Masters in Cybersecurity

Integration of Wi-Fi-Only Devices in 5G Core Networks: Addressing Authentication and Identity Management Challenges

Author

David Araújo, *DETI*, *IT*
davidaraujo@ua.pt

Supervisors

Doctor Daniel Nunes Corujo, *DETI*, *IT*
Doctor Francisco Fontes, *Altice Labs*

June 2025 — Aveiro, PT

Table of Contents

1. The Core Problem and Its Significance
2. Research Objectives
3. State of the Art and The Specific Gap
4. Framework Concept and Architecture
5. Key Mechanisms: Authentication, Identity, Traffic
6. Implementation: Testbed and Orchestration Logic
7. Validation: Key Results
8. Conclusion and Contributions
9. Limitations and Future Work

The Core Problem and Its Significance

The Challenge

Current 3GPP standards don't fully address integrating **Wi-Fi-only devices lacking 5G credentials** into the 5G network, preventing standard 5G authentication.

Impact

A significant hurdle for enterprise/residential environments with many such devices.

Motivation

Solving this is crucial for 5G's success, enabling true **5G-Wi-Fi convergence** and extending 5G benefits (eMBB, mMTC, URLLC) to this vast device ecosystem.

Research Objectives

To address this problem, this research aimed to:

1. **Investigate Secure Authentication:** Design a robust local authentication mechanism.
2. **Develop Device Identity Management:** Propose a method for 5GC to recognize and manage these device connections individually.
3. **Propose an Integrated Solution:** Develop a framework for seamless, secure integration with minimal impact.

State of the Art and The Specific Gap

Non-3GPP Capable Device Types Behind RGs

- **N5GC** have limited 5G capabilities but can authenticate
- **NAUN3** have no 5G capabilities and cannot directly authenticate and are often grouped.

A robust mechanism for **individualized**, **secure authentication** of *credential-less* Wi-Fi-only devices and their subsequent per-device management within the 5GC is the focus of this project.

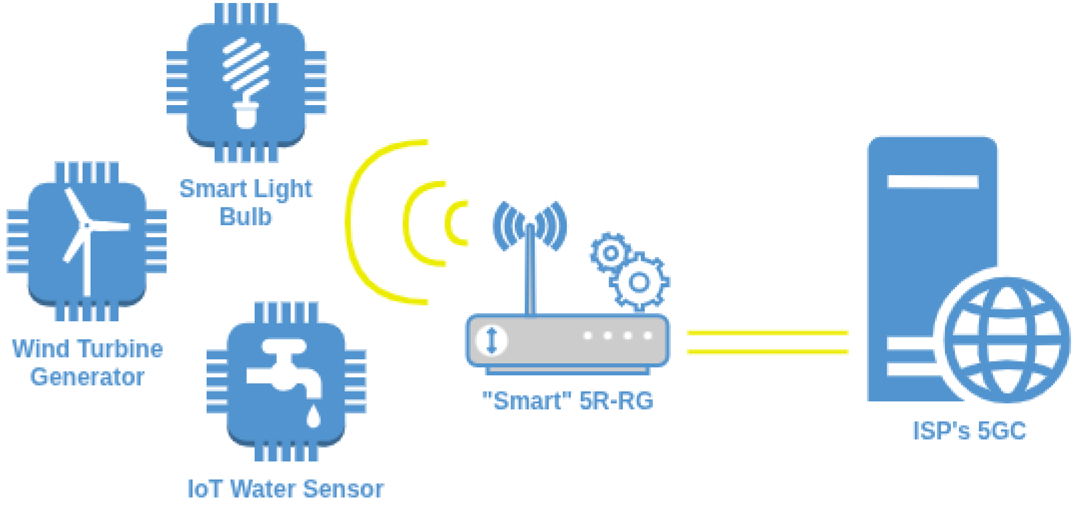
Framework Concept and Architecture

Overview and Guiding Principles

A *smart* 5G Residential Gateway (5G-RG) capable of mediating the secure integration.

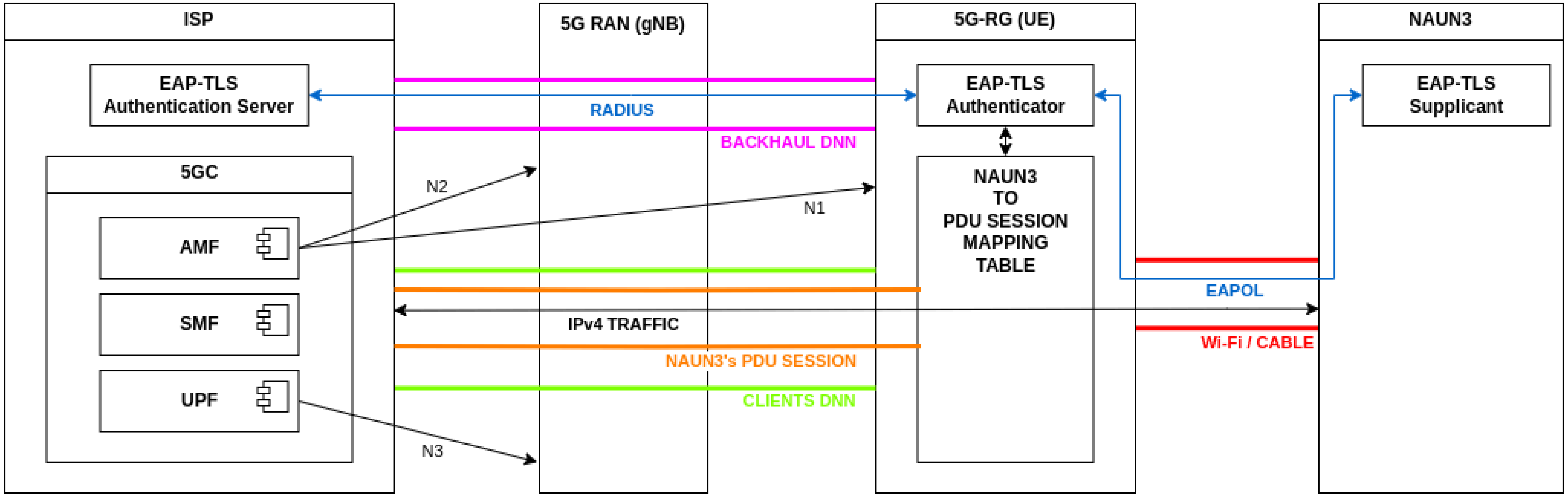
Key Design Principles

- Adaptation logic centralized at the 5G-RG.
- Minimal impact on end-devices and 5GC.



Framework Concept and Architecture

Overall Architecture

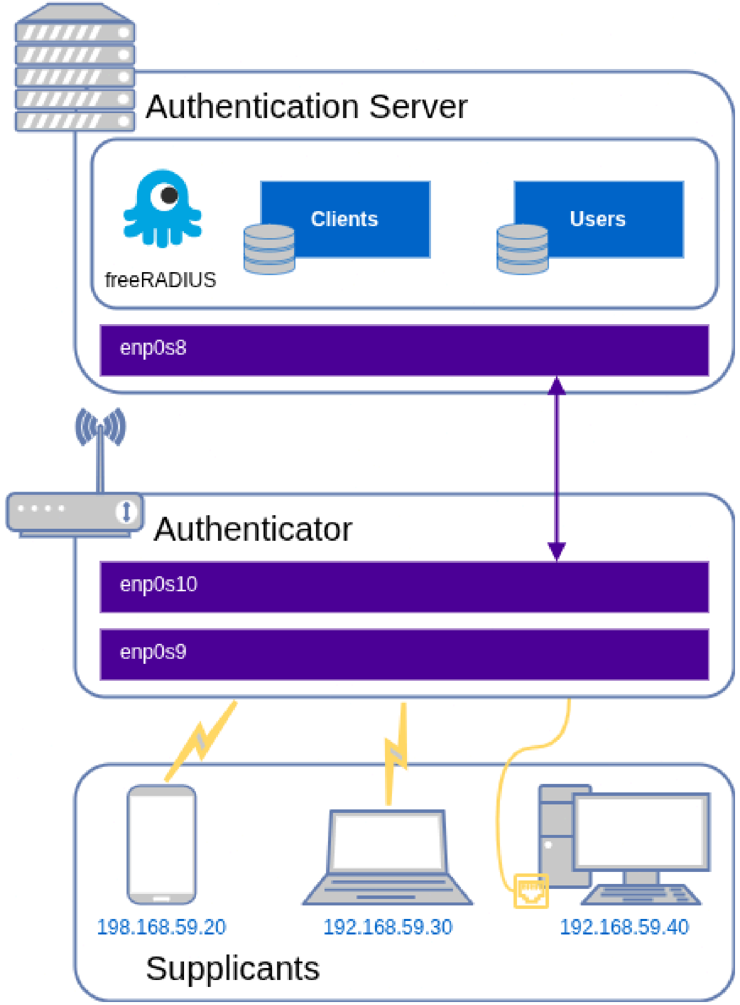


Framework Concept and Architecture

Authentication Mechanism

EAP-TLS is used for mutual, certificate-based local authentication.

- NAUN3 Device (**Supplicant**): Holds a client certificate.
- 5G-RG (**Authenticator**/Relay): Uses hostapd to relay EAP messages.
- RADIUS **Authentication Server**: ISP-operated, validates the device's certificate.

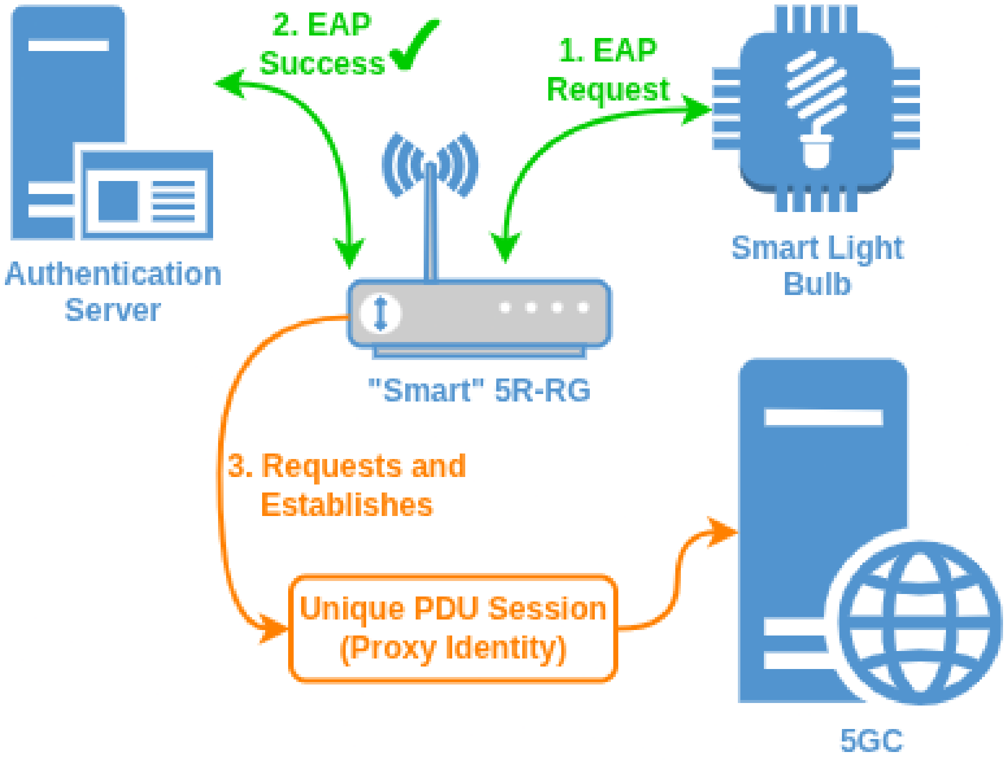


Framework Concept and Architecture

Identity Management (PDU Session as Proxy)

After successful EAP-TLS authentication:

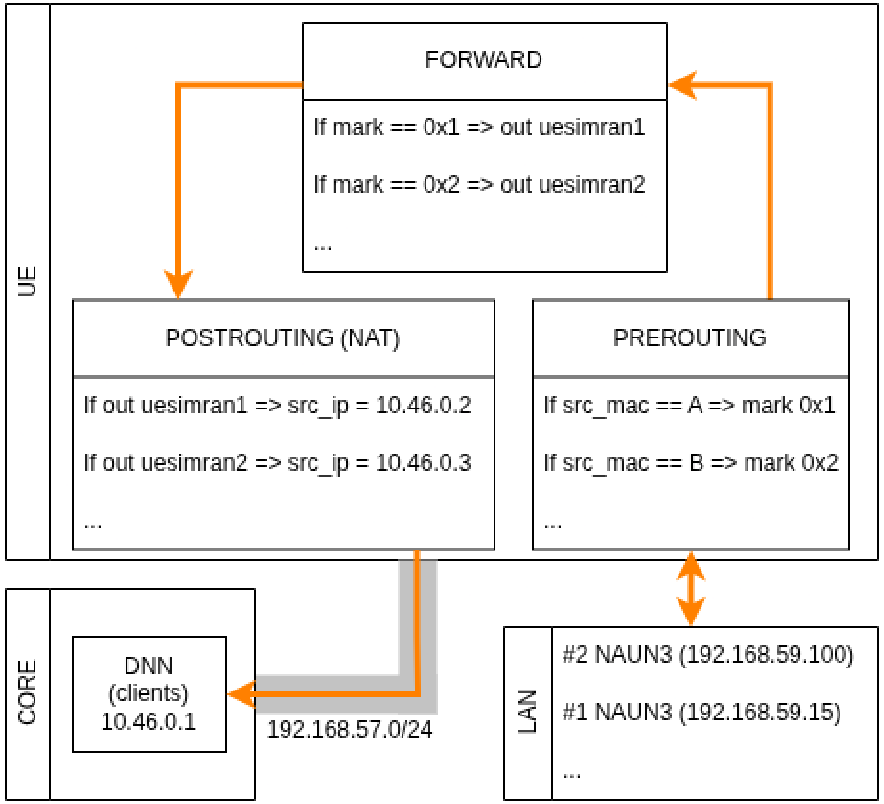
1. The 5G-RG requests a **new, dedicated** PDU Session.
2. This PDU Session becomes the **dynamic proxy identity** for the NAUN3.
3. The 5G-RG maintains a **mapping table** with NAUN3 MAC Addresses to PDU Session ID.



Framework Concept and Architecture

Traffic Management and Policy-Based Routing

1. **Packet Marking:** Incoming packets from the NAUN3's MAC are marked.
2. **Policy Routing:** Marked packets are directed to a specific table.
3. **Dedicated Route:** Traffic is routed via to a unique PDU interface.
4. **NAT:** Traffic is then masqueraded using the PDU session's 5GC-assigned IP address.



UE

FORWARD

If mark == 0x1 => out uesimran1

If mark == 0x2 => out uesimran2

...

POSTROUTING (NAT)

If out uesimran1 => src_ip = 10.46.0.2

If out uesimran2 => src_ip = 10.46.0.3

...

PREROUTING

If src_mac == A => mark 0x1

If src_mac == B => mark 0x2

...

CORE

DNN (clients) 10.46.0.1

192.168.57.0/24

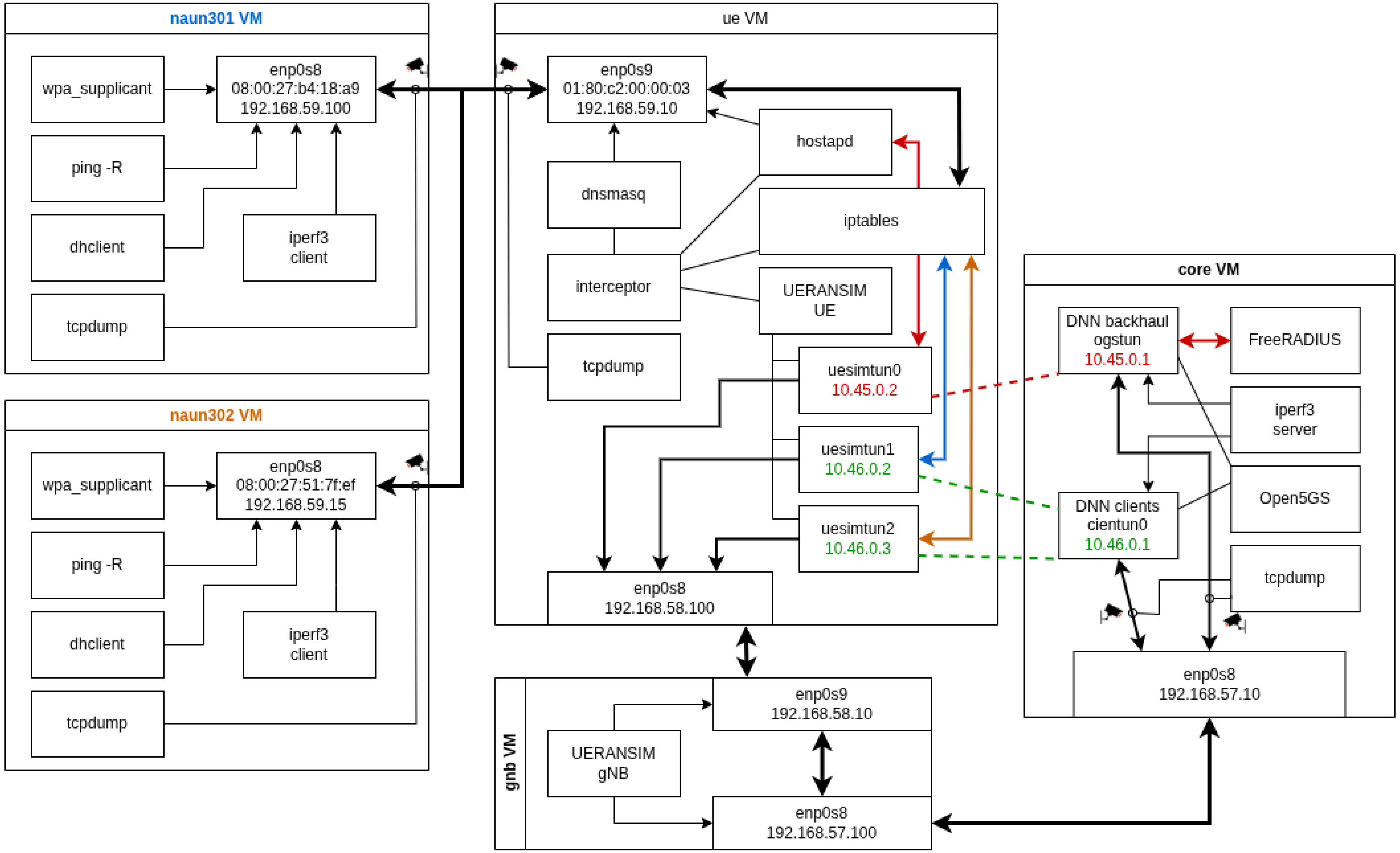
LAN

#2 NAUN3 (192.168.59.100)

#1 NAUN3 (192.168.59.15)

...

Testbed, Components, and `interceptor` Logic


naun301 VM
wpa_supplicant
enp0s8
08:00:27:b4:18:a9
192.168.59.100
ping -R
dhclient
iperf3
client
tcpdump
naun302 VM
wpa_supplicant
enp0s8
08:00:27:51:7f:ef
192.168.59.15
ping -R
dhclient
iperf3
client
tcpdump
ue VM
enp0s9
01:80:c2:00:00:03
192.168.59.10
hostapd
dnsmasq
iptables
interceptor
UERANSIM
UE
tcpdump
uesimtun0
10.45.0.2
uesimtun1
10.46.0.2
uesimtun2
10.46.0.3
enp0s8
192.168.58.100
gnb VM
UERANSIM
gNB
enp0s9
192.168.58.10
enp0s8
192.168.57.100
core VM
DNN backhaul
ogstun
10.45.0.1
FreeRADIUS
iperf3
server
DNN clients
cientun0
10.46.0.1
Open5GS
tcpdump
enp0s8
192.168.57.10