Pushing the Limits of 5G Private Networks: A Practical Examination of Network Stressors

Onur Yener, Marcin Brzozowski, Ronald Chitauro, and Peter Langendörfer
IHP - Leibniz-Institut für Innovative Mikroelektronik,
Im Technologiepark 25,
15236 Frankfurt (Oder),
Germany.
Email: {yener, brzozowski, chitauro, langendoerfer}@ihp-microelectronics.com

***Abstract*—The adoption of 5G private networks is revolutionizing industrial connectivity, yet it brings numerous challenges that need addressing to ensure safety and reliability. Our research utilizes an OpenAirInterface (OAI) based 5G testbed to explore and mitigate these challenges. We particularly focus on stressors such as jamming to evaluate network resilience. Our methodology involves setting up a comprehensive testbed, collecting data under various stress conditions, and implementing solutions. Initial findings demonstrate that small environmental changes and structural interferences significantly impact network performance. We observed that indoor variables and uplink communication pose substantial challenges, underscoring the need for advanced algorithms to detect and mitigate jamming attacks in dynamic scenarios. Our results highlight the importance of real-time spectrum analysis and adaptive network management in maintaining optimal performance. This study aims to contribute to the development of robust, resilient 5G networks suitable for complex industrial environments.**

***Index Terms*—5G Private Networks, OpenAirInterface, Jamming, Network Stressors, Industrial Connectivity, Network Resilience**

I. Introduction

5G private networks are transforming industries with their enhanced connectivity. As industries adopt these networks, understanding and overcoming their challenges become significant. Deploying 5G networks in industrial environments presents several critical challenges, such as the potential for interference, security vulnerabilities, and ensuring reliable communication in demanding conditions. This study focuses on identifying and mitigating these challenges, particularly in terms of reliability and security. For example, jamming is a key concern as it represents a deliberate stressor that can be activated by an attacker, potentially disrupting communication and leading to operational failures. Investigating the impact of such threats helps in developing robust solutions to enhance network resilience. Our research involves setting up a 5G testbed which was possible with OpenAirInterface (OAI) [1], an open-source software framework for implementing 4G and 5G mobile networks. This framework enables research, development, and testing of wireless communication systems. We use the advantages of OAI's open-source nature and flexibility, enhancing our testing environment with the integration of FlexRIC [2] which is a software development kit (SDK) that enables to build specialized service-oriented controllers on top of the network. This combination allows us to explore the limits of 5G network reliability in complex industrial setups. Challenges, such as jamming, will be tested on the 5G testbed and collectively referred to as "stressors" to evaluate the system's resilience and performance under various conditions. The practical part of the plan involves collecting data from different stressed scenarios, analyzing the data, and then implementing solutions, while we expect FlexRIC to play an important role in this process. The major contributions of this paper are:

- Introducing network stressors in private 5G network
- Explaining Jamming testbed configuration
- Clarifying preliminary results from the data which is collected during jamming.

The rest of the paper is structured as follows: In Section II, we dive into related works to position our contributions in the broader research landscape. We introduce stressors in private 5G networks in Section III. In Section IV, we describe our 5G testbed, detailing our hardware and software configurations, the jamming setup, and the parameters collected, shedding light on key indicators for developing smart algorithms. Moreover, we share valuable observations from our ongoing data collection phase, discussing preliminary results. We outline our future work in Section V and conclude our paper in Section VI.

II. Related Work

Campus networks and private 5G networks are becoming increasingly prevalent as organizations seek to leverage the benefits of advanced connectivity solutions. The deployment of these networks is driven by the need for enhanced security, reliability, and performance in industrial and academic environments. Consequently, significant research has emerged to address the various challenges associated with 5G networks.

Several papers provide comprehensive overviews of the general challenges in 5G networks. References [3], and [4] delve into the security concerns and potential solutions for 5G networks. These surveys offer valuable insights into the theoretical aspects of 5G security and challenges but do not necessarily involve experimental validation of these issues.

Our research aims to fill this gap by not only discussing the stressors affecting 5G networks but also experimentally

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

investigating one of the critical challenges: jamming and its impact on network performance.

In related experimental work, a few papers explore the intersection of open-source systems and jamming. One notable study [5] provides valuable insights using OAI to test jamming scenarios, it primarily focuses on uplink communication and does not conduct over-the-air experiments, which limits its applicability to real-world conditions. By combining theoretical insights with practical experimentation, our work contributes to a deeper understanding of how to ensure the resilience and reliability of private 5G networks in the face of various stressors, particularly jamming attacks.

III. Introduction To Stressors

In this section, we identify stressors as potential issues that can destabilize a 5G private network in an industrial environment.

A. Interference

Interference occurs when unwanted signals disrupt the intended 5G signal, leading to degraded signal quality and reduced data rates. Several common sources of interference in industrial environments include:

- Electromagnetic Interference (EMI): High-voltage machinery, power lines, and other industrial equipment generate electromagnetic fields that can disrupt signal transmission [6].
- Multi-Path Interference: When signals reflect off surfaces like walls, floors, and machinery, they create multiple signal paths that can interfere with each other. This can cause signals to arrive at the receiver at different times, resulting in phase shifts and signal degradation [7].
- Co-Channel Interference: Happens when multiple devices operate on the same frequency, causing mutual interference and reducing signal quality.
- Physical Obstructions: Barriers such as walls, buildings, and large machinery can block or absorb transmitted signals, weakening their strength and quality. These obstructions can also contribute to multi-path interference by creating reflective surfaces.

In 5G networks, signal quality is quantified using parameters such as Signal-to-Interference-plus-Noise Ratio (SINR) and Bit Error Rate (BER). SINR is a critical metric that indicates the quality of the received signal relative to interference and noise levels, directly impacting data throughput and reliability. Higher SINR values correspond to better signal quality and lower interference, while lower SINR values indicate significant interference and noise. BER measures the proportion of erroneous bits received compared to the total bits sent, with higher BER values signifying greater interference-related errors [8].

To mitigate interference, several network design strategies can be employed:

- Strategic Device Spacing: Proper spacing of devices to minimize co-channel interference.
- Frequency Management: Avoiding the use of shared radio frequencies to reduce co-channel interference.
- Antenna Placement and Shielding: Optimal positioning and shielding of antennas to mitigate physical and multi-path interference.
- Beamforming and MIMO (Multiple Input Multiple Output): Techniques that dynamically adjust signal paths to reduce interference and enhance SINR.
- Directional Antennas: Using directional antennas to focus the signal towards intended receivers and away from interference sources.

Even with these strategies, completely eliminating interference is challenging due to design constraints, equipment limitations, and dynamic environmental factors. Continuous monitoring and adaptive network management are essential to maintain optimal network performance. Real-time spectrum analysis and dynamic frequency selection are important in identifying and mitigating interference sources promptly.

B. Network Congestion

Network congestion occurs when the amount of data traffic exceeds what the network can handle, leading to delays in data transmission, lost data packets, and reduced data transfer rates. This problem can be caused by factors such as the number of connected devices and the type of data being transmitted. In situations where many sensors or devices are sending data at the same time, congestion can become a serious issue.

Network capacity refers to the maximum amount of data a network can handle at once. It depends on several factors:

- Bandwidth: This is the amount of data that can be transmitted in a given time period. Higher bandwidth means more data can flow through the network simultaneously.
- Latency: This is the delay in sending data from one point to another. Higher latency can make congestion worse.
- Network Design: The layout of the network, including how devices are connected, affects how efficiently data can be routed and managed.
- Device Performance: The ability of network devices like routers and switches to handle and process data also impacts network capacity.

Some strategies such as optimizing network infrastructure capacity, implementing traffic management techniques, and prioritizing critical data traffic has been deployed by vendors to prevent congestion. Moreover, upgrading hardware, employing traffic management tools, or redesigning network topology can be other solutions for mitigating network congestion effectively.

C. Security Threats

5G private networks face vulnerabilities to secure threats such as Denial of Service (DoS) attacks, malware incursions, eavesdropping, Man-in-the-Middle (MitM) attacks, and physical attacks. Mitigating these threats needs comprehensive security strategies. Network robustness can be achieved through improvements such as traffic filtering, encryption, detection systems, and secure device management [9]. In the following

sections, jamming, a specific form of DoS attack, will be the primary focus in the stressed 5G testbed setup.

IV. Stressors Setup

To conduct effective stress testing for our 5G network, we selected OpenAirInterface (OAI) as the foundation for our testbed. The open-source nature of OAI allows us to access and understand the underlying code, which simplifies the process of configuring and adapting the testbed to meet our specific needs. This transparency enables us to explore and modify the 5G implementation, add new features, and adjust the behavior of the network according to our experimental requirements. This flexibility is a significant advantage compared to closed systems from major vendors. Additionally, this choice not only helps with our budget but also enables us to be creative and experiment with new ideas on an adjustable testbed. On the other hand, potential downsides include limited documentation, lack of community support, and stability issue.

To further enhance our testing setup, we have integrated FlexRIC, a software development kit (SDK) designed for developing specialized service-oriented controllers on top of the network. FlexRIC enables dynamic reconfiguration of the network, which is particularly valuable for mitigating the effects of various stressors. This capability is often not available with vendor-specific 5G solutions, making FlexRIC an important component in optimizing our stress testing environment.

In this section, we cover four key components: the OAI testbed, the Jamming testbed, the parameters collected through this setup, and the preliminary results.

A. OpenAirInterface 5G Standalone Testbed

The OAI 5G SA (Stand-Alone) testbed follows standard 5G setup practices and consists of two main parts: Core Network (CN) and the Radio Access Network (RAN). The RAN includes base stations, known as gNodeB (gNB)s, which connect to the Core Network to enable full 5G functionality.

The Core Network (CN) is the backbone of the 5G testing setup, and our testbed has OAI 5G CN. There are other options like free5GC [10] and Open5GS [11] for the core network, but we're currently using OAI CN to keep things simple.

The Radio Access Network (RAN) in our testbed is structured around the gNodeB, which is divided into three functional units: Radio Unit (RU), Distributed Unit (DU), and the Centralized Unit (CU). For our testbed, we use a software-defined radio (SDR), specifically the USRP B210, as the Radio Unit. The USRP B210 is a versatile SDR platform that supports a wide range of frequencies and can be used for various 5G experimentation purposes. Although provided maximum bandwidth (56 MHz) is not enough for advanced 5G standards, it is sufficient for an experimental testbed. The DU and CU functionalities are implemented through OAI software. The testbed setup also includes a computer that runs both the Core Network and base station software, with the USRP B210 connected to this computer to serve as the radio unit. A summary of the testbed components is provided in Table I. Our 5G SA network is configured with TDD on Band 78, utilizing a 40 MHz bandwidth.

TABLE I
Hard- and Software Specifications

	Components	Specification
OAI Hardware	CPU	Intel Xeon® W-2145
	RAM	32 GB
	Hard Disk	500 GB
Radio Device	gNB	USRP B210 (X310, N321)
	Antenna	Quectel YE0003AA
	UE	Quectel RM500Q, Pixel 6,OAI UE OAI UE with USRP
Software	OS	Ubuntu 20.04
	Kernel	Low Latency
	OAI Branch	Develop
	Core Network	OAI 5G Core

Running the testbed is straightforward going through this tutorial [12]. After running the core network and the base station in separate Ubuntu terminals, a user equipment (UE) tries to connect to the network. As a UE, there are multiple options to use with OAI. Our testbed has Quectel RM500Q, Google Pixel 6, and OAI UE with USRP options for UEs. For now, Quectel 5G modems with Windows computers are used as UEs. However, the other UEs will be tested in the future with different scenarios.

B. Barrage Jamming Testbed

To challenge our testbed, we opted to use barrage jamming because of its known efficacy and straightforward implementation.

We used Bash and Python to develop the jamming scripts, which run on a USRP B210 in the same range as our 5G network. These scripts feature adjustable attributes, allowing us to modify parameters such as duration, sleep time, and power within a single run. A command-line interface was implemented to set these ranges before running the jamming script.

In our implementation, the central frequency is predetermined and remains constant throughout the execution. However, parameters like transmission power, jamming duration, and intervals of non-transmission (sleep periods) can be varied during the script's execution.

Since a barrage jammer can cover the whole bandwidth of the 5G communication which is 40 MHz, we can jam the entire communication channel for maximum effectiveness.

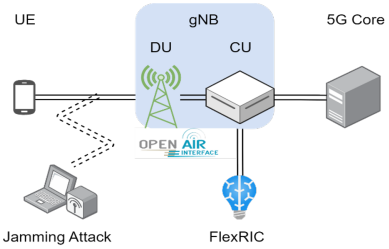

Fig. 1. 5G SA Testbed Setup.

TABLE II
KEY 5G NETWORK PERFORMANCE PARAMETERS

Parameter	**Description**
Received Signal Strength Indicator (RSSI)	The average received power, helping us understand the network's overall strength.
Reference Signal Recieved Power (RSRP)	The average power of signals specific to each cell in the network
Signal-to-Noise Ratio (SINR)	The strength of the useful signal compared to interference and background noise.
Power Headroom (PHR)	Essential for managing power efficiently, it helps to know how much power a device has available.
Block Error Rate (BLER)	Tells how well data are transmitted, showing the number of mistakes in received data.
Channel Quality Information (CQI)	A measure of how good or bad the radio channel is, helping us achieve the desired signal quality.
Modulation and Coding Scheme (MCS)	A key factor affecting the size of data blocks and the efficiency of data transfer.
Rank Indicator (RI)	Sent by devices to the network, indicating how many different data streams the network can handle.
Bitrate	The total number of bits transferred per second, directly affecting how fast the network can send and receive data.

C. The parameters Collected from Testbed

In our pursuit to advance 5G network performance, we focus on specific indicators gathered from our testbed. Evaluating the network's status is critical for effective management and optimization. This involves systematic collection and analysis of various network parameters, offering valuable insights into the network's operational efficiency and overall health.

We monitor key parameters essential for assessing 5G network performance. These parameters, which are standard in evaluating physical layer performance, provide fundamental insights into the network's operation. By monitoring these indicators, we gain a clear understanding of how the network performs under various conditions. A summary of the parameters is provided in Table II.

D. Preliminary Results

In our ongoing data collection phase, we've closely observed our 5G testbed to gather valuable insights. Here are the key observations: 1) Small movements nearby can disrupt the signal and impact data reliability. Optimization of the test environment is essential for more accurate results. Understanding this vulnerability underscores the importance of fine-tuning the testbed for optimal performance.

2) The structure of the building significantly influences outcomes during indoor testing. Understanding and accounting for these indoor variables are necessary for devising effective real-world solutions. Variables such as signal propagation and interference patterns within confined spaces need careful consideration.

3) The OpenAirInterface (OAI) base station is sensitive, especially when UEs are not directly connected. Challenges during uplink communication can lead to errors and potential disruptions in base station functionality. Addressing these issues is important for optimizing uplink communication strategies and maintaining seamless connectivity.

4) Targeting the downlink signal during data collection is a smarter approach for operational network continuity. Navigating jamming complexities requires careful adjustment of signal strength to allow data alteration without fully disconnecting UEs or the base station. Striking the right balance in jamming signal strength is vital for effective data collection without compromising network integrity.

5) Distinguishing between movement and jamming becomes particularly challenging when devices are in motion. Developing an algorithm capable of detecting jamming attacks in dynamic scenarios is a key focus. This challenge highlights the need for advanced algorithms to interpret data accurately in scenarios involving dynamic device movements and potential jamming incidents.

6) Some KPIs show a strong correlation with jamming. As an example, Figure 2 shows one instance from the data collection process which is an analysis of the Downlink Block Error Rate (DL BLER) over time in conjunction with the Jamming Gain (dB) in a 5G network test environment. The time series data are plotted on the x-axis, spanning a specific duration, while the y-axis on the left represents various network performance metrics, including the DL BLER, and the y-axis on the right corresponds to the Jamming Gain. The orange line represents the DL BLER, showcasing its variations over the recorded time period. Notably, there are several spikes in the DL BLER, indicating periods where the error rate in the downlink transmission increased significantly. The red bars indicate the Jamming Gain in dB, which is plotted on a secondary y-axis on the right. These bars show the intensity and duration of jamming incidents. Every red bar corresponds to an occurrence of jamming, with varying heights reflecting different levels of jamming gain. When the dB is set over 80, the base station stops working and it is not possible to collect data. In order to see the affect of the Jamming, the dB is set between 70-80 dB. The repeated spikes in DL BLER during jamming events suggest that the network experiences substantial degradation in downlink quality whenever jamming is introduced.

The severity of DL BLER spikes varies with the intensity of the jamming gain, indicating a proportional relationship between jamming strength and error rate increase. The strong correlation between increased jamming gain and the rise in DL BLER highlights the critical need for effective jamming detection and mitigation strategies to ensure network reliability and performance. Moreover, it is possible to compare the results for all of the listed parameters on the right side of Figure 2, here as an example DL BLER is chosen.

V. FUTURE WORK

Moving forward, our main focus will be on two key things: collecting more data and developing our algorithms. In terms of data collection, we plan to try out different scenarios and

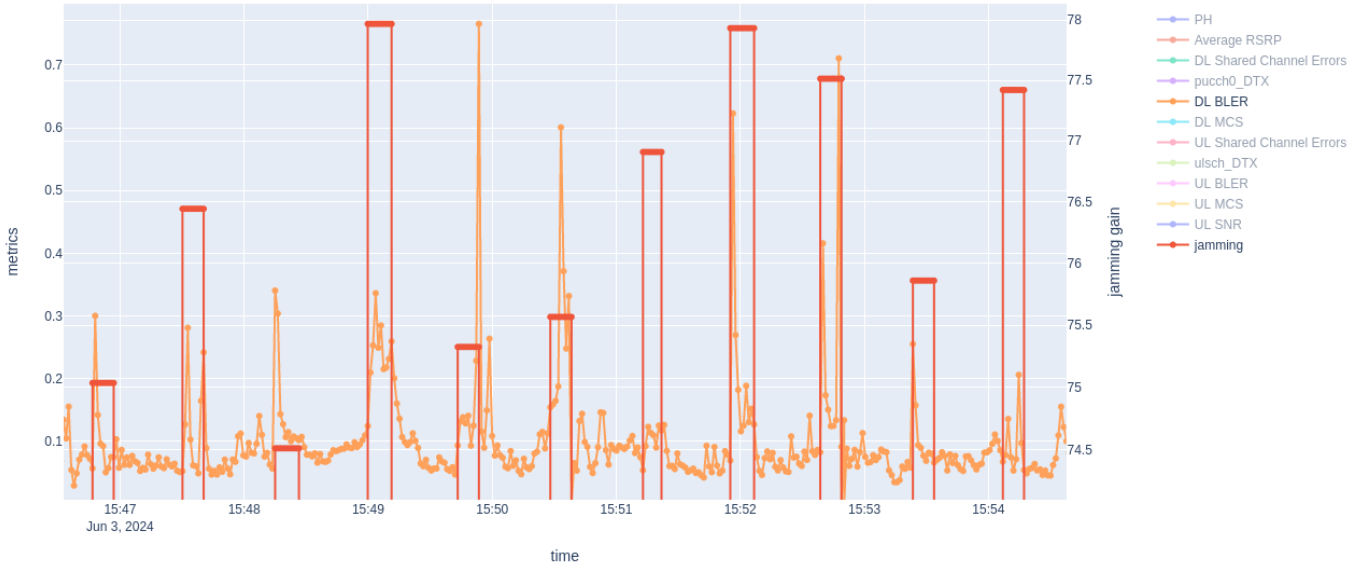

Fig. 2. Downlink Block Error Rate (DL BLER) over time in conjunction with the Jamming Gain in dB

equipment setups. This includes situations where we have multiple User Equipment (UEs) connected to a single gNB, setups with multiple UEs and multiple gNBs, and experiments involving UEs in motion with jamming, using different jamming techniques.

We also want to mix things up by trying out different UEs and various USRP units. This helps us understand how different setups perform and compare to each other.

Once we've gathered enough data, we'll shift our focus to implementing FlexRIC, turning our algorithmic ideas into practical solutions. Beyond that, our curiosity extends to exploring more parameters. We want to dig deeper into what makes our network safer and more reliable. This active exploration ensures that our network stays strong and flexible, ready to face the challenges of indoor 5G private networking.

VI. Conclusion

To wrap up, our research investigates the challenges faced by 5G private networks in industrial settings. We tackle issues like interference, congestion, security challenges. Using the OpenAirInterface testbed and FlexRIC, we create a setup to test 5G in industrial settings.

Looking forward, we focus on collecting data and refining algorithms to make these networks more adaptable. Our ongoing efforts aim to strengthen industrial 5G networks, making them robust in the dynamic world of telecommunications.

Acknowledgment

The research leading to these results has received funding from the German Federal Office for Information Security under grant no 01MO23014C, the German Federal Ministry for Digital and Transport under grant no 19OI22013B, and from the German Federal Ministry of Education and Research under grant no 16KISK009 and 16ME0424.

References

[1] Florian Kaltenberger et al."The OpenAirInterface 5G new radio implementation: Current status and roadmap". In: WSA 2019, 23rd ITG Workshop on Smart Antennas, Demo Session, 24-26 April 2019, Vienna, Austria. 2019

[2] Robert Schmidt, Mikel Irazabal, and Navid Nikaein. "FlexRIC: An SDK for next-Generation SD-RANs". In: CoNEXT '21. 2021.

[3] M. Wen et al., "Private 5G Networks: Concepts, Architectures, and Research Landscape," in IEEE Journal of Selected Topics in Signal Processing, vol. 16, no. 1, pp. 7-25, Jan. 2022, doi: 10.1109/JSTSP.2021.3137669.

[4] J. Prados-Garzon, P. Ameigeiras, J. Ordonez-Lucena, P. Muñoz, O. Adamuz-Hinojosa and D. Camps-Mur, "5G Non-Public Networks: Standardization, Architectures and Challenges," in IEEE Access, vol. 9, pp. 153893-153908, 2021, doi: 10.1109/ACCESS.2021.3127482.

[5] M. E. Flores, D. D. Poisson, C. J. Stevens, A. V. Nieves and A. M. Wyglinski, "Implementation and Evaluation of a Smart Uplink Jamming Attack in a Public 5G Network," in IEEE Access, vol. 11, pp. 75993-76007, 2023, doi: 10.1109/ACCESS.2023.3296701.

[6] R. Dionísio, T. Lolić and P. Torres, "Electromagnetic Interference Analysis of Industrial IoT Networks: From Legacy Systems to 5G," 2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW), Riga, Latvia, 2020, pp. 41-46, doi: 10.1109/MTTW51045.2020.9245057.

[7] M. U. A. Siddiqui, F. Qamar, F. Ahmed, Q. N. Nguyen and R. Hassan, "Interference Management in 5G and Beyond Network: Requirements, Challenges and Future Directions," in IEEE Access, vol. 9, pp. 68932-68965, 2021, doi: 10.1109/ACCESS.2021.3073543.

[8] Chen, Li-Sheng & Ho, Chih-Hsiang & Chen, Cheng-Chang & Kuo, Sy-Yen. (2022). Learning Scheme for Adaptive Modulation and Coding in 5G New Radio. 430-434. 10.1109/ICSRS56243.2022.10067597.

[9] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Yliant-tila and A. Gurtov, "5G security: Analysis of threats and solutions," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 2017, pp. 193-199, doi: 10.1109/CSCN.2017.8088621.

[10] "free5GC: Open-source project for 5G mobile core network" free5GC. Available: https://free5gc.org/. (Accessed: August 7, 2024)

[11] "Open5GS: Open Source 5G Core Network." Open5GS. Available: https://open5gs.org/. (Accessed: August 7, 2024)

[12] " OAI 5G NR SA tutorial with COTS UE" OpenAIrInterface. Available: https://gitlab.eurecom.fr/oai/openairinterface5g//blob/develop/doc/NR_SA_Tutorial_COTS_UE.md (Accessed:August 7,2024)