TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

5G SA NETWORK FOR DRONE SWARM APPLICATIONS: PRELIMINARY DEPLOYMENT AND TESTING

Teodor GIURGICĂ, Annamaria SÂRBU, Kevin TEBBE, Gerd SCHOLL

Abstract: *This work presents the design, implementation and experimental validation of an end-to-end 5G Standalone (5G SA) network based on containerized deployment of open-source technologies. The development process started from a virtualized environment and migrated towards a Docker-based architecture for both the 5G core and next generation node B (gNB).*

The 5G Core and gNB were integrated and validated using customized user equipment (UE), enabling realistic testing of registration procedures, packet data unit (PDU) session establishment, and user-plane data transfer. In the final stage, the system was extended to a hardware-based implementation using a software-defined radio (SDR) platform, enabling over-the-air (OTA) pre-validation of the transmitted 5G New Radio (NR) signal. Experimental results confirm 5G SA attachment, stable data transfer and compliant radio emission behavior within the n78 band.

Keywords:*5G SA, Containerized 5G Core, Docker-based Deployment, gNB Implementation, New Radio (NR), Software-Defined Radio (SDR), Custom User Equipment, UAV*

1. INTRODUCTION

Drone swarms are typically treated as networked control systems in which safety-critical coordination depends on frequent, reliable exchange of state and control information with tight latency and jitter bound [1]. Reviews of swarm and multi-UAV communication architectures report that control-plane traffic (telemetry and coordination messages) has relatively low data rate but requires millisecond-level latency and high reliability, while user-plane traffic such as video or sensor streams demands higher throughput while tolerating more relaxed delay and loss constraints [2].

5G NR directly address these requirements by using Ultra-Reliable Low-Latency Communications (URLLC) to achieve ms radio-interface latencies and reliability up to 99.999% for short control packets. In addition, 5G Quality of Service (QoS) flows enables differentiated handling of delay-sensitive control traffic and best-effort data traffic [3]. Open-source 5G SA implementations such as Open5GS, srsRAN, and OpenAirInterface have enabled experimental end-to-end platforms on general-purpose hardware with SDR-based gNBs, demonstrating over-the-air registration, PDU session establishment, and latency/throughput measurements with 3GPP-defined user equipment (UE) [4]. These cores are being deployed as containerized network functions to obtain reproducible, flexible testbeds while preserving basic 3GPP-compliant behaviour, enabling controlled evaluation of connectivity and performance in different configurations [4, 5].

Therefore, the paper investigates how an open-source, containerized 5G Standalone network with an SDR-based gNB can be implemented and validated over-the-air using commercial UEs to demonstrate connectivity suitable for drone swarm communication requirements. The key contributions include: (i) the implementation of a containerized end-to-end 5G SA architecture integrating both the Open5GS core and an SDR-based srsRAN gNB using Docker Compose; (ii) over-the-air validation with commercial 5G user equipment,

including spectrum-level verification of compliant 5G NR operation in the n78 band; and (iii) experimental evaluation of representative control/data-like traffic patterns, providing indicative latency, jitter, and throughput measurements relevant to latency-sensitive UAV swarm communication scenarios.

2. 5G SA NETWORK DESIGN

The implementation of an end-to-end 5G Standalone (SA) network requires both the 5G Core Network and the 5G NR gNB to which UE connects, as defined in the 3GPP system architecture [6]. The core network relies on a persistent database to store subscription information, authentication data, and session parameters. In this implementation, MongoDB was selected as the database backend due to its compatibility with the chosen open-source 5G core and its suitability for containerized deployments. Fig. 1 illustrates the logical view of the implemented end-to-end 5G SA architecture, highlighting the core network, backhaul, and fronthaul segments, together with the main communication interfaces [5].

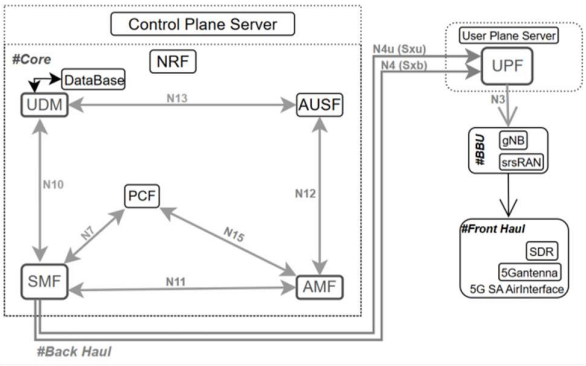


Fig. 1. 5G SA Architecture: core, backhaul, and fronthaul protocol integration (logical view and communication interfaces)

The selected 5G core network implementation is Open5GS, which follows the 3GPP-defined service-based architecture (SBA) and clearly separates the control plane from the user plane improving robustness and modularity [7,8].

The core network is composed of multiple Network Functions (NFs), each responsible for a specific role such as access and mobility management, session management, authentication, policy control, or user data forwarding, in line with the functional decomposition defined for the 5G core [8]. This microservice-oriented design ensures that the failure or restart of a single NF does not lead to a complete system outage, which is particularly advantageous for experimental and containerized environments [9]. User-plane traffic exiting the 5G core is transported through the backhaul segment toward the base station, consistent with the 5G transport network model separating backhaul and fronthaul according to standard 5G transport network concepts [5,10].

Communication between different elements of the 5G system is realized through standardized interfaces,. Within the core network, NFs communicate via service-based interfaces (SBI) for control-plane procedures. Key SBIs include N11 between the access and mobility management function (AMF) and the session management function (SMF), N10 between the SMF and the unified data management (UDM), N7 between the SMF and the policy control function (PCF), N12 between the AMF and the authentication server function (AUSF), and N15 between the PCF and the AMF. These interfaces collectively enable control-plane signaling, session management, authentication, and policy enforcement [7,11]. The interface between the core network and the gNB is realized through the N3 interface for user-plane traffic, while N2 supports control-plane signaling between the gNB and the core [12].

On the radio side, the gNB communicates with the UE through the 5G NR Uu interface. The use of standardized interfaces across core, backhaul, and fronthaul segments ensures interoperability and allows the implemented testbed to closely follow 3GPP architectural principles while remaining suitable for experimental evaluation [12, 8].

3. 5G SA UE REGISTRATION AND SYSTEM OPERATION

Fig. 2 illustrates the control-plane operational flow associated with system initialization, gNB–core connectivity, and UE registration in the implemented 5G SA network. The process begins with system startup, where the core

network services are initialized and their operational status is verified; if the core services fail to initialize correctly, error-handling and retry mechanisms are triggered until a consistent system state is achieved. Once the Open5GS core is successfully initialized, the system transitions to a state in which it is ready to establish the gNB–core connection. The gNB then attempts to connect to the core network over the NG control and user plane interfaces (N2/N3), and, in the event of a connection failure, reconnection attempts are performed until a stable gNB–core association is established, at which point the system becomes ready to accept UE registration requests [13].

When the system is ready for UE access, the UE registration procedure is initiated using Non-Access Stratum (NAS) signaling and NG Application Protocol (NGAP) between the UE, gNB and 5G core. The process starts with primary authentication between the UE and the core network (e.g., 5G-AKA), which constitutes a first decision point: if authentication is unsuccessful, the registration request is rejected and the UE is not admitted to the network; if authentication succeeds, the procedure continues with the NAS security mode control, which establishes integrity and encryption for subsequent signaling messages before further control-plane communication [14].

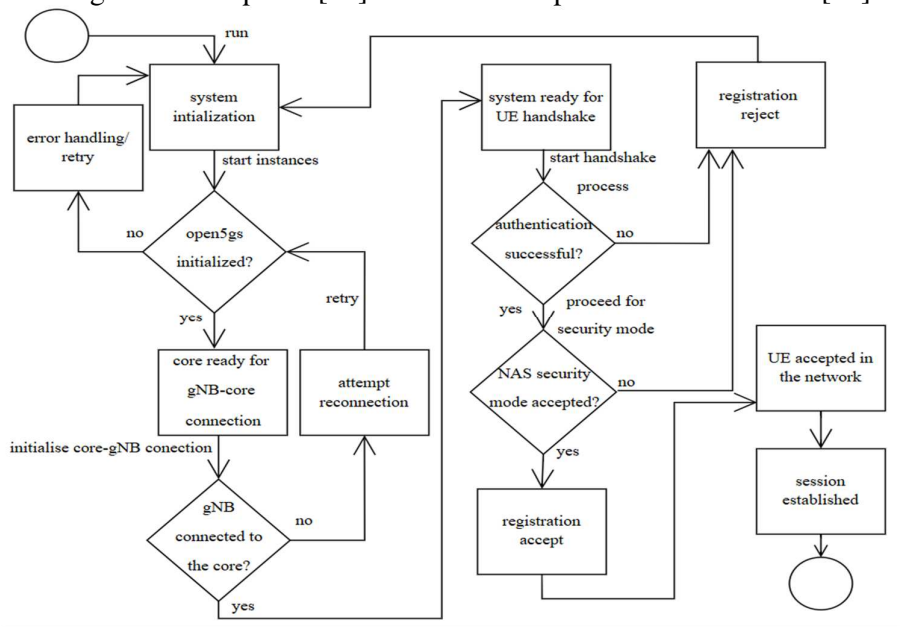


Fig. 2 5G-SA System Operation and UE Registration Flow

Acceptance of the NAS security mode constitutes a second decision point: if the requested security mode is rejected, the registration is terminated to preserve network security, whereas, when both authentication and NAS security procedures complete successfully, the core network issues a registration accept and the UE is admitted into the network. Following successful registration, the UE can establish a PDU session, enabling user-plane data transfer between the UE and the core network according to the 5G SA architecture, with control-plane signaling and user-plane communication then coexisting in a stable operational state [15].

Overall, the diagram emphasizes the sequential and stateful nature of 5G SA control-plane operation, highlighting key decision points in authentication and security, as well as retry and error-handling behavior that contribute to robustness and predictable behavior in experimental deployments.

The experimental results confirm successful execution of 3GPP-defined 5G SA procedures, including UE registration, authentication (5G-AKA), NAS security mode establishment, and PDU session setup, as specified in 3GPP TS 23.501 and related signaling procedures. Successful attachment without rejection and stable session persistence indicate behavior consistent with expected 3GPP-compliant operation.

It is important to emphasize that the reported measurements represent functional validation rather than conformance certification or complete performance testing.

4. VIRTUALIZATION AND CONTAINERIZATION

The initial implementation of the 5G SA testbed was realized in a virtualized environment based on two separate virtual machines (VMs). This approach was adopted as a baseline due to its simplicity and widespread use in early virtualized mobile core and 5G experimental deployments [16]. In this configuration, the first VM hosted the 5G core network implemented with Open5GS together with the MongoDB database, while the second VM ran UERANSIM, providing both gNB and UE functionalities in a fully emulated environment, as it can be seen in fig. 3.

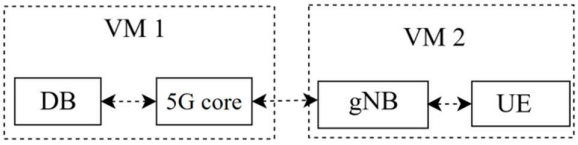


Fig. 3. Virtualized implementation

Within this setup, all core network functions, including subscriber management, authentication, and session handling, operated and end-to-end connectivity could be validated using the emulated UE. The virtualized environment enabled functional verification of UE registration, PDU session establishment, and basic IP connectivity without requiring radio hardware. However, the UE and radio access network were entirely software-emulated, which constrained the ability to assess over-the-air performance, radio propagation effects, and hardware-related limitations. While VMs offer strong isolation, they produce overhead in terms of resource consumption, startup time, and system footprint, which becomes critical when targeting deployment on edge computing devices or embedded platforms with constrained compute and memory resources [17].

To mitigate these limitations, the architecture was migrated from full virtualization to a containerized deployment model based on Docker. The main objective of this transition was to improve portability, reduce resource overhead, and facilitate deployment on edge computing devices while preserving the functional behavior of the 5G system [18,19].

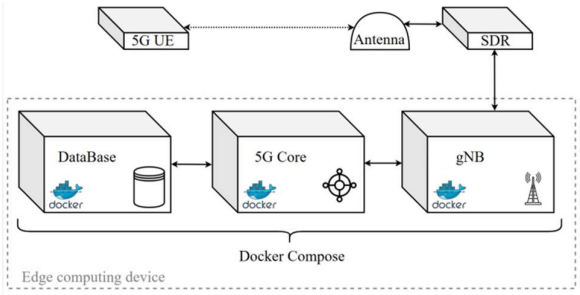


Fig. 4. Containerized architecture

In the containerized setup, the 5G core network, database, and base station components were deployed as Docker services orchestrated using Docker Compose, as seen in fig. 4.

The Docker Compose configuration defines three main services: the MongoDB database, the Open5GS 5G core, and the srsRAN gNB. Each service is specified in YAML configuration files, which declare container images, network interfaces, exposed ports, persistent volumes, and health checks. A dedicated Docker network is defined to provide controlled and deterministic communication between containers, replacing the manual network configuration previously required in the VM-based setup. The MongoDB container stores subscriber profiles, authentication credentials, and session-related data required by the core network functions. Subscriber information is populated using command-line utilities such as the Open5GS database control tools, while access to the MongoDB web interface is enabled for inspection and verification of stored data. Persistent volumes are configured to ensure that database content is preserved across container restarts. The Open5GS core container hosts the control-plane and user-plane network functions and communicates with the database container over the Docker network. The srsRAN gNB container implements the radio access network protocol stack and connects to the core network using standardized 5G interfaces, such as N2 for control-plane signaling and N3 for user-plane traffic. Startup scripts enforce the initialization

order so that the database and core services become available before the gNB attempts to connect. In contrast to the initial VM-based deployment, the containerized architecture allows the UE to be external and physical rather than emulated. Commercial 5G user equipment and modem-based devices are connected over the air to the containerized gNB via an SDR-based radio frontend, enabling more realistic experimentation while retaining a lightweight and portable 5G core deployment [20]. Overall, the migration from a VM-based setup to a Docker-based architecture improves portability, scalability, and deployment flexibility. Containerization reduces system overhead, simplifies service orchestration, and enables execution on edge and cloud-edge platforms, while remaining compatible with open-source 5G software components and hardware-based radio access.

5. HARDWARE IMPLEMENTATION

Hardware implementation targeted end-to-end validation with real radio transmission and commercial user equipment. The private 5G SA system was deployed on a Dell Precision 3590 laptop (Intel Core i7 CPU, 32 GB RAM, Ubuntu 22.04 LTS), which hosted all 5G core and gNB software components inside Docker containers. The laptop was directly connected via USB 3.0 to an Ettus USRP B205mini-i SDR, covering the 70 MHz–6 GHz band, and to a Poynting A-PUCK-0005 omnidirectional antenna with approximately 6 dBi gain, enabling over-the-air 5G NR operation and the formation of an isolated 5G SA cell [21]. The hardware implementation of the system can be seen in fig. 5. All containers (Open5GS core functions, MongoDB database, and srsRAN gNB) executed on the laptop, with the USRP B205mini-i acting as the RF front end and converting baseband I/Q samples into RF signals radiated by the A-PUCK-0005 antenna. For the further phase of the project, the laptop will be replaced by NVDIA Jetson Nano microcomputer enabling a more compact, lightweight, and energy-efficient deployment suitable for UAVs, where reduced size, weight, and power consumption are critical.

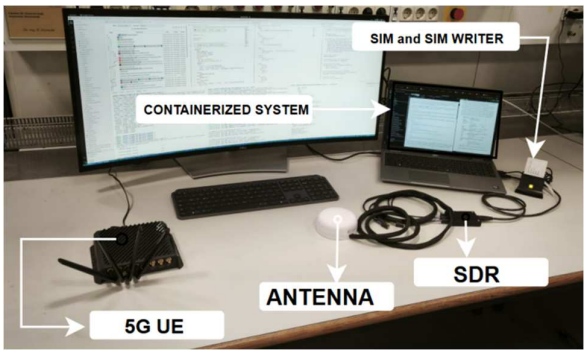


Fig. 5. Hardware implementation of the 5G SA network

As physical UE, an Ericsson Cradlepoint R1900 enterprise-grade 5G router was employed. The router was equipped with a programmable Subscriber Identity Module (SIM) card, written using a dedicated SIM writer and provisioning tools.

Subscriber credentials were provisioned to align with the corresponding records in the Open5GS MongoDB database. These credentials included the International Mobile Subscriber Identity (IMSI), Public Land Mobile Network (PLMN) identifier, Access Point Name (APN), authentication key (Ki), and operator variant algorithm configuration (OPc). This configuration ensured consistent subscriber authentication and successful network registration in the absence of operator-issued SIM cards [22].

After provisioning, the Cradlepoint R1900 successfully registered to the private 5G SA cell and established a PDU session. Network address translation and routing on the laptop enabled traffic from the 5G core to reach the campus network and the public internet. An UE connected to the router's WLAN interface, thereby accessing external IP networks through the private 5G infrastructure. Basic validation consisted of ICMP echo tests and TCP throughput measurements from the router towards external hosts, confirming stable data transfer, acceptable latency, and routing across the containerized core, SDR-based gNB, and external network gateways [23]. Fig. 6 illustrates the IP-level network topology and routing configuration used to enable end-to-end connectivity between the private 5G SA network and external IP networks. The Open5GS core runs inside a Docker container attached to a

dedicated Docker bridge network, while the user plane assigns IP addresses to the UE from a private address space (10.45.0.0/16). Traffic originating from the UE is forwarded through the user plane function and translated via network address translation (NAT) at the container and host levels, allowing packets to exit the Docker network and reach the host machine interface. At the host level, additional NAT and routing rules forward traffic towards the campus gateway, which provides access to the public Internet. On the UE side, the enterprise 5G router performs local NAT for devices connected to its WLAN interface, enabling transparent Internet access through the private 5G infrastructure. This layered routing and NAT configuration demonstrates integration of the containerized 5G core with external IP networks and validates the practical usability of the system beyond isolated laboratory conditions.

To quantify the operational behavior of the implemented system, basic performance measurements were conducted over the network topology shown in fig. 6. The objective of these measurements was to validate functional end-to-end connectivity and obtain indicative values for latency, jitter, and throughput, rather than to perform exhaustive performance benchmarking.

ICMP echo tests performed from the enterprise 5G router towards external hosts revealed round-trip latency values in the range of approximately 26–42 ms, with an average latency of about 35 ms and no packet loss observed. These results indicate functional connectivity across the containerized 5G core, SDR-based gNB, and external IP routing infrastructure. TCP-based throughput measurements confirmed successful data transfer through the private 5G SA network, with downstream throughput reaching approximately 43 Mbps and upstream throughput around 2.6 Mbps.

Additional latency and jitter measurements reported an average end-to-end latency of roughly 139 ms and jitter values on the order of 25 ms under sustained TCP traffic, reflecting the combined effects of SDR processing, network address translation, and campus network routing. The measured latency values reflect cumulative processing across the SDR baseband chain, USB interfacing, container networking, NAT translation, and external routing segments, and therefore represent baseline performance of a non-optimized SDR-based 5G SA deployment without URLLC-specific scheduling, QoS prioritization, or real-time kernel enhancements.

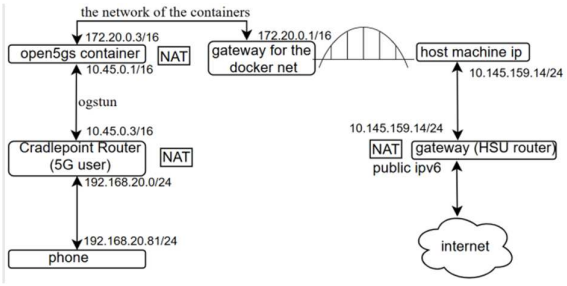


Fig. 6. Network topology and IP routing for end-to-end connectivity in the containerized 5G SA deployment

From an application perspective, the results are compatible with payload-oriented traffic such as video or sensor streams, whereas stricter delay bounds would be required for time-critical control loops in drone swarm scenarios. Although explicit QoS flow differentiation was not implemented, two representative traffic categories were evaluated conceptually: control-like traffic (low-rate, small packets) and data-like traffic (throughput-oriented TCP flows). Within the 5G SA framework, such traffic types can be mapped to distinct QoS Flow Identifiers (QFI) and associated 5QI profiles, and the current architecture supports future extension.

The current validation was performed with a single active UE. However, the containerized architecture supports horizontal scaling of gNB and core functions. Multi-UE scalability experiments, including simultaneous registration, concurrent PDU sessions, and aggregated throughput analysis, constitute planned future work.

6. RADIO TESTING AND PREVALIDATION

For radio prevalidation purposes, a Waveshare 5G modem based on the Quectel RM500Q-GL module, operating in 5G NR SA mode, was utilized and configured as the UE. The modem was connected to the system via USB and controlled using attention (AT) commands through the Minicom terminal. The UE successfully registered with the local 5G network identified as Open5GS, established a

PDU session, and was assigned the IP address 10.45.0.2, demonstrating user-plane connectivity by successfully exchanging ICMP echo messages with the 5G core at 10.45.0.1.

The results present in fig. 7, confirm 5G SA attachment for the 5G modem used as UE, IP allocation, and user-plane connectivity, with low and consistent RTT values observed during ICMP echo testing, issued by attention commands.

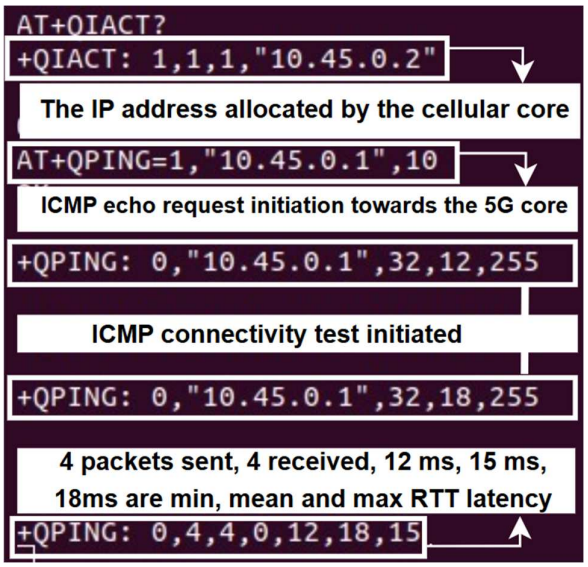


Fig. 7. 5G modem connection and latency test

Fig. 8 presents the complete experimental setup used for radio testing and validation, including the host laptop running the containerized 5G core and gNB (UE implemented as the 5G modem), the SDR-based RF front-end of the 5G core with its corresponding omnidirectional antenna, and the R&S FSVR spectrum analyzer equipped with the Aaronia HyperLOG 7040 directive antenna model FSVR used to observe over-the-air (OTA) real-time 5G NR emissions.

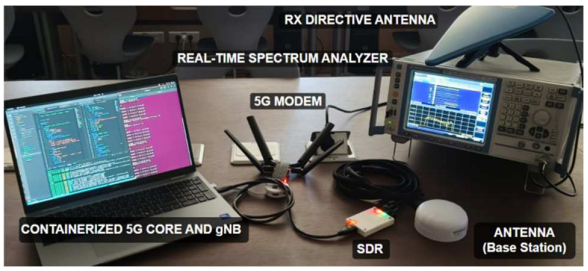


Fig. 8. OTA testing of 5G SA network

In fig.9, the real-time spectrum analyzer view illustrates both the persistent signaling block (SSB) component and the dynamic activation of the 20 MHz NR channel during multiple ICMP ping transmissions (visible as continuous horizontal lines) from the user equipment to the 5G core, demonstrating that user-plane data occupies the spectrum only when traffic is present, while the channel remains idle otherwise.

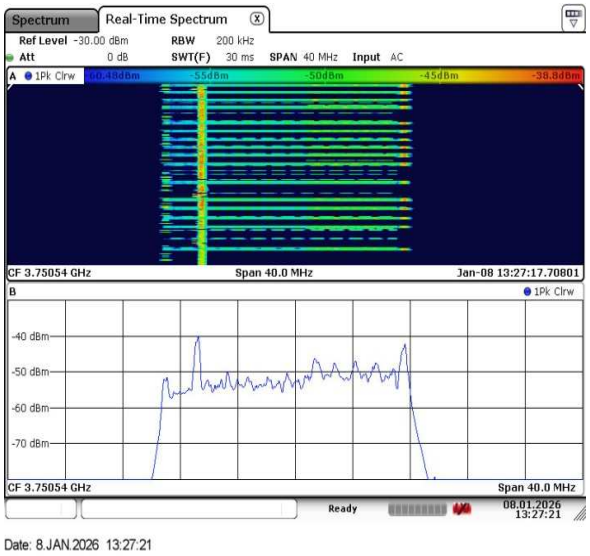


Fig. 9. Real-time spectrogram and spectrum of 5G NR OTA transmission under UE traffic (ping)

Fig.10 presents the measured channel power of the 5G NR downlink signal centered at 3.75 GHz with a configured bandwidth of 20 MHz, where only the synchronization and SSB are present, indicating base station transmission in idle mode with no active user equipment data traffic.

As expected in idle mode, the base station does not continuously occupy the full configured 20 MHz channel bandwidth; instead, only periodic SSB bursts are transmitted for cell discovery, synchronization, and system information acquisition. The absence of sustained wideband power across the channel indicates that no user-plane data traffic or dedicated physical channels (e.g., PDSCH) are active, validating base station behavior and expected 5G NR operation under idle conditions.

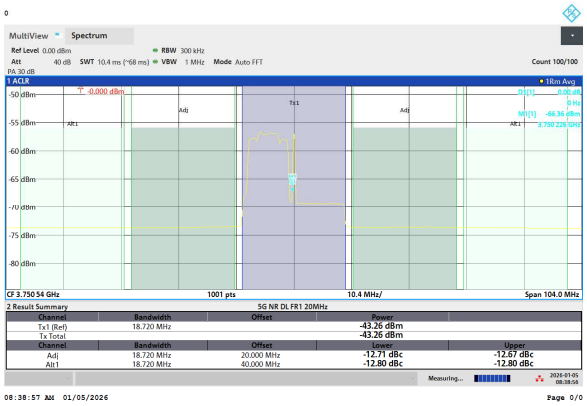


Fig. 10. Channel power measurement of 5G NR base station signal in idle mode

The measurement demonstrates effective confinement of the transmitted power within the allocated 5G NR channel, with no significant spectral leakage observed in the adjacent frequency bands. The power levels in the neighboring channels remain well below the in-band emissions, indicating proper transmitter filtering and compliance with adjacent channel leakage ratio (ACLR) requirements.

7. CONCLUSION

This paper presents the preliminary design, implementation, and experimental validation of an end-to-end 5G SA network deployed using open-source components and containerized architecture. The key contribution of this paper lie in the reproducible functional architectural integration methodology followed by OTA pre-validation .

The proposed system demonstrates functional execution of essential 3GPP 5G SA procedures, including UE registration, authentication, PDU session establishment, and user-plane data transfer. The transition from a virtual machine–based setup to a Docker-based deployment significantly improves modularity, portability, and resource efficiency, highlighting the suitability of containerization for experimental and edge-oriented 5G infrastructures.

Radio-level prevalidation confirms compliant 5G NR behavior in the configured 3.3 GHz - 3.8 GHz band, including idle-mode operation characterized by periodic synchronization signal block (SSB) transmission and dynamic activation of user-plane resources only in the presence of traffic. These observations pre-verify idle-to-active state transitions and proper spectrum utilization.

While the reported latency and throughput measurements are indicative, they provide a baseline for SDR-based experimental deployments. The proposed platform establishes a practical research infrastructure for future work involving latency-sensitive UAV communication, multi UE-scenarios, and swarm networking. Future work will also include the integration of custom, containerized UE, advanced traffic differentiation mechanisms, and deployment on embedded edge platforms such as NVIDIA Jetson. Hardware-in-the-loop validation using real UAV flight controllers generating telemetry and control feedback loops over the 5G SA network will also be considered.

8. REFERENCES

[1] Asaamoning, G., Mendes, P., Rosário, D., and Cerqueira, E., *Drone Swarms as Networked Control Systems by Integration of Networking and Computing*, Sensors, vol. 21, no. 8, 2021. https://doi.org/10.3390/s21082642

[2] Chen, X., Tang, J., and Lao, S., *Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols*, Applied Sciences, vol. 10, no. 10, 2020. https://doi.org/10.3390/app10103661

[3] Banafaa, M., Pepeoğlu, Ö., Shayea, I., Alhammadi, A., Shamsan, Z., Razaz, M., Alsagabi, M., & Al-Sowayan, S. (2024). *A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges*. IEEE Access, 12, 7786-7826. https://doi.org/10.1109/access.2023.3349208

[4] Zaivyi, R., Melnychok, O., & Skochelias, V. (2025). *Data Transmission Between a Drone Swarm and a Ground Base: Modern Methods and Technologies - A Narrative Review*. Premier Journal of Science. https://doi.org/10.70389/pjs.100116.

[5] Oliva, A., Costa, X., Azcorra, A., Giglio, A., Cavaliere, F., Tiegelbekkers, D., Lessmann, J., Haustein, T., Mourad, A., & Iovanna, P.

(2015). *Xhaul: Toward Integrated Fronthaul/Backhaul Architecture in 5G Networks*. IEEE Wireless Communications, 22, 32-40. https://doi.org/10.1109/mwc.2015.7306535.

[6] 3GPP TS 23.501, *System Architecture for the 5G System (5GS); Stage 2*, 3rd Generation Partnership Project (3GPP)

[7] Zhang, C., Wen, X., Wang, L., Lu, Z., & , L. (2018). *Performance Evaluation of Candidate Protocol Stack for Service-Based Interfaces in 5G Core Network*. 2018 IEEE International Conference on Communications Workshops (ICC Workshops),1-6. https://doi.org/10.1109/iccw.2018.8403675

[8] Shariat, M., Bulakci, Ö., Domenico, A., Mannweiler, C., Gramaglia, M., Wei, Q., Aravinthan, G., Pateromichelakis, E., Moggio, F., Tsolkas, D., Gajić, B., Crippa, M., & Khatibi, S. (2019). *A Flexible Network Architecture for 5G Systems*. Wirel. Commun. Mob. Comput., 2019, 5264012:1-5264012:19. https://doi.org/10.1155/2019/5264012.

[9] Hoa, L., Dang, T., & Vo, V. (2025). *An integrated model of threshold-based scaling and fractional admission controlling to improve resource utilization efficiency in 5G core networks*. PLOS One, 20. https://doi.org/10.1371/journal.pone.0330072.

[10] Pizzinat, A., Chanclou, P., Saliou, F., & Diallo, T. (2015). *Things You Should Know About Fronthaul*. Journal of Lightwave Technology, 33, 1077-1083. https://doi.org/10.1109/jlt.2014.2382872.

[11] Rudolph, H., Kunz, A., Iacono, L., & Nguyen, H. (2019). *Security Challenges of the 3GPP 5G Service Based Architecture*. IEEE Communications Standards Magazine, 3,60-65. https://doi.org/10.1109/mcomstd.2019.1800034.

[12] Da Silva Coelho, W., Benhamiche, A., Perrot, N., & Secci, S. (2020). *Network Function Mapping: From 3G Entities to 5G Service-Based Functions Decomposition*. IEEE Communications Standards Magazine, 4,46-52. https://doi.org/10.1109/mcomstd.001.1900040.

[13] Bitsikas, E., Khandker, S., Salous, A., Ranganathan, A., Jover, R., & Pöpper, C. (2023). *UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework*. Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. https://doi.org/10.1145/3558482.3590194.

[14] Jover, R., & Marojevic, V. (2018). *Security and Protocol Exploit Analysis of the 5G Specifications*. IEEE Access, 7, 24956-24963. https://doi.org/10.1109/access.2019.2899254

[15] Aydin, Y., Kurt, G., Ozdemir, E., & Yanikomeroglu, H. (2022). *Authentication and Handover Challenges and Methods for Drone Swarms*. IEEE Journal of Radio Frequency Identification, 6, 220-228. https://doi.org/10.1109/jrfid.2022.3158392.

[16] Bellin, A., Centenaro, M., & Granelli, F. (2023). *A Preliminary Study on the Power Consumption of Virtualized Edge 5G Core Networks*. 2023 IEEE 9th International Conference on Network Softwarization (NetSoft),420-425. https://doi.org/10.1109/netsoft57336.2023.10175489.

[17] Zahoor, S., Ahmad, I., Rehman, A., Eldin, E., Ghamry, N., & Shafiq, M. (2023). *Performance Evaluation of Virtualization Methodologies to Facilitate NFV Deployment*. Computers, Materials & Continua. https://doi.org/10.32604/cmc.2023.035960.

[18] Luong, D., Thieu, H., Outtagarts, A., & Ghamri-Doudane, Y. (2018). *Cloudification and Autoscaling Orchestration for Container-Based Mobile Networks toward 5G: Experimentation, Challenges and Perspectives*. 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), 1-7. https://doi.org/10.1109/vtcspring.2018.8417602.

[19] H. Beuster, K. Tebbe, T. R. Doebbert, and G. Scholl, *Measurements of the Safety Function Response Time on a Private 5G and IO-Link Wireless Testbed*, 2024 IEEE 29th International Conference on Emerging

Technologies and Factory Automation (ETFA). IEEE, pp. 1–4, Sep. 10, 2024. doi: 10.1109/etfa61755.2024.10710762.

[20] Barrachina-Muñoz, S., Payaró, M., & Mangues-Bafalluy, J. (2022). *Cloud-native 5G experimental platform with over-the-air transmissions and end-to-end monitoring*. 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 692-697. https://doi.org/10.1109/csndsp54353.2022.9908028.

[21] Tripathi, A., Bashar, F., Chowdhury, M., Da Silva, A., & Midkiff, S. (2025). *Benchmarking Software Defined Radio Based 5G Deployments With srsRAN: Lessons Learned*. 2025 IEEE Wireless Communications and Networking Conference (WCNC), 1-6. https://doi.org/10.1109/wcnc61545.2025.10978285.

[22] Bikkasani, D. (2025). *SIM Provisioning in 5G and IoT: Securing Mobile Connectivity for the Future*. International Journal of Science and Research (IJSR). https://doi.org/10.21275/sr25123092902.

[23] Kiela, K., Jurgo, M., Macaitis, V., & Navickas, R. (2021). *5G Standalone and 4G Multi-Carrier Network-in-a-Box Using a Software Defined Radio Framework.* Sensors (Basel, Switzerland), 21. https://doi.org/10.3390/s21165653.

Rețea 5G SA pentru aplicații de tip roi de drone: implementare și testare preliminară

Rezumat: Această lucrare prezintă proiectarea, implementarea și validarea experimentală a unei rețele 5G Standalone (5G SA) bazată pe implementarea containerizată a tehnologiilor open-source. Procesul de dezvoltare a început într-un mediu virtualizat și a migrat către o arhitectură bazată pe Docker atât pentru nucleul 5G, cât și pentru next generation node B (gNB).

Nucleul 5G și gNB au fost integrate și validate utilizând echipamente pentru utilizatori (UE) personalizate, permițând testarea realistă a procedurilor de înregistrare, stabilirea sesiunilor de unități de date în pachete (PDU) și transferul de date în planul utilizatorului. În etapa finală, sistemul a fost extins la o implementare hardware utilizând o platformă radio definită prin software (SDR), permițând prevalidarea over-the-air (OTA) a semnalului 5G New Radio (NR) transmis. Rezultatele experimentale confirmă atașarea 5G SA, transferul stabil de date și comportamentul conform al emisiilor radio în banda n78.

Teodor GIURGICĂ, Bachelor's student, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, Department of Telecommunications, IT and Cybersecurity, Faculty of Military Management, s.giurgica.teodor@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.

Annamaria SÂRBU, Associate Professor, PhD, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, Department of Telecommunications, IT and Cybersecurity, Faculty of Military Management, sarbu.annamaria@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.

Kevin TEBBE, PhD Candidate, Helmut Schmidt University - University of the Federal Armed Forces Hamburg, Germany, Department of Electrical Measurement Engineering, Faculty of Electrical Engineering, kevintebbe@hsu-hh.de, Holstenhofweg 85, Hamburg, Germany.

Gerd SCHOLL, Professor (Prof. Dr.-Ing.), Helmut Schmidt University - University of the Federal Armed Forces Hamburg, Germany, Department of Electrical Measurement Engineering, Faculty of Electrical Engineering, scholl@hsu-hh.de, Holstenhofweg 85, Hamburg, Germany.