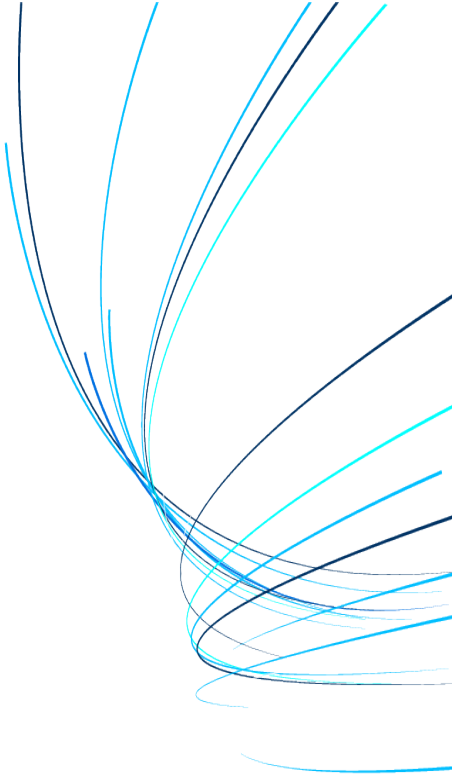
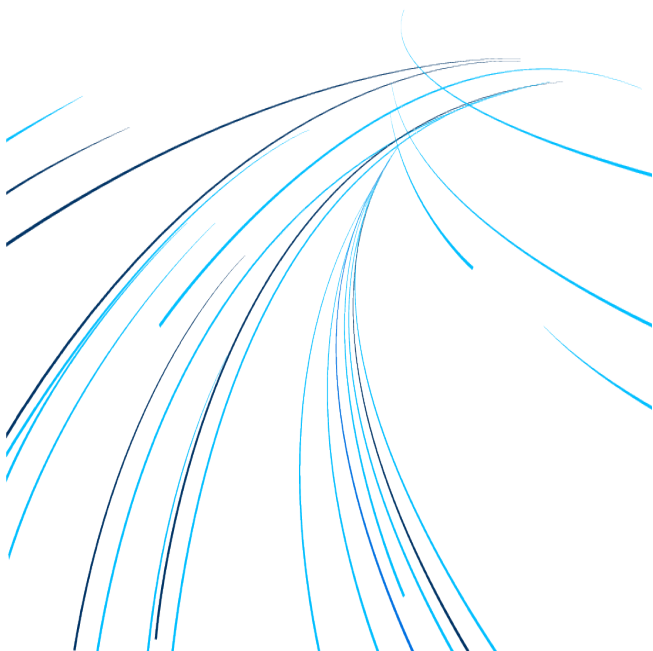
SNI5GECT: A Practical Approach to Inject aNRchy into 5G NR

Shijie Luo, Matheus E. Garbelini,
Sudipta Chattopadhyay, and Jianying Zhou



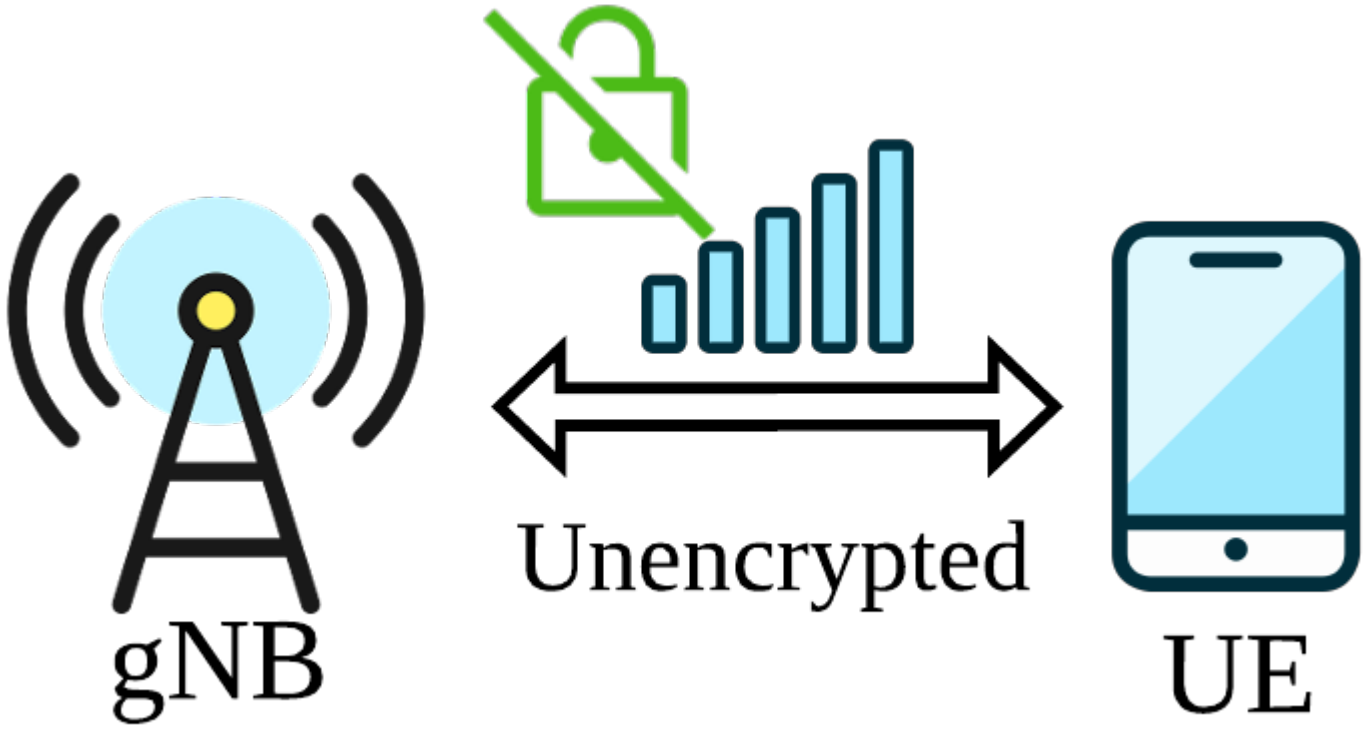


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

ASSET RESEARCH GROUP

iTrust
Centre for Research in Cyber Security

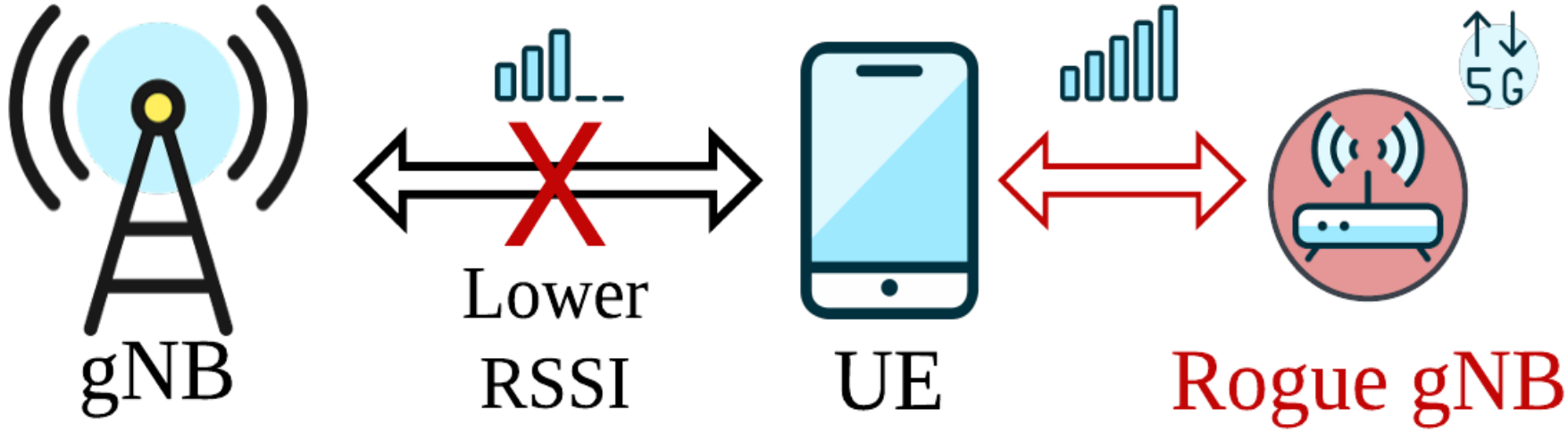
Threat Model



Both **Physical layer signals** and **messages exchanged before the security context is established** remain unencrypted.

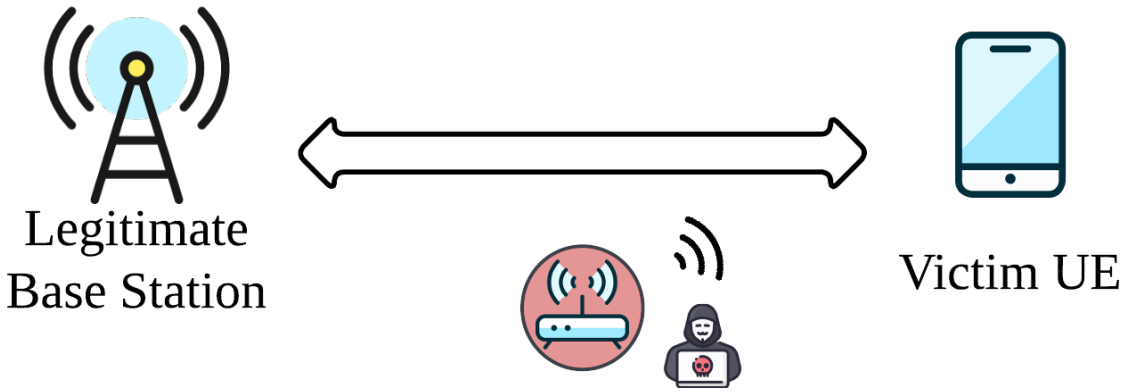
➤ *This leaves a potential for these signals to be intercepted or even spoofed by an attacker.*

Motivation



- Most prior works assume a **man-in-the-middle** attacker based on a **rogue base station**.
- Broadcast signals make rogue base stations **easily detectable**.
- **Lack of** tools to passively sniff over-the-air traffic between UE and base station

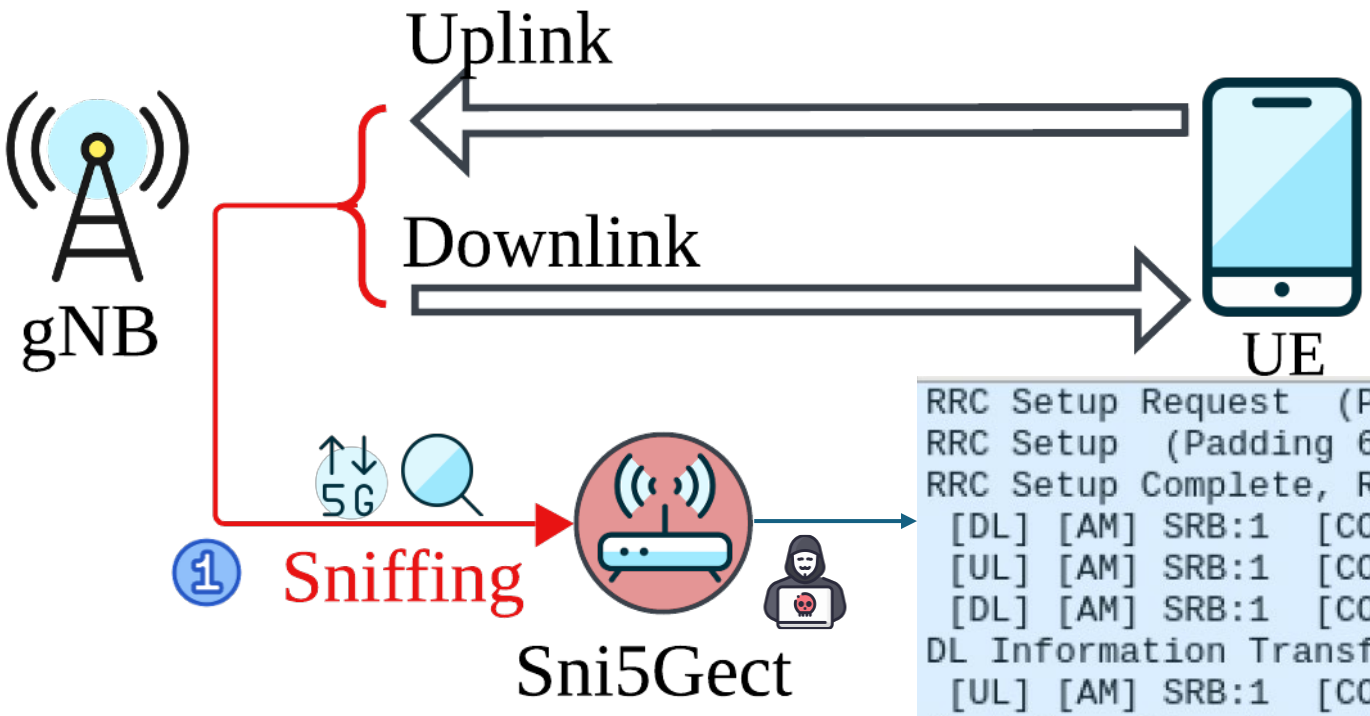
Attacker Model



- **Adversary:** A passive or active attacker located within radio range of the target UE and gNB
- **Access Level**
  - No privileged access to the base station or core network
  - No access to subscriber credentials or cryptographic keys
- **Attacker Capability**
  - Able to eavesdrop on unencrypted messages (e.g.,RRC Setup,Registration Request)
  - Capable of injecting or replaying messages over the downlink communication channel toward the UE

Sni5Gect: Sniff + 5G + Inject

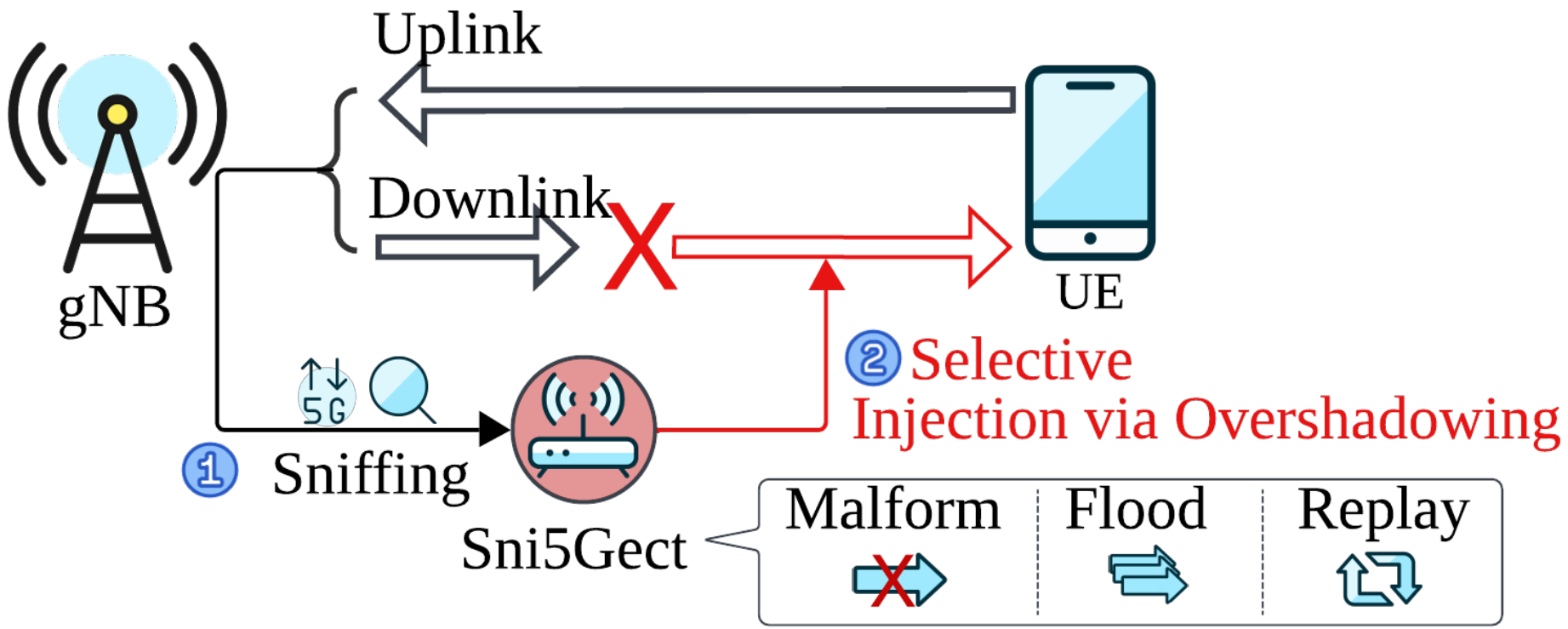
Step 1: Sniff uplink & downlink traffic to learn the communication state




```
RRC Setup Request  (PHR PH=59 PCMAX_f_c=47)   (Padding 0 by
RRC Setup  (Padding 6 bytes)
RRC Setup Complete, Registration request, Registration requ
 [DL] [AM] SRB:1  [CONTROL]  ACK_SN=1          ||   , DL Info
 [UL] [AM] SRB:1  [CONTROL]  ACK_SN=1          ||   , UL Info
 [DL] [AM] SRB:1  [CONTROL]  ACK_SN=2        (Padding 78 byt
DL Information Transfer, Authentication request  [51-bytes]
 [UL] [AM] SRB:1  [CONTROL]  ACK_SN=2        (Short BSR LCG
UL Information Transfer, Authentication response  [37-bytes
 [DL] [AM] SRB:1  [CONTROL]  ACK_SN=3          ||    [DL] [AM
DL Information Transfer, Security mode command  (Padding 75
 [UL] [AM] SRB:1  [CONTROL]  ACK_SN=3          ||   , UL Info
 [DL] [AM] SRB:1  [CONTROL]  ACK_SN=4        (Padding 78 byt
Security Mode Command  [9-bytes]  (Padding 70 bytes)
```

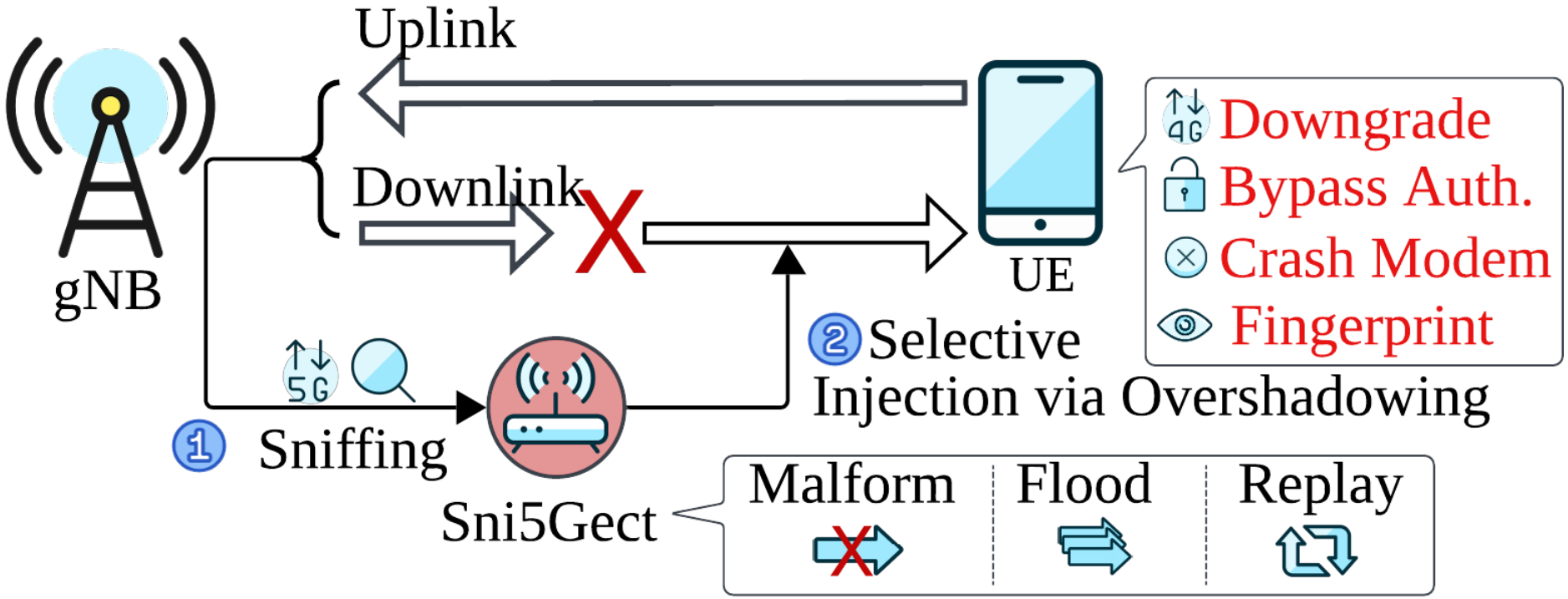
Sni5Gect: Sniff + 5G + Inject

Step 2: Inject forged messages at precise state to influence UE behavior



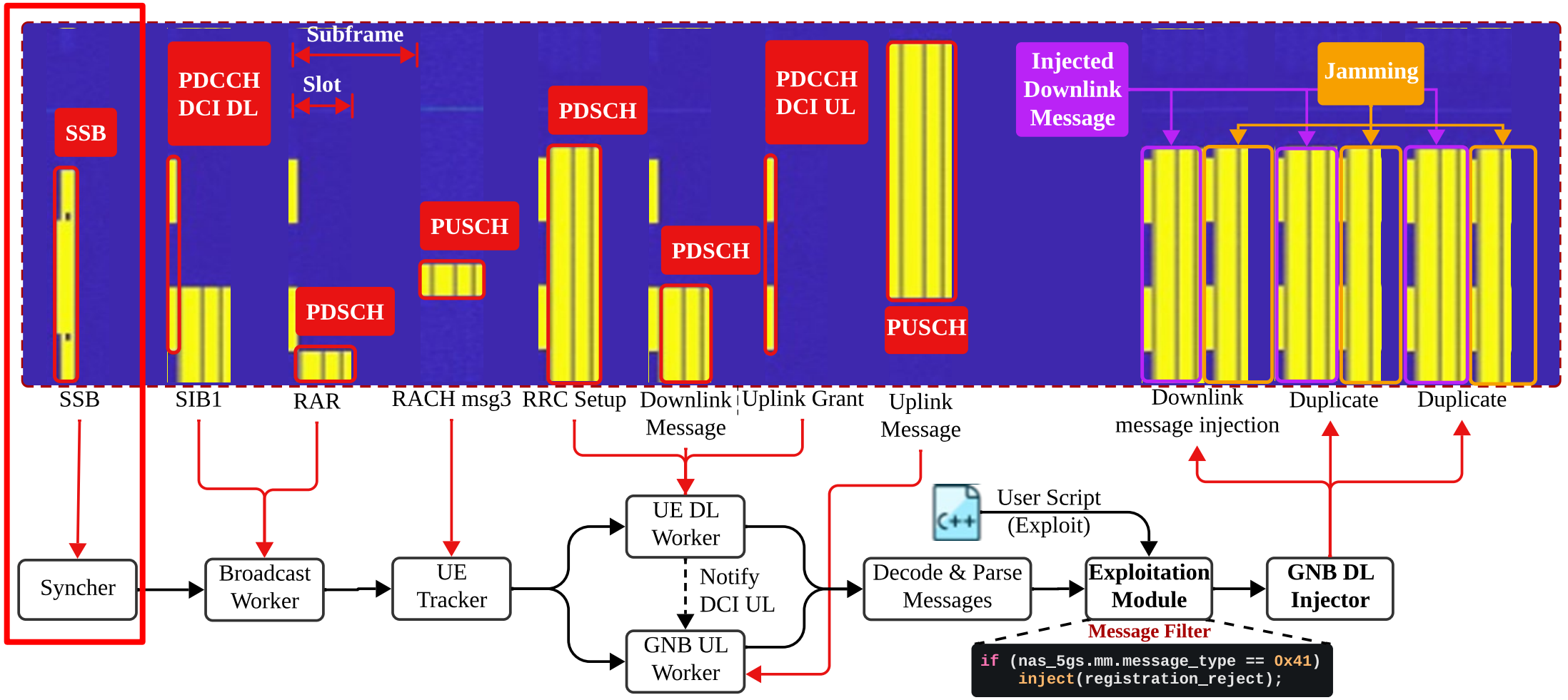
Sni5Gect: Sniff + 5G + Inject

UE cannot distinguish the sender and accepts injected messages



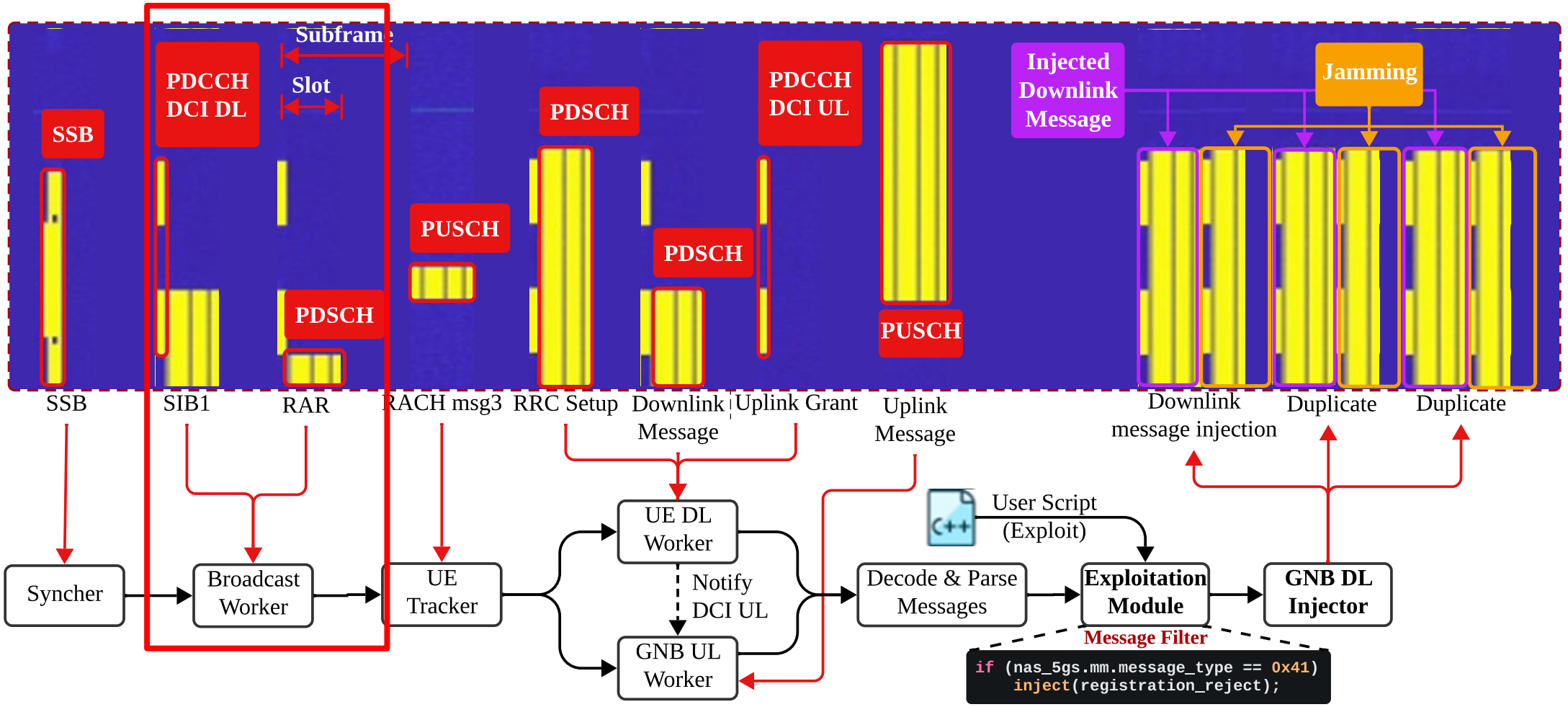
Sni5Gect: Design

Syncher: time and frequency synchronization



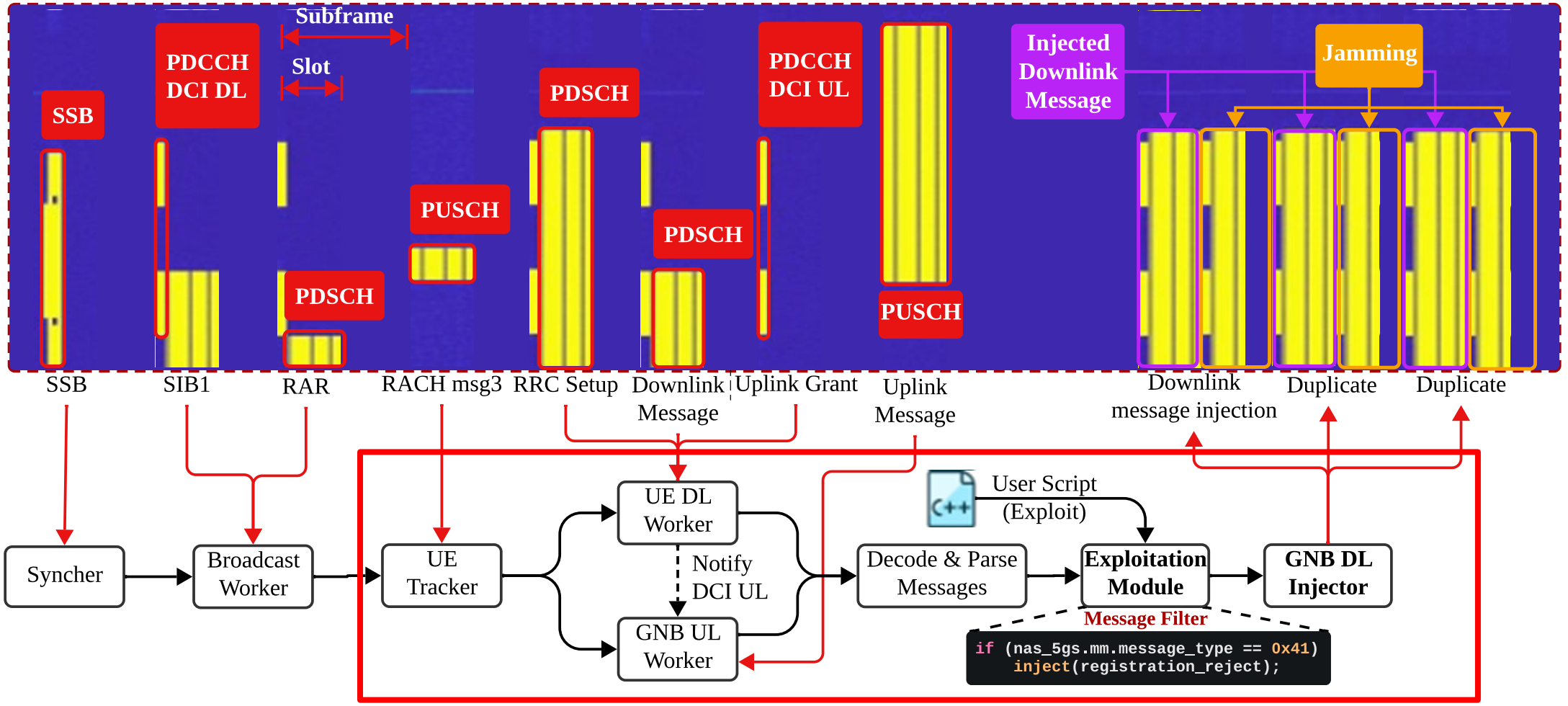
Sni5Gect: Design

Broadcast Worker: retrieve cell configuration and detect new UE connections



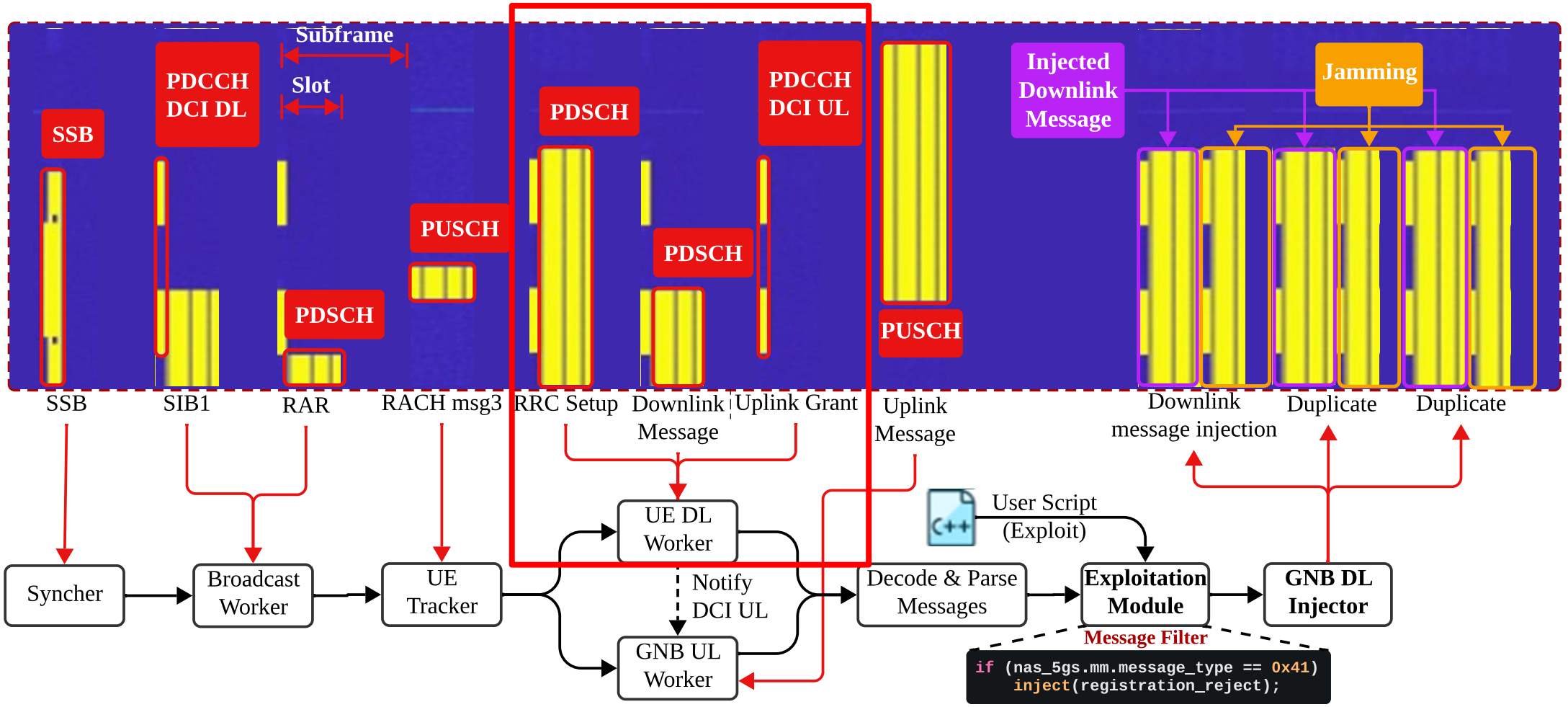
Sni5Gect: Design

UETracker: monitor the UE connection state and configuration



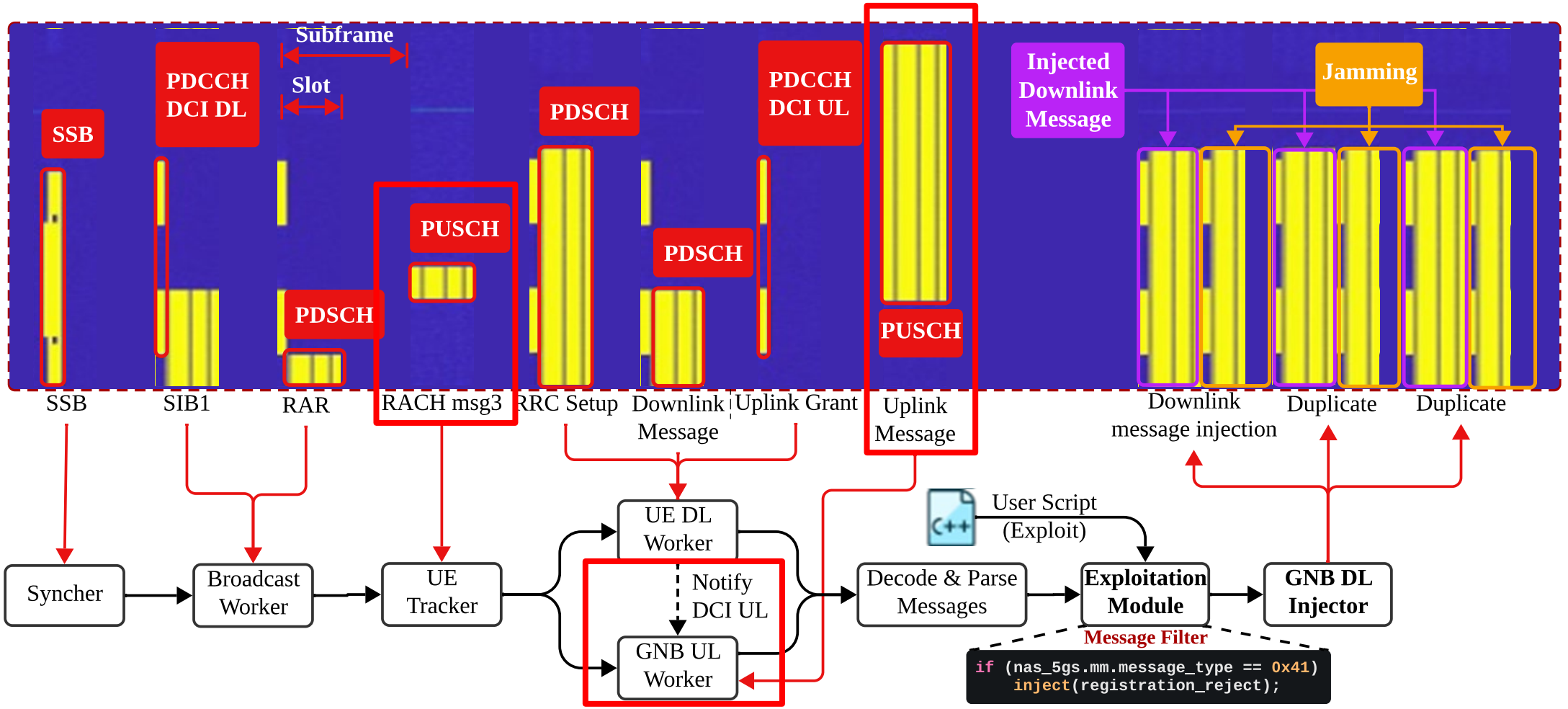
Sni5Gect: Design

UE DL Worker: decodes downlink messages from gNB to UE



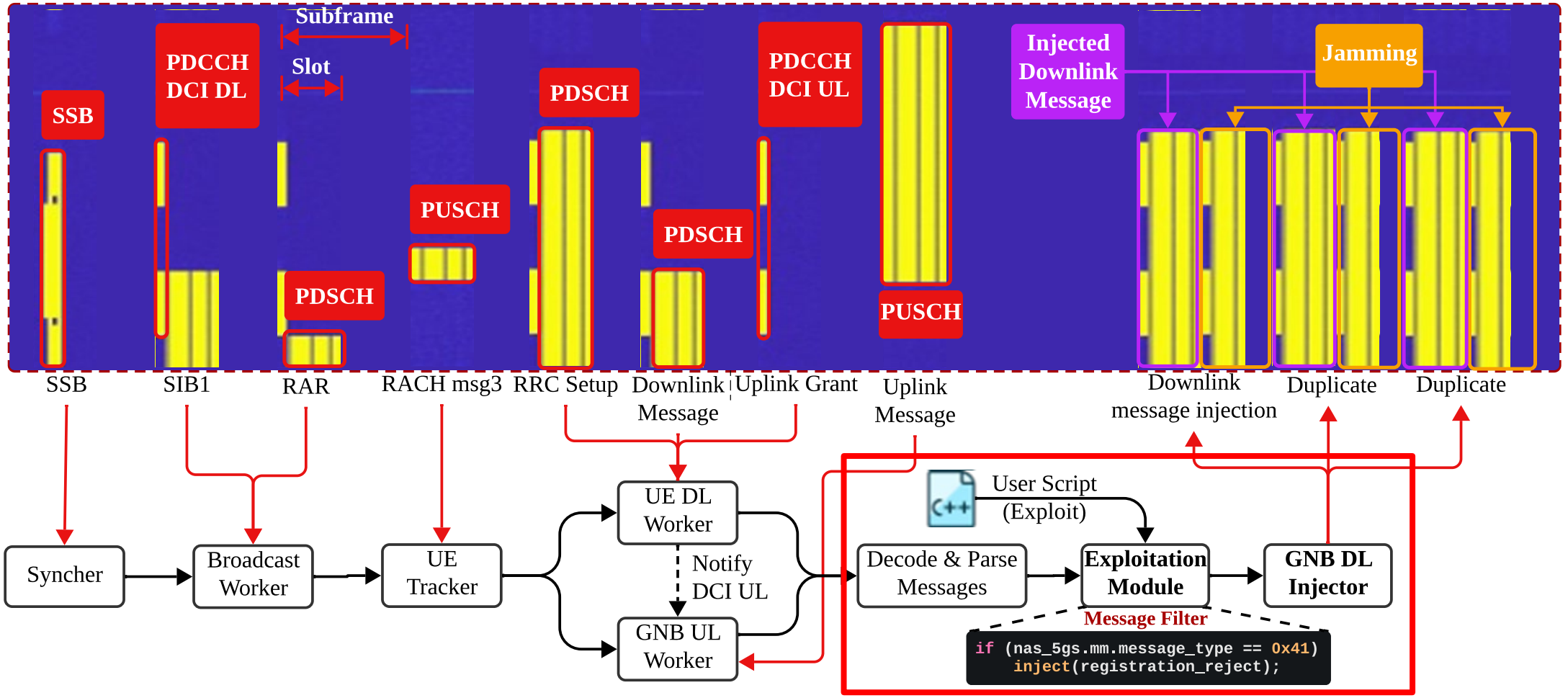
Sni5Gect: Design

GNB UL Worker: decodes uplink messages from UE to gNB



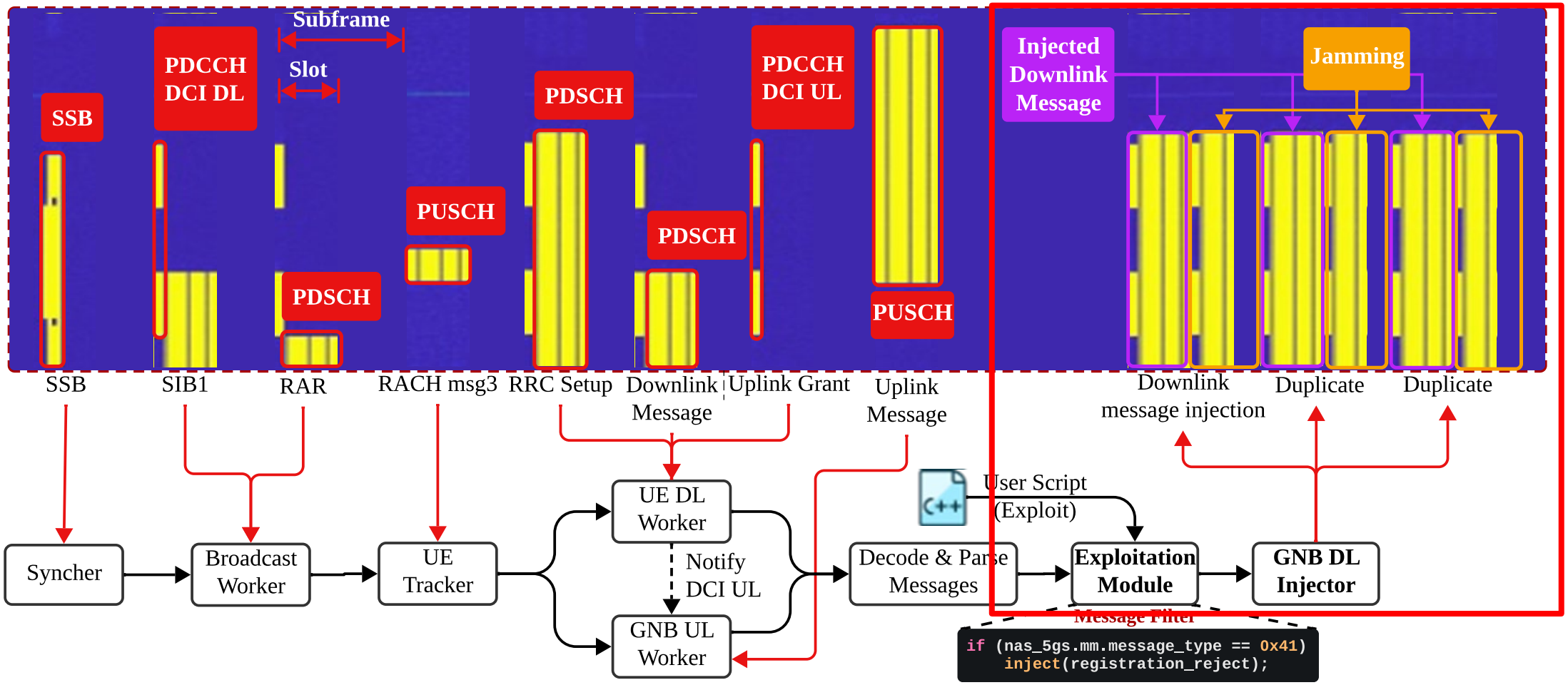
Sni5Gect: Design

Exploit Module: custom user-defined scripts for triggering attacks



Sni5Gect: Design

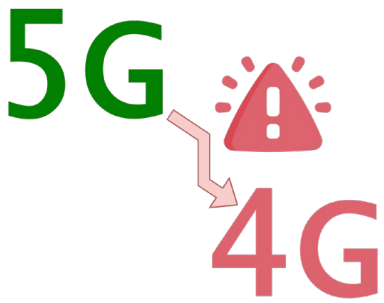
GNB DL Injector: Encodes and injects crafted downlink messages to target UE



Attack Scenarios with Sni5Gect

One-shot Attacks

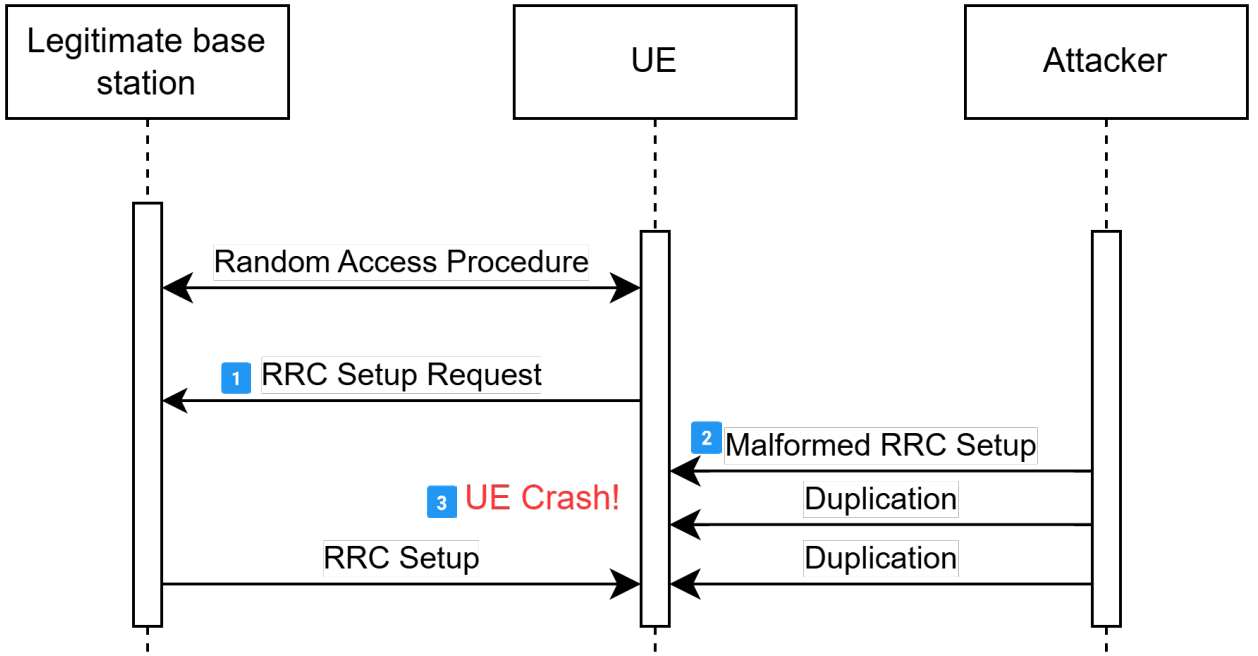
One-shot Attacks with Response



Multi-stage Attacks

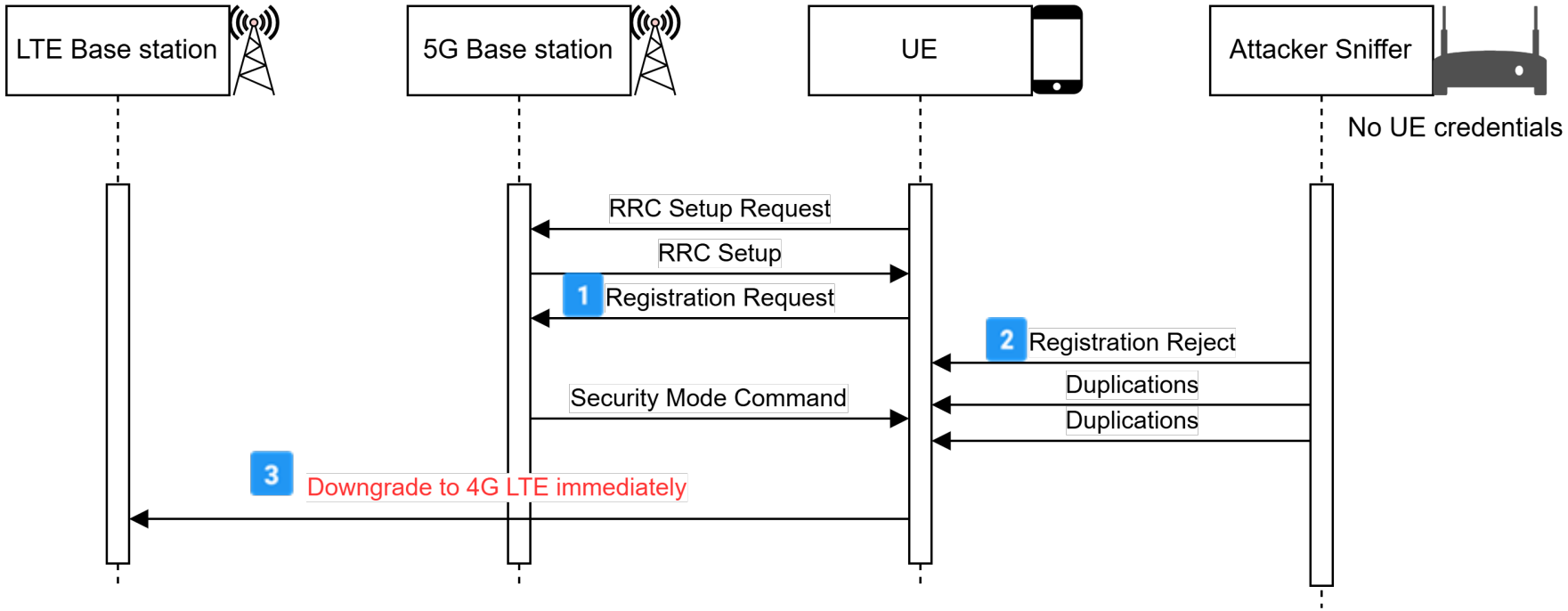
One-Shot Attack: Immediate Reaction

- **Inject a single message → UE reacts instantly**
  - Example: Malformed RRC Setup → UE crash



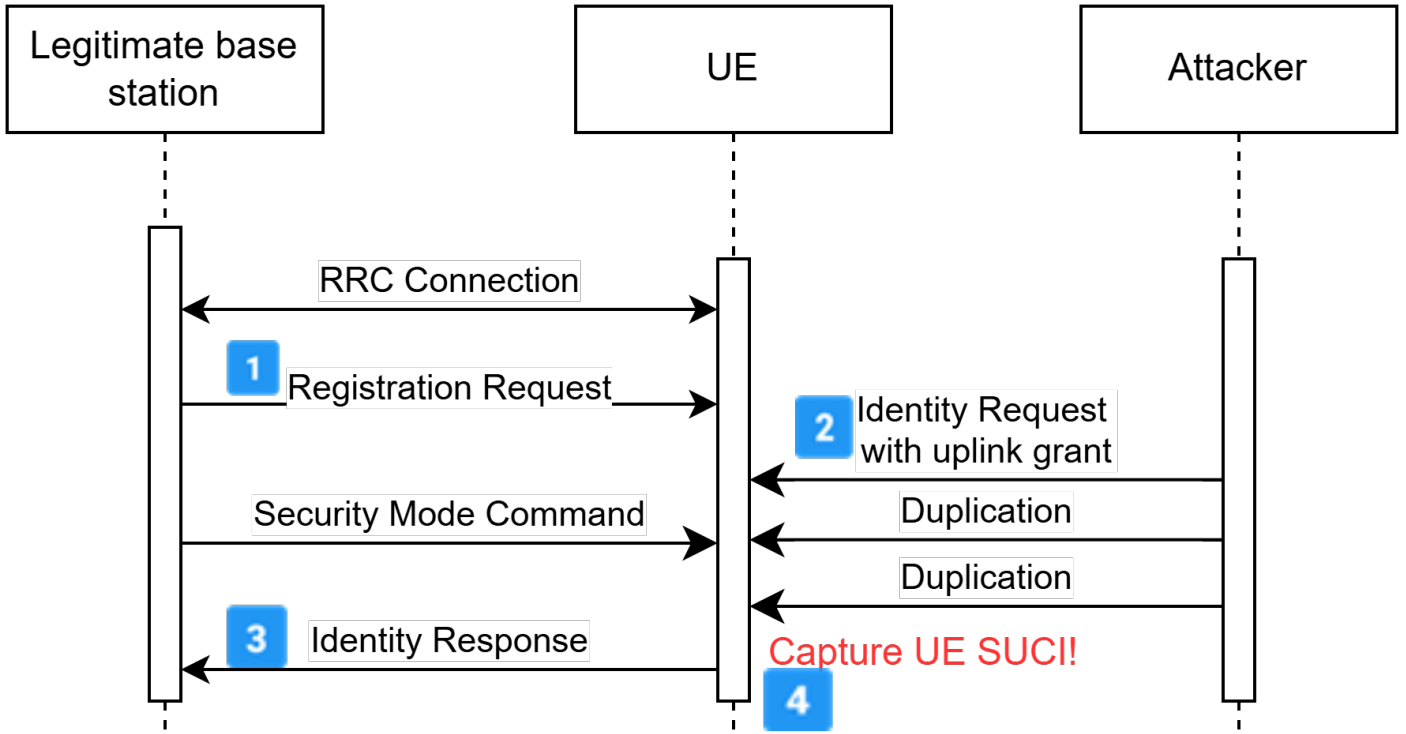
One-Shot Attack: Immediate Reaction

- **Inject a single message → UE reacts instantly**
  - Example: Registration Reject → UE downgrades to LTE



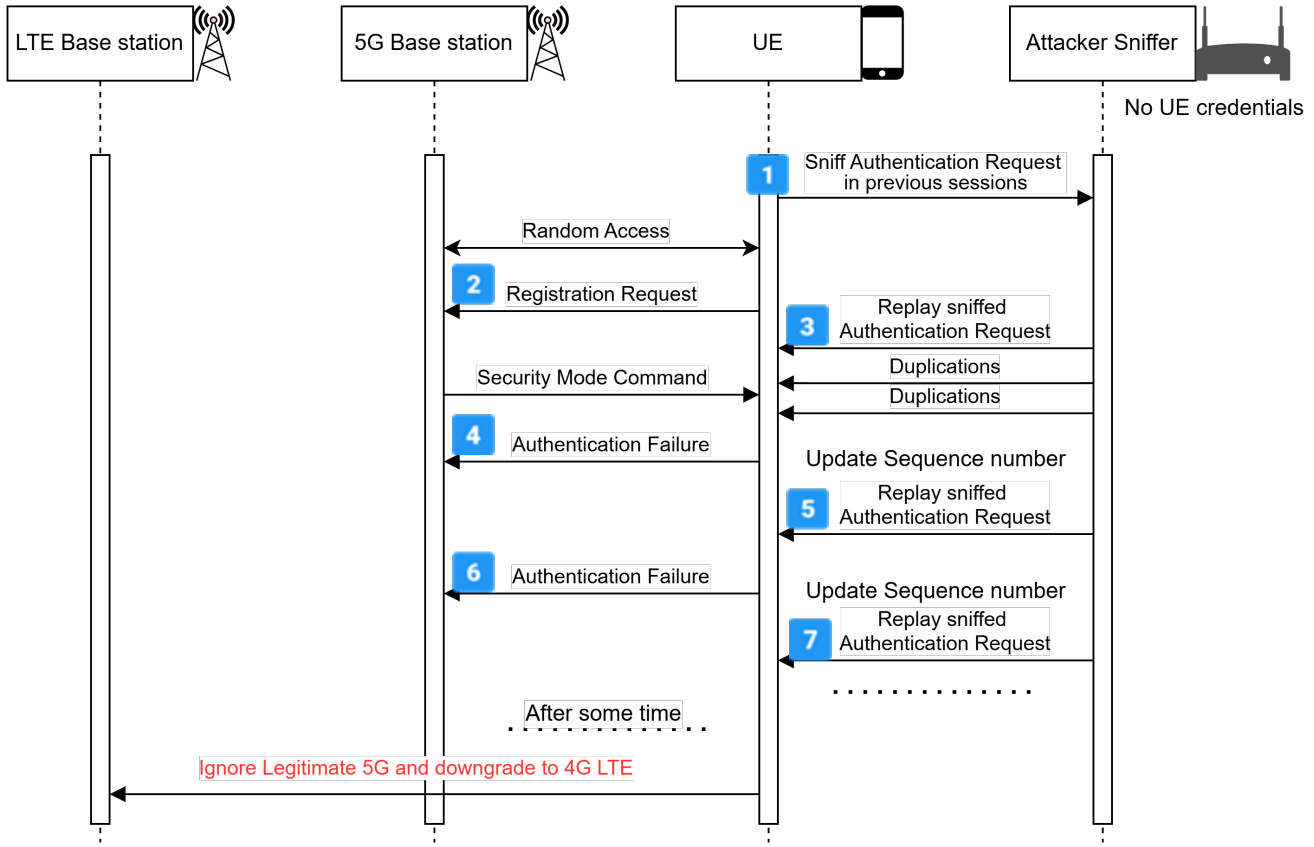
One-Shot Attack with Response

- **Inject a single message → UE replies**
  - Example: Identity Request → Identity Response



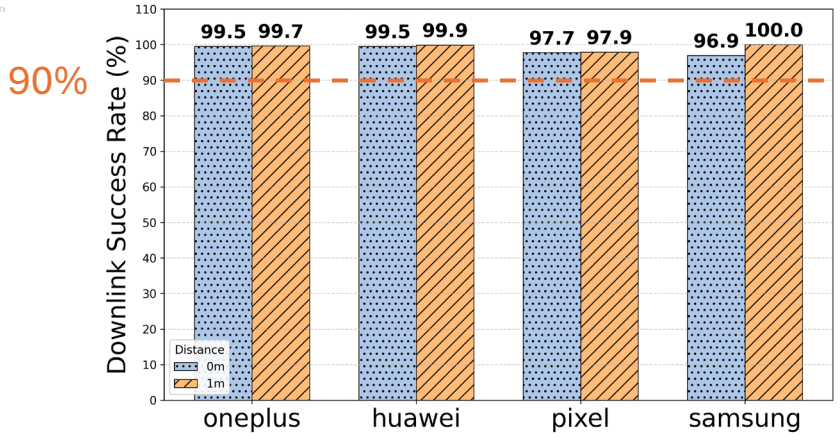
Multi-stage Attacks

- **Sniff + inject messages at multiple states**
  - Example: Authentication Replay → UE downgrades to LTE

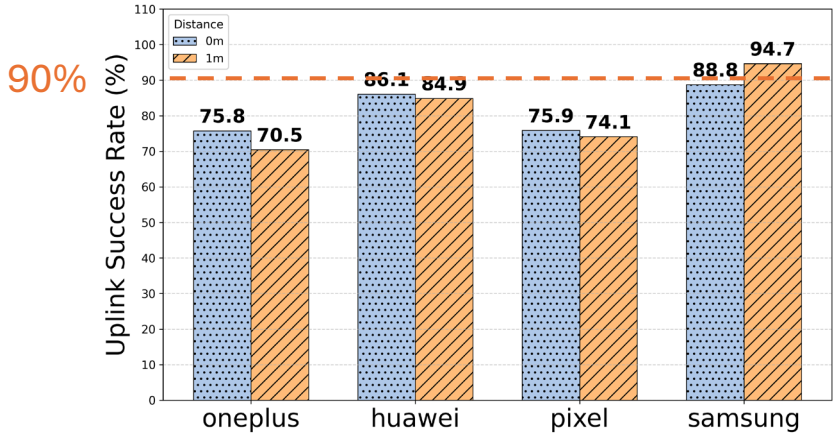


Acknowledged by GSMA: CVD-2024-0096

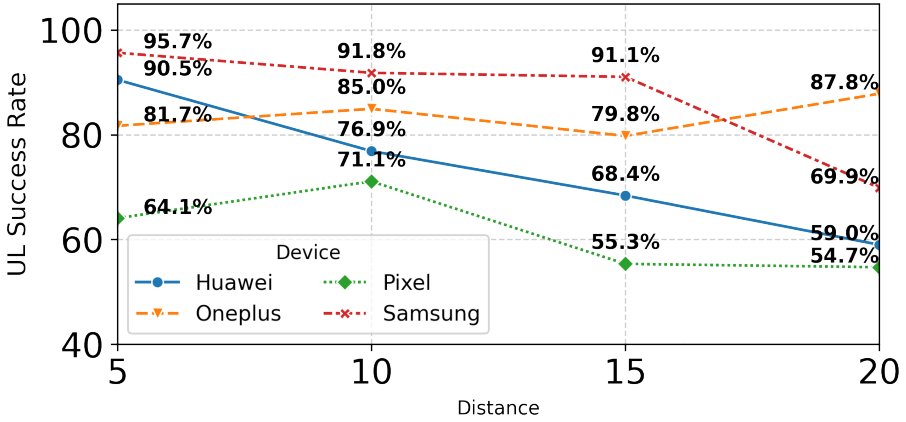
Sni5Gect Evaluation: Sniffing



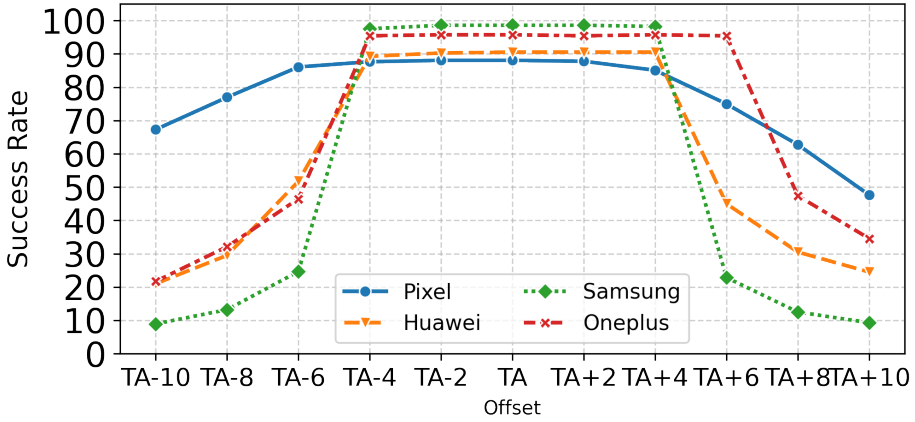
Downlink Sniffing Success Rate



Uplink Sniffing Success Rate

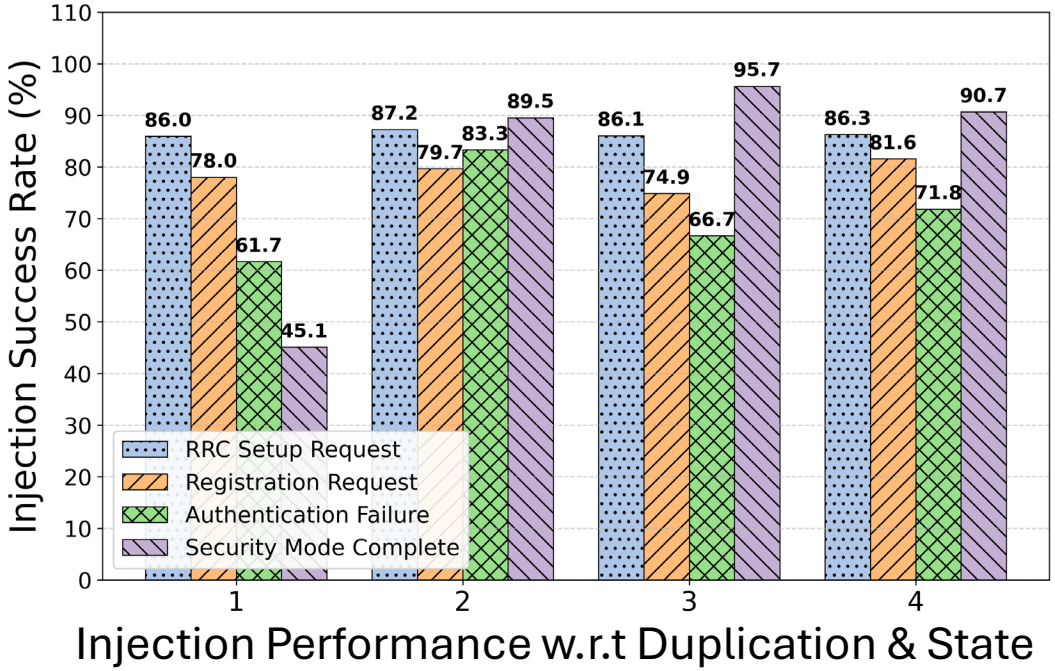


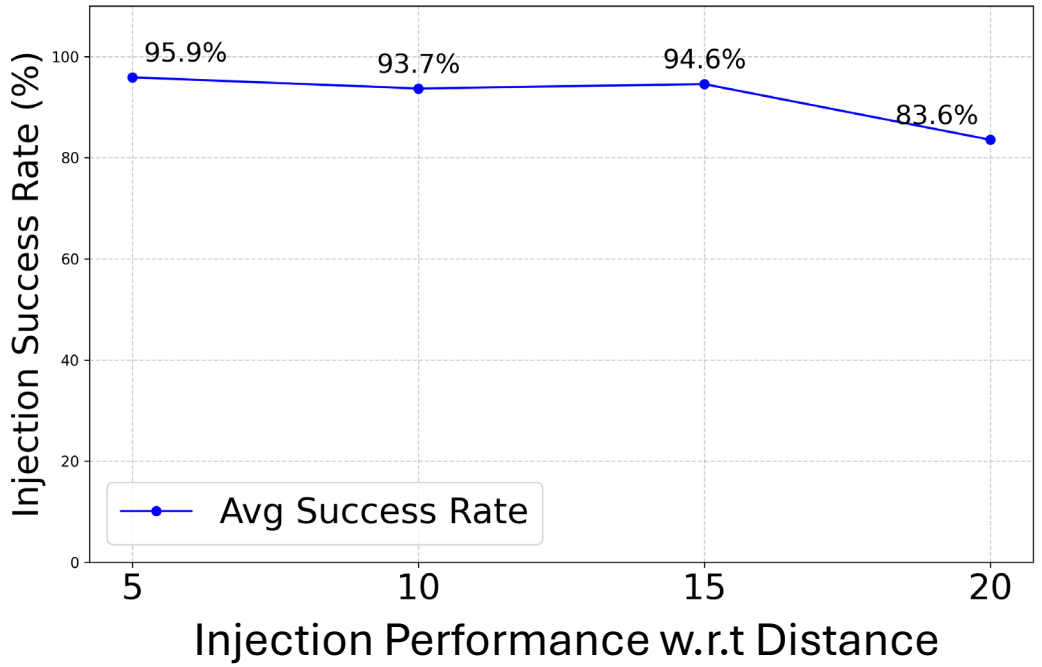
Uplink Sniffing w.r.t Distance



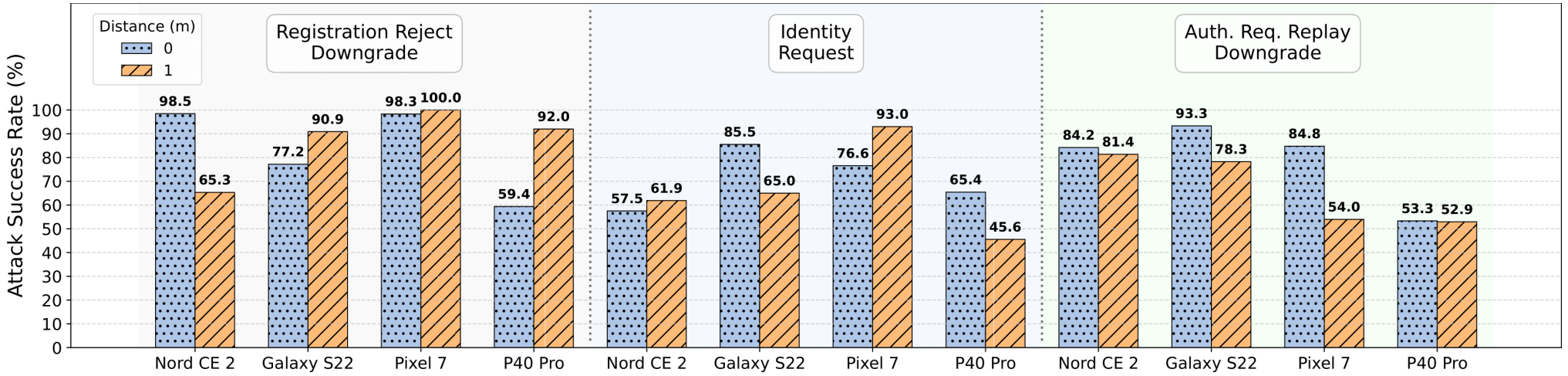
Uplink Sniffing w.r.t TA Offset

Sni5Gect Evaluation: Injection

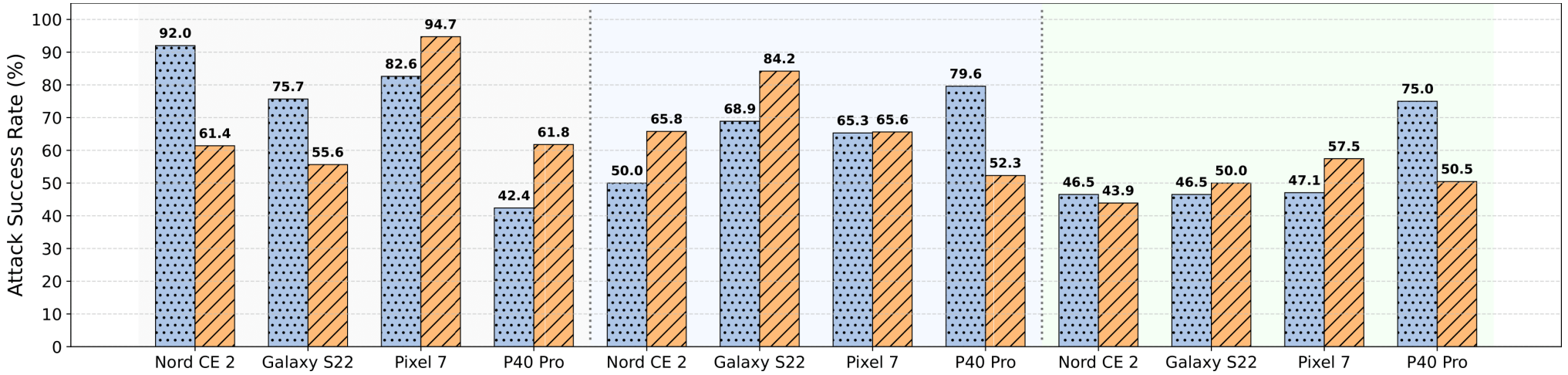




Sni5Gect Evaluations: Attacks



Attack Success Rates by Device, Distance, and Attack Type using srsRAN as legitimate gNB



Attack Success Rates by Device, Distance, and Attack Type using Effnet as legitimate gNB

Reusability of Sni5Gect

🔒 Attack Evaluation

Realistic testing without rogue BS

📊 Throughput Analysis

Measure traffic volume via DCI

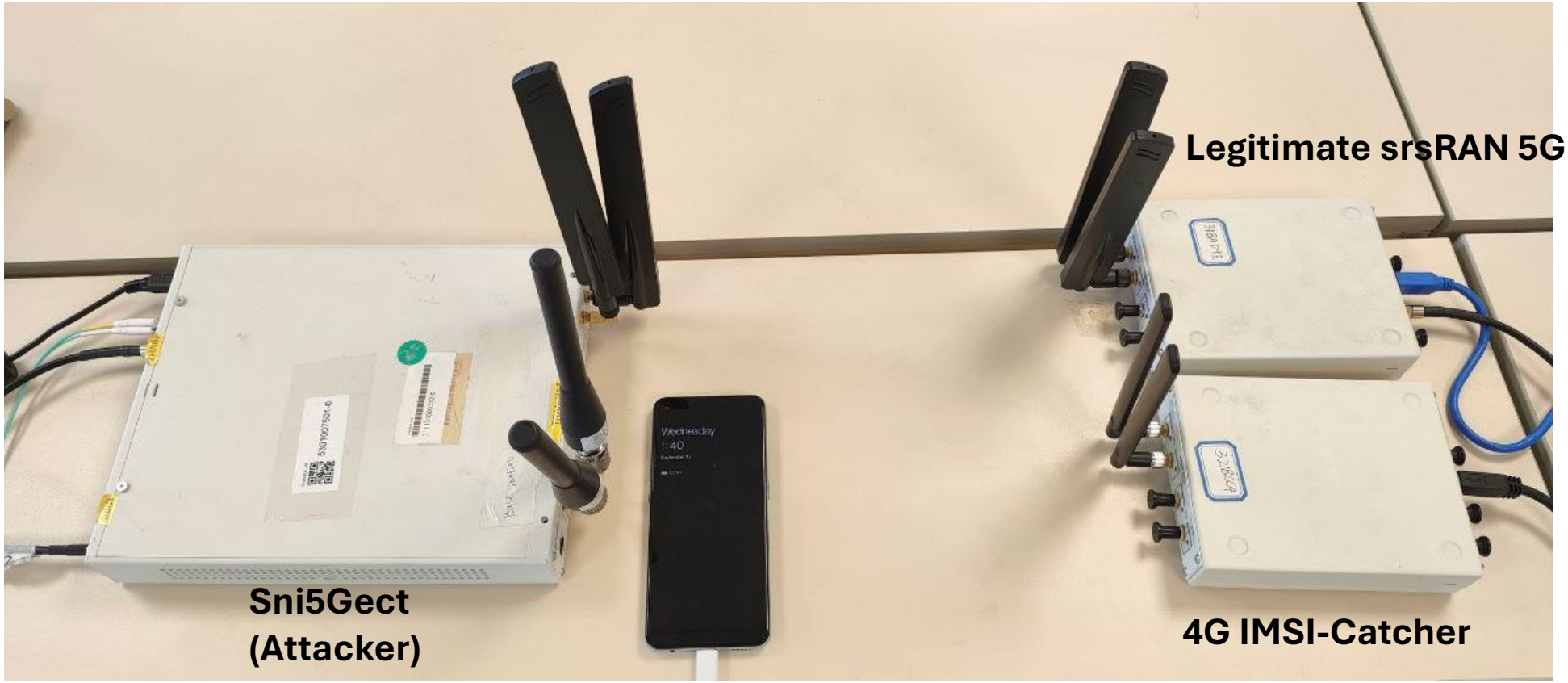
🕵️ Traffic Analysis

Study UE ↔ BS communication & privacy

🚨 Anomaly Detection

PCAP dataset for detection research

Demo


Legitimate srsRAN 5G
Sni5Gect
(Attacker)
4G IMSI-Catcher
Victim UE