

Securing Cellular and Open RAN Systems through Real-World Experimentations

Imtiaz Karim

Assistant Professor, Department of Computer Science
The University of Texas at Dallas



PAWR PI Meeting · September 28, 2026

What rides on the cellular network

Cellular is no longer a telephony service. It is the **default connectivity substrate**—and each new class of dependent system inherits whatever security the protocol provides.

8.8 billion

wireless connections

5.8 billion

unique subscribers — 70%
of humanity

170

countries



Phone calls
and internet



Internet
of things



Autonomous
vehicles



Supply chain
management



Connected
healthcare



Integrated
sensing

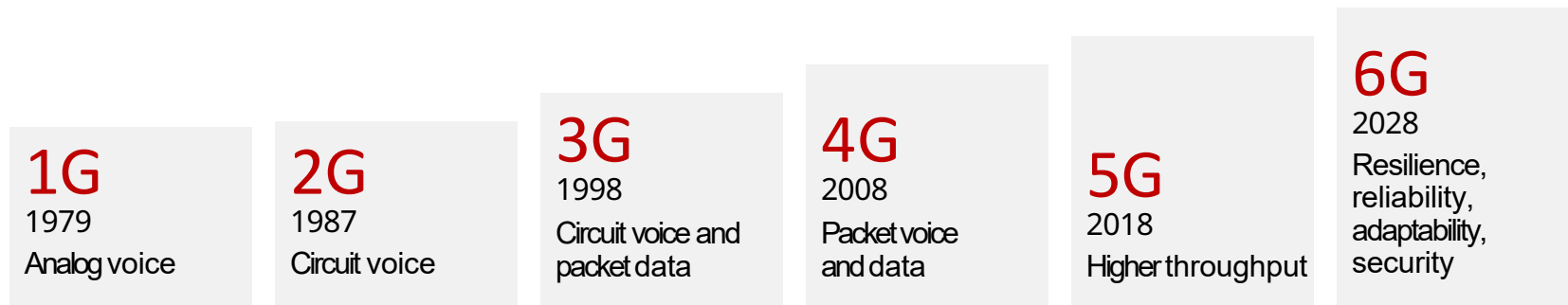


Non-terrestrial
networks

The consequence of a protocol-level flaw is no longer a dropped call. It is a vehicle that mis-navigates, a clinical device that loses its uplink, or a fleet that cannot be tracked—which is why bootstrapping security is worth attacking at the protocol level rather than patching per application.

EVOLUTION

Six generations of throughput, fewer of security



- **1G to 2G—minimal security.** Weak or absent authentication and encryption, with the network never proving its identity to the device.
- **3G to 5G—AKA, better encryption, mutual authentication.** Real cryptographic machinery arrives, but only after a device has already selected and trusted a cell.

6G is being designed to be secure. 4G and 5G are already deployed.

Billions of devices will spend their service life on generations whose bootstrapping phase was never authenticated.

Fake base stations are a persistent, unsolved problem

- No authentication of initial broadcast messages; connection setup in the bootstrapping phase is **unprotected**.
- FBSes remain viable in 5G despite SUCI—concealing the identifier does not fix pre-authentication signaling.
- Certificate and digital-signature proposals need spec changes, add overhead, and complicate roaming key sharing.
- **Billions** of already-deployed devices cannot wait for a new specification to roll out.

Where existing detection falls short

Heuristic and signature rules break under adaptive adversaries. Crowd-sourcing does not scale to billions of devices. Dedicated hardware and companion nodes are costly. Lower-layer methods miss multi-step attacks entirely.

21

multi-step attacks reproduced over the air, from DoS to location tracking

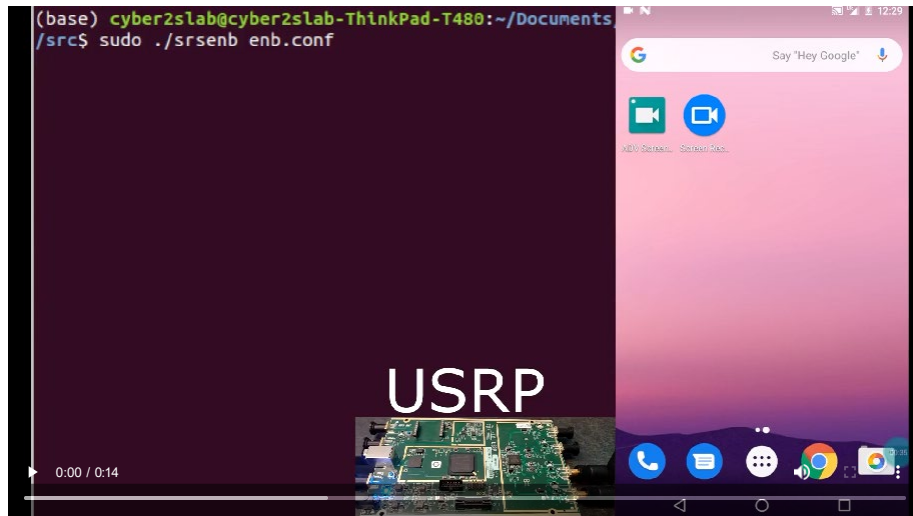
0

public datasets of real FBS traces existed before this work

5 levels

of attacker capability, from a naive high-power cell to a parameter-cloning adaptive adversary

Panic Attack



What you are watching

A rogue base station broadcasts a spoofed emergency alert to every device in range. The phones behave exactly as specified—there is no exploit and no malware involved.

Why it works

Broadcast messages are consumed before any authentication exists, so a device has no way to ask whether the cell sending the alert is real.

Everything in the rest of this talk follows from this one property: if the bootstrapping phase cannot be authenticated, it has to be **detected**.

POWDER as the experimental component

Deploying an FBS in public is illegal, so every claim in this work rests on a **city-scale testbed** with a dedicated spectrum allocation and real radios.



Over-the-air, not simulated

Real packets between real devices in a dedicated frequency band, not simulated wire transmissions.



Mobility that is genuinely mobile

UEs mounted on campus shuttles produce real handovers as signal quality changes.



Full control-plane access

Open5GS core with srsRAN and OAI base stations, used equally to avoid stack bias.

Building capability into the stack, not just using it

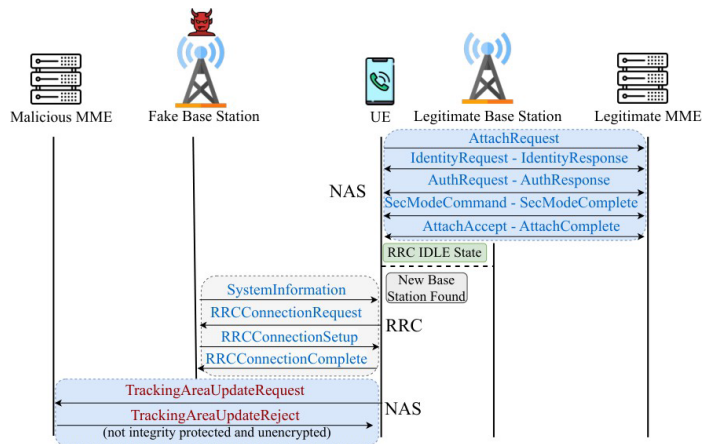
srsRAN and OAI do not implement TrackingAreaUpdateRequest in the UE, so UE-initiated handover was unavailable. We implemented it —then modified the eNodeB RRC and MAC layers and srsEPC to forward radio measurements to the core. The testbed work is as much **protocol-stack engineering** as it is measurement.

PART I

UE-side detection: FBSDetector

Detecting fake base stations and multi-step attacks from layer-3 NAS and RRC traces, in-device, with no protocol change and no extra hardware.

Building FBSAD and MSAD on POWDER



Communication process of an FBS carrying out a multi-step attack.

- Legitimate core + BS pair and a fake core + BS pair, spawned side by side; the FBS attracts UEs with higher signal strength.
- Mobility included by design, so a benign handover is never mistaken for an attack.
- **21 multi-step attacks** implemented in both srsRAN and OAI and executed over the air.
- Attacker levels 0–4: naive high power, optimal power, full parameter cloning, MSAs, adaptive reshaping.
- Protocol filtering with tshark; 119 NAS and 183 RRC fields become the feature set.

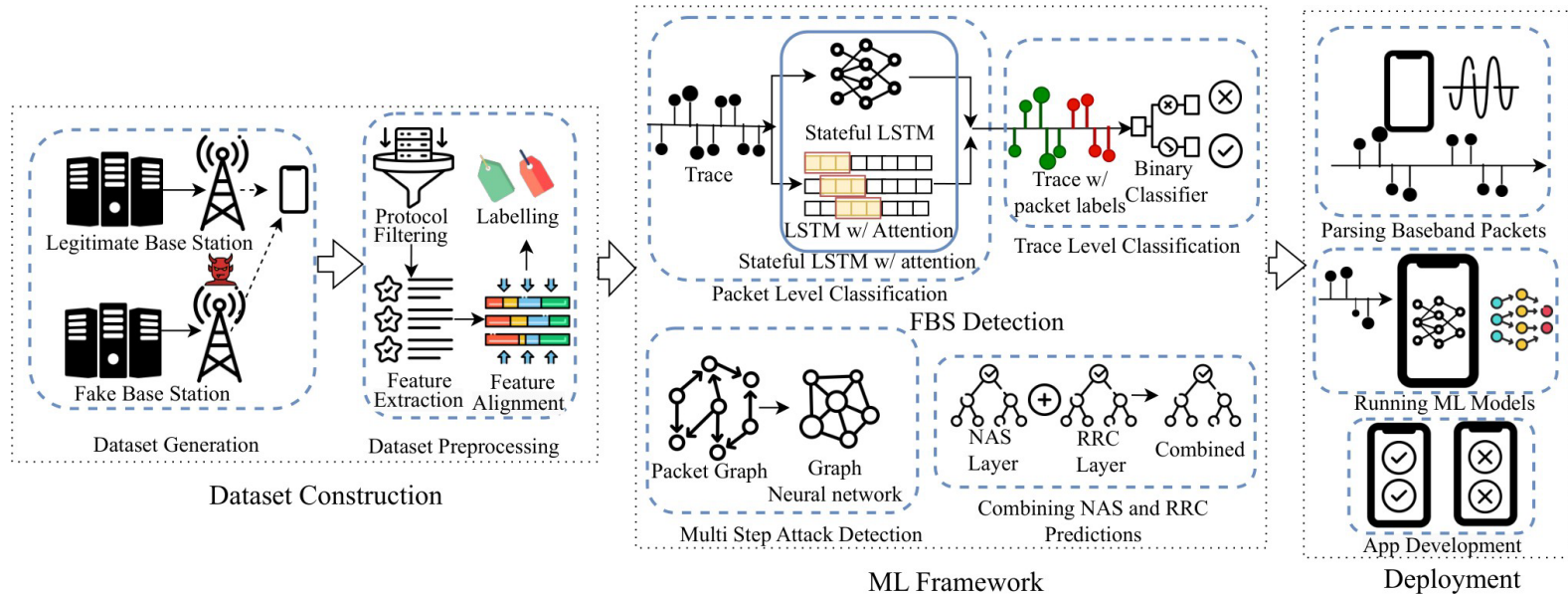
9.2 GB
raw traces

NAS + RRC
layer-3 control plane

srsRAN + OAI
used equally

Open5GS
core with handover

FBSDetector: dataset, models, deployment



Three components: dataset construction on POWDER, a two-branch ML framework, and on-device deployment.

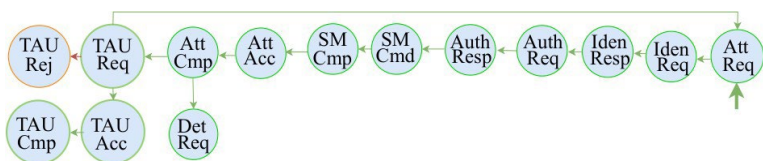
Why detection needs two granularities

- The same packet can be benign or malicious —what matters is **when and in what context** it was sent.
- Packet level: a stateful LSTM with attention in parallel layers, so long-range state survives across sequences while attention isolates the decisive fields.
- Trace level: a light binary classifier over the labeled packet sequence supplies the surrounding context.
- Fusing NAS and RRC with Dempster–Shafer weighted confidence lifts the final trace verdict to **96% accuracy at 2.96% FPR**.

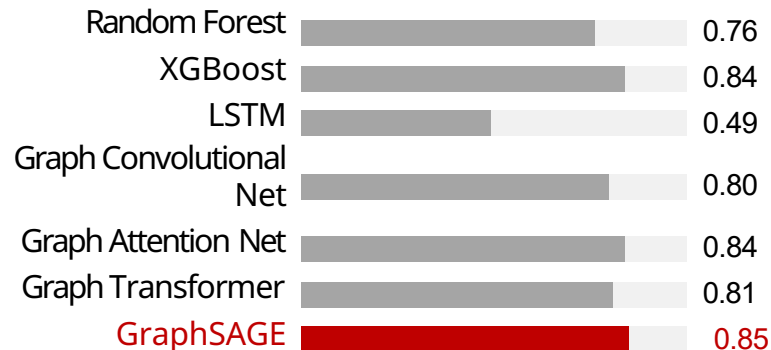
Sequence length is a real hyperparameter, accuracy peaks at **9–15 packets for NAS** and **80–120 for RRC**—the windows that fit a complete FBS session's message distribution.

Multi-step attacks are graphs

Each attack has a signature path through the message-transition graph. Nodes are packet types, edges are transitions labeled benign or attack-generated.



TAU Reject attack: the graph enters the attack path when TAUREject follows TAUREquest.



Packet-level NAS accuracy — **GraphSAGE** leads every sequence and classical model.

Unseen or reshaped attacks deviate to a path that is not edge-disjoint from the original — maximum overlapping sub-graphs recover them. Fused NAS + FRC: **86.5% accuracy**, **3.28% FPR** across all 21 attacks.

From testbed to a phone in a pocket

- MobileInsight parses baseband traces; TensorFlow Lite runs the pretrained models on device; Flutter provides the app.
- On detection the user is notified, can switch cells or block the current one—and for an IMSI catcher the app can **turn the radio off before the identity leaks**.
- Controlled lab validation with two USRP B210s, Open5GS, and a commercial Google Fi SIM.

835 KB

average memory

< 2 mW

power, vs 4 mW for prior work

5 / 5

general FBS instances detected

88 / 105

MSA instances correctly attributed

Long-term evaluation in the wild

24-hour stress test: all 21 attacks run 5 times each over 105,561 NAS+RRC packets, with 6 false-positive notifications. 7 days of ordinary use across two countries: 326,385 packets, 2 alerts. AIMSICD and SnoopSnitch, run in the same lab setup against the same FBS, never detected it.

Holding up against an adaptive adversary

Reshaped attacks

A level-4 adversary alters non-critical fields and injects extraneous messages to break temporal orderings. All reshaped packets are still classified as the original attack.

Unseen attacks

Leave-one-attack-out cross-validation: held-out attacks are misclassified into another attack class, never into benign — the deviation still raises an alert.

Overshadowing, zero-shot

Signal overshadowing needs no FBS and was never in training. Generated with a synchronized second SDR, it is still detected with 86% accuracy from layer-3 alone.

Why signature-based detection breaks

Attack (adaptive adversary)	Phoenix (PLTL): packets kept in the true class	FBSDetector
Attach Reject	21% — most packets land in Numb Attack	67.3%
TAU Reject	5.5% — most packets land in Service Reject	78.3%
Measurement Report	10.7% — most packets land in Numb Attack	69.8%
Authentication Failure	112% — most packets land in Attach Reject	72.3%

PART II

Network-side detection: NSFBSDetector

Moving the vantage point into the core network, where S1AP signaling from every eNodeB and the operator's own registration state are already available.

What a single device cannot see

A UE observes only its own signaling and its own radio measurements. It cannot correlate across users, and it has no access to the operator's ground truth.

Global visibility

The core processes every S1AP message from every eNodeB — clusters of handover failures toward unknown targets are visible only here.

Authoritative knowledge

The Base Station Almanac holds the identity, location, and configuration of every legitimate cell. A cell in signaling but absent from the almanac is immediately suspect.

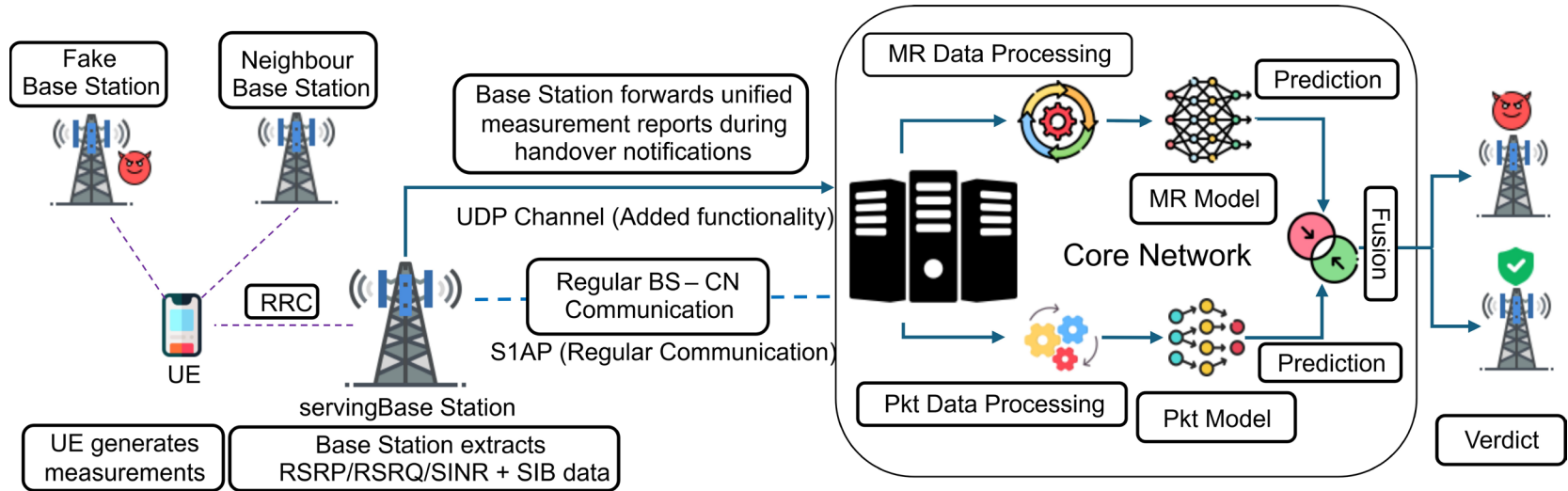
Cross-UE correlation

Multiple UEs in one area reporting an unknown PCI at high power localizes the threat with far more confidence than any single report.

Complementary layer

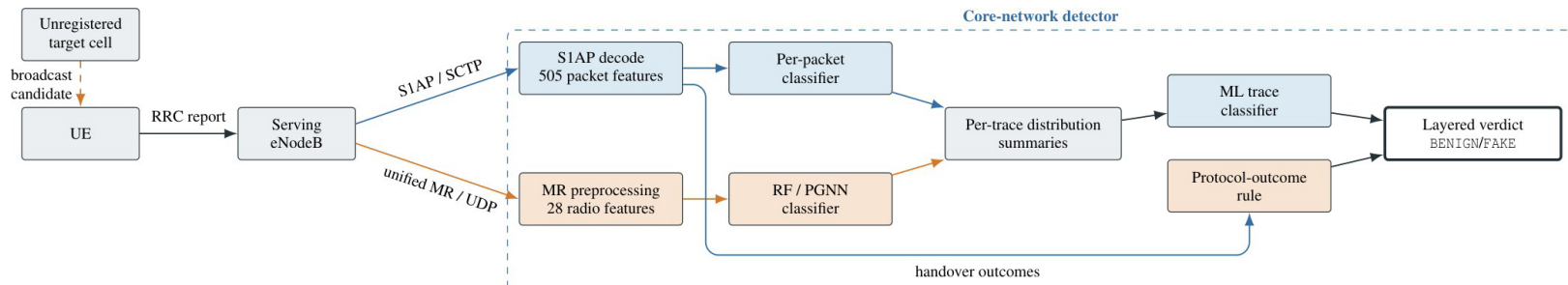
An adversary crafted to evade UE-side heuristics still has to survive a different feature set and a broader observation scope.

Enriching the 5G core's view



The base station forwards unified measurement reports over a new UDP channel while standard base-station-core signalling continues untouched; the core runs a measurement-report branch and a packet branch, then fuses them into a verdict.

Two streams, learned fusion, and an auditable rule



SIAP packets

505 features per packet: message types, procedure codes, cause values, cell identifiers, bearer and security fields.

Measurement reports

28 compact radio features: serving and neighbor RSRP/RSRQ, SINR mean and variance, TA-derived distance.

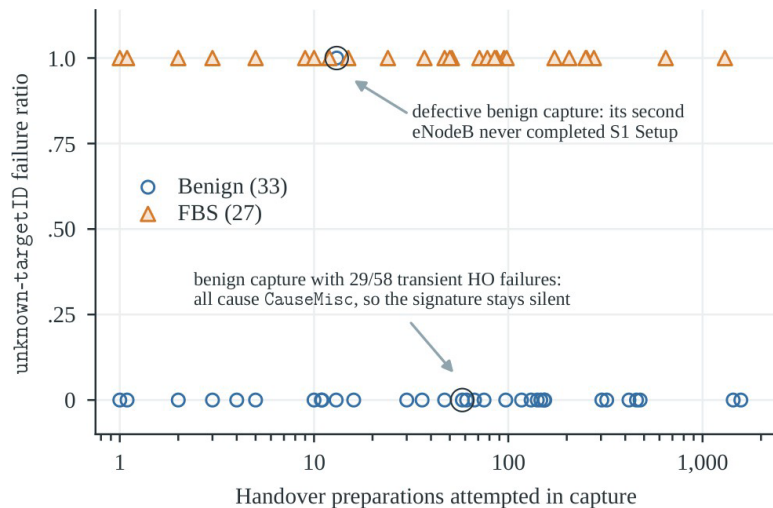
Learned trace fusion

33 distribution features —counts, thresholds, quantiles, extrema, cross-branch interactions —into an MLP.

Averaging the branch probabilities destroys the signal. An FBS trace is bimodal — most packets look routine while a burst of handover signaling scores high — so the distribution summary keeps what the mean throws away.

KEY FINDING

A rogue cell cannot register with the core



Every unique capture: handover preparations attempted vs. fraction failing with unknown-targetID.

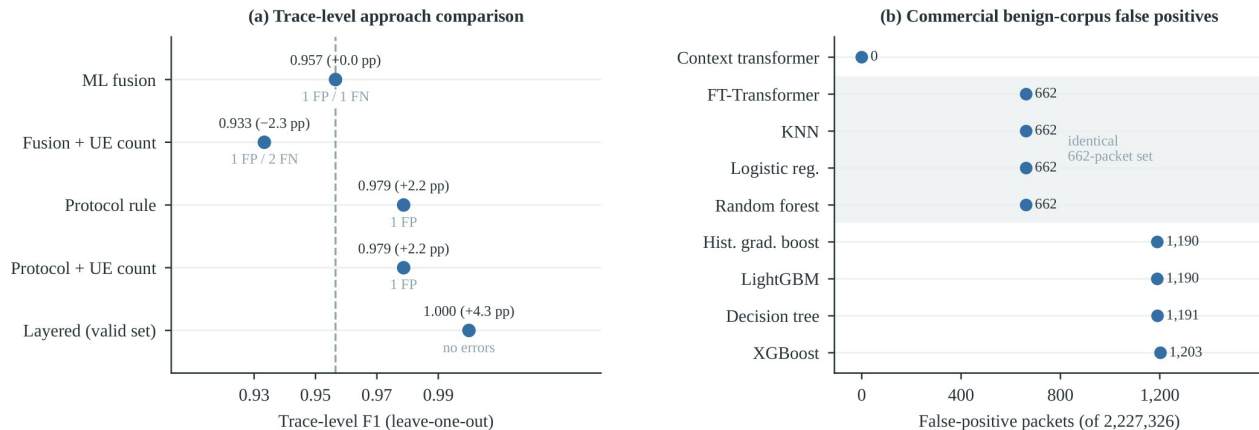
- A legitimate neighbor has performed S1 Setup with the AMF, so handover preparation resolves and completes.
- An FBS has no operator credentials and never performs S1 Setup—the MME returns **HandoverPreparationFailure** with cause unknown-targetID.
- Across the corpus the split is perfectly bimodal: every FBS capture at 1.0, every intact benign capture at 0.0, over three decades of handover volume.

ho_fail_unknown_target_ratio ≥ 0.5

Zero parameters, zero training, trivially auditable by an operator—F10.979 with no missed attacks.

RESULTS

Trace-level detection and commercial false alarms



Left: trace-level F1 by approach, leave-one-out over 51 deduplicated traces. Right: false positives on 2.23M packets of commercial benign S1AP traffic.

98.0%

trace accuracy,
100% recall

F1 0.979

protocol rule alone,
zero misses

0.03%

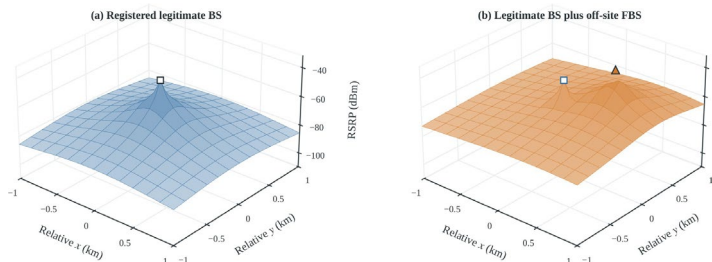
FPR on a production core

0 FPs

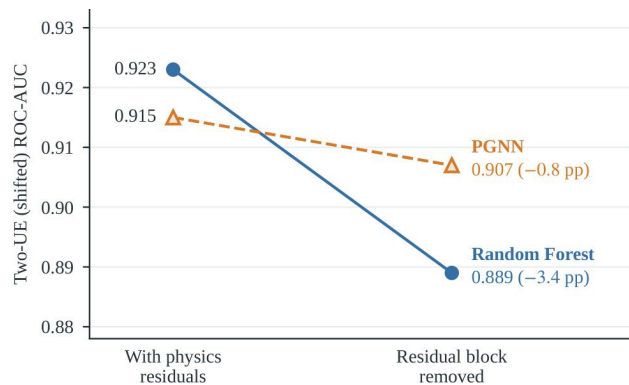
windowed Context
Transformer

Physics-guided modeling of benign propagation

Transmit power is attacker-controlled, so we calibrate a log-distance path-loss law on benign data and classify on **power-invariant residuals** only.



A registered cell peaks at its known site; an off-site FBS claiming that identity peaks elsewhere.

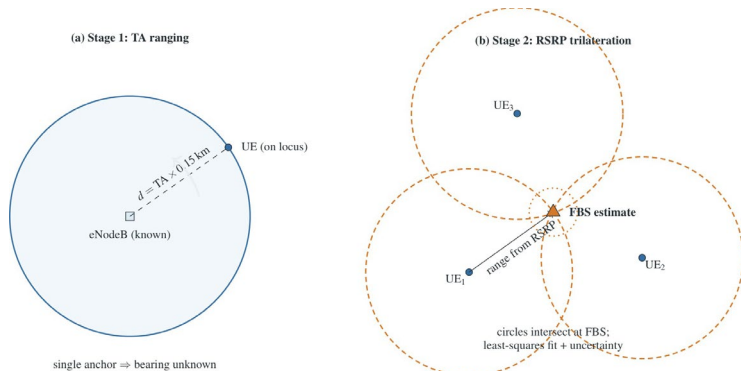


Path-loss residual ablation under regime shift.

Under regime shift, removing the residual block costs the Random Forest 3.4 AUC points; the PGNN loses 0.8. From 10% of labels upward, the PGNN holds a 3.5–4.5 point AUC advantage with far lower seed variance.

LOCALIZATION

Locating the fake cell from data already in the network



Analytical illustration; coordinates are schematic. A controlled ground-truth study is left to future work.

1

UE position from Timing Advance

$d = TA \times 0.15$ km from the known eNodeB site.

One anchor gives a circular locus with no bearing; multiple visible eNodeBs let the circles intersect.

2

FBS position from RSRP trilateration

Invert the calibrated path-loss model on each UE's reported FBS RSRP, then least-squares fit the intersection. Detection and localization share one stream.

Industry interest in deploying this work

Both halves of the system have drawn interest from operators and device makers—and in each case the interest lands exactly where that half is strongest.

Polaris Wireless

Network-side detection in operator infrastructure

Interested in running network-side FBS detection inside their own infrastructure. We worked with them to implement the pipeline in their system and evaluate it against their data.

Telit Cinterion

FBS detection in the baseband itself

Interested in implementing FBS detection directly in their cellular modules. This is the deployment path that removes the app's dependence on a rooted phone and MobileInsight.

What the two together suggest

The layered defense argued for in the papers is also the one industry is reaching for independently—an operator wants the core-network view, a module vendor wants the device view, and neither substitutes for the other.

Academic uptake of the POWDER datasets

Since release, other groups have reached out and built new work on the traces we collected on POWDER.

Explainability

Making detection verdicts interpretable rather than accepting a black-box classification.

FBS as anomaly detection

Models trained on large amounts of benign data learn to detect FBSes as an anomaly in the trace.

FBS positioning

Optimizing the positioning of FBSes to maximize the impact of the attack.

Network sensing

Pushing inference further down onto network sensing by observing the signal transmission.

The dataset is the contribution that keeps compounding

The work has motivated research well beyond our own agenda—and it has demonstrated what POWDER itself can do: build reproducible adversarial cellular datasets and run controlled attack experiments over the air, at a fidelity no simulation offers and no individual lab can assemble alone.

Next: Open RAN profiles and xApps

Detection as an xApp

Move the detection logic into the near-real-time RAN Intelligent Controller using POWDER's Open RAN profiles, so the same models run where the RAN already exposes its state.

From detection to mitigation

An xApp can act, not just alert: blacklist a suspected cell, adjust handover parameters, or steer UEs away from the rogue cell.

Integrated sensing

Reuse the measurement stream for sensing tasks beyond security—the same RSRP, SINR, and TA data that localizes an FBS characterizes the radio environment.

Open problems on the roadmap

- **Identity-spoofing FBSes.** The protocol rule fires because the target is unregistered; an FBS advertising a registered neighbor's identity makes the target resolvable. Propagation physics is what it still cannot spoof.
- **Porting to 5G.** NG-AP replaces S1AP and the AMF replaces the MME; most layer-3 procedures are unchanged, so the model designs should carry over once an open 5G SA stack supports handover.
- **Grounding the physics.** Supply the forward model with real eNodeB coordinates and calibrate path-loss envelopes from operator planning data rather than benign testbed captures.

Detect on both sides of the air interface

Real over-the-air data changes what you can claim.

FBSAD, MSAD, and NSFBSDataset were all collected on POWDER with real radios, real mobility, and a dedicated spectrum allocation—and all are publicly released.

UE-side ML detects what rules cannot.

96% FBS accuracy and 86% MSA recognition, robust to reshaped and unseen attacks, running in 835 kB and under 2 mW on an ordinary phone.

The network side sees something the device never will.

Every handover toward a rogue cell fails with unknown-targetID, because an FBS cannot perform S1 Setup. A zero-parameter rule on that catches every FBS trace in our corpus.

Layer detectors that fail independently.

Statistical fusion, a protocol invariant, and a physics-consistency model each cover a different evasion—together they raise the bar much further than any one alone.

Thank you

Datasets, models: zenodo.org/records/14720824