IEEE Communications Society (ComSoc)
Technical Committee on Communications Quality & Reliability (CQR)
Emerging Technology Reliability Roundtable 2024 (ETR-RT24)
May 21-22 (Tuesday-Wednesday), 2024
Lisbon, Portugal

# Security and Reliability in Heterogeneous Networks


Peter Thermos
21 Roszel Road, Suite 105,
Princeton, NJ 08540
peter.thermos@palindrometech.com
www.palindrometech.com


IEEE ComSoc IEEE Communications Society

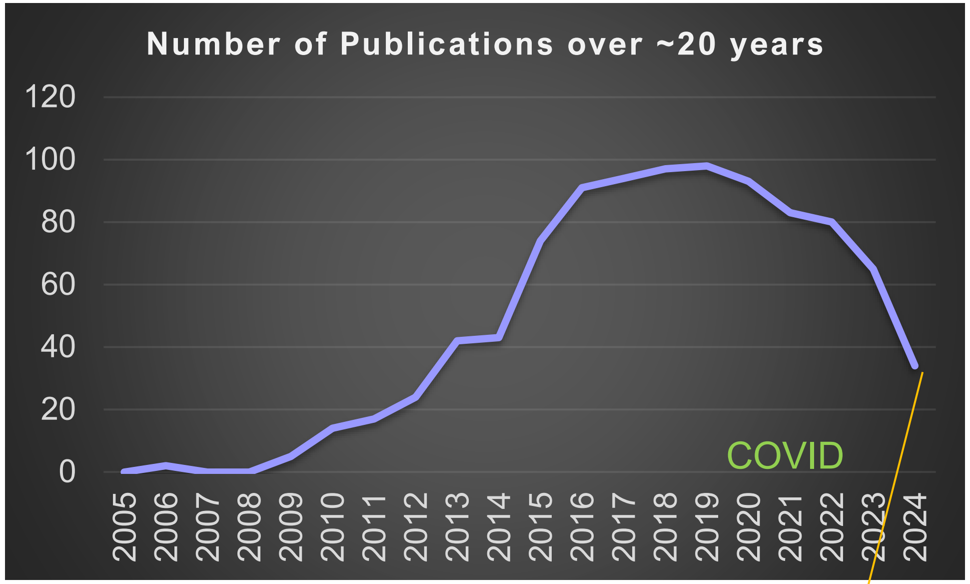
Palindrome Technologies
ASSURANCE | TRUST | CONFIDENCE

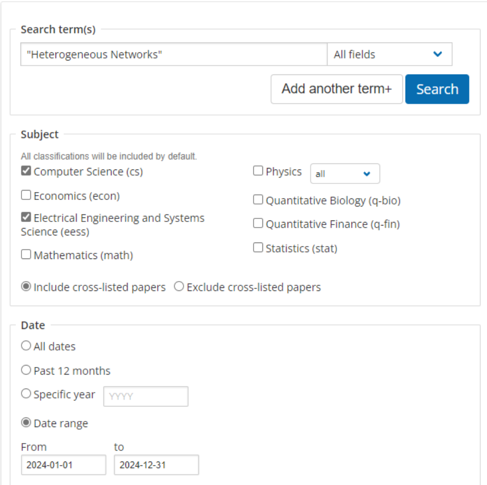
# Agenda

- HetNets – background
- Security and Reliability Challenges
  - *Interference*
  - *Complexity*
  - *Security*
- Hydra – Research Prototype

# HetNets Background

- Volume of research papers on “HetNets” has steadily increase over time. This slowed down during COVID but resuming attention thereafter
- HetNets vs Heterogeneous Networks:
  - *HetNets are focused on implementations that use the same shared spectrum and same wireless technology, for example LTE*
  - *Heterogeneous networks include different network access technologies (e.g., 5G, WiFi) and different providers*

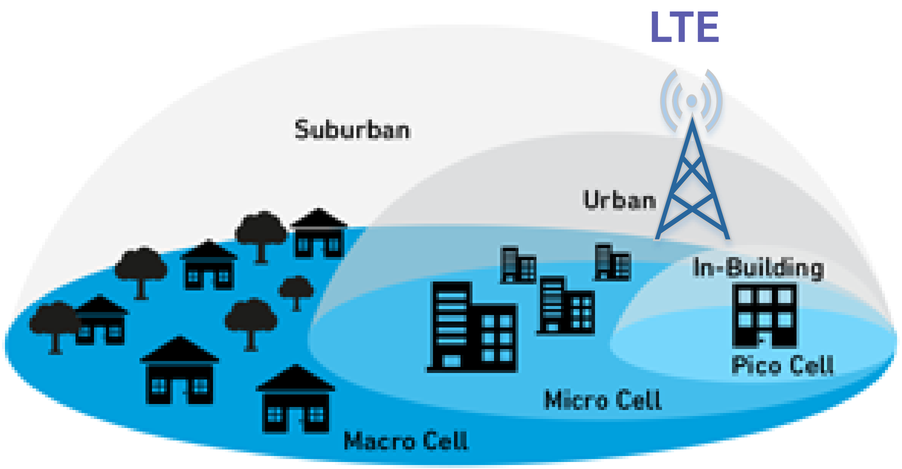


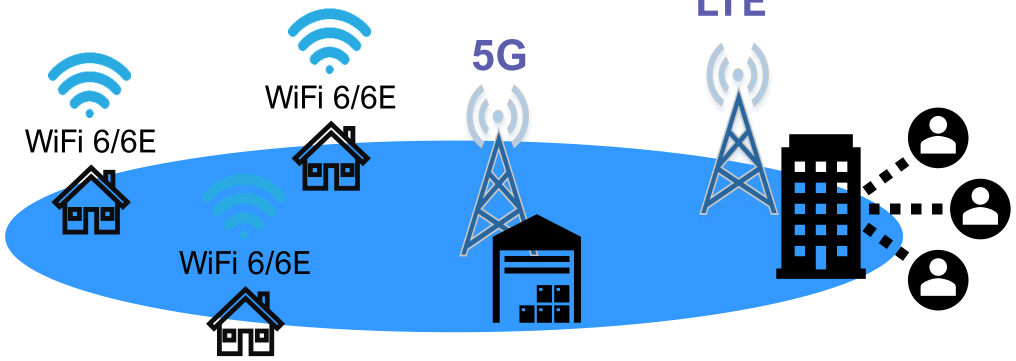

Q1 of 2024 had 34 published papers which is about 30 greater compared to prior years

# HetNet Technologies

- Current solutions and limitations:
  - *Coexist in shared spectrum (e.g., LTE & WiFi offered in the 3.5 Ghz)*
  - *Focusing only on Radio Interference (*Inter Cell Interference Coordination - *ICIC)*
  - Vendor proprietary
  - *Unpredictable performance*
  - *Unified Network Access and Security*
  - *Lack of intelligent orchestration across disparate RF technologies and vendors*




HetNets vs Heterogeneous Networks



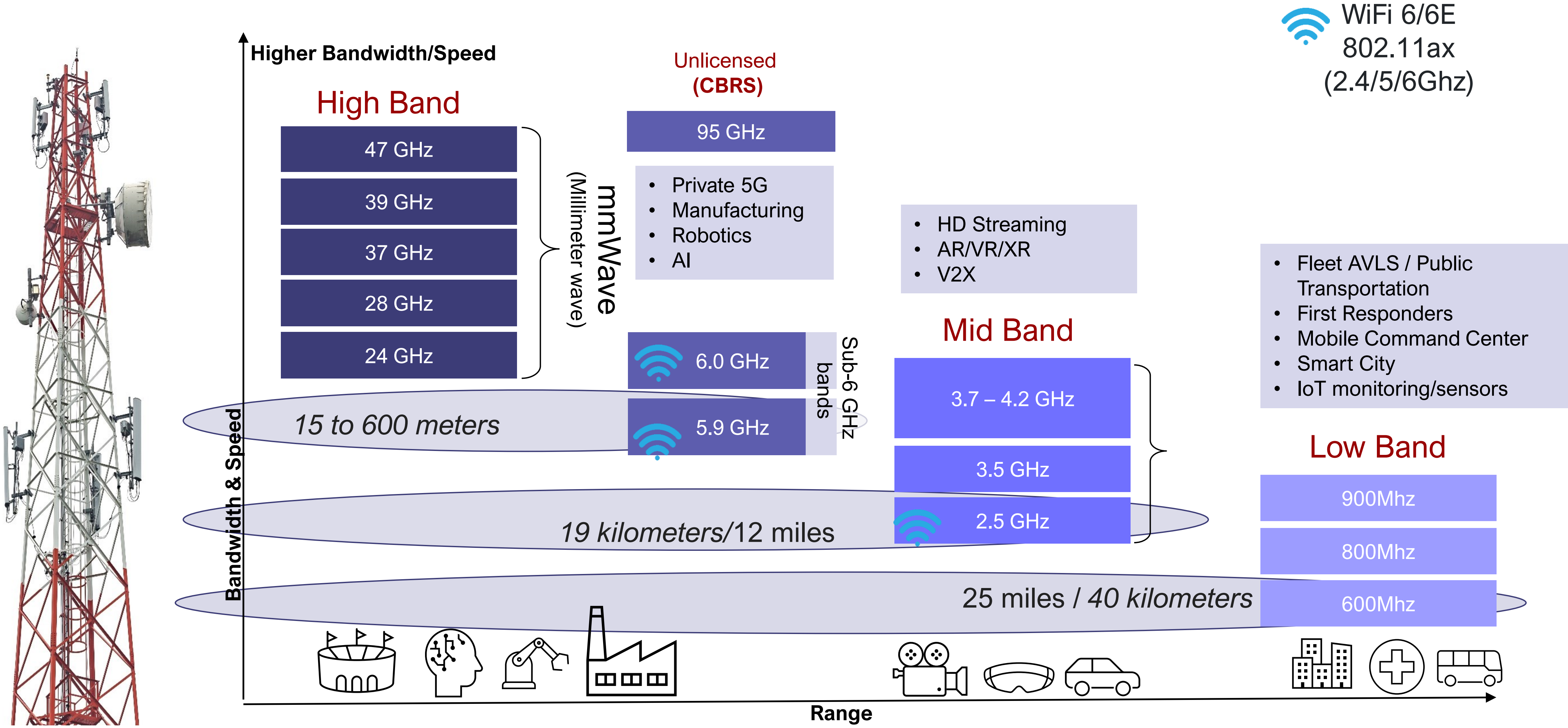
# Hetnet Control Frameworks

- Network centric HetNets
- Client Controlled HetNets
- Hybrid Controlled HetNets

"While transport layer protocols tend to optimize for traditional QoS metrics such as throughput, latency and loss, application layer-based multihoming can consider additional factors such as economic cost and content sharing."

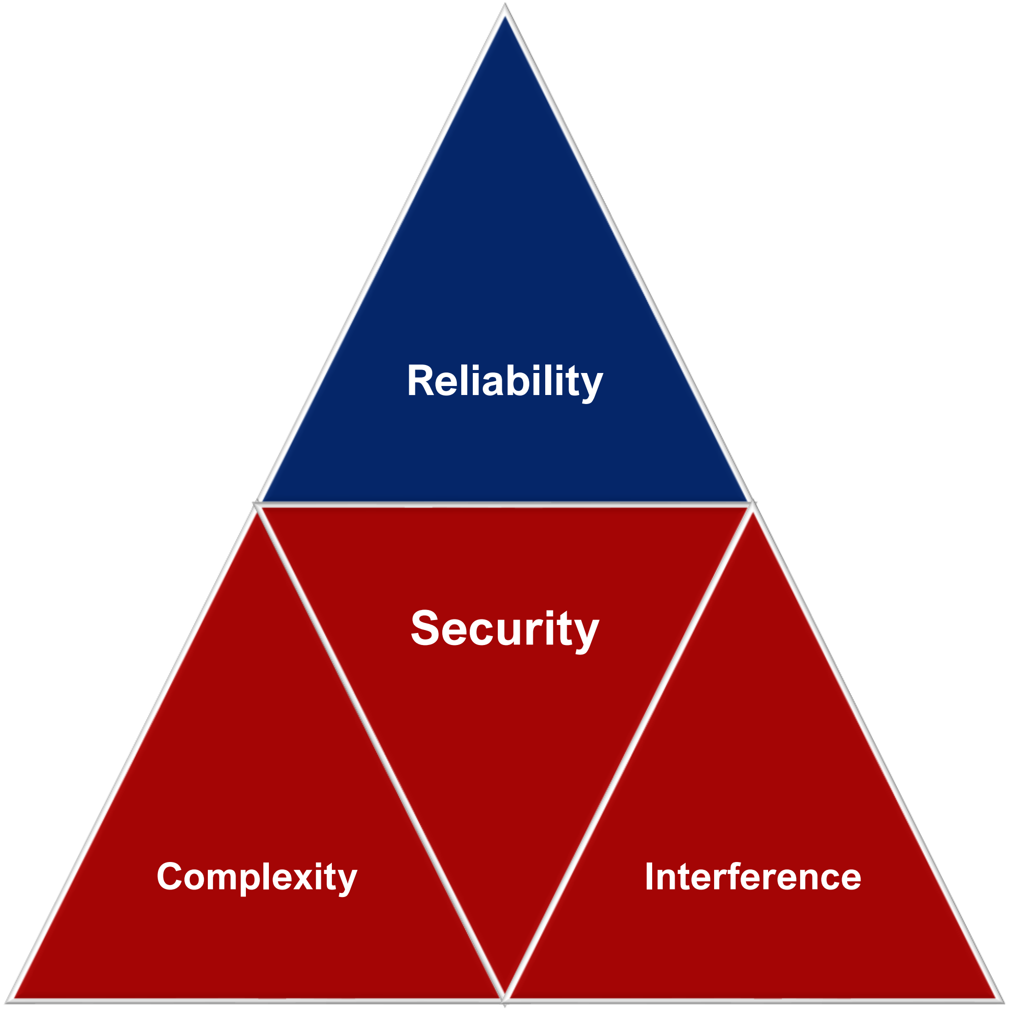
[IEEE "A Survey of Client-Controlled HetNets for 5G", M. Wang, J. Chen, E. Aryafar, M. Chiang, March 2017]

# 5G & WiFi 6 bands



# Security and Reliability Challenges

- Interference
- Complexity
- Security

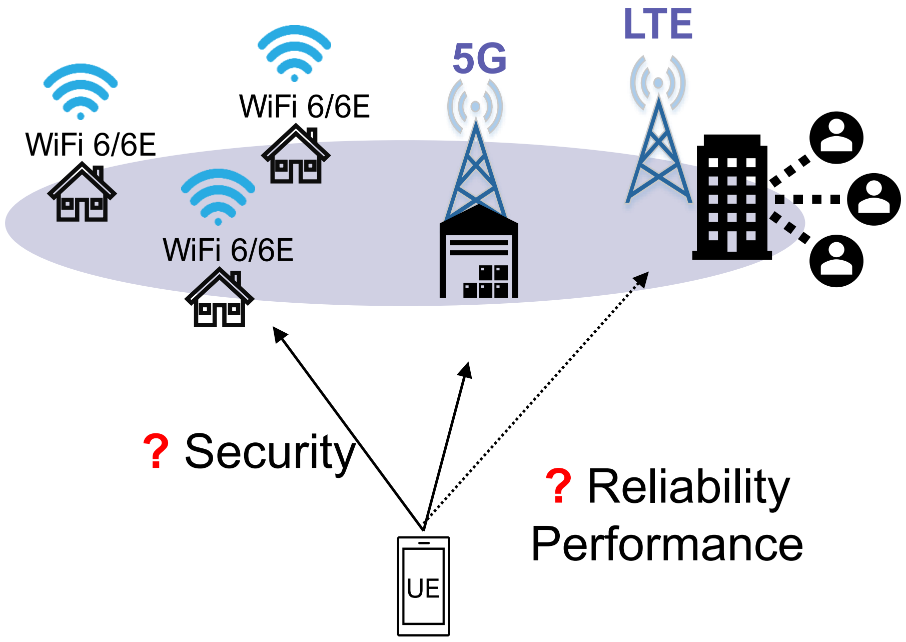


# Challenges

Heterogeneous networks (e.g., 5G/CBRS, WiFi 6/6E) introduce three core challenges, namely:

Inter-dependent

- ***Reliability***
- ***Security***
- ***Interference***
- ***Complexity of network interfaces and access methods***




User experience (QoE)

- Disruption due inconsistent network selection
- Mobility management
- Spectrum Interference

# Interference

- 5G operates in a crowded and dynamic spectrum environment that can cause interference among different users, devices, and networks. Interference can degrade the signal quality and reduce the network capacity and coverage.
- WiFi 6 uses 6 GHz band, in addition to the 2.4 GHz and 5 GHz. However, 6 GHz band is also used by other devices and services, such as satellite communications, radars, and microwave ovens, which may cause interference and degrade the signal quality of WiFi 6.

# Complexity

- Backward compatibility
  - *Legacy devices cannot take advantage of WiFi 6 capabilities*
- Range limitations
  - *Wi-Fi 6 and Wi-Fi 6E use higher frequencies and more complex modulation schemes to achieve faster speeds, but this can also result in reduced range compared to previous Wi-Fi standards.*
- 5G Complexity
  - *The complexity of 5G increases the risk of errors, failures, and vulnerabilities that can compromise the reliability of the network. For example, 5G uses a heterogeneous network architecture that integrates different types of access networks, such as cellular, Wi-Fi, and satellite.*

# Security Challenges

- **5G Security**
  - 5G exposes a larger attack surface and more potential entry points for malicious actors, due to its increased complexity, heterogeneity, and connectivity.
  - 5G supports critical and sensitive applications, such as autonomous vehicles, smart grids, and remote surgery, that require high levels of security and trust.
  - 5G involves multiple stakeholders and entities, such as network operators, service providers, device manufacturers, and users, that need to cooperate and coordinate to ensure the security of the network.
- **WiFi Security**
  - WiFi 6 introduces a new security protocol, called WPA3
  - However, WPA3 also has some vulnerabilities and flaws, such as the Dragonblood
  - WiFi 6 devices and access points may not support WPA3, or may support different versions or configurations of WPA3, which may create compatibility and interoperability issues.

# 5G Threat Domains – Top 10

1. Hardware (UE, IoT devices, gNB/eFemtos/extenders)
2. RAN Signaling
3. 5G Core Signaling
4. Network Slicing
5. Network Peering Functions – Security Edge Protection Proxy (SEPP)
   - *Partner networks*
6. Network Exposure Functions (NEF)
7. Network Infrastructure (fronthaul/mid-haul/backhaul)
8. Virtualization / Cloud Infrastructure / MEC (Multi-access Edge Computing)
9. Management and Network Orchestration Applications (MANO/OAM&P/OSS)
10. Software Supply Chain (SBOM)

# 4/5G Threats & Attacks

- **Traffic Analysis & Eavesdropping**
  - *Active / Passive eavesdropping*
  - *IMSI catching*
  - *4G and 5G user location tracking*
  - *GPRS encryption cryptanalysis*
  - *Hijacked TCP connection eavesdropping*
  - *VoLTE eavesdropping*
  - *Privacy attacks using side channel information*
  - *Dragonfly Handshake (*attacker can decrypt all data that the victim transmits*)*
- **Impersonation**
  - *5G/4G/3G to 2G downgrade*
  - *Impersonating calls and texts*
  - *FBS enabled LTE billing compromise*
  - *WiFi Evil Twin (Man in the middle attack)*

- **Service Disruption / Annoyance**
  - DoS attack against mobile device
  - DoS attack against the network
  - Radio jamming
  - SMS spam

# 4G / 5G / WiFi - Example Attacks

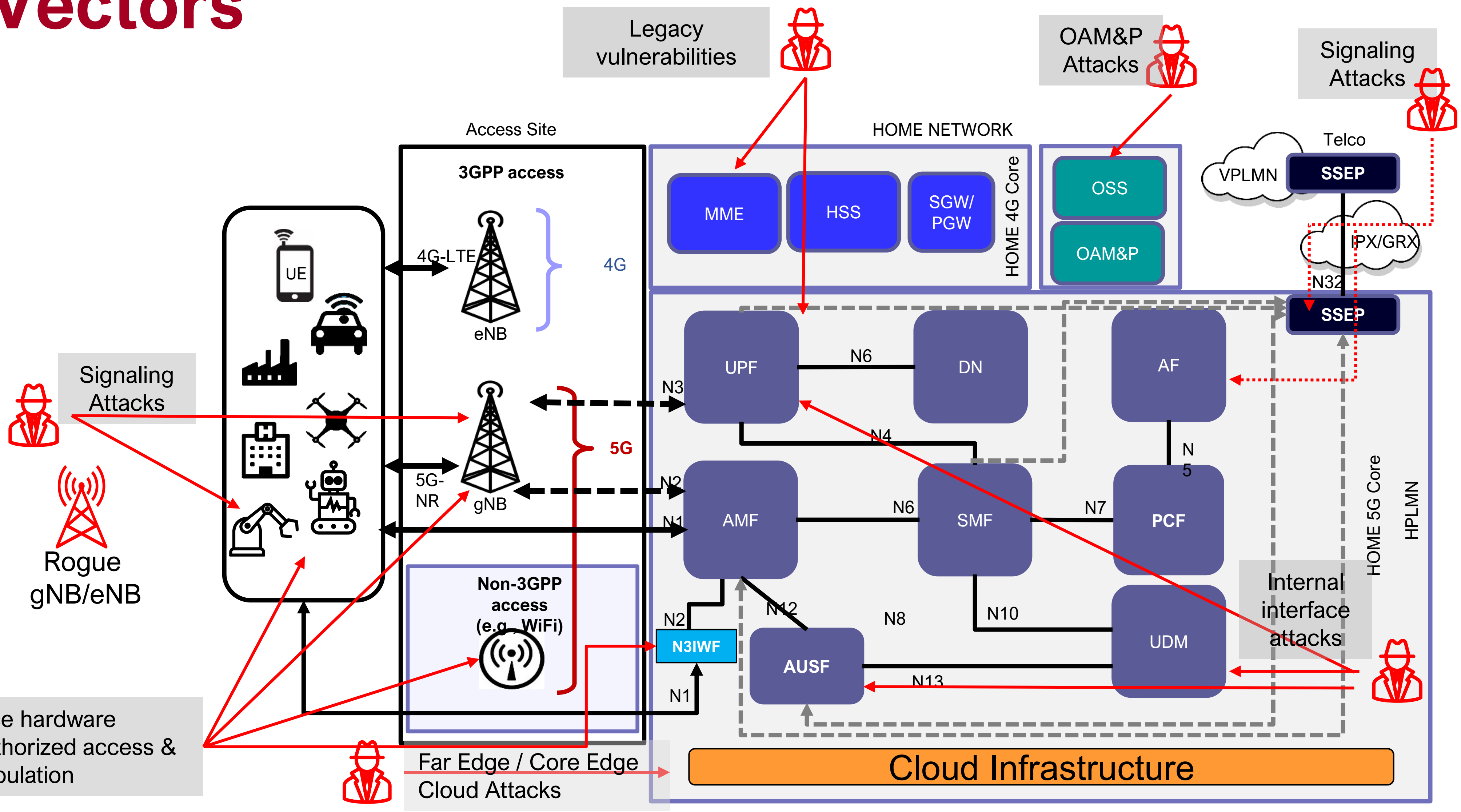
- **5G Security**
  - TORPEDO - PRIVACY (LOCATION)
  - PIERCER - PRIVACY (IDENTITY)
  - IMSI CRACKING - PRIVACY (IDENTITY)
  - IMP4GT: IMPersonation Attacks in 4G NeTworks
  - Identity Mapping - RNTI and TMSI Mapping (Passive)
  - Website Fingerprinting -Layer 2 scheduling metadata (Passive)
  - ALTER - Lack of Layer 2 Integrity protection (Active)
- **WiFi Security**
  - KRACK attacks (**K**ey **R**einstallation **A**tta**ck**s)
  - Dragonblood attack
  - FragAttacks (**fr**agmentation and **ag**gregation **attacks**)

# Co-existence Security Issues

- **Handover security**
  - Latency of complex authentication and handshake protocols cannot be tolerated
  - Opportunity for attacks during handoff (e.g.,, Rogue-Base-Station, DoS) due to weak state of connectivity
- **Spectrum attacks (CRN's)**
  - **Spectrum Depletion => Service degradation or disruption**
    - Jamming / Eavesdropping
  - **Spectrum sensing attacks**
    - Primary User Emulation (PUE) Attack
    - Spectrum Sensing Data Falsification (SSDF) attack
      - a malicious user transmits the deceived sensing information in order to make an inaccurate decision of the activity of PU
  - **Spectrum information inference attack (DIA)**
    - malicious attackers can collect sensitive operational data of both incumbent users (IUs) and Secondary Users (SU), which makes privacy protection critical in this paradigm

# Attack Vectors

- Application
- Signaling
- Transport/Backhaul Network
- Cloud/OS
- Hardware



# Mitigation Strategies

- Spectrum interference & management
- Signaling and User Plane Protection
  - *Rogue Base Station*
    - Deploy and implement two-way authentication and Subscription Permanent Identifier (SUPI) encryption for later technologies. Enforce the use of Subscription Concealed Identifier (SUCI) per 3GPP specification
    - Use a network management system or signalling monitoring system to detect the presence of Fake Base Station (FBS).
    - Network radio detection: Changes in the radio measurements within the radio network can also be used to detect radio signals from FBS by monitoring the following parameters to identify unusual patterns
- Network API Security
- Network Element Configuration
  - *Zero Trust Principles / Defense in depth*
  - ***Trust but Verify*** *- Security Assurance Testing*

Thank you

?

# Contacts

**Peter Thermos**
MSc, CGEIT, CDPSE,
FITSP, CCSFP
Founder & CTO

Cell: +1(732) 688-0413
Peter.thermos@palindrometech.com

**21 Roszel Road, Suite #105**
**Princeton, 08540 NJ, USA**
**www.palindrometech.com**

**Sony Cherukara**
CISSP
VP Security Engineering & Ops

Cell: +1 908 347-6650
Sony.cherukara@palindrometech.com

**21 Roszel Road, Suite #105**
**Princeton, 08540 NJ, USA**
**www.palindrometech.com**

**Aman Singh**
Chief Scientist
Security Research

Cell: +1 (917) 257-8369
Aman.singh@palindrometech.com

**21 Roszel Road, Suite #105**
**Princeton, 08540 NJ, USA**
**www.palindrometech.com**

**Thomas Marks**
Principal

Office: +1 (844) 429-2792
Thomas.marks@palindrometech.com

**21 Roszel Road, Suite #105**
**Princeton, 08540 NJ, USA**
**www.palindrometech.com**

**Shashank Murali**
Sr. Security Engineer

Cell: +1 (929) 213-7010
Shashank.murali@palindrometech.com

**21 Roszel Road, Suite #105**
**Princeton, 08540 NJ, USA**
**www.palindrometech.com**