Open 5G Testbed: A Cyber Range Platform for Security Research

Azza H. Ahmed, Thomas Dreibholz, Foivos Ioannis Michelinakis, Tarik Čičić
Simula Metropolitan Centre for Digital Engineering
Oslo, Norway

simulamet

Context & Motivation

Why 5G Security & Experimentation Matters

The 5G Security Frontier

5G is more than just speed; it serves as critical infrastructure for smart cities, IoT, and autonomous transport. However, this evolution introduces significant risks:

- **Expanded Attack Surface:** Distributed architecture and billions of connected devices expose new entry points.
- **Complex Technologies:** NFV, SDN, and Network Slicing create a dynamic, virtualized ecosystem that is harder to secure.
- **Critical Impact:** Breaches now threaten public safety and essential services, not just data privacy.

The Experimentation Gap

High Cost

Existing testbeds often require expensive, commercial-grade hardware and software licenses, making them inaccessible for many universities.

Closed Systems

Many platforms are proprietary or restricted to large industrial consortia, limiting transparency and the ability to audit code.

Reproducibility

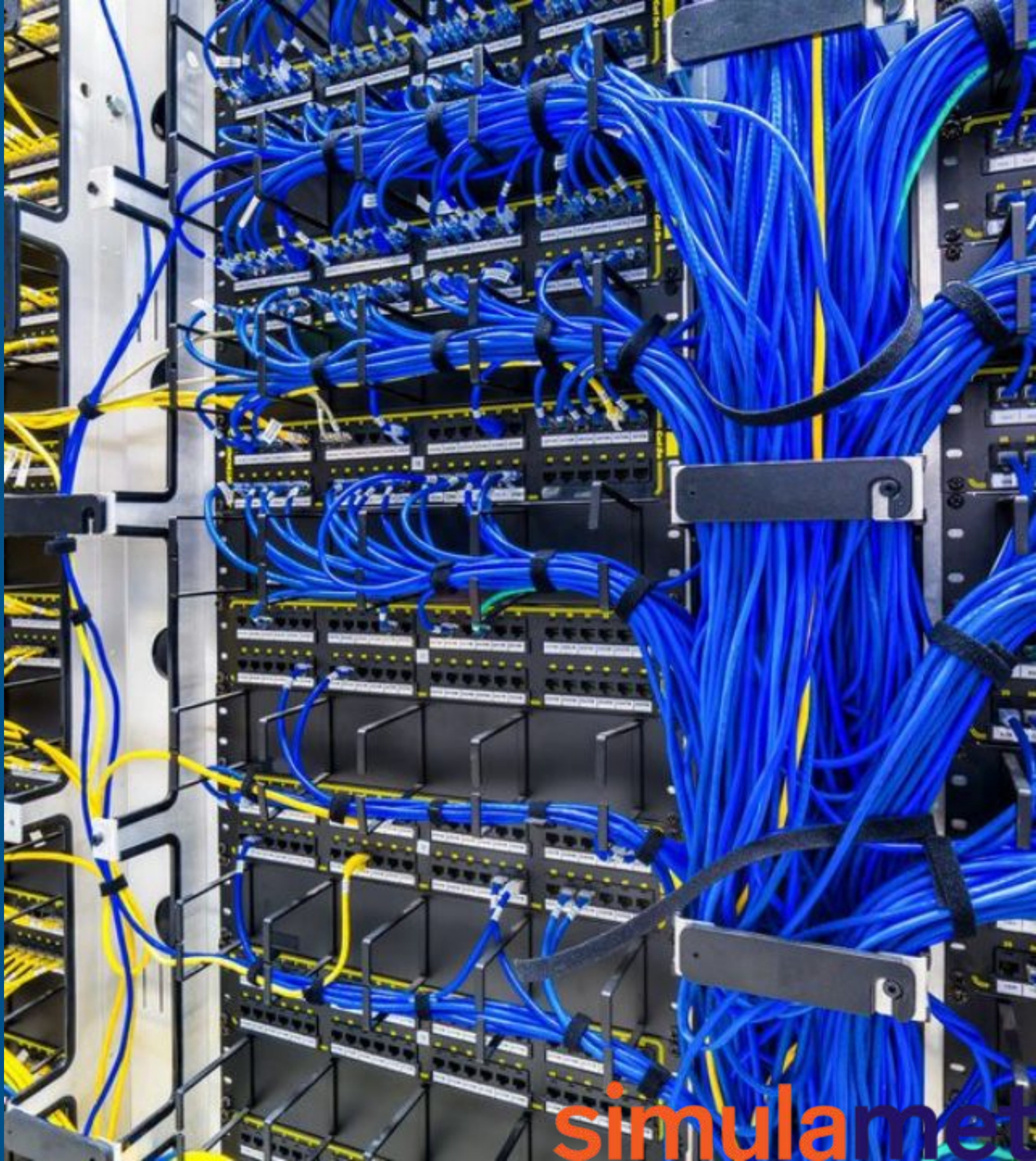
Lack of open configuration and documentation makes it difficult for the broader research community to validate findings or replicate setups.

simulamet

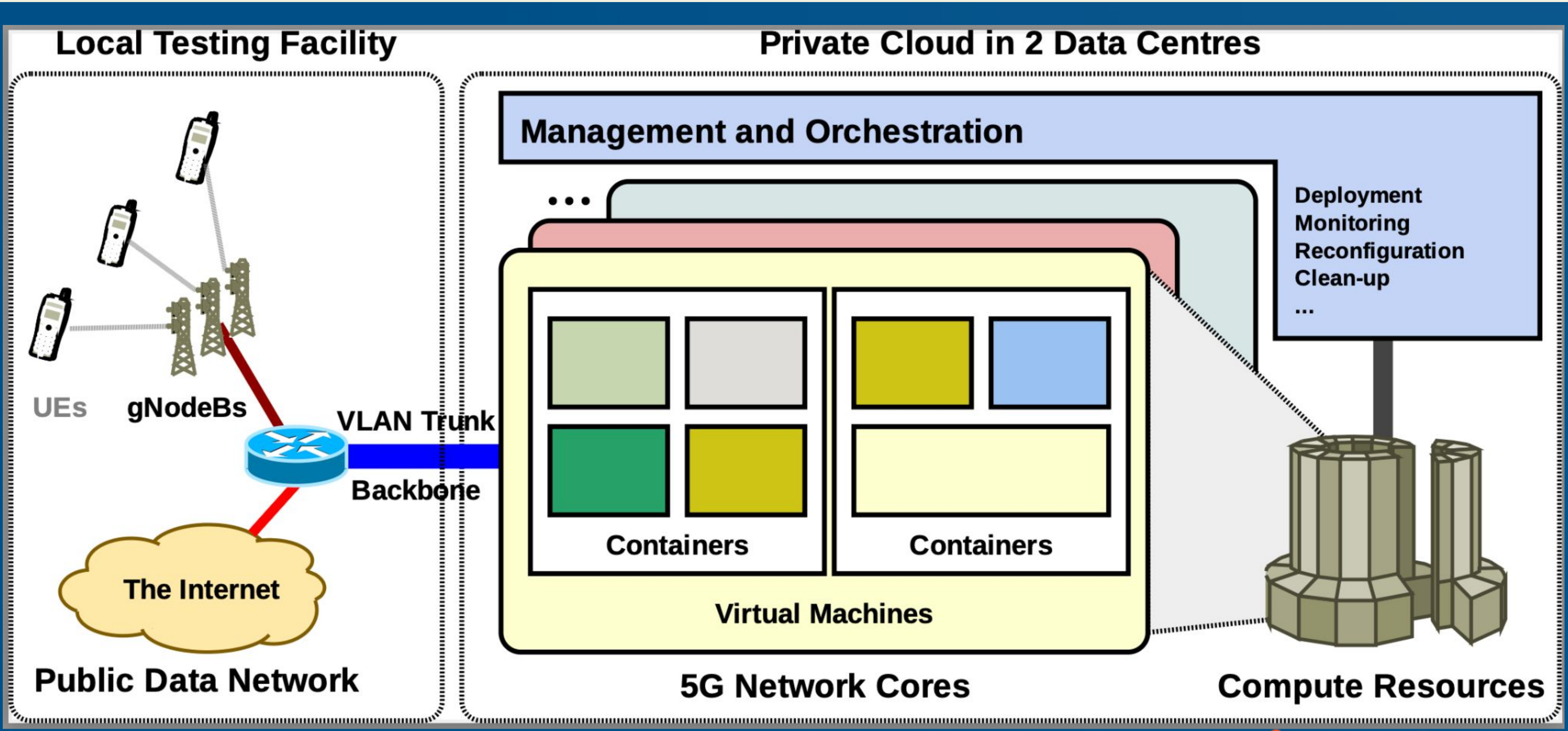
Our Solution: Open 5G Testbed

We present a fully software-based, low-cost 5G Stand-Alone (SA) testbed designed specifically for security research and education.

- Built on OpenAirInterface (OAI)
- Uses COTS SDR Hardware
- Modular & Containerized
- Ideal for Cyber Range & Education



Our Testbed Architecture



simulamet

Hardware Architecture

COTS Components

We utilize accessible commercial off-the-shelf hardware to lower barriers to entry.

Software Defined Radios (SDR)

Ettus USRP B210: Low-cost, connects via USB 3.0. Good for basic testing.
Ettus USRP N310: High performance, 10GbE connectivity. Full 5G throughput.

User Equipment (UE)

Quectel RM50xQ-G Modems: Preferred over smartphones for debugging capabilities and reliable 5G SA connectivity.

Software & Tooling Stack

- **Private Cloud Infrastructure:** Hosted on Proxmox, OpenStack, and Kubernetes across physically separate data centers for scale and multi-tenancy.
- **Custom Base Images:** Automated build pipeline using Packer to ensure reproducibility across "Minimal", "Basic", and "Development" environments.
- **Experimentation Tools:** Pre-packaged container tools including T-Shark (protocol analysis), SysStat (performance monitoring), HiPerConTracer (latency measurement), NetPerfMeter (throughput measurement)
- **Containerized Core:** 5G Core Network functions deployed via Docker Compose, facilitating easy configuration and reset for student labs.

SimulaMet Open Source Tools

- **HiPerConTracer:** Accurate latency and connectivity measurements

  https://www.nntb.no/~dreibh/hipercontracer/

- **NetPerfMeter:** Advanced multi-protocol throughput measurements (TCP, MPTCP, SCTP, UDP, DCCP, QUIC)

  https://www.nntb.no/~dreibh/netperfmeter/

- **DynMHS:** Automatic IP routing rule configuration for multi-homed setups

  https://www.nntb.no/~dreibh/dynmhs/

- **System-Tools:** Collection of tools for system management and configuration

  https://www.nntb.no/~dreibh/system-tools/

- **Virtual Machine Image Builder and System Installation Scripts**: Scripts for automated system installations

  https://www.nntb.no/~dreibh/vmimage-builder-scripts/

simulamet

Case Study 1: RAN Privacy Attacks

Capturing User Identifiers

We demonstrate vulnerabilities in user identity protection across network generations.

The Attack Scenario:
Deploying a fake base station (IMSI catcher) to force UEs to connect and reveal their identity.

- **4G/5G NSA:** Captures the permanent IMSI.
- **5G SA:** Uses SUCI (Subscription Concealed Identifier). While SUCI protects the permanent ID (SUPI), implementation flaws (e.g., null encryption) can still expose users.

simulamet

Case Study 2: Core Network DoS

Target: AMF

The Access and Mobility Management Function (AMF) is the primary entry point for control plane signaling. It is critical for user registration and mobility.

Attack Vector:
A malicious UE floods the AMF with specially crafted SCTP packets, exhausting processing resources.

The Impact

By saturating the AMF, legitimate users are unable to attach to the network, resulting in a Denial of Service.

Educational Value:
Students use tools like SysStat to observe CPU spikes and T-Shark to analyze packet distribution, learning both attack mechanics and detection strategies.

simulamet

Operational Lessons Learned

- **Hardware Tuning is Critical:** Disabling CPU C-states and hyper-threading is mandatory for stable 5G timing. USRP N310 requires specific "XG" firmware for dual 10Gbps operation.
- **Device Selection:** COTS smartphones (e.g., Pixel 8) have limited debugging access. Quectel modems are far superior for research due to AT command access.
- **Protocol Analysis:** Wireshark coloring rules are essential for visual debugging. We customized T-Shark filters to isolate NGAP and SCTP control traffic effectively.
- **MANO Complexity:** While standard in industry, full MANO (Management and Orchestration) proved too heavy for a research lab. A lightweight Docker-based approach offered better agility.

simulamet

Future Directions

We aim to lower the barrier for rigorous 5G security research. Future plans include integrating O-RAN components for AI-driven experimentation and expanding AI-based detection mechanisms.

simulamet

Questions?

Thank you for your attention.

Contact us:
Azza H. Ahmed (azza@simula.no), Thomas Dreibholz (dreibh@simula.no),
Foivos Ioannis Michelinakis (foivos@simula.no), Tarik Čičić (tarik@simula.no)

github.com/simula/oai-cn5g-fed