International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Security Challenges and Solutions in Private Wireless (LTE/5G) Network Implementations

Rahul Bangera

Ellicott City, MD, USA.
rahulmbangera@gmail.com

Abstract:
The digitalization of critical infrastructure, often called Industry 4.0, has accelerated quickly, especially the adoption of private wireless networks. While Private Long-Term Evolution (LTE) and Fifth Generation (5G) networks offer greater determinism and reliability than Wi-Fi, they also present a unique and evolving threat landscape. This paper analyzes the security architecture of private cellular networks, comparing the legacy vulnerabilities of LTE with the "secure-by-design" enhancements of 5G Standalone (SA) architecture. It examines critical risks, including signaling attacks on the Service-Based Architecture (SBA), side-channel vulnerabilities in network slicing, and physical layer jamming. Additionally, we evaluate mitigation strategies such as Zero Trust Architecture (ZTA), AI-driven anomaly detection, and improvements introduced in 3GPP Releases 16 and 17.

Keywords: 5G, Long Term Evolution (LTE), HTTP/2 signaling, Industrial Internet of Things (IIoT), jamming mitigation, network slicing, Non-Public Networks (NPN), Zero Trust Architecture (ZTA).

I. INTRODUCTION

Private wireless networks are becoming the backbone of connectivity for mission-critical environments, including manufacturing, healthcare, and logistics. Unlike public networks, private networks (Non-Public Networks or NPNs) allow enterprises to retain data sovereignty and customize network parameters for specific Service Level Agreements (SLAs), such as ultra-low latency or massive machine-type communications [1].

However, the migration to 5G marks a paradigm shift from hardware-centric telecom architectures to cloud-native software environments. The 5G Core (5GC) relies on a Service-Based Architecture (SBA) that uses standard IT protocols like HTTP/2 and JSON. While this enhances flexibility, it also exposes the network to web-based vulnerabilities previously unfamiliar to the telecommunications domain [2]. Additionally, deploying private networks requires enterprises to assume roles traditionally held by Mobile Network Operators (MNOs), which demands a deep understanding of cellular security protocols.

This paper offers a technical analysis of these challenges, supported by recent academic research and industry standards. It compares deployment models, examines the threat surface, and proposes robust defense mechanisms tailored for private implementations.

II. PRIVATE NETWORK DEPLOYMENT MODELS

The security posture of a private network is strongly influenced by its architectural design. 3GPP Technical Specifications outline two main models for NPNs: Standalone Non-Public Networks (SNPN) and Public Network Integrated Non-Public Networks (PNI-NPN) [3] [4].

A. Standalone Non-Public Networks (SNPN)

An SNPN operates independently from the public mobile network. The enterprise manages the Radio Access Network (RAN), the Core Network, and the subscriber database (Unified Data Management or

UDM).

- **Security Advantage:** SNPNs provide physical isolation (air-gapping) from the public internet and PLMN, eliminating attack vectors from remote external attackers [3].
- **Identity Management:** Enterprises can issue their own credentials (SIM/eSIM) and implement custom authentication policies, such as EAP-TLS, to integrate with existing corporate PKI [5].

B. Public Network Integrated NPN (PNI-NPN)

In this model, the private network shares resources (RAN or Control Plane) with a public PLMN, using Network Slicing to logically separate enterprise traffic. In this model, the private network shares resources (RAN or Control Plane) with a public PLMN, using Network Slicing to logically separate enterprise traffic.

- **Closed Access Groups (CAG):** To secure the shared RAN, CAGs create allow-lists that ensure only authorized devices can access the private cells [4].
- **Security Risks:** Relying on shared infrastructure can lead to MNO configuration errors and potential side-channel attacks if logical isolation fails to prevent resource leakage between slices [6].

Table 1: Comparative Analysis of Deployment Models Comparative Analysis of Deployment Models

Feature	Standalone NPN (SNPN)	PNI-NPN (Integrated)	Security Implication
Isolation	Physical (Air-gapped)	Logical (Slicing)	SNPN prevents external pivoting; PNI-NPN relies on MNO trust.
Data Sovereignty	Local on-premise	Varies (Local Breakout)	SNPN ensures data never leaves the facility.
Auth Control	Enterprise (Full Control)	MNO (SIM based)	SNPN allows custom auth (e.g., certificate-based).
Threat Surface	Localized	Extended to PLMN	PNI-NPN inherits roaming and signaling vulnerabilities.

III. COMPARATIVE SECURITY: PRIVATE LTE VS. PRIVATE 5G

While LTE offers strong connectivity, 5G introduces essential security improvements to address known vulnerabilities from earlier generations.

A. Subscriber Identity Privacy

- **LTE Weakness:** LTE networks transmit the International Mobile Subscriber Identity (IMSI) in clear text during the initial attach process. This enables adversaries to use "IMSI Catchers" to identify and track specific users or devices [7].
- **5G Enhancement:** 5G replaces the IMSI with the Subscription Permanent Identifier (SUPI). Importantly, the SUPI is never transmitted in the clear. It is encrypted with the Home Network Public Key to create a Subscription Concealed Identifier (SUCI) before being sent over the air [8]. This makes traditional IMSI catchers ineffective against 5G SA networks unless the "Null Scheme" (no encryption) is used. Recent field studies show that while the standard supports this, actual implementation varies by vendor and operator [9].

B. User Plane Integrity

- **LTE Weakness:** LTE encrypts user data but lacks integrity protection. A "Man-in-the-Middle" attacker could theoretically modify the ciphertext (bit-flipping) undetected, potentially altering commands in industrial control systems [5] [9].
- **5G Enhancement:** 5G introduces User Plane Integrity Protection (UPIP) over the N3 interface.

This ensures that any modification to data packets during transit is detected and rejected, which is a critical requirement for Ultra-Reliable Low Latency Communications (URLLC) in safety-critical systems [8].

IV. THE THREAT LANDSCAPE OF PRIVATE 5G

The use of cloud-native technologies and shared resources in 5G introduces new security vulnerabilities.

A. Signaling Exploits in the Service-Based Architecture (SBA)

The 5G Core utilizes HTTP/2 for communication among Network Functions (NFs).

- **HTTP/2 Attacks:** Vulnerabilities such as "Stream Multiplexing" enable an attacker to flood a critical NF (e.g., the AMF) with multiple streams simultaneously, resulting in a Denial-of-Service (DoS) attack. Also, "HPACK Bomb" attacks can leverage header compression to drain memory resources [2].

B. Network Slicing and Side-Channel Attacks

In multi-tenant PNI-NPN environments, slices share physical compute resources (CPU, cache).

- **Cache Side-Channels:** Research shows that malicious tenants can exploit the shared Last Level Cache (LLC) to extract sensitive information from a co-located victim slice, such as through Prime+Probe attacks. This damages the logical isolation that slicing provides [6].
- **Mitigation Difficulty:** Addressing these hardware-level vulnerabilities requires strict resource pinning or "cache coloring," which can decrease resource efficiency [10].

C. Physical Layer Jamming

Smart jammers using Machine Learning (ML) can target specific 5G control channels (PDCCH) or synchronization signals (SSB), disrupting communication with high energy efficiency. In industrial settings, this can disable autonomous mobile robots (AMRs). Recent studies employing computer vision on spectrograms have demonstrated high accuracy in detecting and classifying these jamming types in real-time private network environments [11].

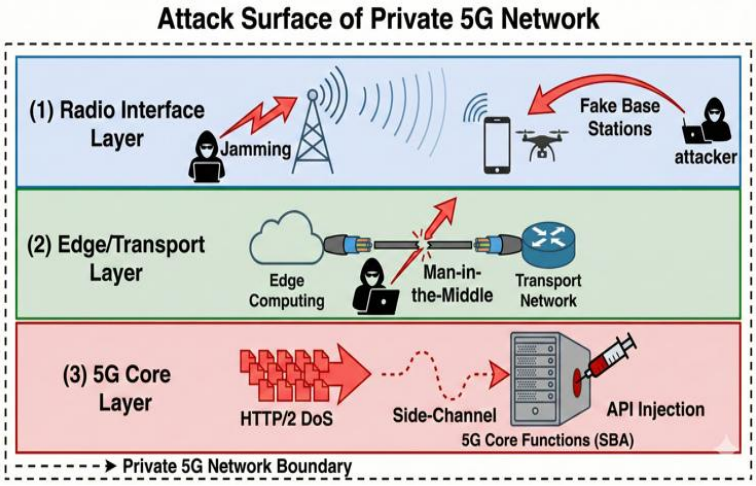

Figure 1: Types of potential threat landscapes in Private 5G Network solutions

V. ADVANCED MITIGATION SOLUTIONS

Securing private networks demands a multi-layered defense approach combining IT security principles with telecommunications standards.

A. Zero Trust Architecture (ZTA) Implementation

Traditional perimeter defenses are inadequate for the 5G SBA. A Zero Trust approach requires that no entity is trusted by default [12].

- **Micro-Segmentation:** All traffic between NFs must be authenticated and encrypted using Mutual TLS (mTLS). The Network Repository Function (NRF) should serve as a Policy Decision Point, authorizing NFs to communicate only if explicitly permitted [13].
- **Policy Control:** The Policy Control Function (PCF) should enforce detailed access rules based not only on identity but also on device context, location, and health status [12].

B. AI-Driven Anomaly Detection

To combat the rapid pace of automated attacks, defenders need to leverage AI.

- **Signaling Defense:** Solutions like "5GShield" use ML to analyze typical HTTP/2 traffic patterns between NFs. They can identify deviations indicating signaling storms or probing attacks with high accuracy (F1-score > 0.99) [8].
- **Anti-Jamming:** The RAN Intelligent Controller (RIC) can utilize Deep Reinforcement Learning (DRL) algorithms to detect jamming in real time and automatically adjust radio parameters (e.g., frequency hopping) to sustain connectivity [11].

C. 3GPP Release 16 Enhancements

- **Secondary Authentication:** Release 16 enables a device to be authenticated by an external AAA server (managed by the enterprise) after the initial network connection. This supports EAP-TLS and integrates the device into the corporate IT security domain [5].

VI. CONCLUSION

The transition to Private 5G networks offers significant transformative potential for the industry but requires a sophisticated security approach. Although 5G addresses LTE's privacy and integrity issues through features like SUPI encryption and UPIP, its cloud-native core introduces Web-IT vulnerabilities. Organizations need to move beyond mere compliance by adopting Zero Trust Architectures, leveraging AI for real-time security, and implementing the latest 3GPP security protocols. Treating the private network as a critical IT/OT asset rather than just a utility enables enterprises to secure the foundation of their digital transformation.

REFERENCES:

1. Infosys, "Private 5G deployment models for enterprises," Infosys Ltd., Bengaluru, India, White Paper, 2023. [Online]. Available: [https://www.infosys.com/services/engineering-services/white-paper/documents/private-5g-deployment.pdf].
2. N. Wehbe, H. A. Alameddine, M. Pourzandi, E. Bou-Harb, and C. Assi, “A security assessment of HTTP/2 usage in 5G service based architecture,” *IEEE Communications Magazine*, vol. 61, no. 1, pp. 48–54, Jan. 2023.
3. H. Frank, C. Colman-Meixner, K. D. R. Assis, S. Yan, and D. Simeonidou, “Techno-economic analysis of 5G non-public network architectures,” *IEEE Access*, vol. 10, pp. 70204–70218, 2022, doi: 10.1109/ACCESS.2022.3187727.
4. *Management and Orchestration; Management of Non-Public Networks (NPN)*, 3GPP TS 28.557 V17.0.0, 3rd Generation Partnership Project (3GPP), 2022.

5. *Security Architecture and Procedures for 5G System*, 3GPP TS 33.501 V17.0.0, 3rd Generation Partnership Project (3GPP), 2022.
6. W. Shao, C. Thapa, R. Holland, S. A. Siddiqui, and S. Camtepe, "Attacking slicing network via side-channel reinforcement learning attack," *arXiv preprint arXiv:2409.11258*, 2024. [Online]. Available: [https://arxiv.org/pdf/2409.11258]
7. Vertu, "4G vs 5G phone security: Network, privacy & vulnerabilities," *Vertu*, Aug. 12, 2025. [Online]. Available: [https://vertu.com/lifestyle/4g-vs-5g-phone-network-security-encryption-privacy-risks/].
8. N. Wehbe, H. A. Alameddine, M. Pourzandi, and C. Assi, "5GShield: HTTP/2 anomaly detection in 5G service-based architecture," in *2023 IFIP Networking Conf. (IFIP Networking)*, Barcelona, Spain, Jun. 2023, pp. 1–9. [Online]. Available: [https://dl.ifip.org/db/conf/networking2023/networking2023/1570888295.pdf]
9. O. Lasierra, N. Ludant, G. Garcia-Aviles, E. Municio, G. Noubir, A. Skarmeta, and X. Costa-Pérez, "Fact-checking 5G security: Bridging the gap between expectations and reality," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 6242–6257, 2025, doi: 10.1109/OJCOMS.2025.3593140.
10. D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2518–2542, 3rd Quart., 2018.
11. R. Chitauro, M. Brzozowski, O. Yener, and P. Langendörfer, "Real-time jamming detection, classification and logging using computer vision in 5G private networks," in *2024 19th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Rio de Janeiro, Brazil, 2024, pp. 1–6, doi: 10.1109/ISWCS61526.2024.10639080.
12. 5G Americas, "5G technologies for private networks," 5G Americas, Bellevue, WA, USA, White Paper, Oct. 2020. [Online]. Available: [https://www.5gamericas.org/wp-content/uploads/2020/10/InDesign-5G-Technologies-for-Private-Networks-WP.pdf].
13. J. Olsson, A. Shorov, L. Abdelrazek, and J. Whitefield, "Zero trust and 5G – Realizing zero trust in networks," *Ericsson Technology Review*, no. 5, pp. 2–11, May 2021. [Online]. Available: [https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g].