Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands

Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, Syed Rafiul Hussain

Systems and Network Security (SyNSec) Lab

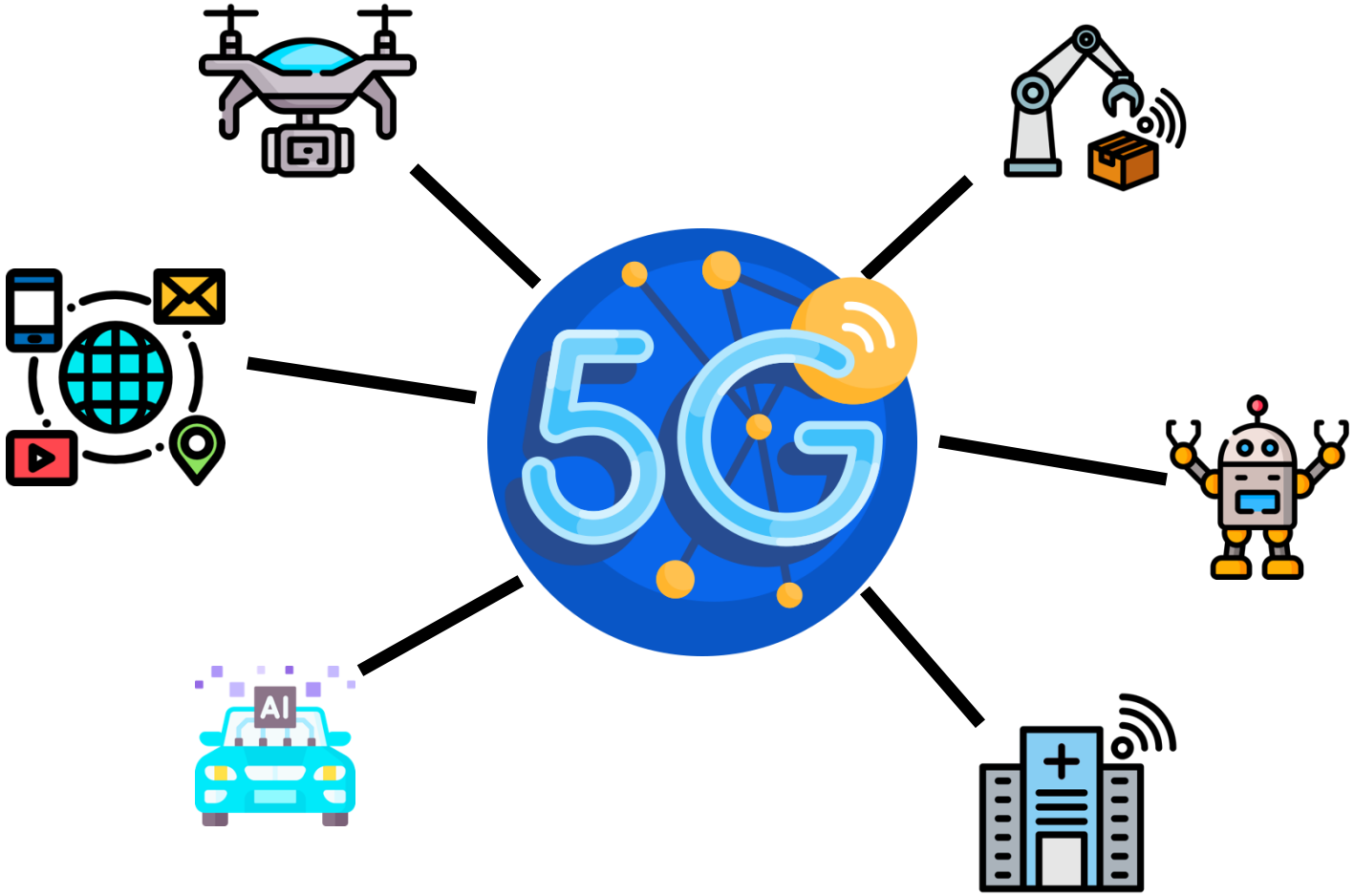
Department of Computer Science and Engineering

Pennsylvania State University

PennState

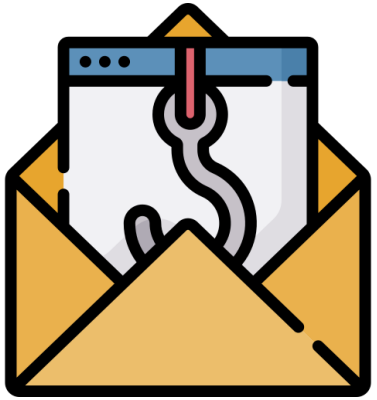
SyNSec

5G Cellular Networks

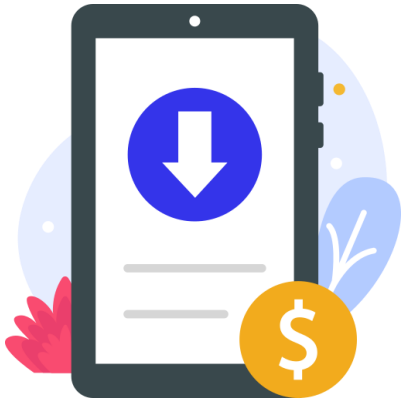


Impacts of Security Policies Violations

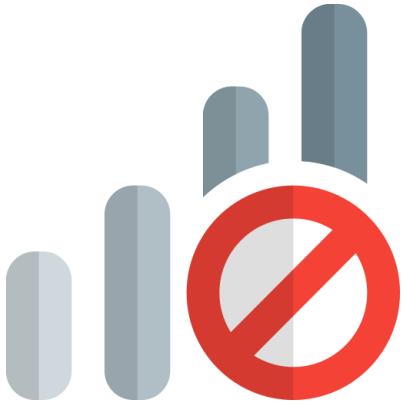
Information Leak



Phishing



Downgrade



Denial-of-Service

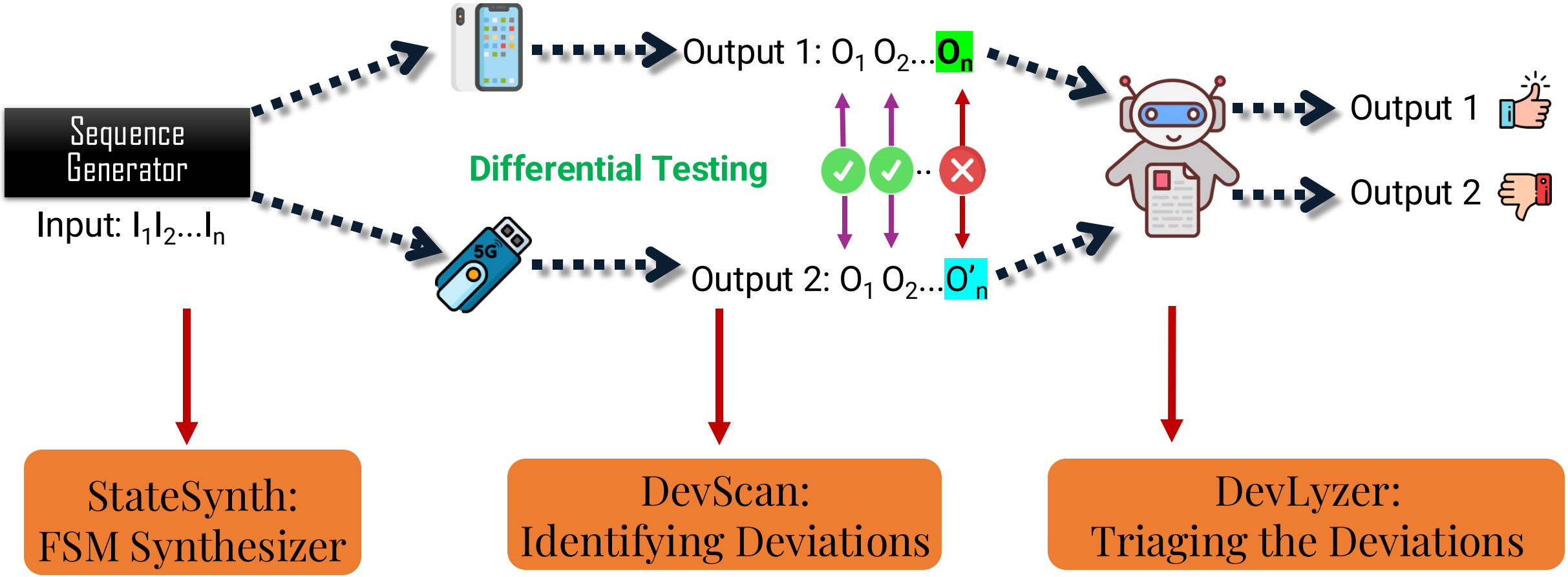
Our Goal

Is it possible to develop an automated framework to efficiently identify security policy violations in 5G UE implementations?

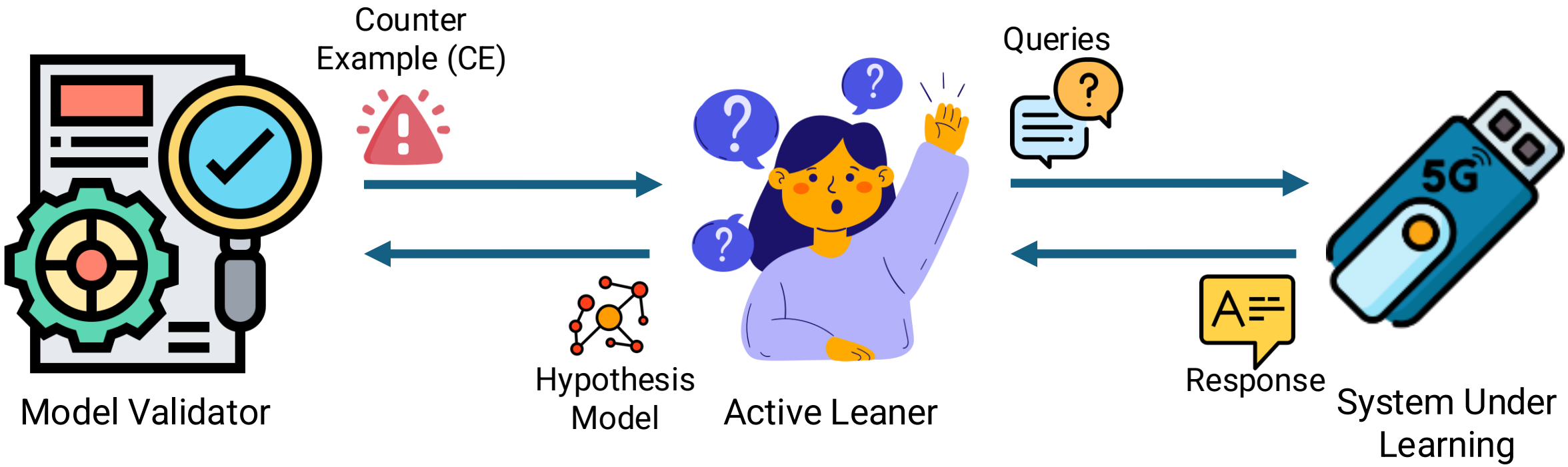
No Comprehensive List of Security Policies

3GPP does not provide such a list which contains a complete set of security policies

High-level Philosophy of Our Approach



Active Automata Learning



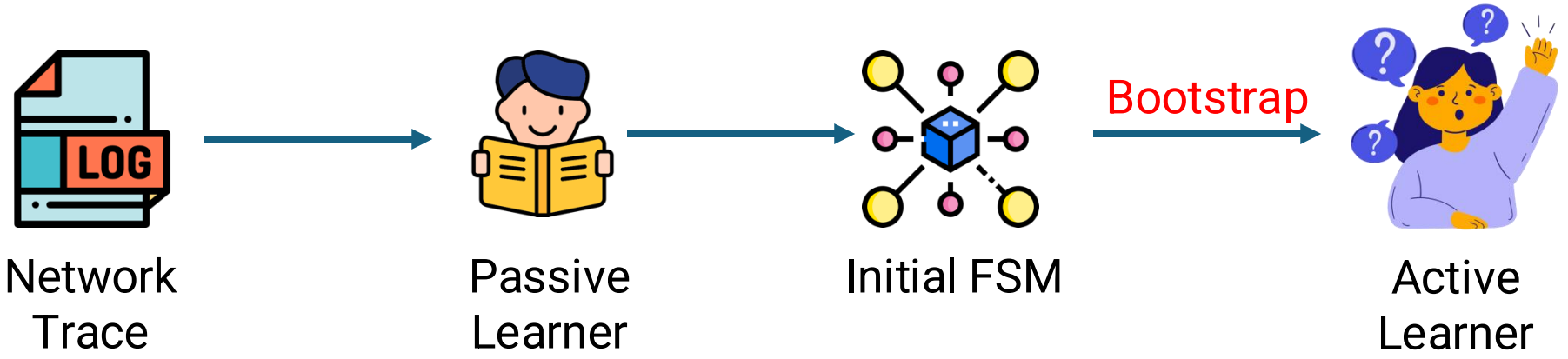
Challenges of Active Automata Learning

Active learner initially does not have any idea about the 5G protocol interactions. It will generate many meaningless queries.

Large number of equivalence checking queries are generated in the model validation stage and most of them are not CE.

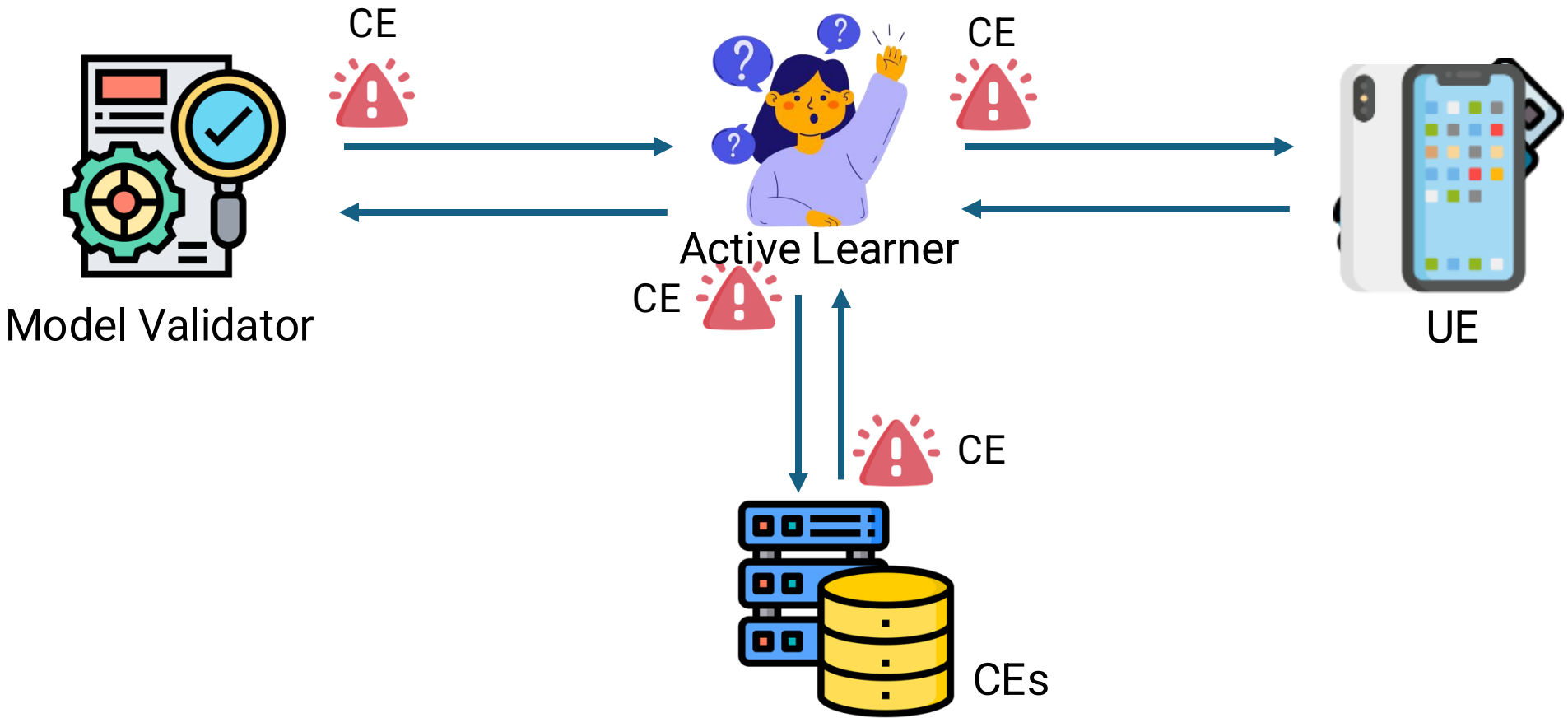
Hybrid Automata Learning

- Synthesize an initial FSM to provide guidance at the beginning of the active learning!

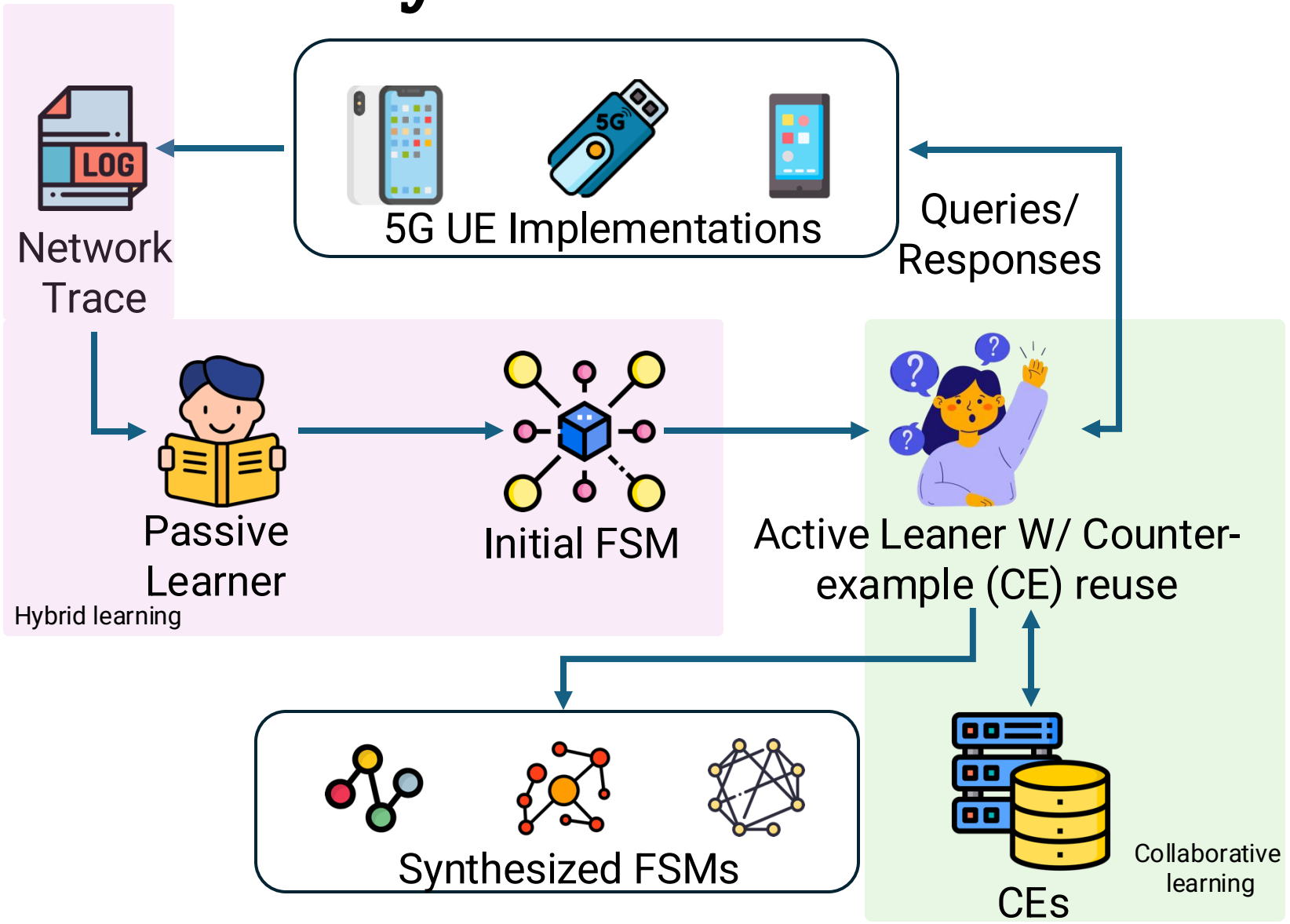


Collaborative Automata Learning

- Since all basebands implement the same protocol, and CEs found during FSM construction of one device are likely to be applicable to other basebands as well.



StateSynth: Workflow



Goal of DevScan

FSM 1

FSM 2

Deviation scanner using symbolic model checker

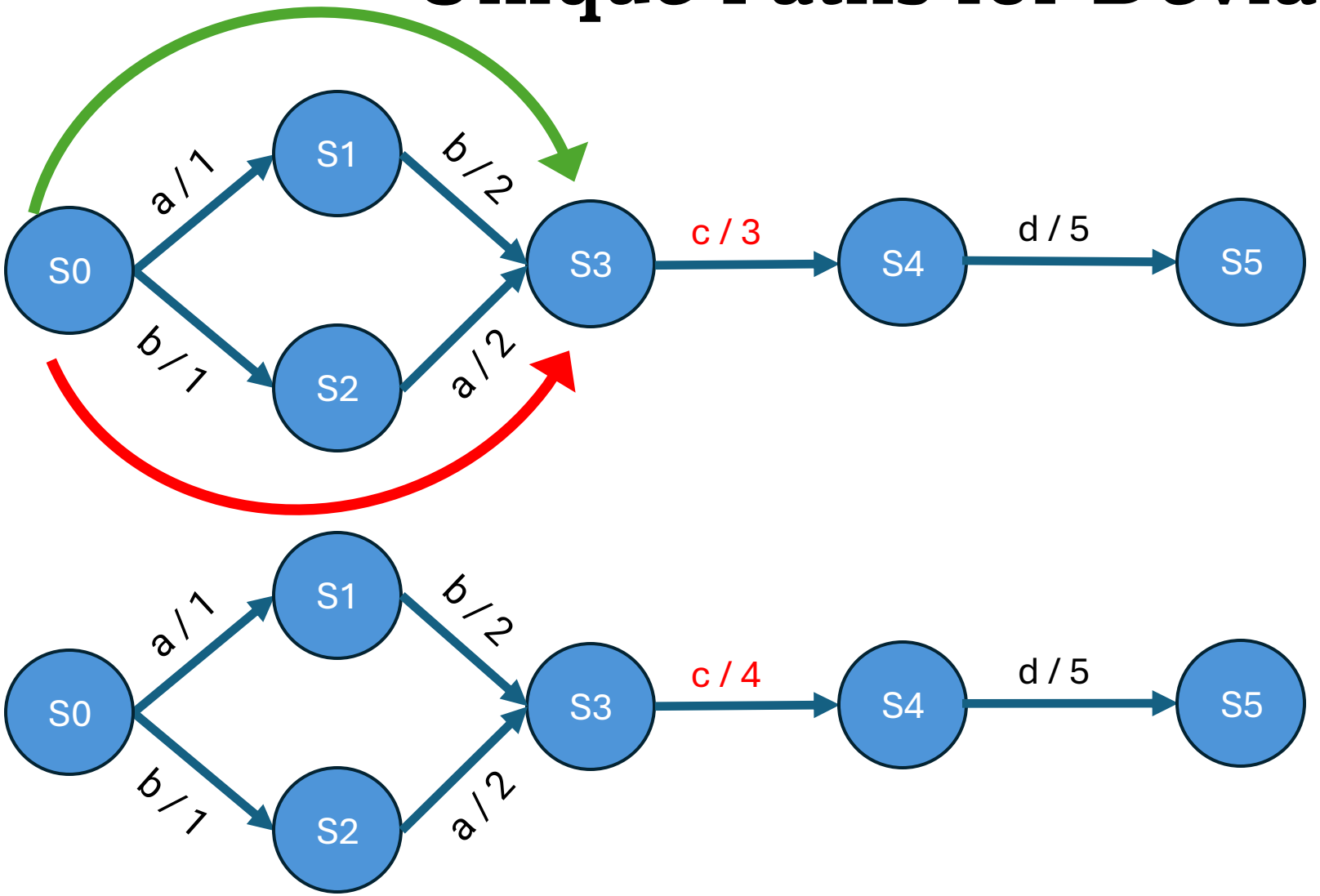
$I_1\ I_2\ I_n\ /\ O_1\ O_2\ O_n$
$I_1\ I_2\ I_n\ /\ O_1\ O_2\ O'_n$

deviations

⚠ Limitation of previous work[1]: prematurely stop their exploration for different variations of a deviation.

[1] Hussain, Syed Rafiul, et al. "Noncompliance as deviant behavior: An automated black-box noncompliance checker for 4g lte cellular devices." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.

Unique Paths for Deviation

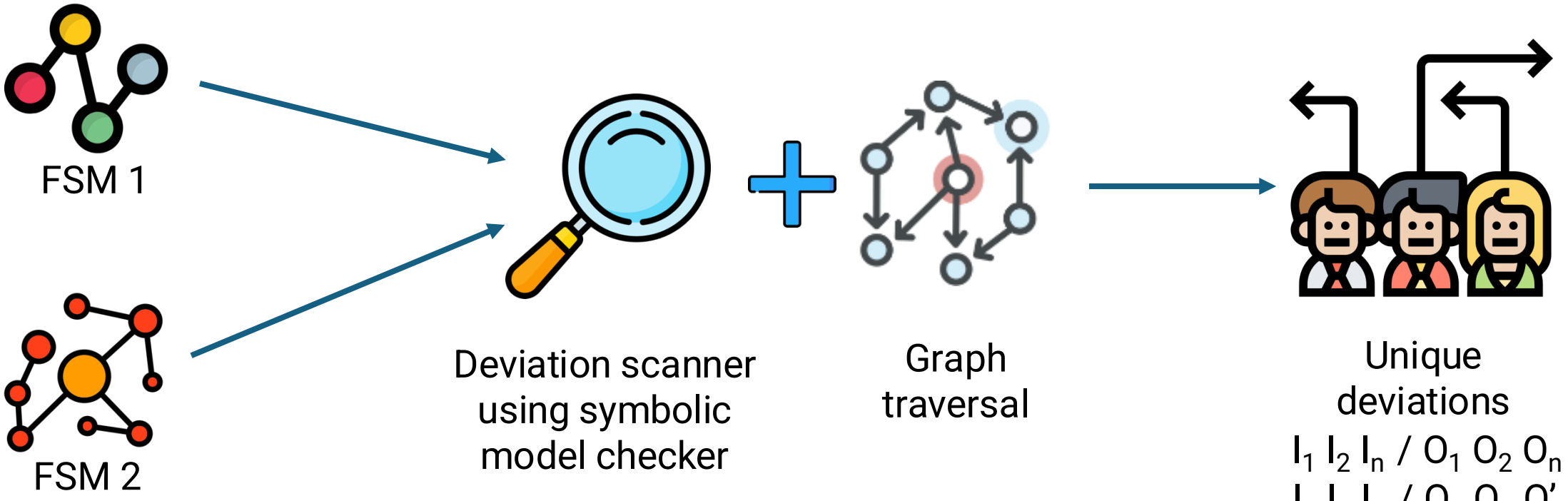


Unique paths for deviation:

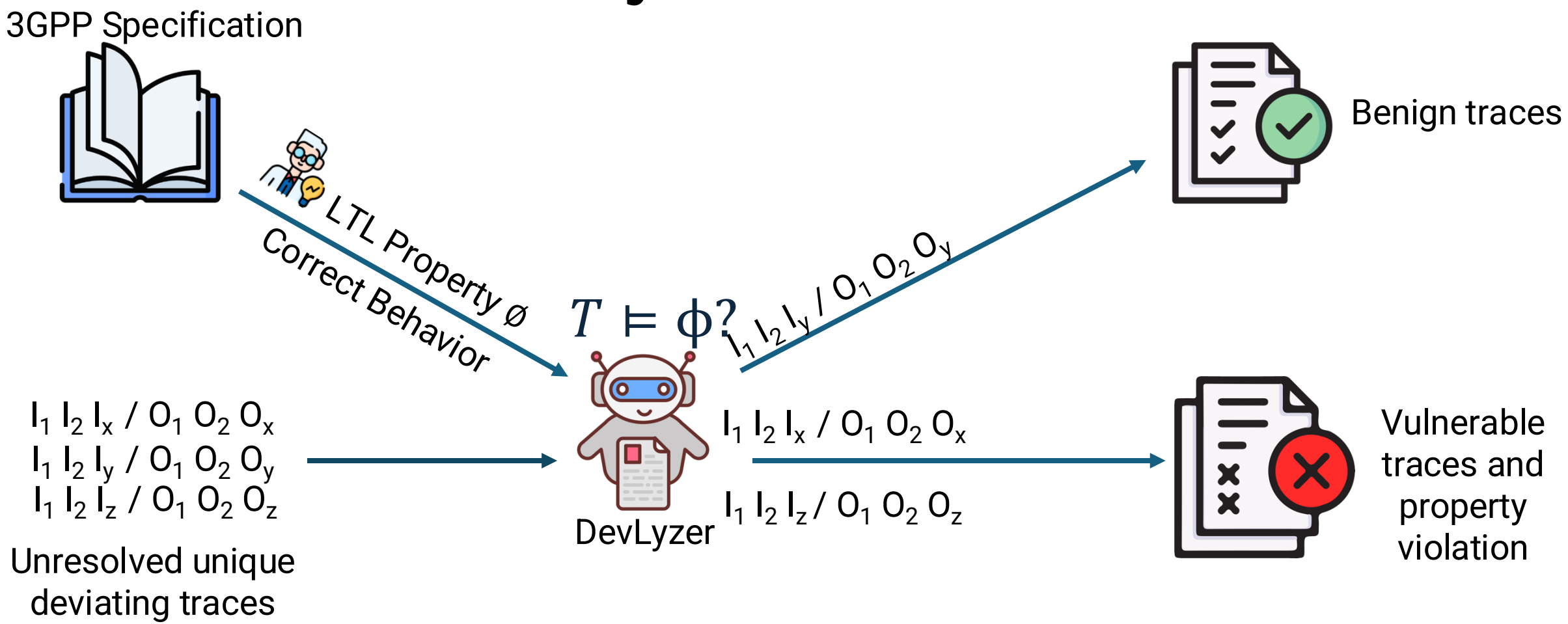
Path 1: S0 → S1 → S3

Path 2: S0 → S2 → S3

DevScan: Workflow



DevLyzer: Workflow

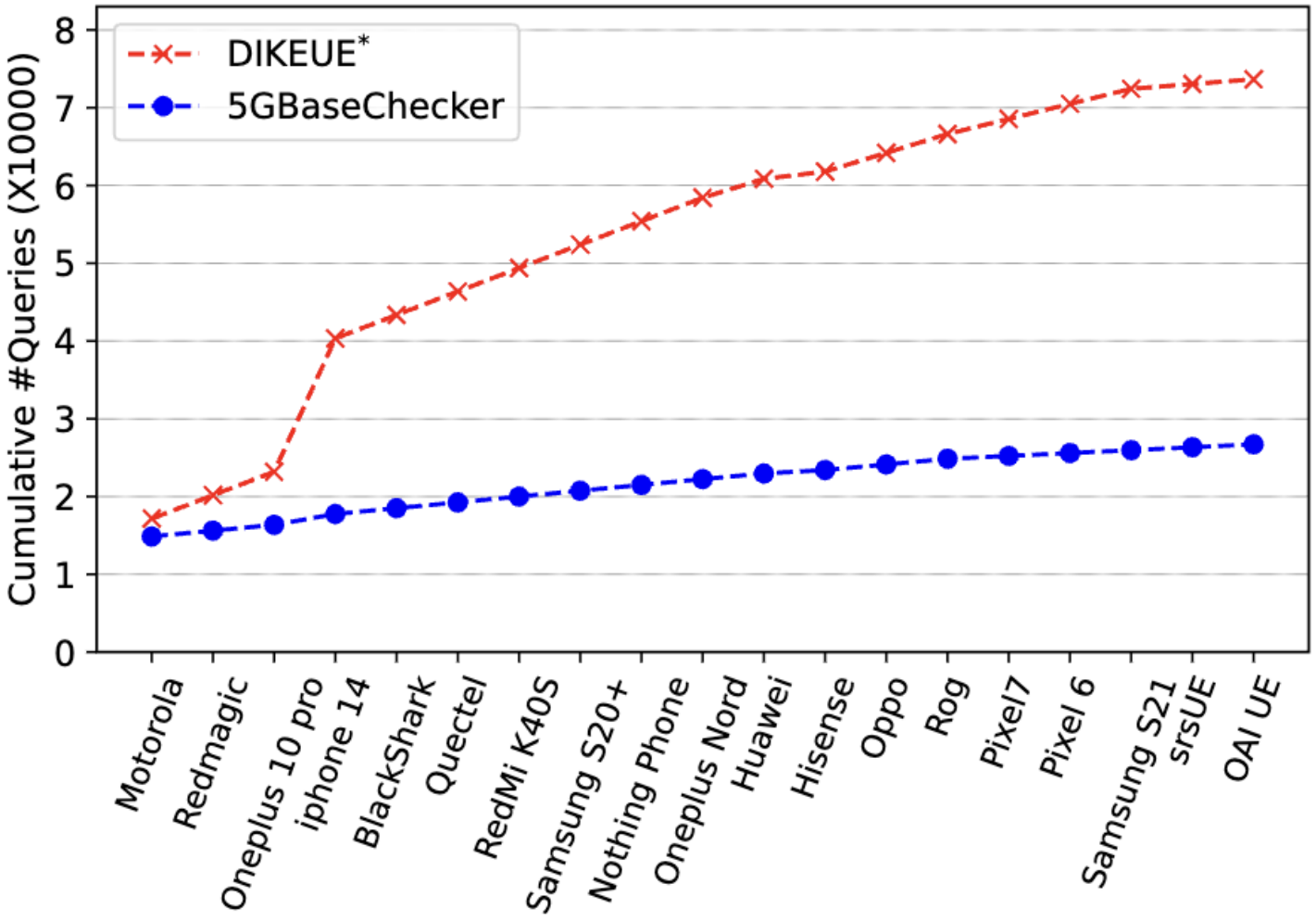


LTL: Linear temporal logic

Evaluation

- We tested 17 Commercial devices from 5 vendors + 2 open-source UE implementations with 5GBaseChecker.

Evaluation of StateSynth

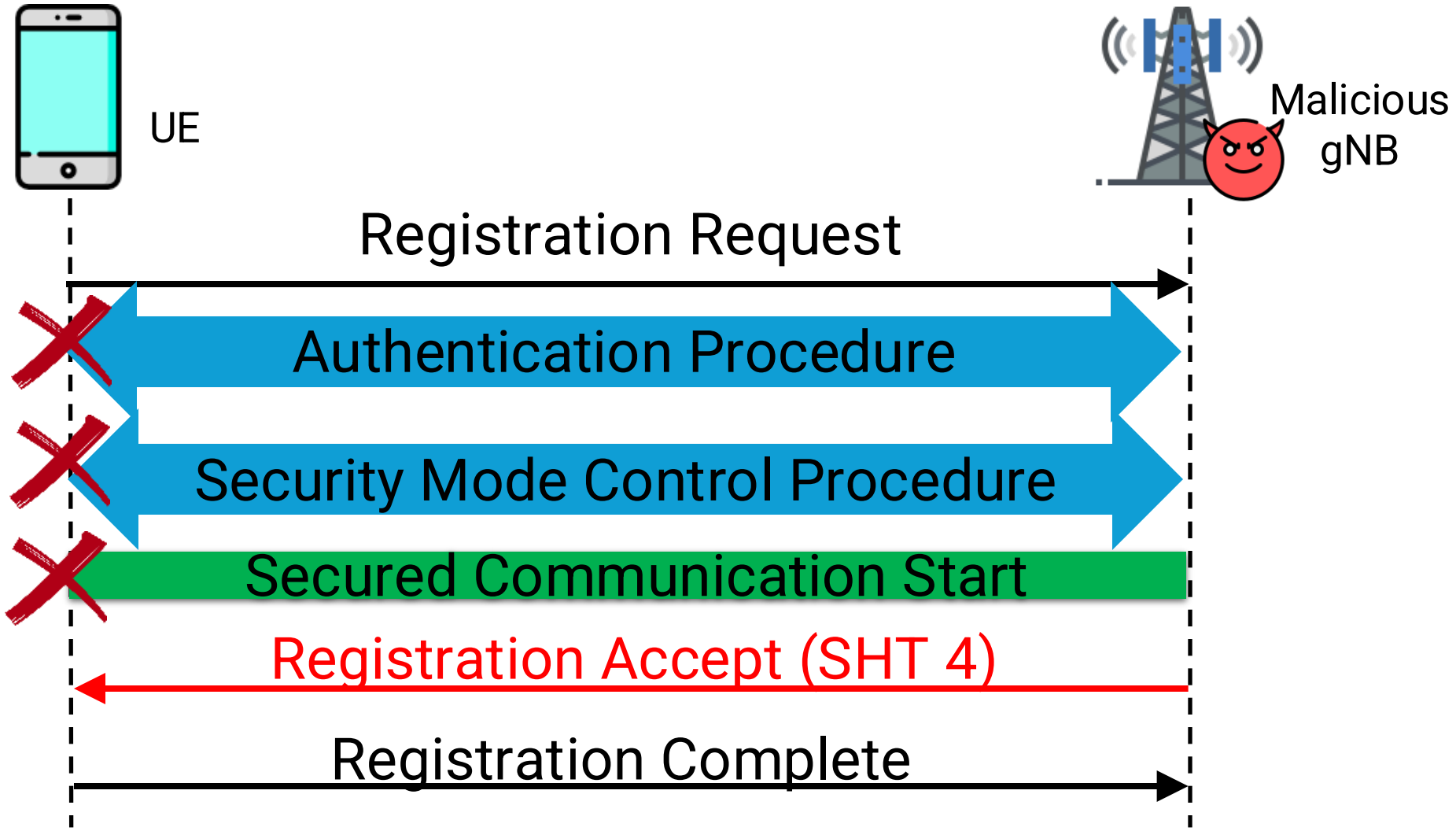


Findings and Impact

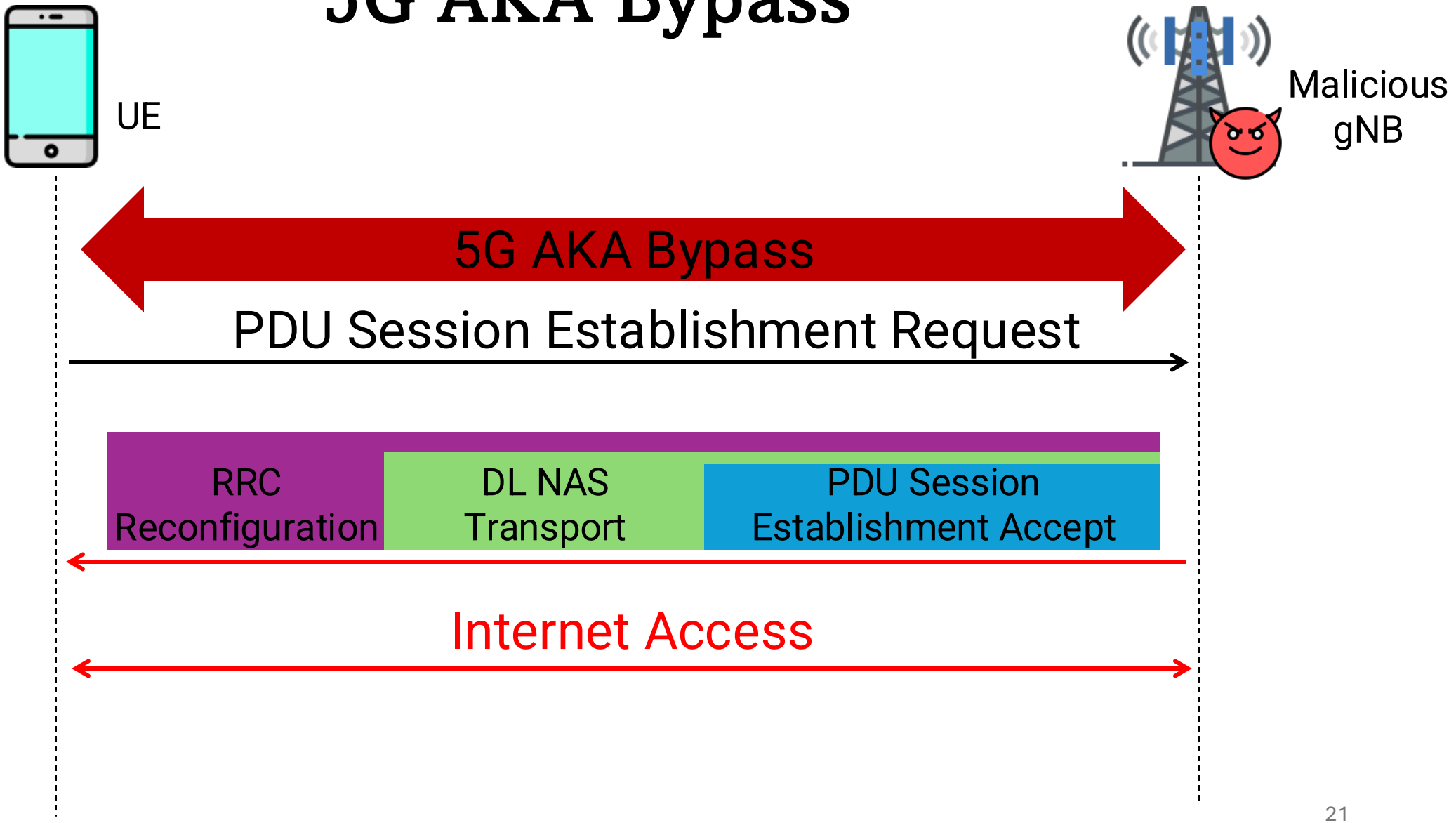
- Uncovered 22 unique issues, 13 could lead to exploitable attacks.
- 12 CVEs assigned and some vendor acknowledgements.
  - CVE-2023-52341, -49928, -50804, -49927, -50803, -52343, -52533, -52534, -52342, -52344; CVE-2024-29152, -28818
- GSMA Mobile Security Research Acknowledgements (CVD-2023-0081)

CVD-2023	0081	Kai Tu, Abdullah Al Ishtiaq, Syed MD Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, Syed Rafiul Hussain	Pennsylvania State University

5G AKA Bypass



5G AKA Bypass



kai@kai: ~/Desktop/5GBaseChecker_Core

```
NN[internet] IPv4[10.45.0.2] IPv6[] (../src/sm
497)
04/06 20:19:47.410: [upf] INFO: [Added] Number of UPF-Sessions
is now 1 (../src/upf/context.c:178)
04/06 20:19:47.410: [gtp] INFO: gtp_connect()
(../lib/gtp/path.c:60)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [gtp] INFO: gtp_connect() [127.0.0.7]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.411: [amf] WARNING: 0x7f40a981c010 (../src/amf/n
amf-handler.c:83)
04/06 20:19:47.411: [sctp] INFO: sctp_senddata (../lib/sctp/ogs
-sctp.c:73)
04/06 20:19:47.446: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 20:19:47.446: [gtp] INFO: gtp_connect() [127.0.0.5]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.446: [amf] INFO: set e->h.sbi.message (../src/am
f/amf-sm.c:511)
```

Attacker Terminal

kai@kai: ~/Desktop/clean/openairinter...

```
 CellGroup
[NR_MAC]   Activating RRC processing timer fo
ms
[NR_MAC]   (949.2) De-activating RRC processi
16
[NR_MAC]   Modified rnti 4a16 with CellGroup
[NR_MAC]   Added new CBRA process for UE RNTI 4a16 with initial
 CellGroup
[NR_RRC]   Receive RRC Reconfiguration Complete message UE 4a16
[PDCP]   ../../../openair2/LAYER2/nr_pdcp/nr_pdcp_oai_api.c:860
:add_drb_am: warning DRB 1 already exist for UE ID/RNTI 18966,
do nothing
[PDCP]   ../../../openair2/LAYER2/nr_pdcp/nr_pdcp_oai_api.c:add
_drb:911: added DRB for UE ID/RNTI 18966
[RLC]   ../../../openair2/LAYER2/nr_rlc/nr_rlc_oai_api.c:761:ad
d_drb_am: DRB 1 already exists for UE with RNTI 4a16, do nothin
g
[RLC]   ../../../openair2/LAYER2/nr_rlc/nr_rlc_oai_api.c:nr_rlc
_add_drb:860: added DRB to UE with RNTI 0x4a16
[NR_RRC]   [gNB 0] Frame  0 : Logical Channel UL-DCCH, Received
 NR_RRCReconfigurationComplete from UE rnti 4a16, reconfiguring
 DRB 1
[NR_RRC]   msg index 0, pdu_sessions index 0, status 2, xid 0):
 nb_of_pdusessions 1,  pdusession_id 5, teid: 1166204179
 [NR_RRC]   NGAP_PDUSESSION_SETUP_RESP: sending the message
[NGAP]   pdusession_setup_resp_p: pdusession ID 5, gnb_addr 127
.0.0.5, SIZE 4
[PDCP]   discard NR PDU rcvd_count=6, entity->rx_deliv 10,sdu_i
n_list 0
```

Attacker Terminal

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Trace Capture

ip.addr == 127.0.0.5 && dns || ngap || gtp

No.	Protocol	Info
961	NGAP	NGSetupRequest
963	NGAP	NGSetupResponse
3169	NGAP/N…	InitialUEMessage, Registration request, Registration request
3249	NGAP/N…	DownlinkNASTransport, Identity request
3255	NGAP/N…	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Identity response
3340	NGAP/N…	DownlinkNASTransport, Registration accept
3351	NGAP/N…	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Registration complete
3465	NGAP/N…	UplinkNASTransport, UL NAS transport, PDU session establishment request
3602	NGAP/N…	SACK (Ack=3, Arwnd=106496) , PDUSessionResourceSetupRequest, DL NAS transport, PDU s
3608	NGAP	SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse

Attack Message

Frame (118 bytes) Bitstring tvb (4 bytes) Unaligned OCTET STRING

Authentication Bypassed!!!

SM-G991B

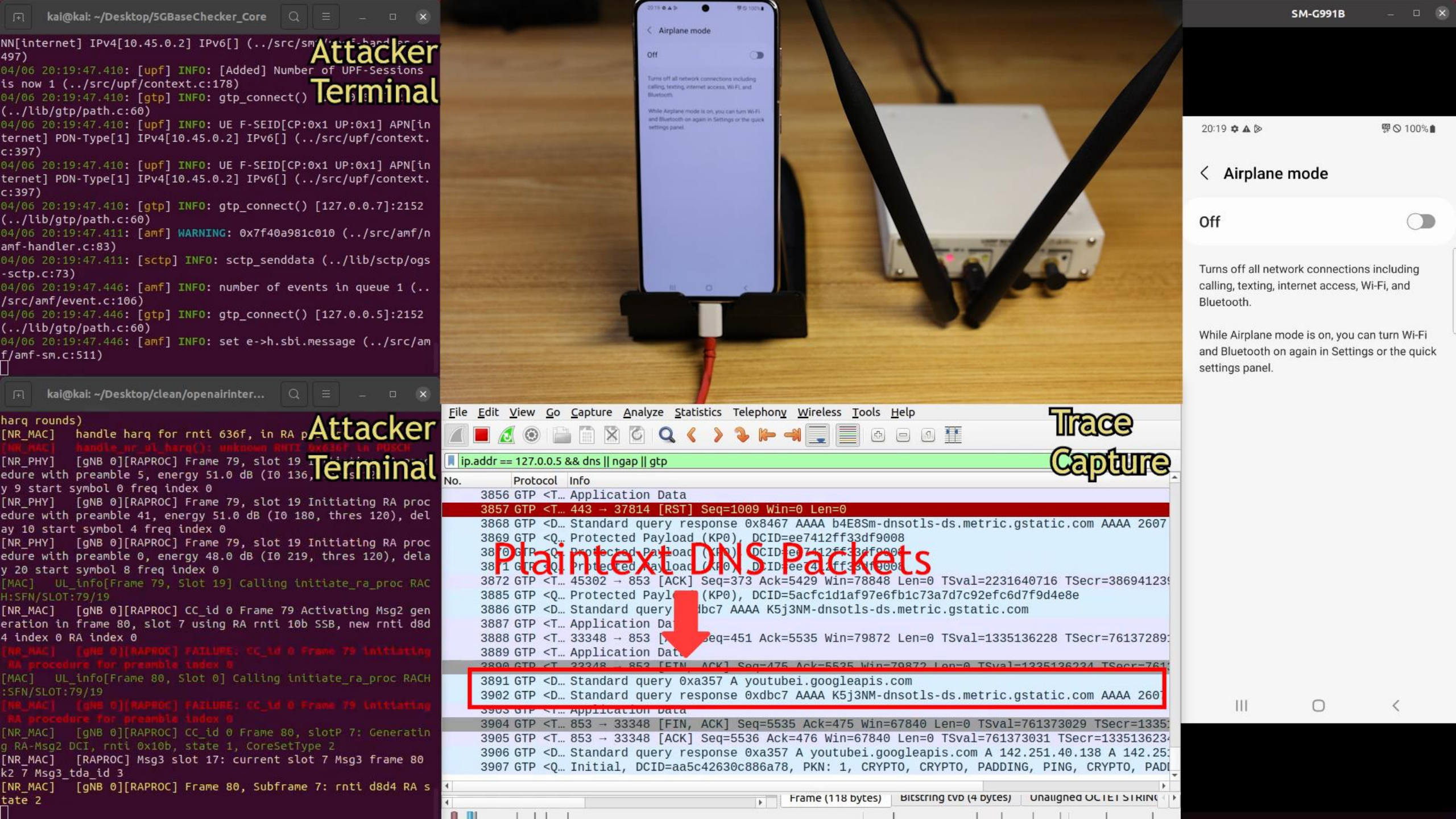
20:19 100%

Airplane mode

Off

Turns off all network connections including calling, texting, internet access, Wi-Fi, and Bluetooth.

While Airplane mode is on, you can turn Wi-Fi and Bluetooth on again in Settings or the quick settings panel.


kai@kai: ~/Desktop/5GBaseChecker_Core
NN[internet] IPv4[10.45.0.2] IPv6[] (../src/sm
497)
04/06 20:19:47.410: [upf] INFO: [Added] Number of UPF-Sessions
is now 1 (../src/upf/context.c:178)
04/06 20:19:47.410: [gtp] INFO: gtp_connect()
(../lib/gtp/path.c:60)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [gtp] INFO: gtp_connect() [127.0.0.7]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.411: [amf] WARNING: 0x7f40a981c010 (../src/amf/n
amf-handler.c:83)
04/06 20:19:47.411: [sctp] INFO: sctp_senddata (../lib/sctp/ogs
-sctp.c:73)
04/06 20:19:47.446: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 20:19:47.446: [gtp] INFO: gtp_connect() [127.0.0.5]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.446: [amf] INFO: set e->h.sbi.message (../src/am
f/amf-sm.c:511)
Attacker Terminal
kai@kai: ~/Desktop/clean/openairinter...
harq rounds)
[NR_MAC] handle harq for rnti 636f, in RA p
[NR_MAC] handle_nr_ul_harq(): unknown RNTI 0x636f in PUSCH
[NR_PHY] [gNB 0][RAPROC] Frame 79, slot 19
edure with preamble 5, energy 51.0 dB (I0 136,
y 9 start symbol 0 freq index 0
[NR_PHY] [gNB 0][RAPROC] Frame 79, slot 19 Initiating RA proc
edure with preamble 41, energy 51.0 dB (I0 180, thres 120), del
ay 10 start symbol 4 freq index 0
[NR_PHY] [gNB 0][RAPROC] Frame 79, slot 19 Initiating RA proc
edure with preamble 0, energy 48.0 dB (I0 219, thres 120), dela
y 20 start symbol 8 freq index 0
[MAC] UL_info[Frame 79, Slot 19] Calling initiate_ra_proc RAC
H:SFN/SLOT:79/19
[NR_MAC] [gNB 0][RAPROC] CC_id 0 Frame 79 Activating Msg2 gen
eration in frame 80, slot 7 using RA rnti 10b SSB, new rnti d8d
4 index 0 RA index 0
[NR_MAC] [gNB 0][RAPROC] FAILURE: CC_id 0 Frame 79 initiating
RA procedure for preamble index 0
[MAC] UL_info[Frame 80, Slot 0] Calling initiate_ra_proc RACH
:SFN/SLOT:79/19
[NR_MAC] [gNB 0][RAPROC] FAILURE: CC_id 0 Frame 79 initiating
RA procedure for preamble index 0
[NR_MAC] [gNB 0][RAPROC] CC_id 0 Frame 80, slotP 7: Generatin
g RA-Msg2 DCI, rnti 0x10b, state 1, CoreSetType 2
[NR_MAC] [RAPROC] Msg3 slot 17: current slot 7 Msg3 frame 80
k2 7 Msg3_tda_id 3
[NR_MAC] [gNB 0][RAPROC] Frame 80, Subframe 7: rnti d8d4 RA s
tate 2
Attacker Terminal
Airplane mode
Off
Turns off all network connections including calling, texting, internet access, Wi-Fi, and Bluetooth.
While Airplane mode is on, you can turn Wi-Fi and Bluetooth on again in Settings or the quick settings panel.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 127.0.0.5 && dns || ngap || gtp
Trace Capture
No. Protocol Info
3856 GTP <T… Application Data
3857 GTP <T… 443 → 37814 [RST] Seq=1009 Win=0 Len=0
3868 GTP <D… Standard query response 0x8467 AAAA b4E8Sm-dnsotls-ds.metric.gstatic.com AAAA 2607
3869 GTP <Q… Protected Payload (KP0), DCID=ee7412ff33df9008
3872 GTP <T… 45302 → 853 [ACK] Seq=373 Ack=5429 Win=78848 Len=0 TSval=2231640716 TSecr=38694123
3885 GTP <Q… Protected Payl (KP0), DCID=5acfc1d1af97e6fb1c73a7d7c92efc6d7f9d4e8e
3886 GTP <D… Standard query dbc7 AAAA K5j3NM-dnsotls-ds.metric.gstatic.com
3887 GTP <T… Application Da
3888 GTP <T… 33348 → 853 [eq=451 Ack=5535 Win=79872 Len=0 TSval=1335136228 TSecr=76137289
3889 GTP <T… Application Dat
3891 GTP <D… Standard query 0xa357 A youtubei.googleapis.com
3902 GTP <D… Standard query response 0xdbc7 AAAA K5j3NM-dnsotls-ds.metric.gstatic.com AAAA 260
3904 GTP <T… 853 → 33348 [FIN, ACK] Seq=5535 Ack=475 Win=67840 Len=0 TSval=761373029 TSecr=1335
3905 GTP <T… 853 → 33348 [ACK] Seq=5536 Ack=476 Win=67840 Len=0 TSval=761373031 TSecr=133513623
3906 GTP <D… Standard query response 0xa357 A youtubei.googleapis.com A 142.251.40.138 A 142.25
3907 GTP <Q… Initial, DCID=aa5c42630c886a78, PKN: 1, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PADI
Plaintext DNS Packets
Frame (118 bytes)
SM-G991B
20:19
100%
Airplane mode
Off
Turns off all network connections including calling, texting, internet access, Wi-Fi, and Bluetooth.
While Airplane mode is on, you can turn Wi-Fi and Bluetooth on again in Settings or the quick settings panel.

Summary

- Designed an automated and black-box security analysis framework called **5GBaseChecker** to analyze 5G basebands.
- Designed a new approach, hybrid and collaborative learning, which significantly reduces the overall time for inferring FSMs
- Designed a deviation analyzer to find security properties.
- 5GBaseChecker: https://github.com/SyNSec-den/5GBaseChecker

Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands

Kai Tu

Email: kjt5562@psu.edu

Website: hellotkk.github.io

Thanks!
Q&A?

PennState

SyNSec