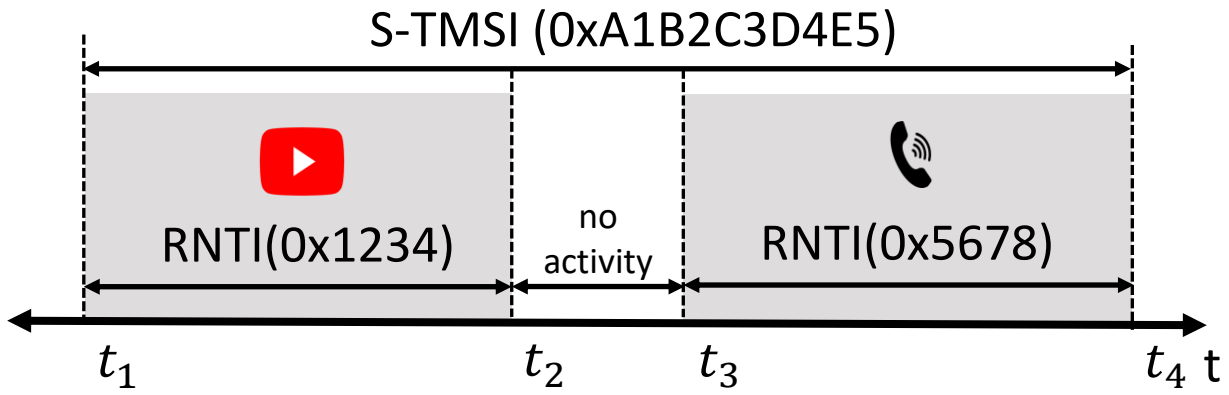
Passive Multi-Target GUTI Identification via Visual-RF Correlation in LTE Networks

Byeongdo Hong, Gunwoo Yoon
The Affiliated Institute of ETRI

Background - LTE Identifiers at Different Layers

- Layer 3 – Identity
  - ***Permanent***: IMSI / MSISDN (phone number)
    - Rarely sent over-the-air
  - ***Temporary***: GUTI (includes S-TMSI)
    - Used for most procedures
  - Role: *Citizen ID*



- Layer 2 – Transport
  - Identifier: C-RNTI (hereafter, RNTI)
  - Role: The Delivery Address
    - Temporary (Per-cell)
    - Used for scheduling data
    - Visible in every subframe (DCI)

C-RNTI: Cell Radio Network Temporary Identifier
DCI: Downlink Control Information
GUTI: Globally Unique Temporary Identifier
IMSI: International Mobile Subscriber Identity
MAC: Medium Access Control
MSISDN: Mobile Station ISDN Number
PHY: Physical Layer
NAS: Non-Access Stratum
RRC: Radio Resource Control
S-TMSI: SAE-Temporary Mobile Subscriber Identity

Why “Temporary” Identifiers Fail to Protect Privacy

DESIGN (Theory)

GUTI (incl. S-TMSI) should be frequently updated to prevent IMSI exposure

Intended as a “temporary” identifier

VS

S-TMSI acquisition ≈ GUTI identification (in practice)

Reason: operator/region fields are effectively fixed in practice

REALITY (in the wild)

33 DAYS

In our measurements,
GUTIs can persist for up to 33 days (Country A)

Effective as a “long-lived” identifier

Key points (data-driven)

Key Evidence

- **Persistence**: Up to 33-day GUTI lifetime
- **Linkability**: prefix patterns enable linking [NDSS’18]

Threat Transfer

- **One-time binding**: camera links person ↔ GUTI
- **Afterwards:** passive RF-only tracking

MNO: Mobile Network Operator

[NDSS’18] Hong *et al.*, “GUTI Reallocation Demystified...”

Our Contribution – GUTI Identification

Fully Passive

- Listen-only (no TX)
- No phone number

Multi-Target (1 FoV)

- Simultaneous multi-device capture
- Independent per-device FSMs

Robust Mapping (FSM)

- Narrow candidates across events
- ≈3 interactions / device

Field-validated across multiple operators in 2 countries

Overall rates shown below.

97%
GUTI extracted

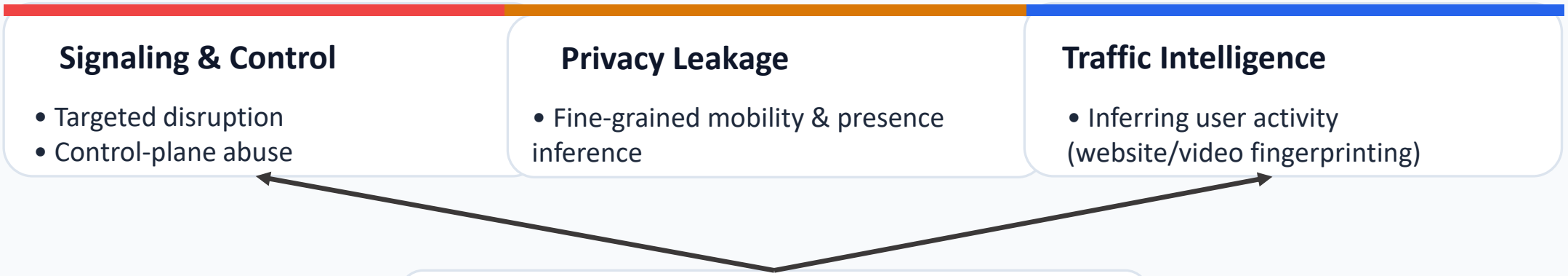
94%
Correctly verified

10
Devices per FoV

We identify GUTIs fully passively and at scale (up to 10 devices) with robust verification.

FoV: Field of View
FSM: Finite State Machine

The Gateway to Further Attacks



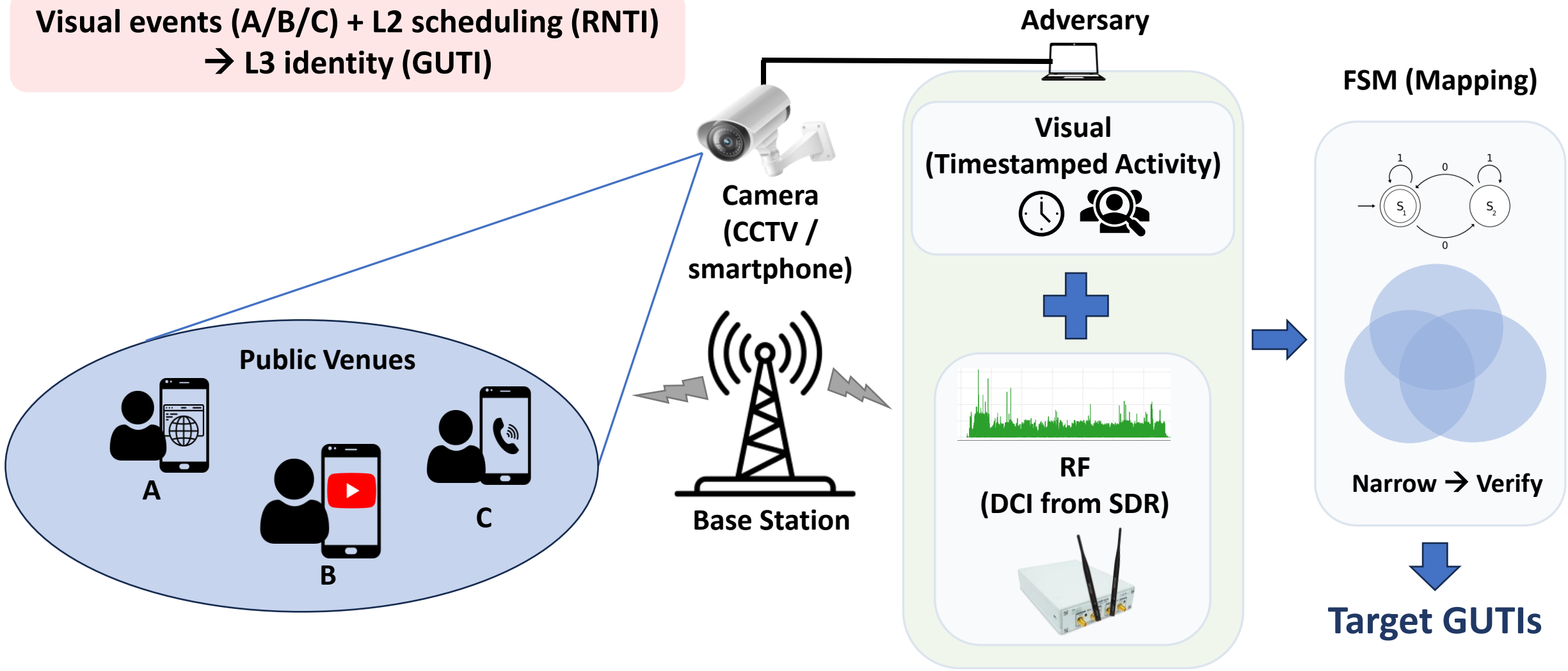
Key takeaway

GUTI acquisition is the missing step that makes many threats **practical.**

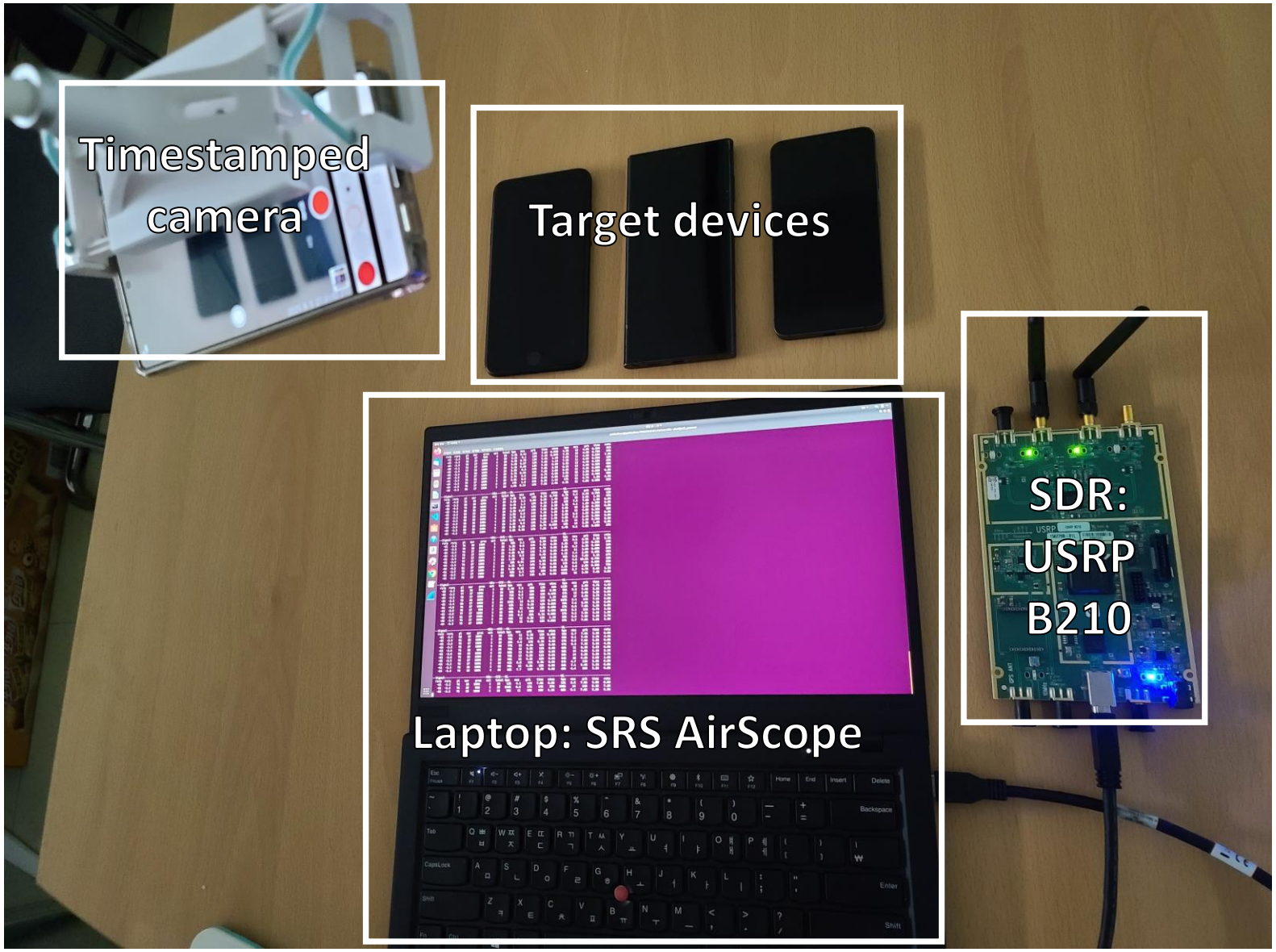
How do we obtain a target's GUTI at scale – passively, without prior identifiers?

Framework – Visual-RF Correlation

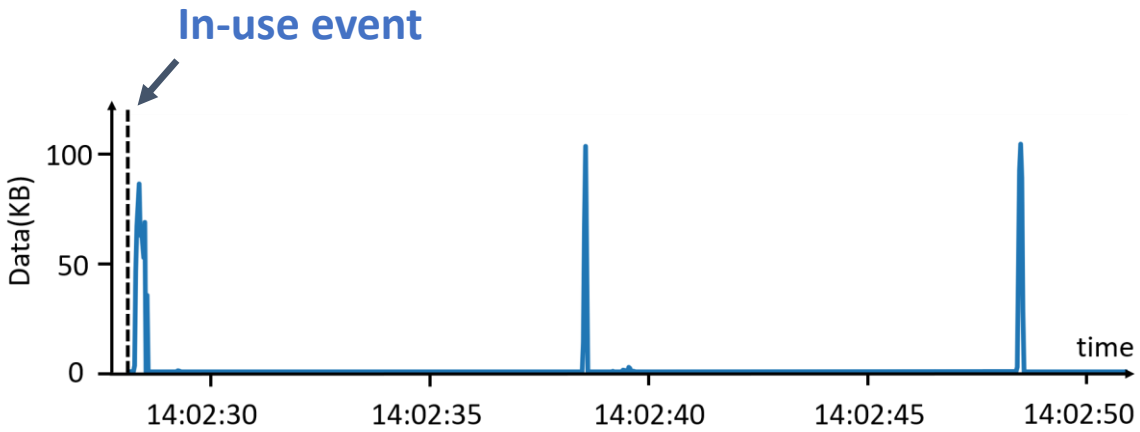
Visual events (A/B/C) + L2 scheduling (RNTI)
→ L3 identity (GUTI)



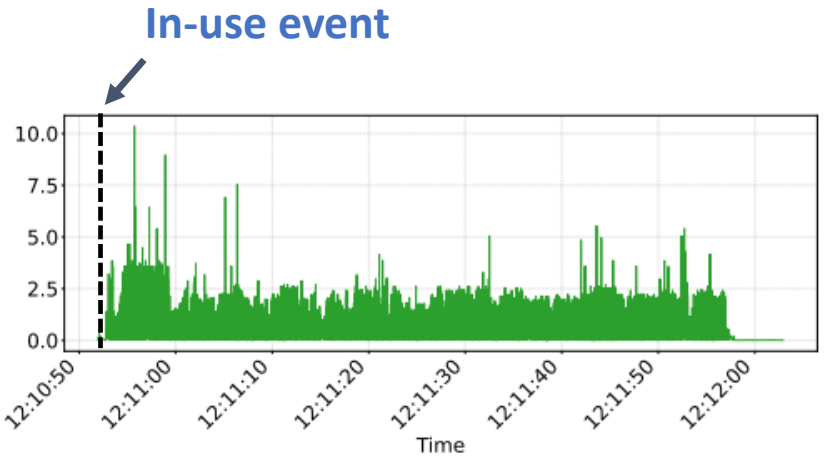
Evaluation Setup



Key Idea: Phone Use → DCI Bursts



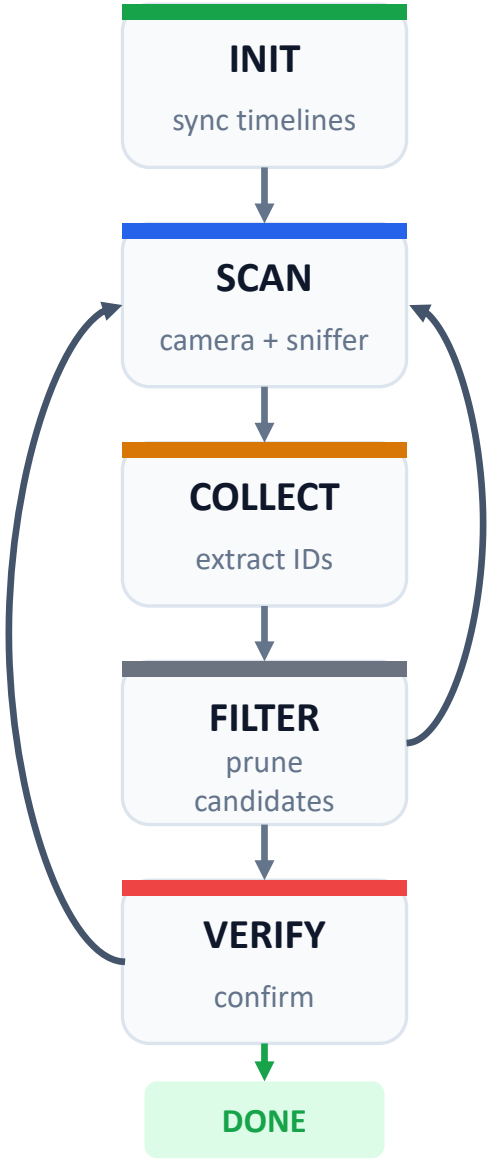
YouTube (bursty)

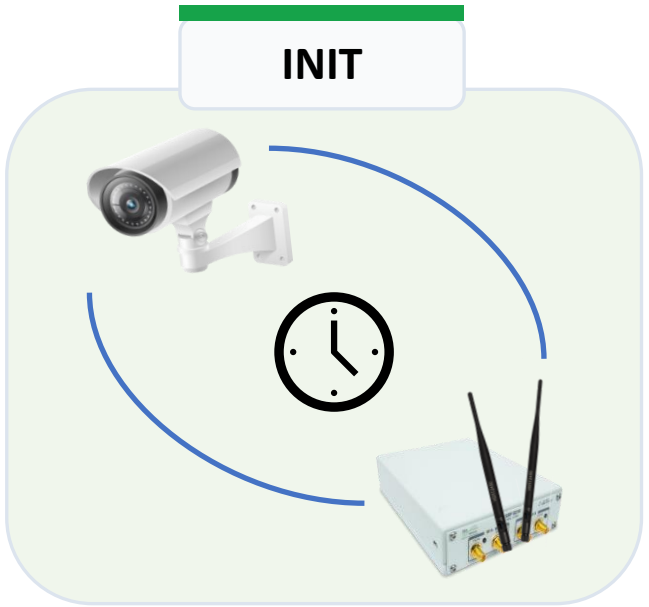


Google Meet VoIP (steady)

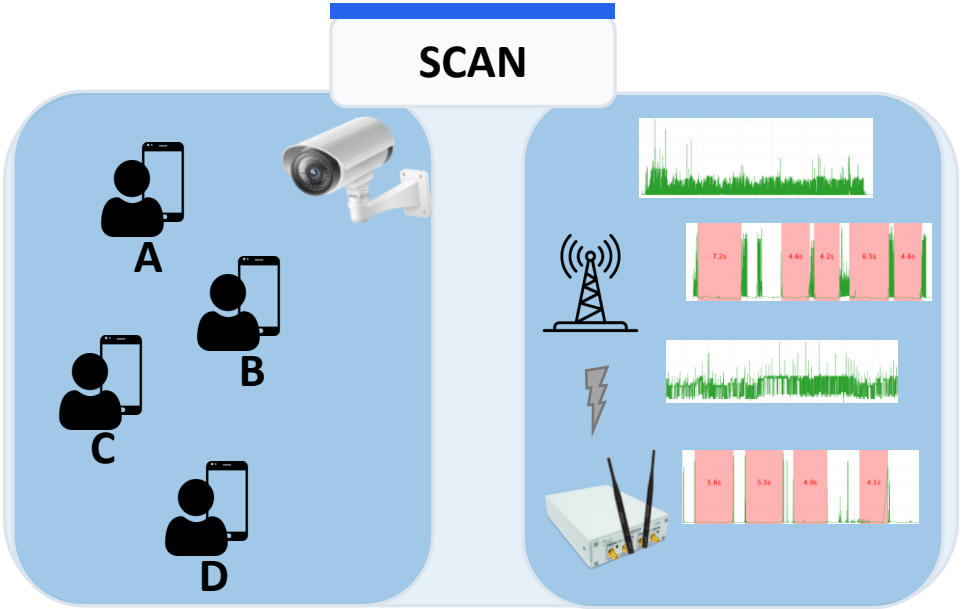
DCI bursts occur whenever the phone is in use—independent of the app/service

FSM-Based Identification (Sketch)





Camera-Sniffer Time Sync



Camera scans user

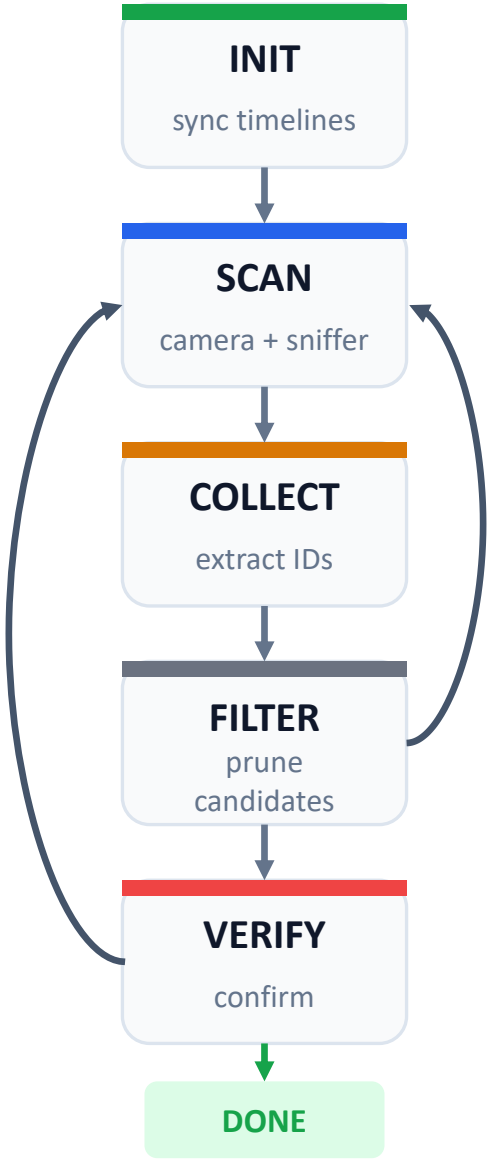
Sniffer scans RNTI and data bursts

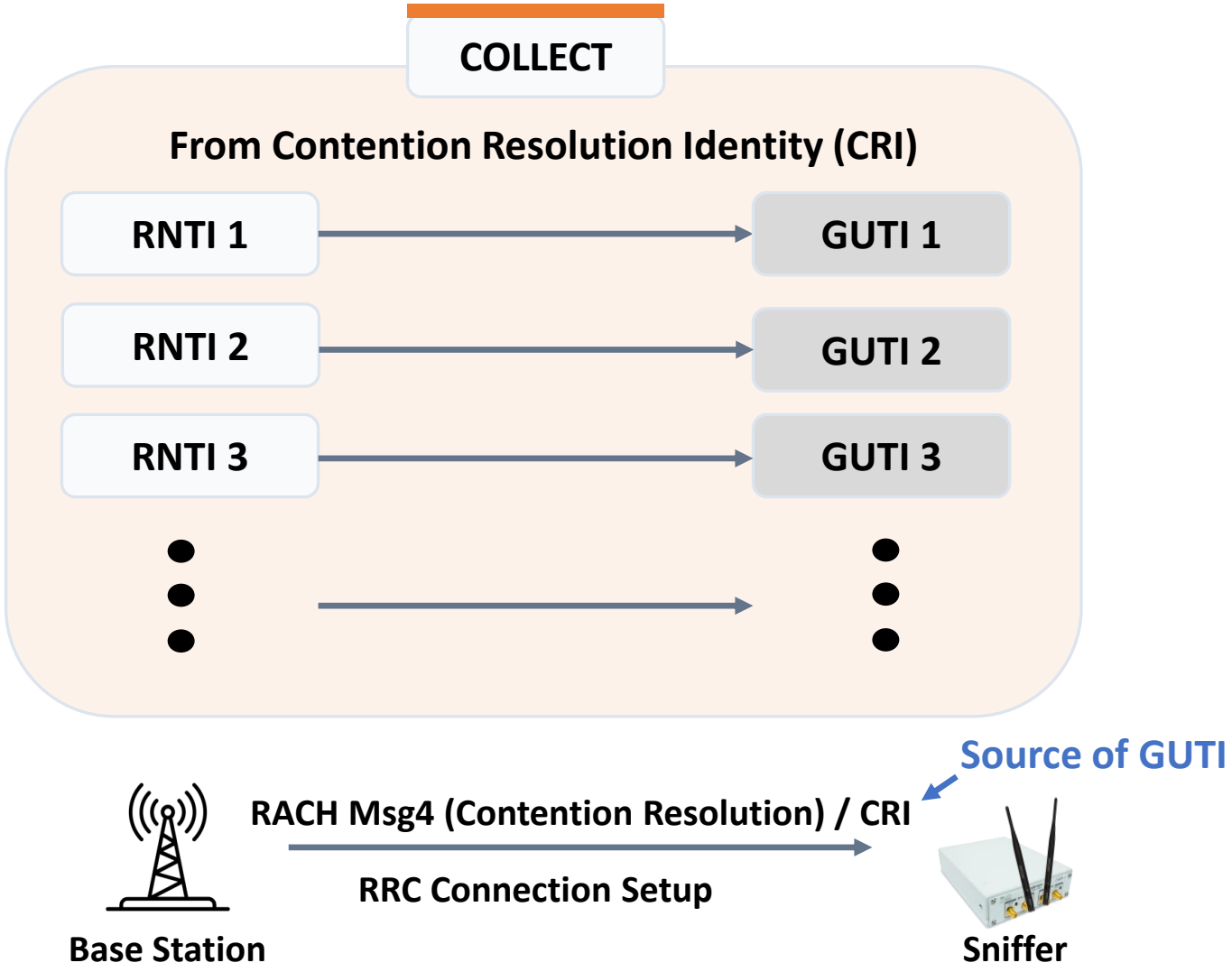
Definition A **data burst** occurs at time ***T*** for an **RNTI** when the **cumulative data within a time window** exceeds a threshold

$$Burst(RNTI, T) = \begin{cases} 1, & if \sum_{t \in [T-t_{th}, T+t_{th}]} (DL_t + UL_t) \geq d_{th}, \\ 0, & otherwise. \end{cases}$$

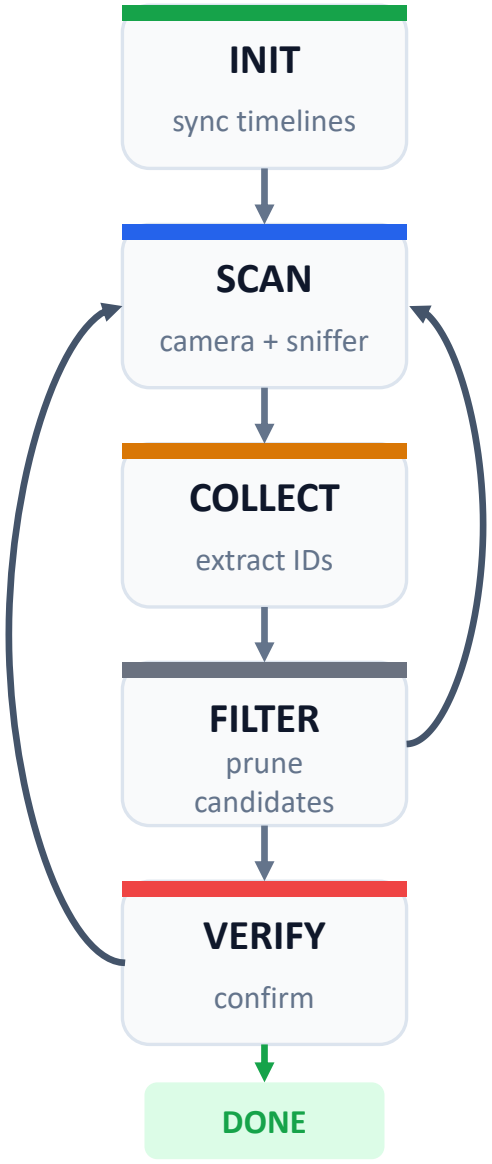
Time window: $[T - t_{th}\ T + t_{th}]$
Data in window: $\sum(DL_t + UL_t)$
Threshold: d_{th} bytes

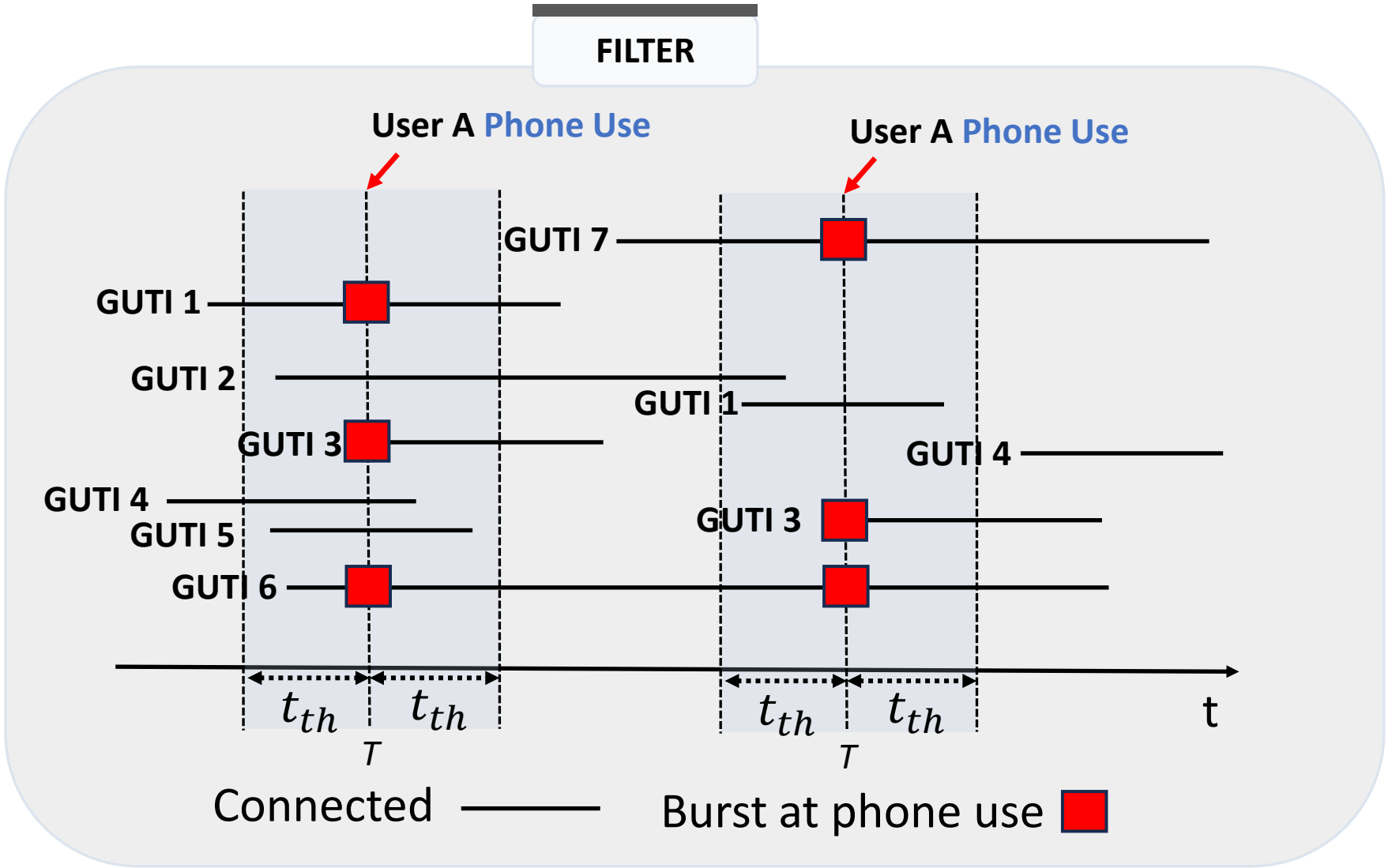
FSM-Based Identification (Sketch)



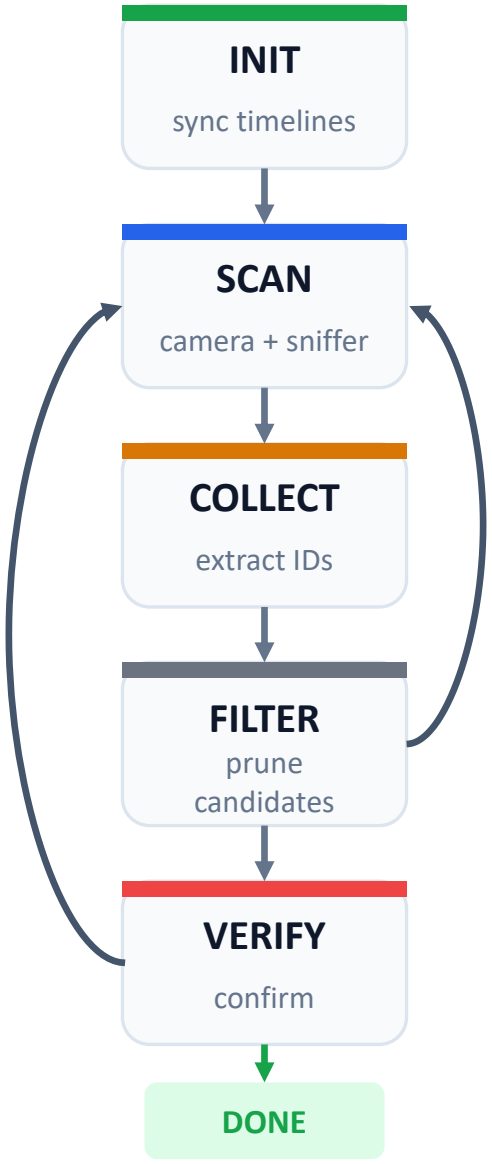


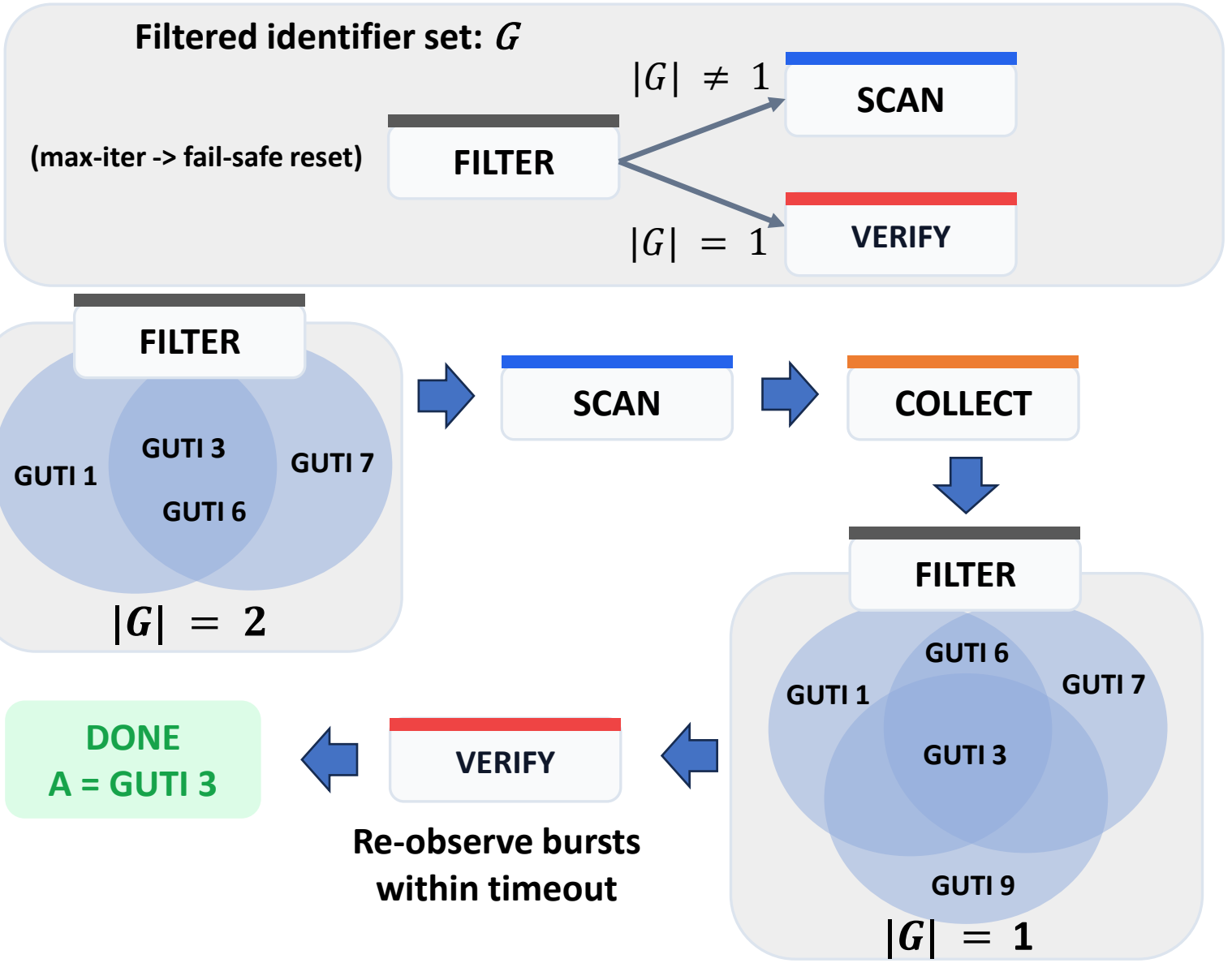
FSM-Based Identification (Sketch)





FSM-Based Identification (Sketch)





Experimental Results

97% (36/37)

Extraction success (overall)

94% (35/37)

Verification success (overall)

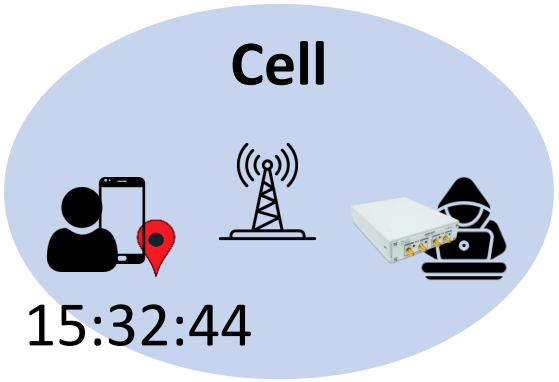
10

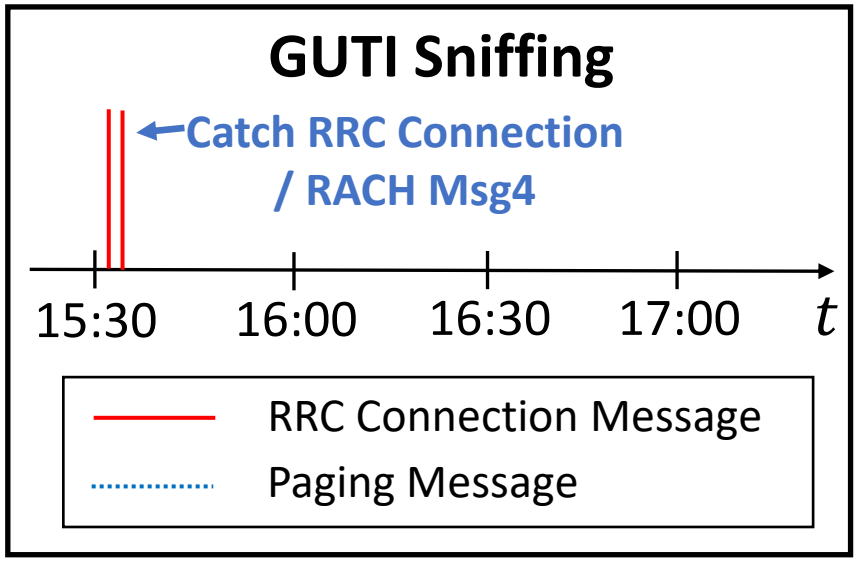
Devices in one FoV

- **Devices/Chipsets**: iPhone 7(A10), 9 different Samsung Galaxy devices (Snapdragon/Exynos)
- **Networks**: MNO-I/II/III (Country A), MNO-IV (Country B)
- **Services**: Call / YouTube / Web / Apple TV / Google Meet
- **Parameters**: time threshold = 2 s, data threshold = 10 kB

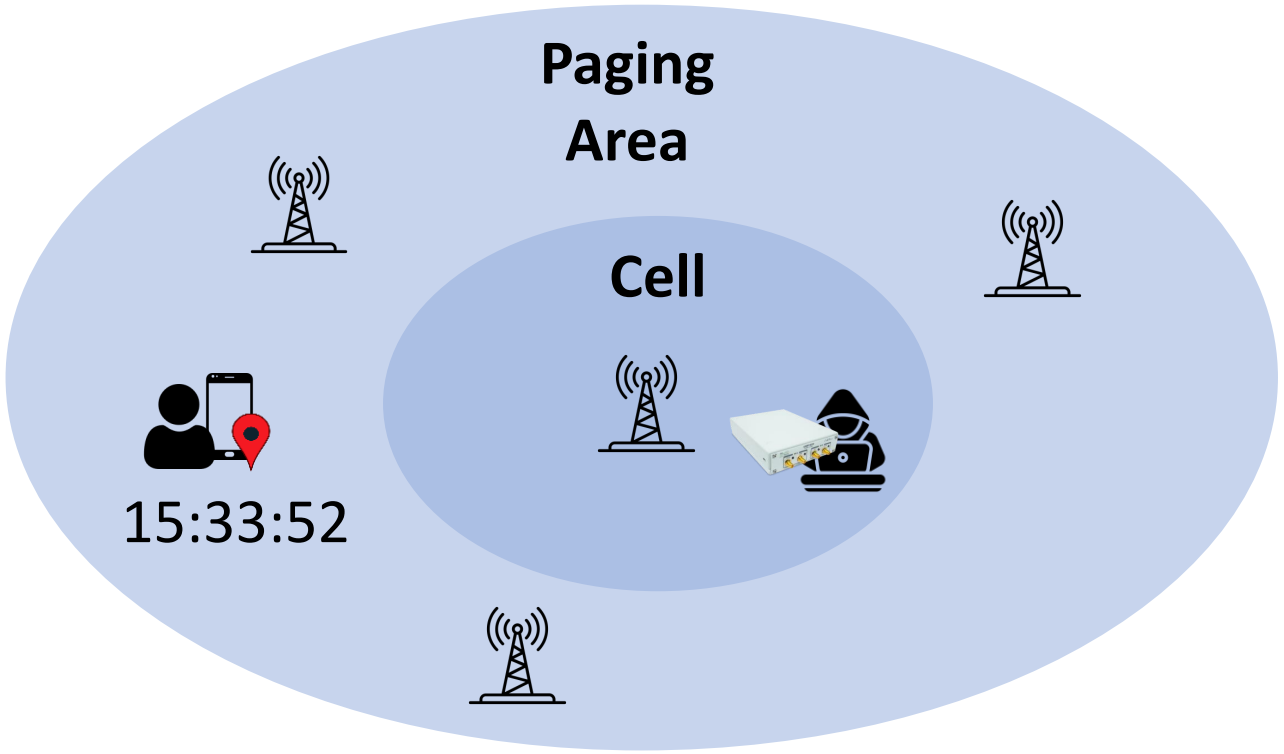
Extraction failure (1/37): sniffer **missed** control-plane messages
Verification failure (2/37):
(1) Extraction fail
(2) Extraction success, but **not enough bursts** to confirm

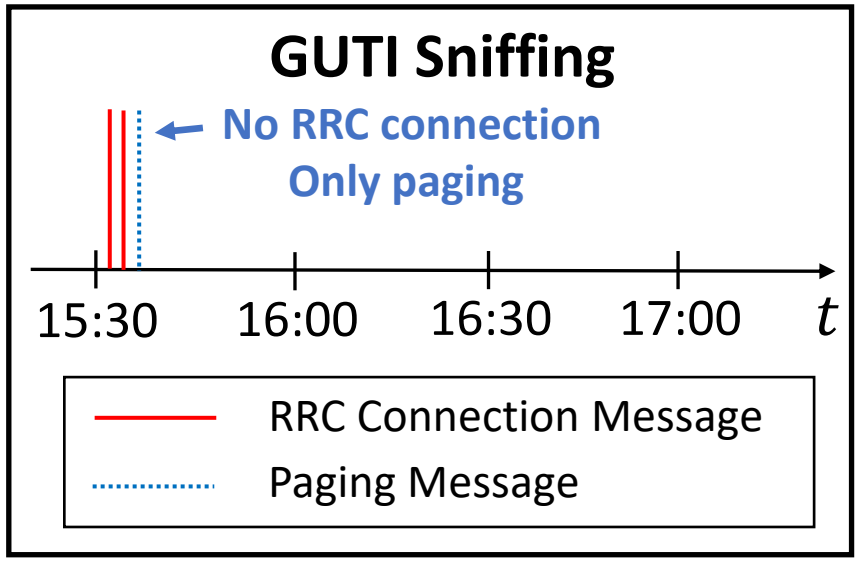
Implication: After Identification



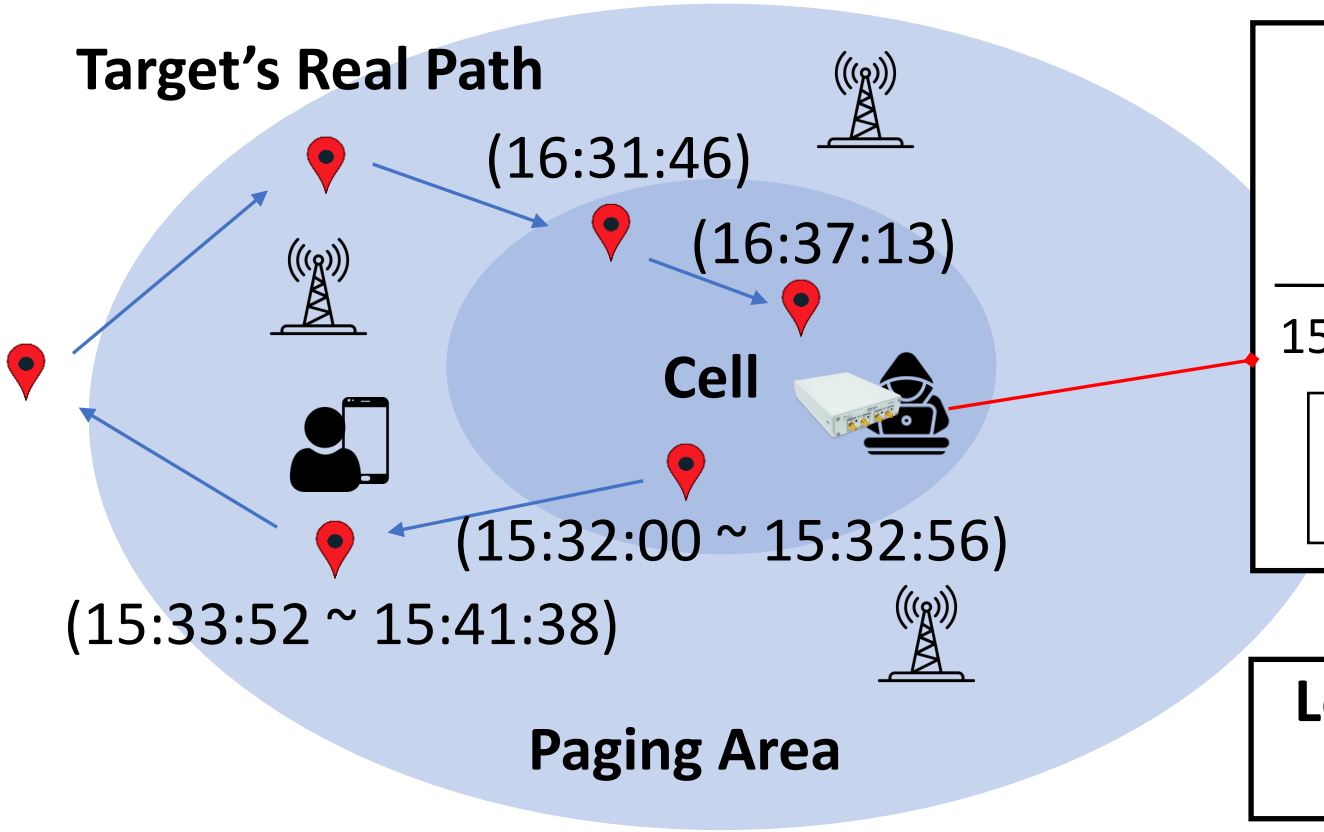


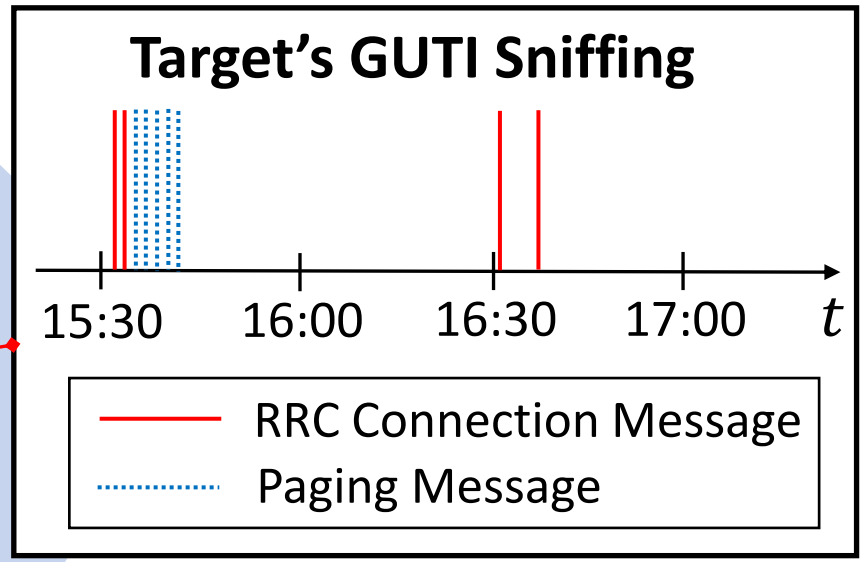
Implication: After Identification





Implication: After Identification





Location Tracking Estimation
C ➡ P ➡ O ➡ P ➡ C

C = Cell, P = Paging area, O = Out of coverage

Discussion – Limitations and Countermeasures

- Limitations
  - **Needs visual access**: camera/LOS required (public venues, fixed view)
  - **RF capture quality**: control-plane loss/blackout can break identification
  - **Short/rare mobile activity**: idle/silent users evade identification
  - **Scope**: evaluated on LTE only

- Countermeasures
  - **Aperiodic GUTI renewal (policy-only, near-term):** enforce a max GUTI lifetime independent of UE behavior
  - **Unpredictable GUTI per Service Request (standard-aligned)**
    - Caveat: attacker may suppress Service Requests by keeping RRC connected [MobiCom'24]
  - **Lightweight deception (decoy IDs):** inject decoy RNTI-GUTI pairs with similar scheduling patterns to keep ≥ 2 candidates
  - **PDCCH encryption:** requires protocol/design changes

PDCCH: Physical Downlink Control Channel

[MobiCom'24] Oh *et al.,* "Enabling Physical Localization ..."

Takeaways

- 1) Multi-channel correlation (camera + RF) breaks assumptions of “temporary” identifiers
- 2) Once linked, long-lived / linkable IDs amplify downstream tracking risks
- 3) Practical mitigations exist: enforce shorter lifetimes + unpredictability

Q & A

Backup Slides

5G Feasibility

- What remains similar to LTE
  - PDCCH scheduling still uses RNTI-based addressing
- Evidence from existing tools
  - Wavejudge, 5GSniffer: decode DL-DCIs
  - NR-Scope: reported RRC decoding
- Key 5G differences (vs. LTE)
  - Only part of 5G S-TMSI is used for contention resolution
- Scope
  - Not validated on 5G standalone deployments
  - Treat as feasibility: empirical 5G-GUTI extraction/tracking remains future work

LTE Identifiers: What Matters for This Attack

PDCCH / DCI (downlink scheduling)

C-RNTI

carries only C-RNTI (no GUTI).

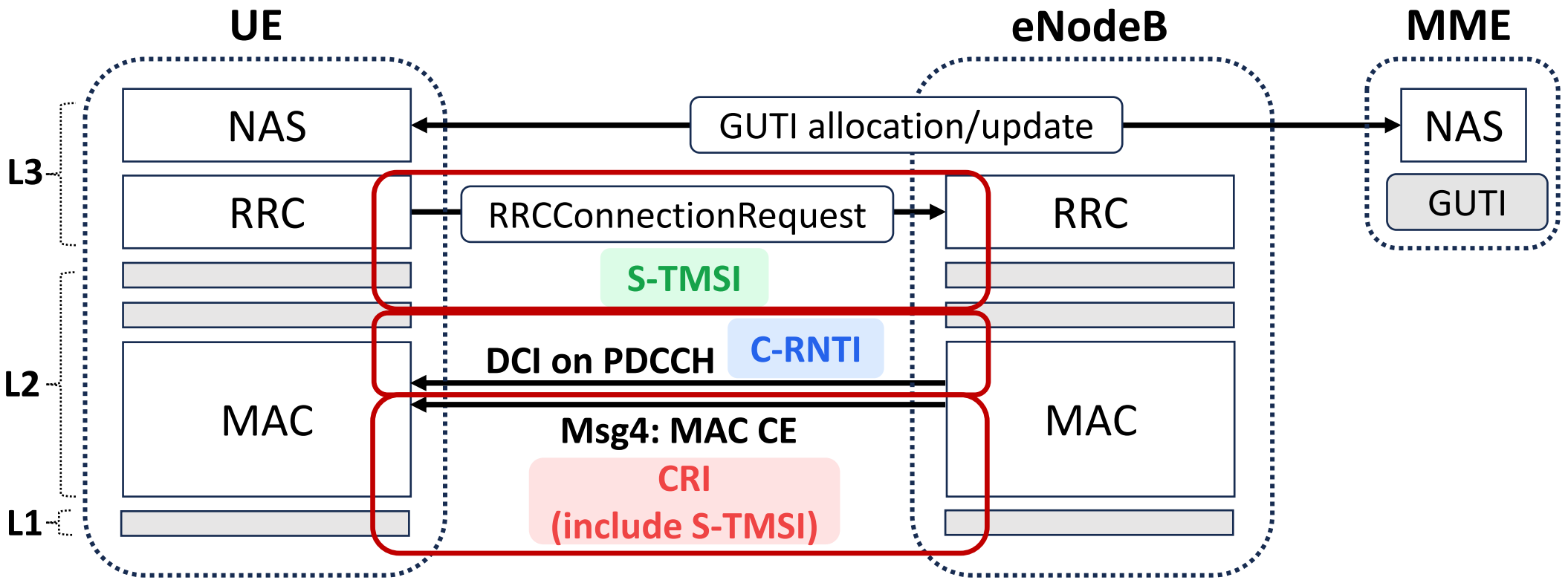
RRCConnectionRequest

S-TMSI

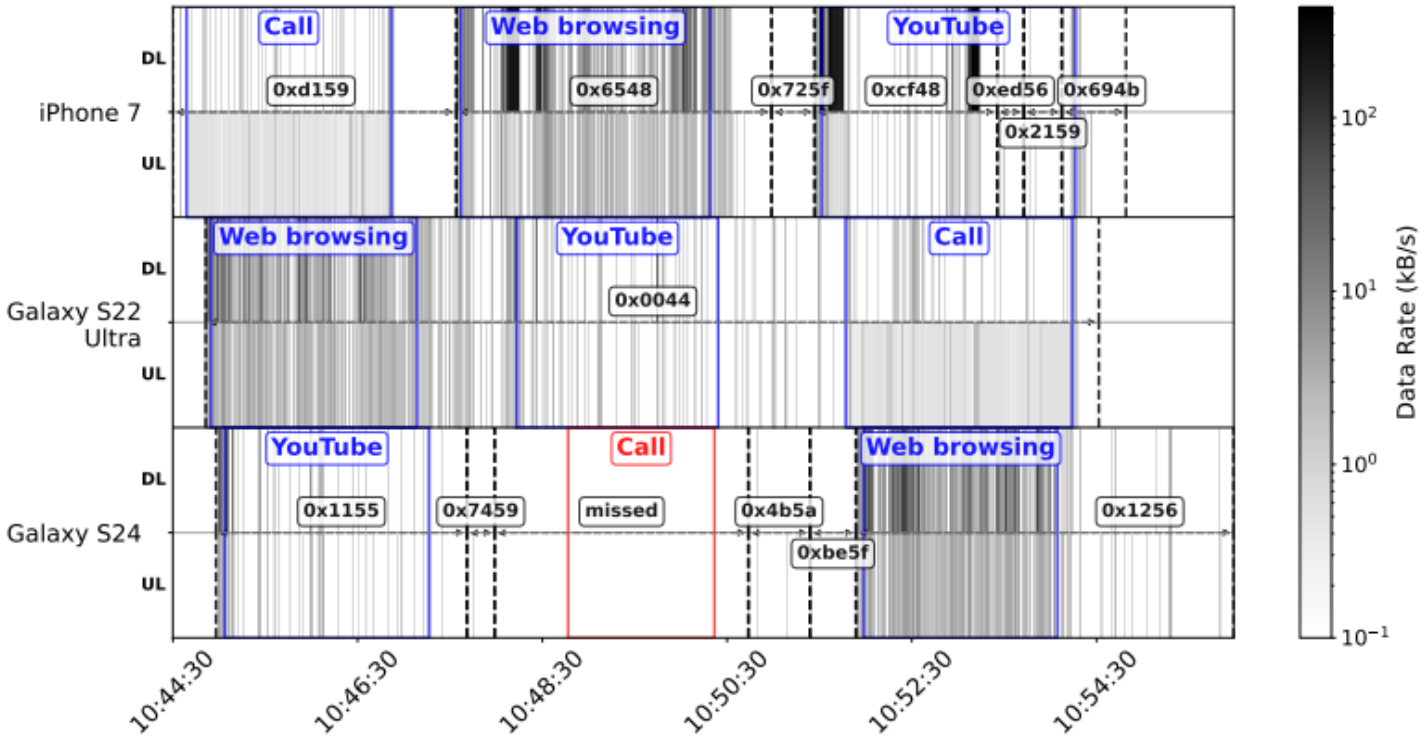
appears in the request

Contention Resolution

CRI



Data Scheduling



DCI-derived traffic pattern (over-the-air, USRP B210)

DCI reveals distinctive ‘bursts’ that align with user activity.

Experimental Results (Paper Version)

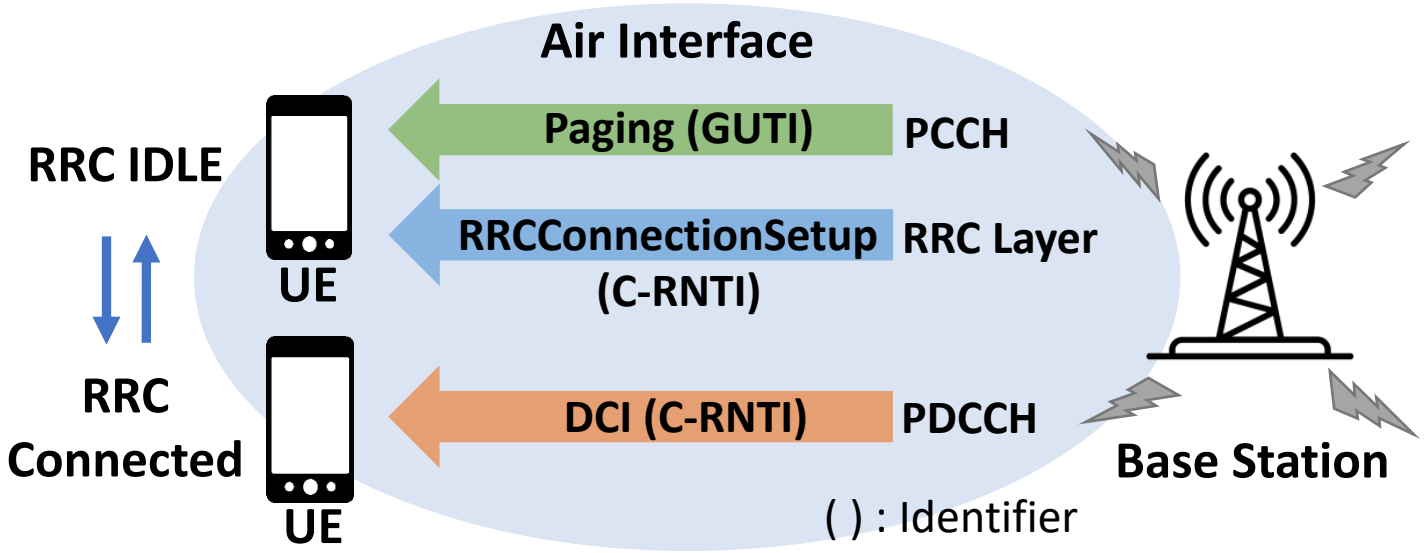
Exp.	Sniffer(s)‡	Device(s)	Chipset	Network	Services†	# Missed	Extraction	Verification
E1	1 (99 %)	Galaxy S20	Snapdragon 865	MNO-II	C–Y–W–C–Y–W	1 (4)	✓	✓
E2	1 (93 %)	Galaxy S20	Snapdragon 865	MNO-II	W–Y–W–Y–W–Y–C	1 (2)	✓	✓
E3	1 (90 %)	Galaxy S20	Snapdragon 865	MNO-I	Y–W–C–Y–W–C	1 (5)	✓	✓
E4	1 (90 %)	Galaxy S22	Snapdragon 8 Gen1	MNO-I	W–C–Y–W–C	2 (3, 4)	✓	✓
E5	1 (84 %)	iPhone 7	A10 Fusion	MNO-II	Y–W–A–Y–W–A	1 (6)	✓	✓
		Galaxy S22	Snapdragon 8 Gen1		Y–W–C–Y–W–C	3 (1, 2, 5)	✓	✓
		Galaxy S24	Exynos 2400		W–C–Y–Y–W–C	4 (1, 2, 5, 6)	✓	✗*
E6	1 (90 %)	iPhone 7	A10 Fusion	MNO-I	C–W–Y–W–C–W–Y	0	✓	✓
		Galaxy S22	Snapdragon 8 Gen1		W–Y–C–W–Y–C	0	✓	✓
		Galaxy S24	Exynos 2400		Y–C–W–Y–C–W	3 (3, 5, 6)	✓	✓
E7	2 (100 %, 100 %)	10 UEs	Various	MNO-II	W (intermittent)§	0	✓	✓
E8	2 (100 %, 89 %)	10 UEs	Various	MNO-III	W (intermittent)§	6¶	✓	✓
E9	1 (78 %)	Galaxy S23 Ultra	Snapdragon 8 Gen2	MNO-IV‖	Y–G–W–G–W–Y	0	✓	✓
E10	1 (73 %)	Galaxy S23 Ultra	Snapdragon 8 Gen2	MNO-IV‖	Y–G–W–G–W	2 (2, 3)	✓	✓
		Galaxy S24	Exynos 2400		G–W–Y–W–Y	1 (4)	✓	✓
E11	1 (81 %)	Galaxy S23 Ultra	Snapdragon 8 Gen2	MNO-IV‖	W–G–G–Y–G–W	5 (2–6)	✗	✗
		Galaxy S24	Exynos 2400		Y–W–Y–W–Y	2 (2, 4)	✓	✓
E12	1 (74 %)	Galaxy S23 Ultra	Snapdragon 8 Gen2	MNO-IV‖	Y–W–G–W–G–Y	0	✓	✓
		Galaxy S24	Exynos 2400		W–G–Y–G–G–Y	0	✓	✓

Error-Rate Analysis

- Highly non-stationary mobile traffic

- Empirical error-rate analysis on real traces (211 min, detector 2 s / 10 kB)
  - False-positive (FP)
    - Probability that two unrelated GUTIs generate >=3 aligned bursts: 0
  - False-negative (FN)
    - Per-burst capture probability (trace): p = 0.8096
    - 5 burst opportunities → FN 7%
    - >=6 opportunities → FN < 3%

Air Interface in LTE



Ethics & Responsible Disclosure

- Controlled experiments (no third-party subjects)
  - No non-consenting users were monitored
- Privacy-preserving evaluation
  - No individual identification attempts in the validation dataset
  - Locations anonymized as Country A / Country B to avoid operator identification
- Responsible disclosure to GSMA
  - Findings shared with members prior to publication