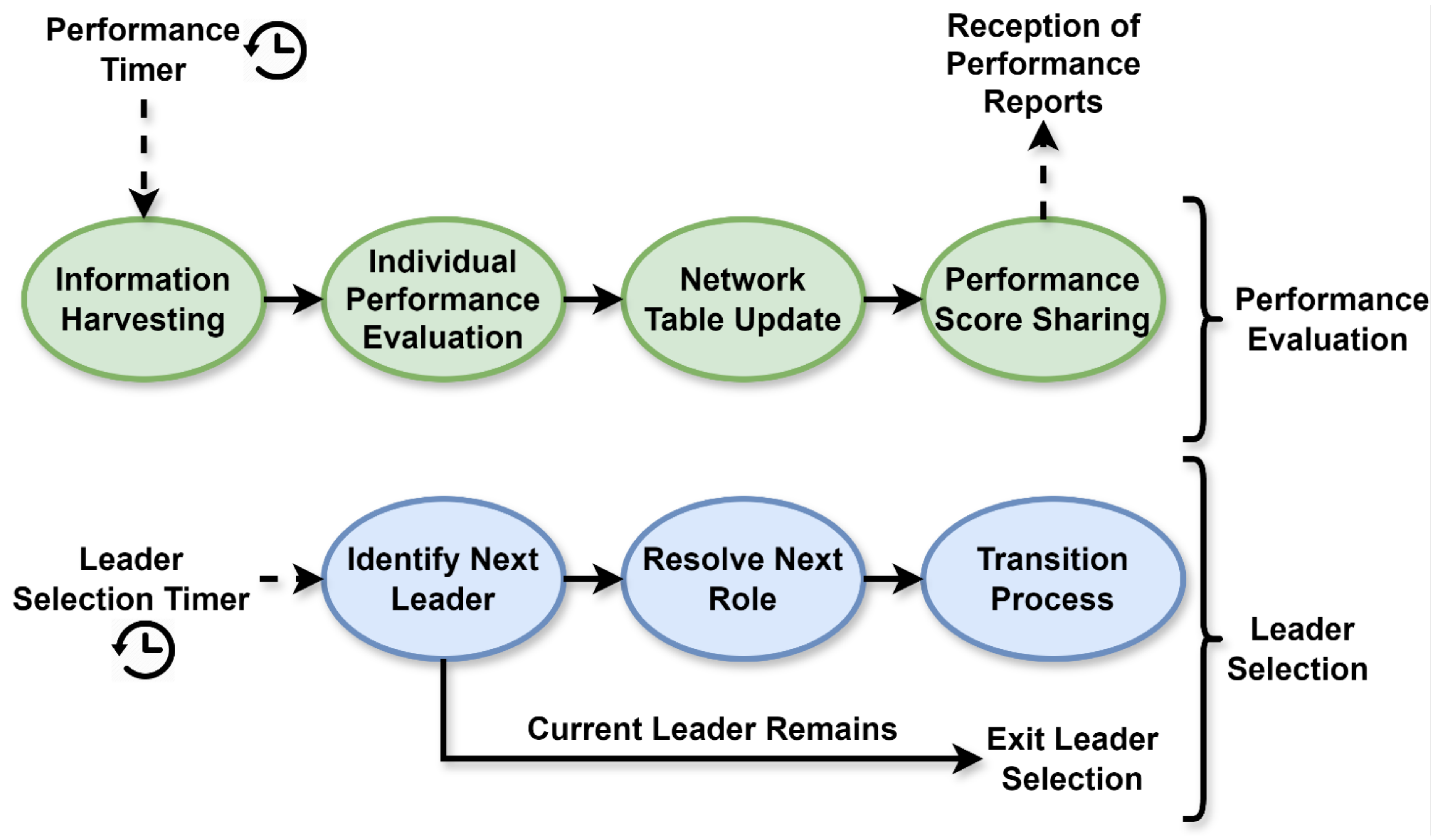
Network Operations

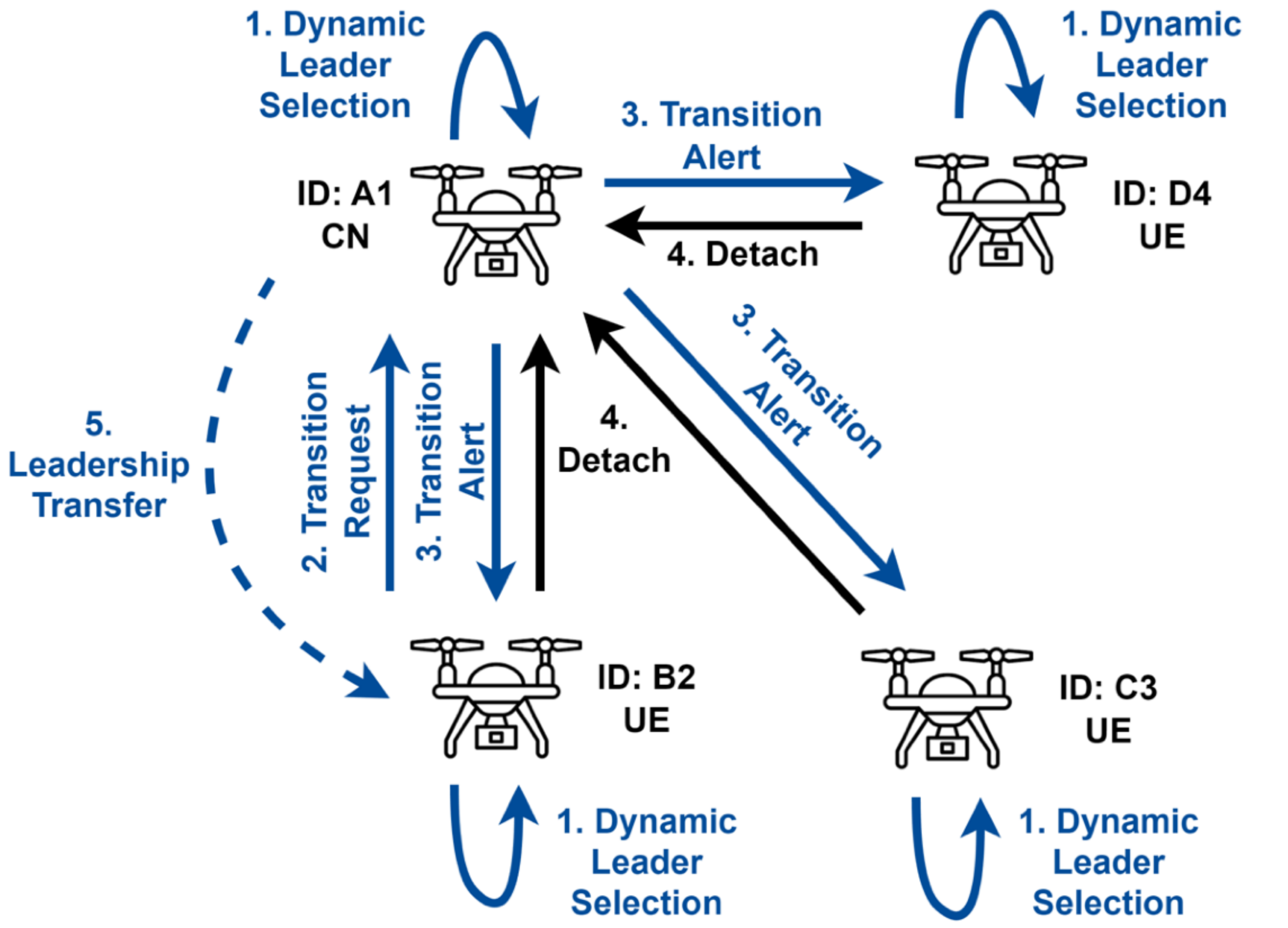
Network Initialization:

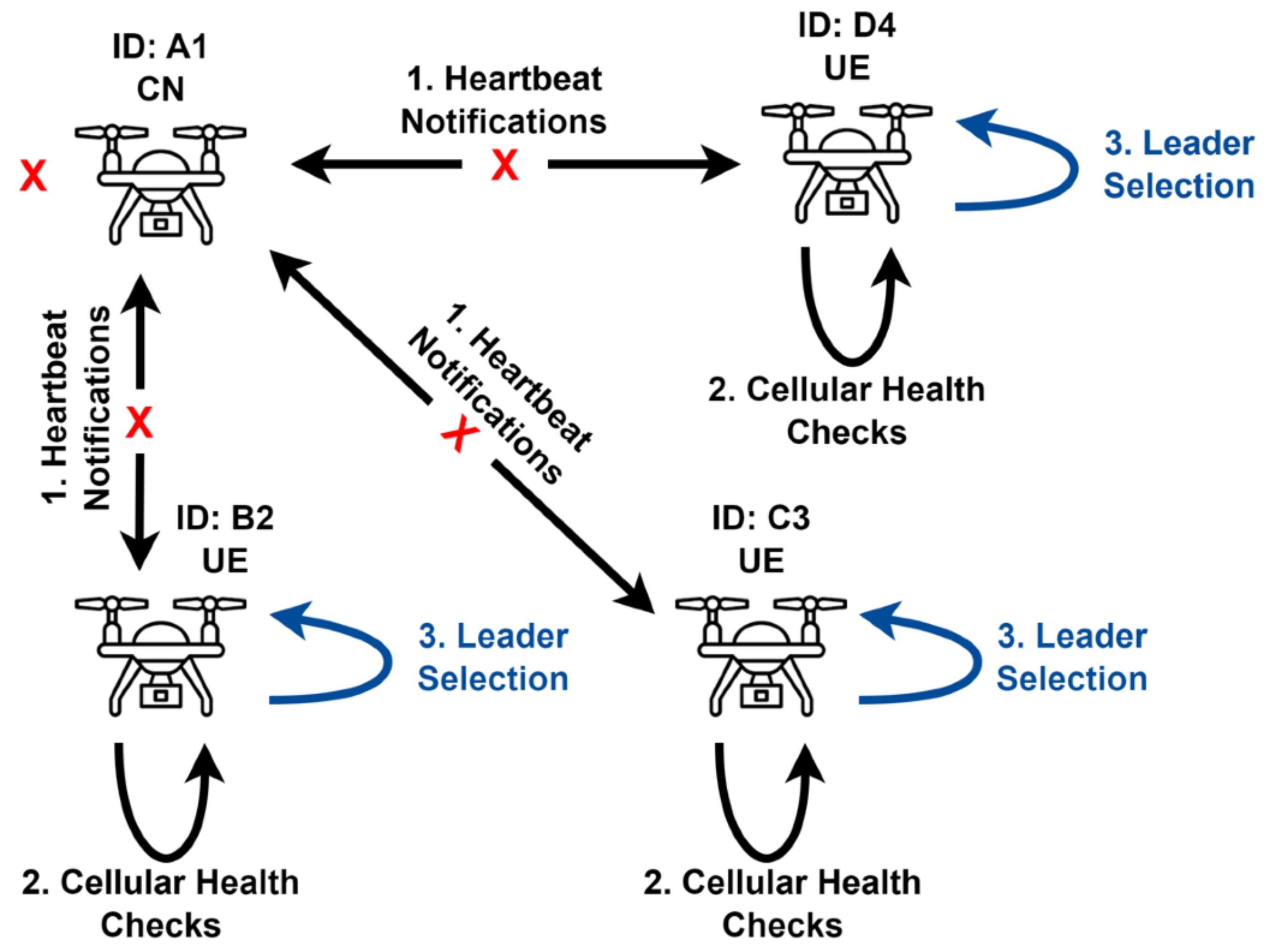
- Preparation Phase
- Discovery & Association Phase

Post-Initialization:

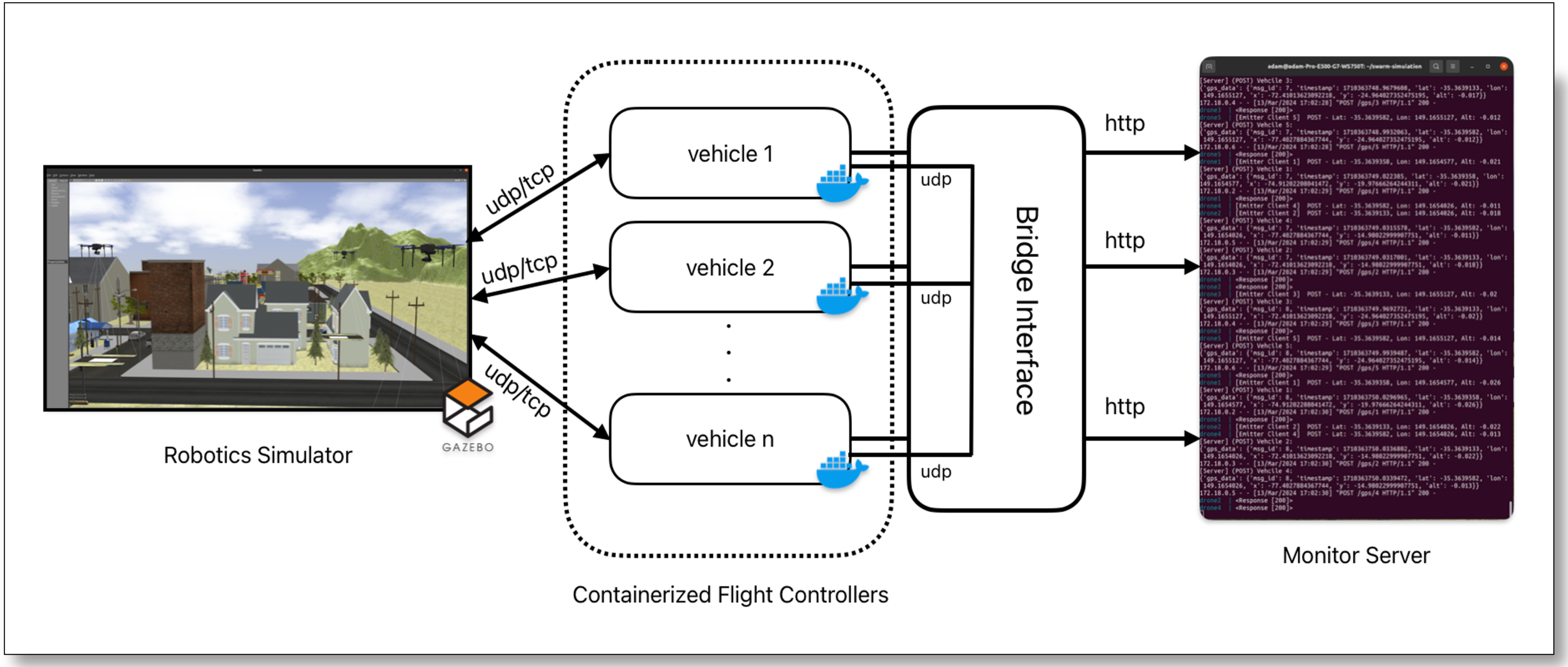
- Heartbeat Process
- Performance self-evaluation
- Performance Sharing
- Leader Selection
- Cellular-level health checks
- Application layer health checks






ID: A1 CN
1. Heartbeat Notifications
ID: D4 UE
X
X
3. Leader Selection
1. Heartbeat Notifications
X
1. Heartbeat Notifications
X
2. Cellular Health Checks
ID: B2 UE
ID: C3 UE
3. Leader Selection
3. Leader Selection
2. Cellular Health Checks
2. Cellular Health Checks

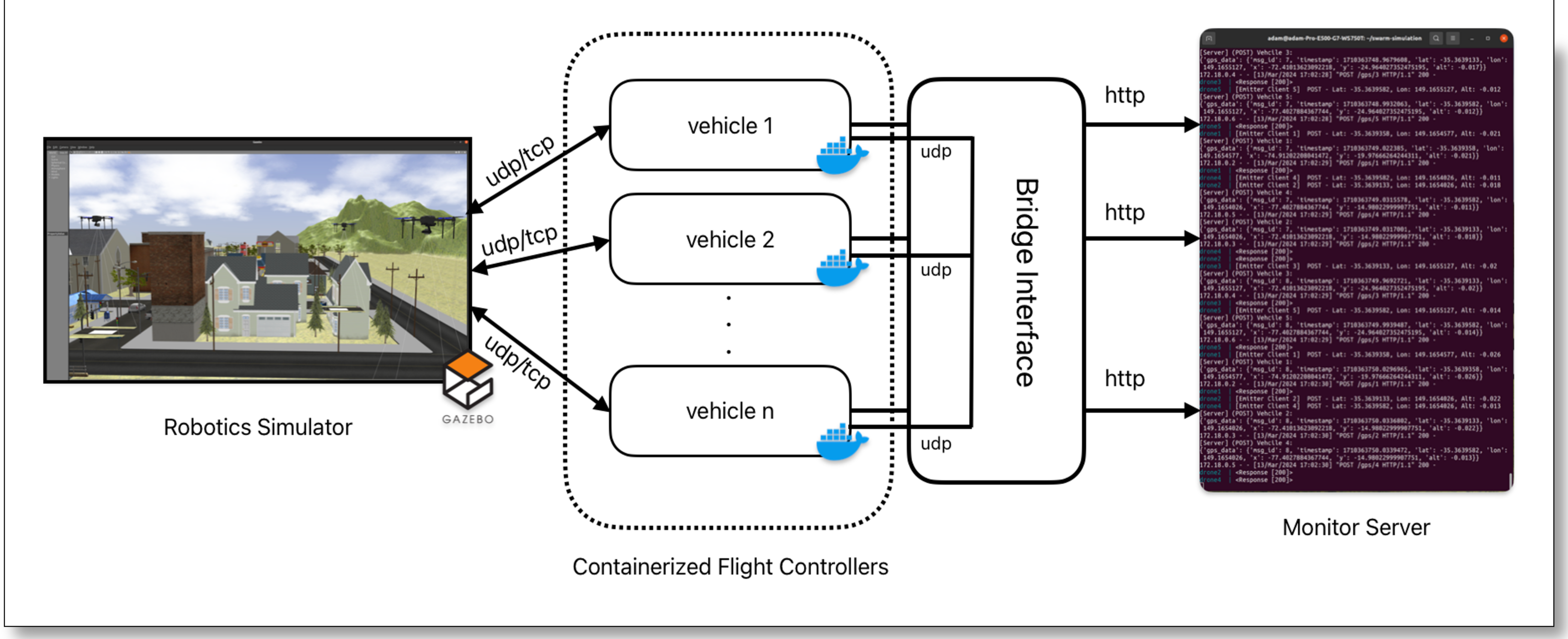
Evaluation Platform



```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.980229999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.980229999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

Evaluation Platform

The simulation environment creates a model for each simulated vehicle in the world it generates and is connected to its corresponding autopilot software instance.



Robotics Simulator

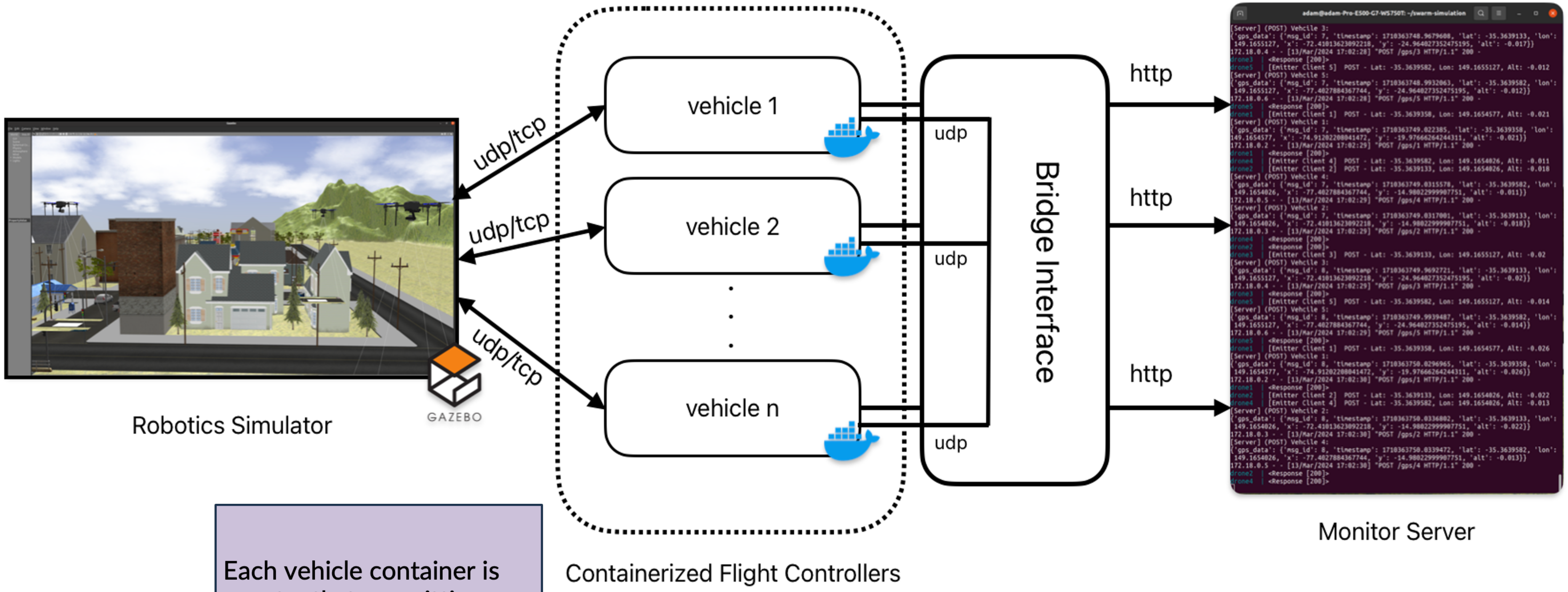
Containerized Flight Controllers

Monitor Server

```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.98022999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.98022999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

Evaluation Platform

The simulation environment creates a model for each simulated vehicle in the world it generates and is connected to its corresponding autopilot software instance.

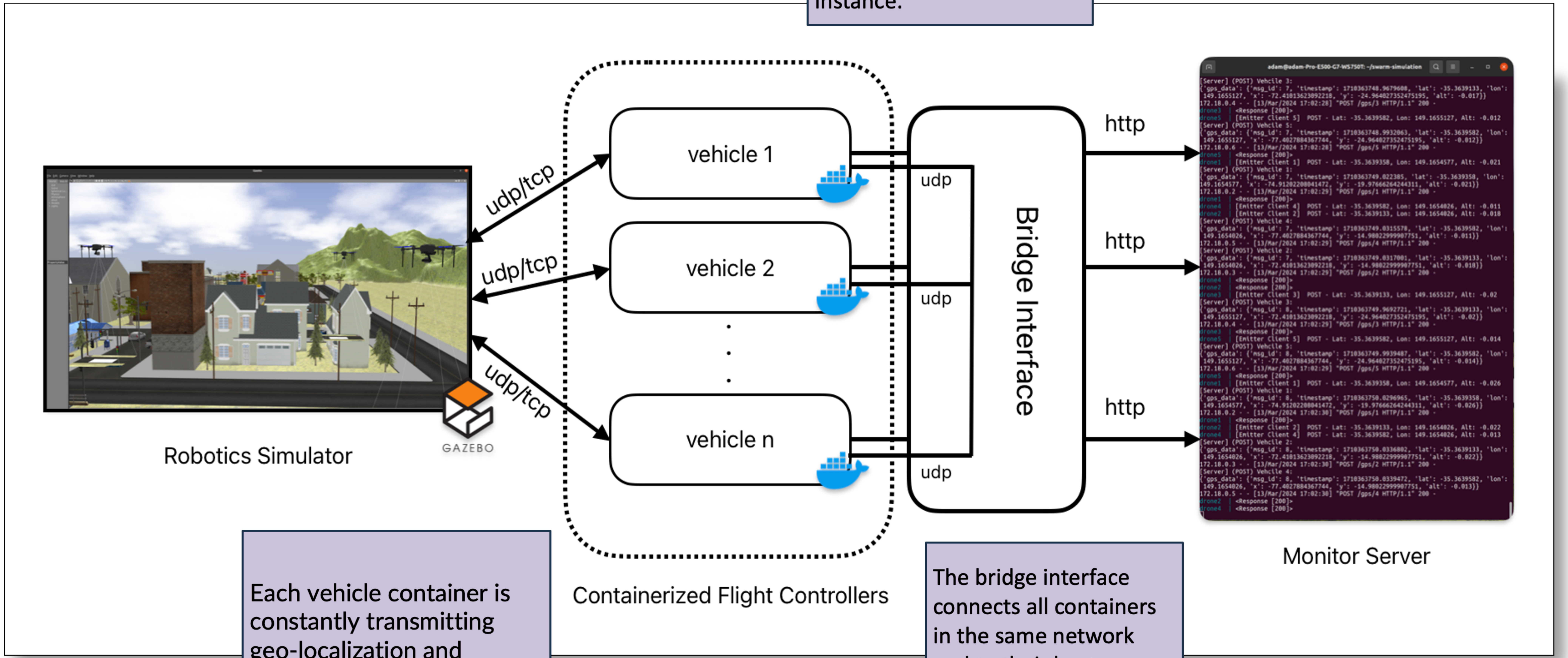


```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.980229999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.980229999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

Each vehicle container is constantly transmitting geo-localization and mission related data to the Monitor server.

Evaluation Platform

The simulation environment creates a model for each simulated vehicle in the world it generates and is connected to its corresponding autopilot software instance.



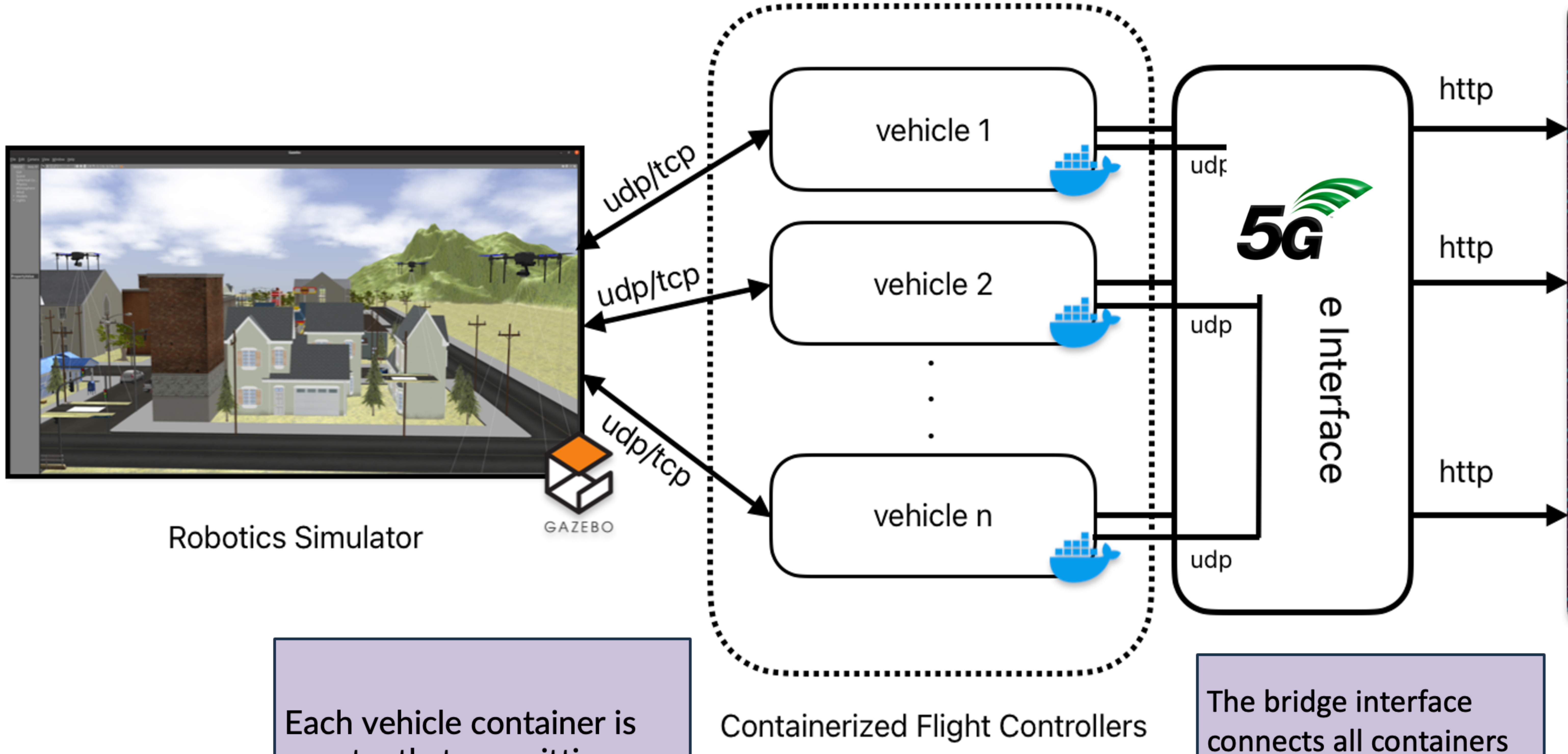
```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.98022999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.98022999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

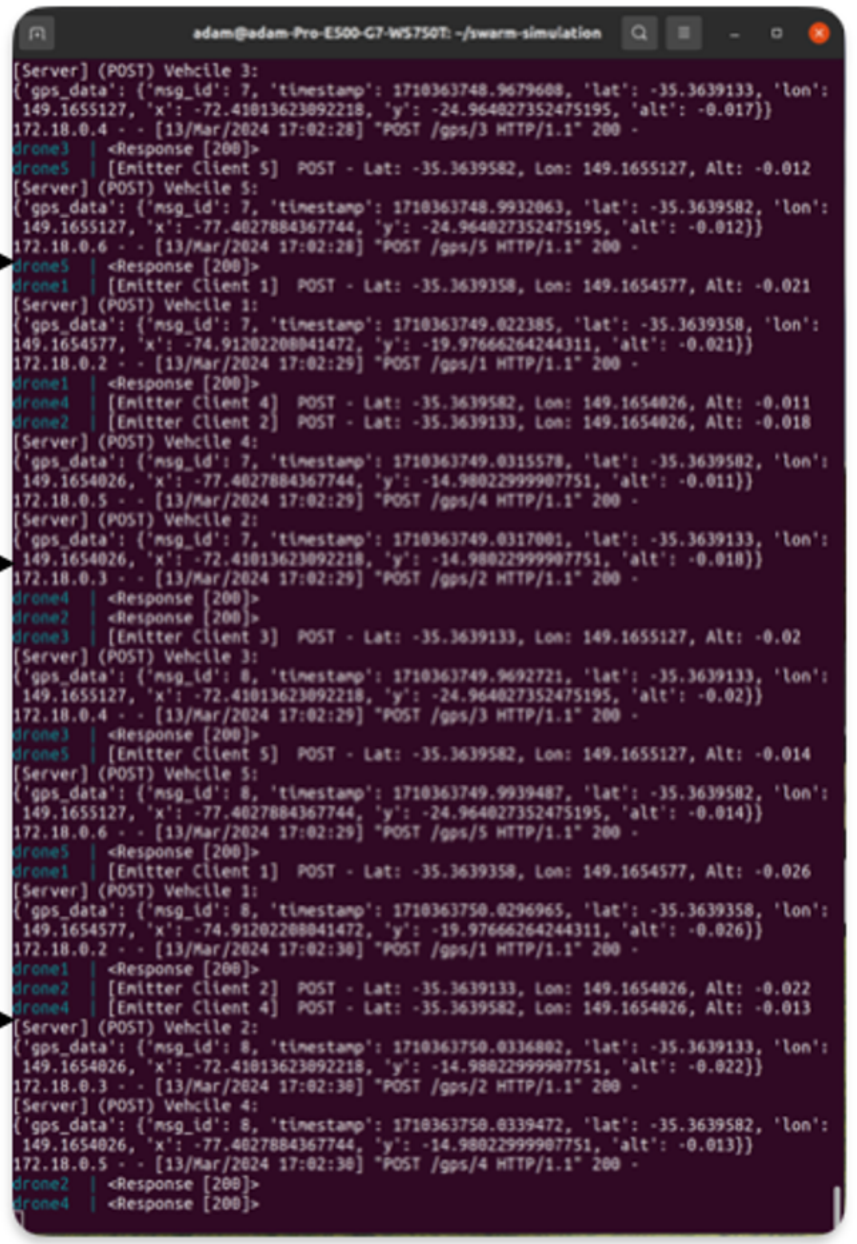
Each vehicle container is constantly transmitting geo-localization and mission related data to the Monitor server.

The bridge interface connects all containers in the same network and to their host machine, enabling intra-swarm communication.

Evaluation Platform

The simulation environment creates a model for each simulated vehicle in the world it generates and is connected to its corresponding autopilot software instance.





```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.976662644244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.980229999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.40278843677744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.976662644244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.980229999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.40278843677744, 'y': -14.980229999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

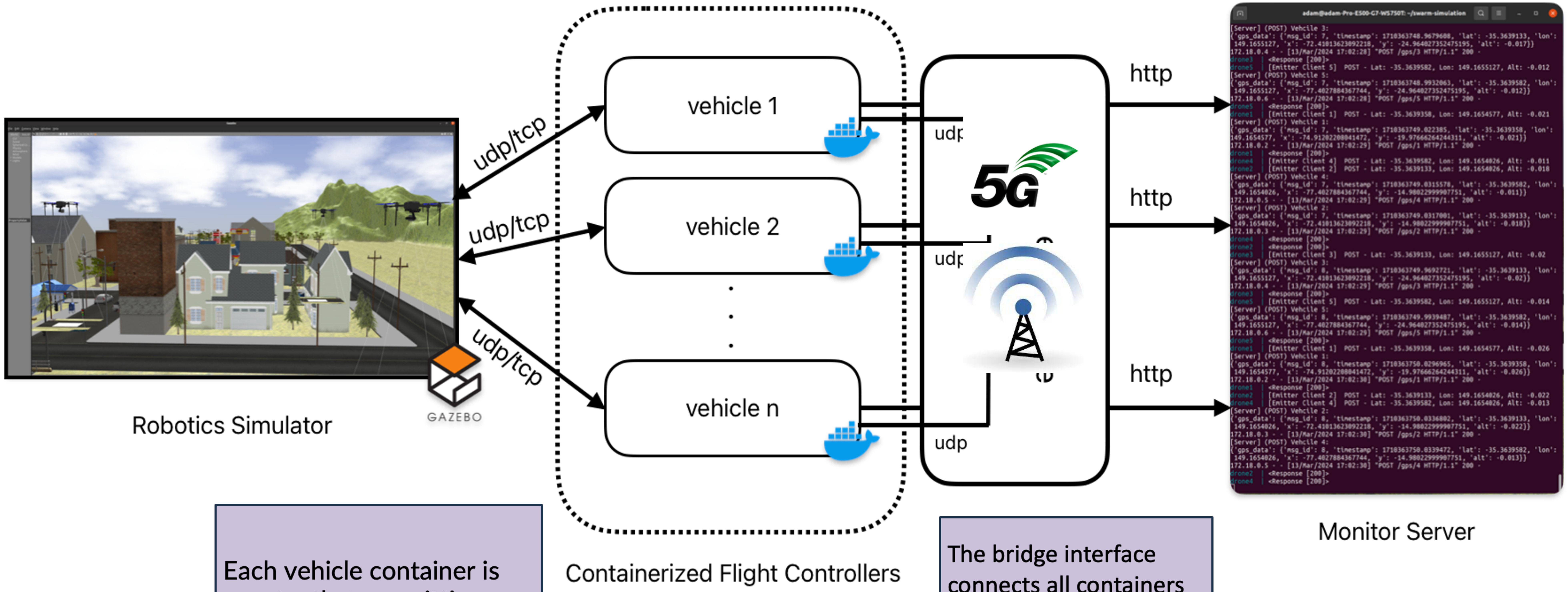
Monitor Server

Each vehicle container is constantly transmitting geo-localization and mission related data to the Monitor server.

The bridge interface connects all containers in the same network and to their host machine, enabling intra-swarm communication.

Evaluation Platform

The simulation environment creates a model for each simulated vehicle in the world it generates and is connected to its corresponding autopilot software instance.

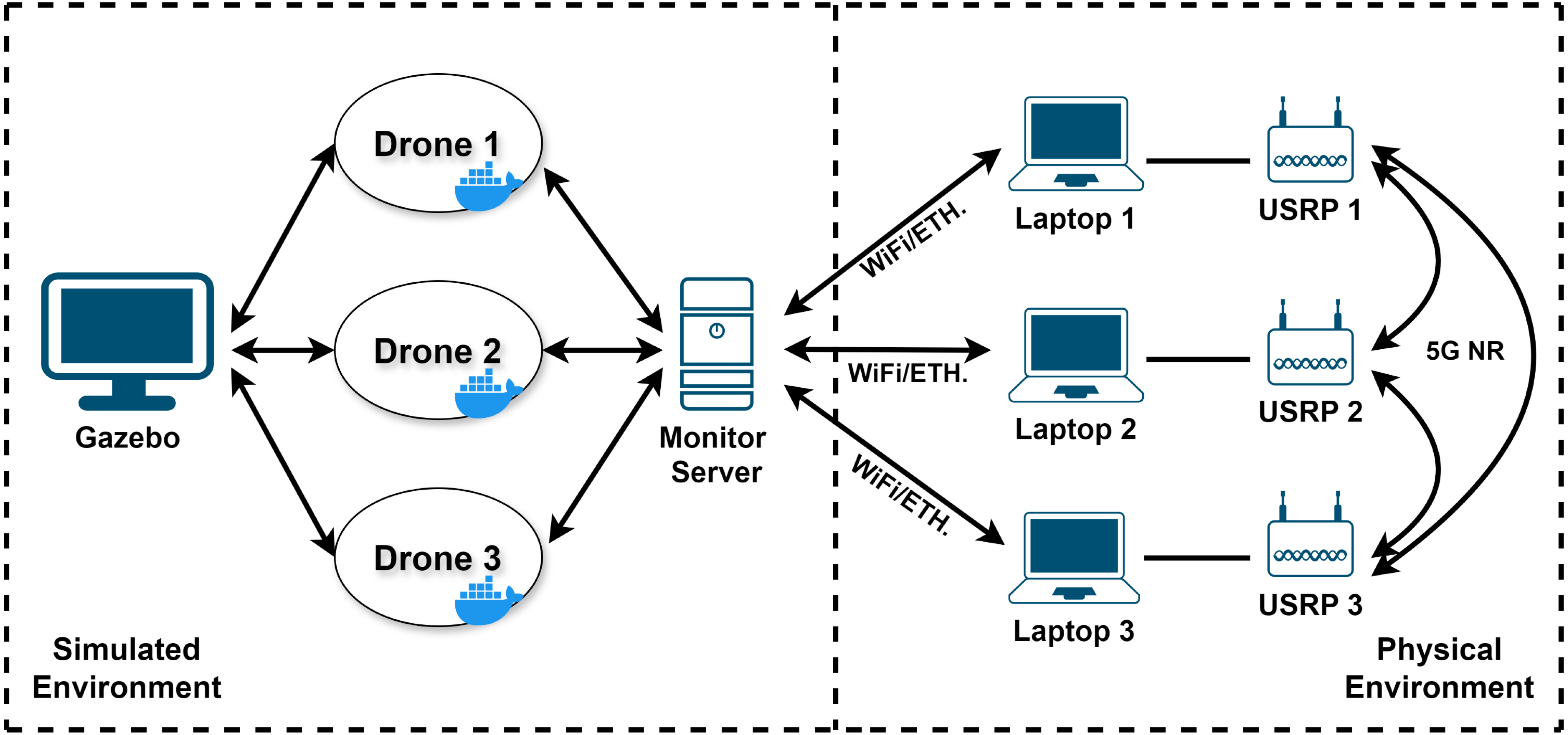


```
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9679608, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.017}}
172.18.0.4 - - [13/Mar/2024 17:02:28] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.012
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363748.9932063, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.012}}
172.18.0.6 - - [13/Mar/2024 17:02:28] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.021
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.022385, 'lat': -35.3639358, 'lon':
149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.021}}
172.18.0.2 - - [13/Mar/2024 17:02:29] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.011
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.018
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0315578, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.98022999907751, 'alt': -0.011}}
172.18.0.5 - - [13/Mar/2024 17:02:29] "POST /gps/4 HTTP/1.1" 200 -
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 7, 'timestamp': 1710363749.0317001, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.018}}
172.18.0.3 - - [13/Mar/2024 17:02:29] "POST /gps/2 HTTP/1.1" 200 -
drone4  | <Response [200]>
drone2  | <Response [200]>
drone3  | [Emitter Client 3]  POST - Lat: -35.3639133, Lon: 149.1655127, Alt: -0.02
[Server] (POST) Vehcile 3:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9692721, 'lat': -35.3639133, 'lon':
 149.1655127, 'x': -72.41013623092218, 'y': -24.964027352475195, 'alt': -0.02}}
172.18.0.4 - - [13/Mar/2024 17:02:29] "POST /gps/3 HTTP/1.1" 200 -
drone3  | <Response [200]>
drone5  | [Emitter Client 5]  POST - Lat: -35.3639582, Lon: 149.1655127, Alt: -0.014
[Server] (POST) Vehcile 5:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363749.9939487, 'lat': -35.3639582, 'lon':
 149.1655127, 'x': -77.4027884367744, 'y': -24.964027352475195, 'alt': -0.014}}
172.18.0.6 - - [13/Mar/2024 17:02:29] "POST /gps/5 HTTP/1.1" 200 -
drone5  | <Response [200]>
drone1  | [Emitter Client 1]  POST - Lat: -35.3639358, Lon: 149.1654577, Alt: -0.026
[Server] (POST) Vehcile 1:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0296965, 'lat': -35.3639358, 'lon':
 149.1654577, 'x': -74.91202208041472, 'y': -19.97666264244311, 'alt': -0.026}}
172.18.0.2 - - [13/Mar/2024 17:02:30] "POST /gps/1 HTTP/1.1" 200 -
drone1  | <Response [200]>
drone2  | [Emitter Client 2]  POST - Lat: -35.3639133, Lon: 149.1654026, Alt: -0.022
drone4  | [Emitter Client 4]  POST - Lat: -35.3639582, Lon: 149.1654026, Alt: -0.013
[Server] (POST) Vehcile 2:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0336802, 'lat': -35.3639133, 'lon':
 149.1654026, 'x': -72.41013623092218, 'y': -14.98022999907751, 'alt': -0.022}}
172.18.0.3 - - [13/Mar/2024 17:02:30] "POST /gps/2 HTTP/1.1" 200 -
[Server] (POST) Vehcile 4:
{'gps_data': {'msg_id': 8, 'timestamp': 1710363750.0339472, 'lat': -35.3639582, 'lon':
 149.1654026, 'x': -77.4027884367744, 'y': -14.98022999907751, 'alt': -0.013}}
172.18.0.5 - - [13/Mar/2024 17:02:30] "POST /gps/4 HTTP/1.1" 200 -
drone2  | <Response [200]>
drone4  | <Response [200]>
```

Each vehicle container is constantly transmitting geo-localization and mission related data to the Monitor server.

The bridge interface connects all containers in the same network and to their host machine, enabling intra-swarm communication.

Evaluation Platform



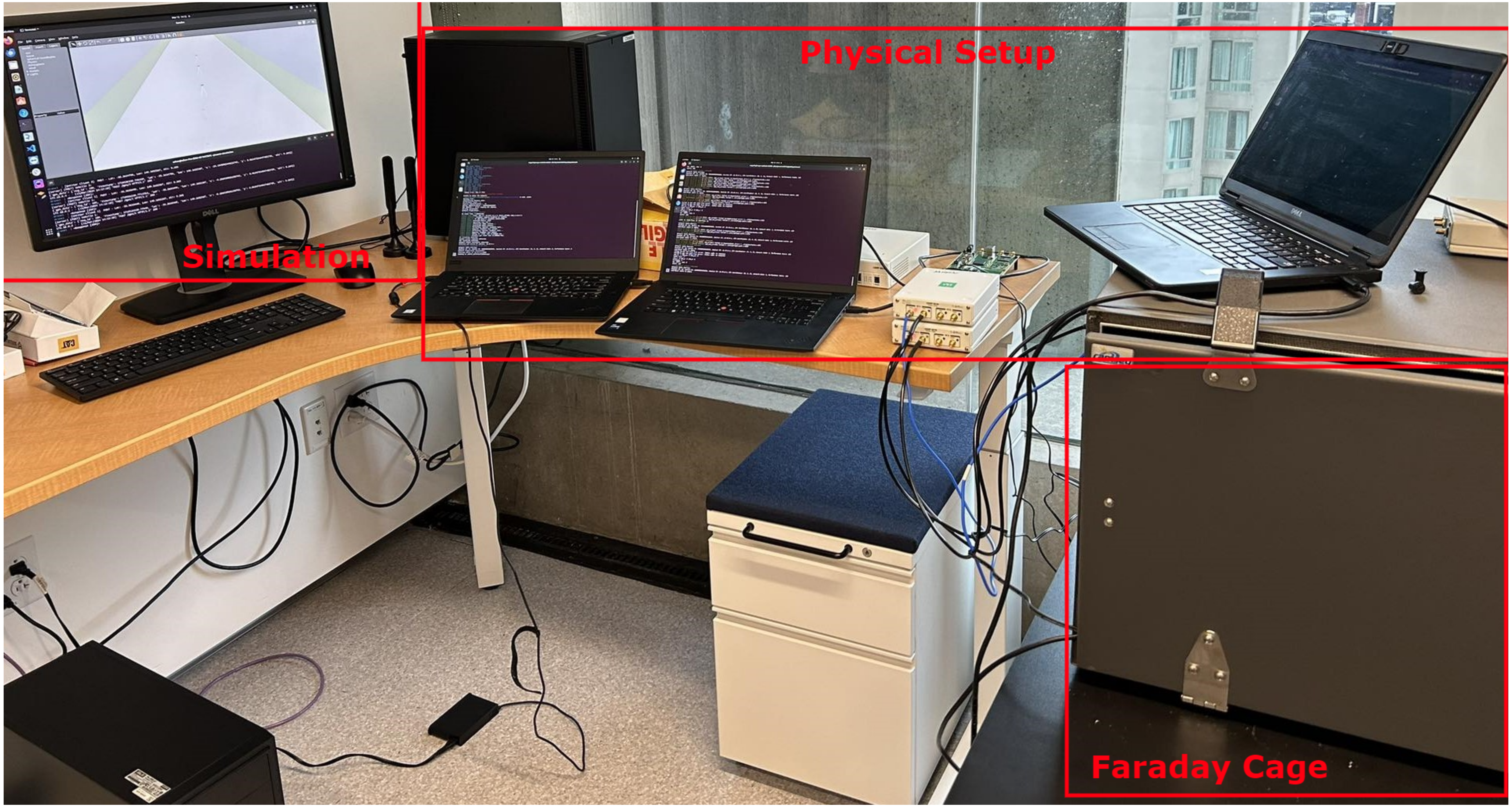
Activities
Terminal
Feb 12 22:13
adam
Trash
adam@adam-Pro-E500-G7-WS750T: ~/...
adam@adam-Pro-E500-G7-...
adam@adam-Pro-E500-G7-...

```
(swarm-env) adam@adam-Pro-E500-G7-WS750T:~/swarm-simulation (e
mit-cartesian-coordinates)$ python3 src/sim_swarm.py multi sma
ll_city_voronoi_5
```

Activities
Terminal
Feb 12 22:13
adam
Trash
adam@adam-Pro-E500-G7-WS750T: ~/...
adam@adam-Pro-E500-G7-...
adam@adam-Pro-E500-G7-...

```
(swarm-env) adam@adam-Pro-E500-G7-WS750T:~/swarm-simulation (e
mit-cartesian-coordinates)$ python3 src/sim_swarm.py multi sma
ll_city_voronoi_5
```

Physical Setup



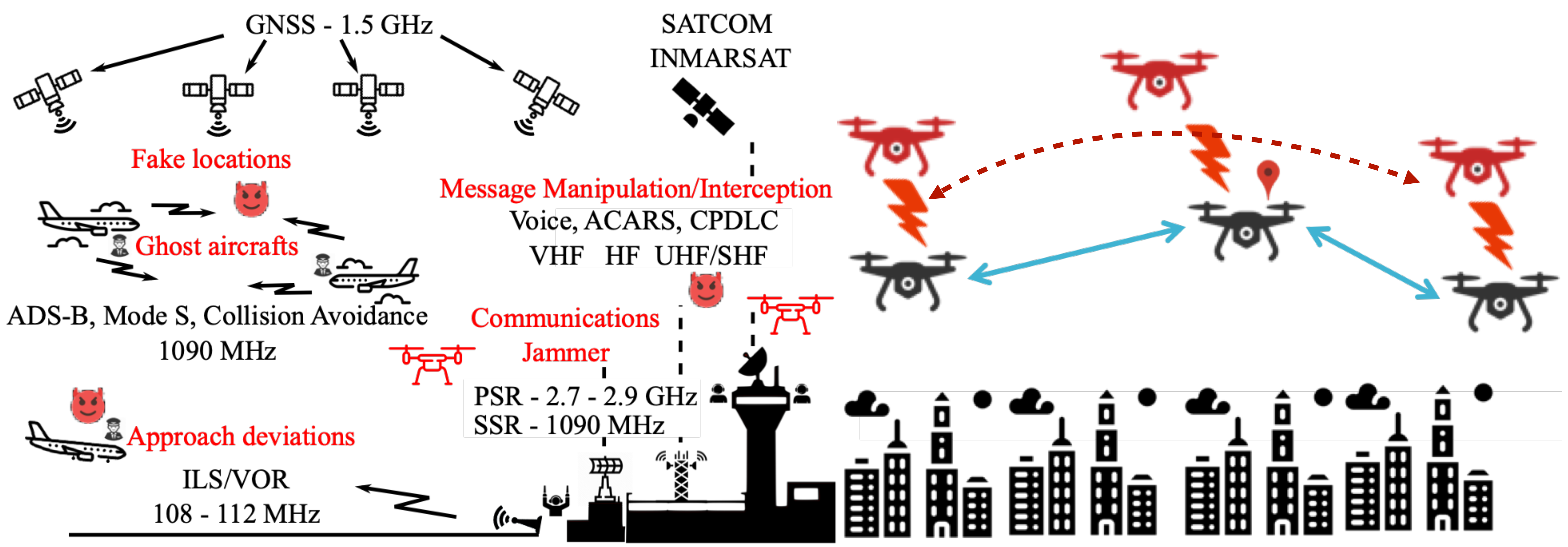
Next steps…

- Secure deployment of private 5G networks at scale specifically tailored for autonomous cyber-physical systems
- Addressing challenges in deploying various distributed/decentralized algorithms developed by the robotics community with available wireless networks

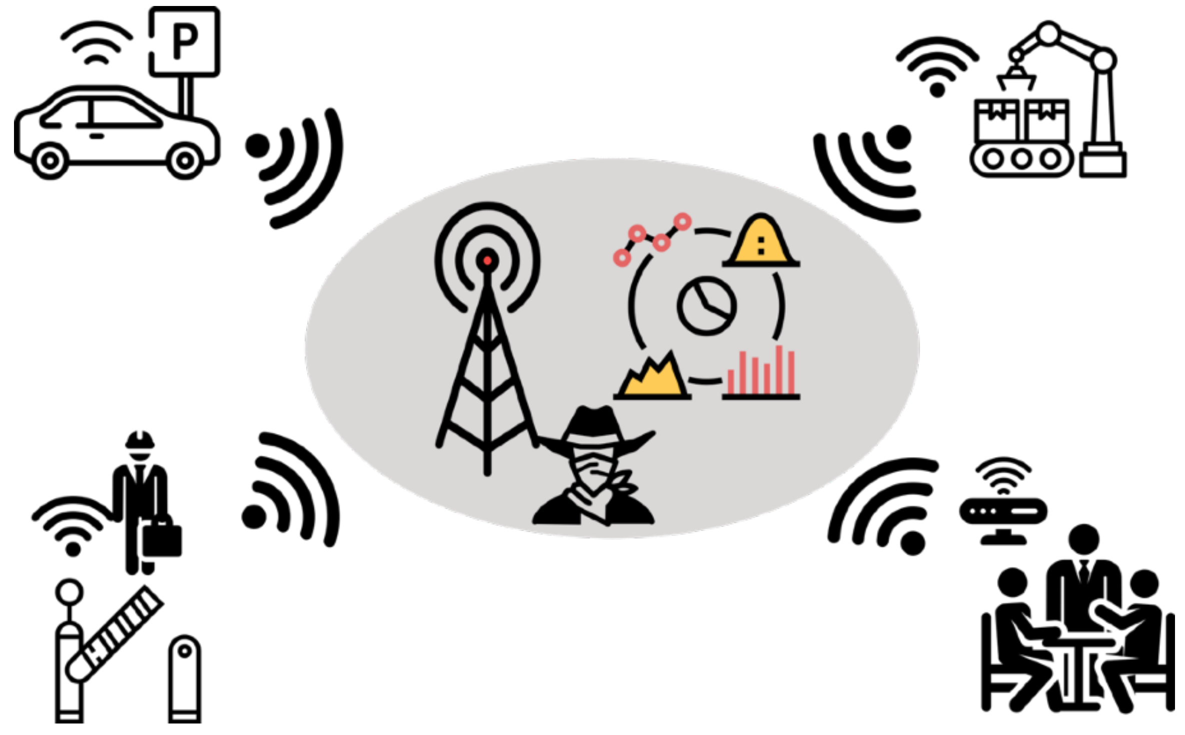
Signal Intelligence Lab @ Northeastern

Security and privacy of wireless networks with a focus on *autonomous cyber-physical systems and smart ecosystems*.

Secure and Private Wide-area Positioning



Aviation and Aerospace Security



Security and Privacy of xIoT

Faculty

Aanjhan Ranganathan
Assistant Professor
www.aanjhan.com

Group Members