

Implementation of Multi-Access Connectivity over 5G and Tactical Networks on COTS Smartphones

Pouyan Ebrahimbabaie, Petro Fagurel, Timothy Halleux, Nathan Prakopetz, Mathias Becquaert

Department of Communications, Information, Systems and Sensors (CISS)

Royal Military Academy (RMA)

Brussels, Belgium

{pouyan.ebrahimbabaievarnosfaderani, petro.fagurel, timothy.halleux, nathan.prakopetz, mathias.becquaert}@mil.be

Abstract—Multi-Access (MA) connectivity is a native 5G feature that enables a User Equipment (UE) to simultaneously access the 5G Core (5GC) through multiple heterogeneous access networks. For military applications, this capability can improve resilience to communication disruption and eavesdropping by leveraging additional access networks such as tactical radios. This paper presents, to the best of our knowledge, the first open-source standard-compliant implementation of Multi-Access (MA) connectivity on Commercial Off-The-Shelf (COTS) Android smartphones. Unlike previous laboratory-based implementations, the proposed implementation addresses key deployment challenges associated with smartphone platforms, including Universal Subscriber Identity Module (USIM)-based authentication and secure-element access from the application processor. Experimental results demonstrate successful simultaneous connectivity to the 5GC through both over-the-air 5G New Radio (NR) and L3Harris AN/PRC-163 tactical radios. The results demonstrate the potential of MA connectivity for resilient communications on COTS smartphones.

Index Terms—5G, Multi-Access Connectivity, Non-3GPP Access, N3IWF, COTS Smartphones, Tactical Radios

I. INTRODUCTION

The fifth generation of mobile technology (5G) represents a major evolution in cellular communications, introducing substantial architectural changes and a broad range of new features compared with previous generations. As envisioned by the 3rd Generation Partnership Project (3GPP) in Release 15, 5G was developed with native support for mission-critical use cases, making it of particular interest for military applications [1].

A. 5G in Military Environments: Capabilities and Limitations

Recognizing the potential of 5G to deliver significantly enhanced military capabilities, defense organizations have undertaken considerable research to explore the operational opportunities of 5G and assess the risks associated with its applications in military contexts. Notable examples include NATO-led studies [1] and RAND research efforts [2].

While these studies underscore the operational benefits of 5G in delivering novel military capabilities, they also note that its civilian-oriented design poses challenges in contested or combat environments [1], [2]. In particular, the 5G air interface, referred to as 5G New Radio (NR), has been identified as vulnerable to a broad range of Electronic Warfare (EW) threats, including jamming and eavesdropping

on unprotected lower-layer signaling [1], [2]. Consequently, effective mitigation techniques are essential to ensure reliable use of 5G in military applications.

B. Multi-Access Connectivity for Resilient Communications

Multi-Access (MA) connectivity is a native 5G feature that enables a User Equipment (UE) to simultaneously access the 5G Core (5GC) through multiple heterogeneous access networks, including the 5G access network, referred to as the Next Generation Radio Access Network (NG-RAN), and Non-3GPP Access Networks (N3ANs) such as Wi-Fi or tactical radio networks.

MA connectivity was primarily designed for civilian use cases, e.g., to provide service continuity between 5G and indoor Wi-Fi [3], [4]. However, its capability to support simultaneous connectivity across multiple access networks makes it particularly relevant in contested and combat environments, where 5G NR is exposed to risks such as *communication disruption* and *eavesdropping* [1]. In such environments, MA connectivity can be employed to mitigate the risks associated with 5G NR [5].

This capability becomes particularly valuable when a tactical access network is available as an additional link. In the presence of communication disruption, it provides a resilient backup path, allowing data transmission to continue even if the 5G link is compromised. Furthermore, by distributing traffic across multiple access networks, the exposure to eavesdropping is reduced, as interception of a single link reveals only part of the transmitted data [5], [6].

C. Enabling Multi-Access Connectivity on COTS Smartphones

Smartphones constitute a major class of 5G UEs and are increasingly employed in military applications due to their widespread availability, ease of use, and support for a broad ecosystem of applications. Accordingly, enabling MA connectivity on smartphones is essential to mitigate the risks associated with 5G NR in contested and combat environments.

Prior studies, including our previous work, have investigated MA connectivity in laboratory-based setups [5]–[8]. In such setups, the UE is typically implemented on general-purpose platforms, such as Ubuntu-based laptops, without

relying on commercial smartphones, native 5G modem integration, or interaction with a real Universal Integrated Circuit Card (UICC).

In these laboratory-based setups, 5G connectivity is typically emulated, while additional access networks, including tactical radios, are incorporated to realize heterogeneous connectivity [5], [6]. A dedicated application, referred to as a *dialer*, is used to manage the signaling procedures required to establish connectivity across these additional access networks [9], [10].

While prior work has primarily focused on laboratory-based implementations, this work advances the state of the art by enabling MA connectivity on real Commercial Off-The-Shelf (COTS) Android smartphones. In particular, we present, to the best of our knowledge, the first open-source implementation of standard-compliant MA connectivity on commercial smartphone platforms.

The transition from controlled laboratory setups to COTS Android smartphones introduces key practical challenges, which this work systematically addresses. These challenges include:

- (1) Enabling the dialer to securely perform authentication by exchanging Application Protocol Data Unit (APDU) messages with the Universal Subscriber Identity Module (USIM).
- (2) Enabling the dialer to support multiple configuration options for registration and Protocol Data Unit (PDU) session establishment. These options include:
 - a) Independent registration and PDU session establishment over the 5G access network and an additional access network using a single UICC hosting one USIM.
 - b) Independent registration and PDU session establishment using two subscriptions, each associated with a separate USIM (e.g., in a dual-SIM device), where one is dedicated to the 5G access network and the other to the additional access network.
- (3) Enabling the dialer to function using Policy-Based Routing (PBR) in place of Virtual Routing and Forwarding (VRF), which is not natively supported in Android and depends on device-specific kernel configurations.
- (4) Isolating the dialer execution environment from the rest of the Android OS to enhance security and stability.
- (5) Accessing the smartphone Secure Element (SE) in the absence of direct modem access, as modem control via *Attention* (AT) commands is typically restricted and vendor-controlled.

The structure of this work is as follows. Section II presents the theoretical background of multi-access 5G systems, focusing on the dialer functionality and the relevant UE components. Section III reviews related work and outlines the key contributions of this paper. Section IV describes the proposed architecture for enabling MA connectivity on COTS smartphones, addressing the associated challenges and corresponding solutions. Section V presents the experimental

setup. Section VI provides the performance evaluation across multiple scenarios. Section VII concludes the paper, and Section VIII outlines future research directions.

II. BACKGROUND

3GPP Technical Specification (TS) 23.501 specifies the reference architectures for MA connectivity in 5G systems [11]. An example of an MA 5G system employing an *untrusted* non-3GPP access network is shown in Fig. 1.

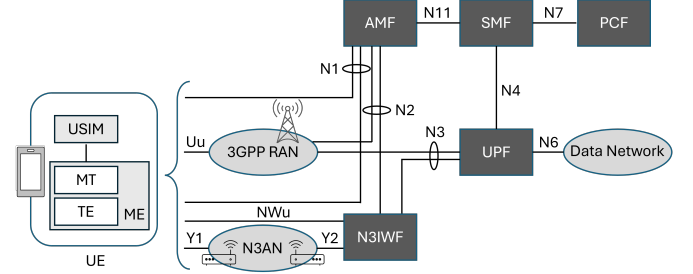


Fig. 1: Multi-Access (MA) 5G system architecture with an untrusted Non-3GPP Access Network (N3AN).

In this architecture, the Non-3GPP Interworking Function (N3IWF) serves as a security gateway between the N3AN and the 5GC, supporting the N2 interface toward the Access and Mobility Management Function (AMF) and the N3 interface toward the User Plane Function (UPF). The N3IWF enables the UE to securely access the 5GC over an untrusted network by establishing Internet Protocol Security (IPsec) tunnels that form the NWu interface [3].

The UE consists of the Mobile Equipment (ME) and the USIM [12]. The ME further comprises the Mobile Termination (MT), responsible for radio transmission and related procedures, and the Terminal Equipment (TE), which hosts end-to-end applications. The USIM stores subscriber identity and security credentials used to support authentication and secure access over both 3GPP and non-3GPP networks [12].

A. UE Dialer Application for NWu Establishment

The establishment of the NWu interface at the UE is handled by a dedicated dialer application, which manages the signaling procedures required to connect to the 5GC over non-3GPP access. The dialer initiates an Internet Key Exchange version 2 (IKEv2) procedure [13] with the N3IWF to establish an IKE Security Association (SA), providing a secure channel for subsequent exchanges [3], [14].

During the authentication phase, Non-Access Stratum (NAS) messages are encapsulated within Extensible Authentication Protocol (EAP)-5G payloads, enabling the UE to perform 5G registration and authentication using credentials stored on the USIM. Upon successful authentication, IPsec Child Security Associations (SAs) are established to form the NWu interface. In particular, one Child SA is used for Control Plane (CP) NAS signaling, while additional Child SAs support User Plane (UP) traffic associated with the PDU

session, thereby ensuring secure connectivity to the 5GC over the non-3GPP access network [3].

Additional details regarding NWu establishment and NAS messaging over N3AN are provided in TS 24.502 (Clause 7) [3] and TS 24.501 (Clause 4.7) [15], respectively.

B. Smartphone Architecture and Challenges for Multi-Access Connectivity

As the focus of this paper is the implementation of MA connectivity on smartphones, this section describes the high-level architecture of a smartphone and highlights the key challenges in implementing MA connectivity. Fig. 2 illustrates the high-level smartphone architecture [16].

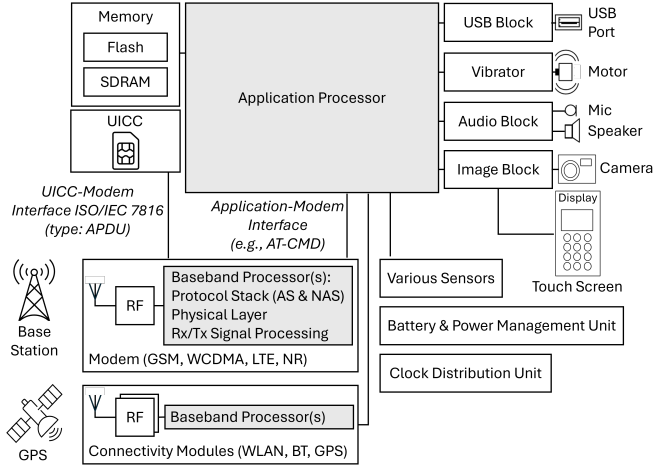


Fig. 2: High-level smartphone architecture.

The main building blocks relevant to MA connectivity include the *application processor*, the *modem*, the *USB* subsystem, and the *UICC*. The application processor executes user applications and networking functions, while the modem handles 3GPP connectivity and interfaces with the UICC through the standardized UICC interface (ISO/IEC 7816) [17]. The USB subsystem enables connectivity to external access networks, such as tactical radios.

The key architectural challenge associated with implementing MA connectivity on smartphones stems from the fact that, unlike 3GPP access, non-3GPP access is not natively integrated into current smartphone modem architectures. Consequently, the dialer responsible for establishing connectivity over non-3GPP access must be implemented on the application processor.

A second architectural challenge arises from the authentication procedure required for non-3GPP access. As discussed in Section II-A, the dialer must exchange authentication-related information with the USIM residing on the UICC in order to support procedures such as subscriber authentication and key derivation. However, unlike the modem, which has direct access to the UICC through the standardized UICC interface, the application processor does not typically have direct low-level access to the UICC. This architectural separation intro-

duces additional challenges for enabling secure APDU-based communication between the dialer and the USIM.

III. RELATED WORK

To date, several studies and projects have investigated MA connectivity in laboratory-based setups. Among the early efforts in this area, the MITRE study [6] focused on implementing Access Traffic Steering, Switching, and Splitting (ATSSS) using a Silvus radio network and UERANSIM [18]. The ROMARS study [8] considered SATCOM-based non-3GPP access using the OpenSAND emulator. In parallel, the MANTRA project [7] investigated multi-access LTE and 5G NSA deployments using a USB dongle providing Wi-Fi and LTE connectivity. In our previous work [5], we investigated MA connectivity in a laboratory-based Ubuntu setup using srsRAN [19], SDR hardware, free5GC, and the open-source N3IWUE project [9].

Despite their differences, these studies share several common limitations:

- (1) Lack of standard USIM-based authentication through APDU exchange with a real UICC. Instead, sensitive subscriber credentials are typically provided directly through plain-text configuration files, introducing significant security and practical deployment limitations.
- (2) Reliance on experimental or emulated software-based environments rather than commercial 5G modems and native over-the-air 5G connectivity.
- (3) Lack of MA connectivity support for a single subscriber. Instead, separate subscriptions are typically used for the 3GPP and non-3GPP access networks.
- (4) Reliance on Ubuntu-based laptop setups, requiring substantial architectural modifications for deployment on Android smartphones at the application-processor level.

The present work delivers an open-source, standard-compliant implementation of MA connectivity on a COTS Android smartphone, supporting standard USIM-based authentication through direct APDU exchange with the UICC on the smartphone itself.

Table I summarizes the key features and limitations of existing MA connectivity implementations.

TABLE I: Implementation feature comparison [5]–[8].

Feature / Study	MITRE	ROMARS	MANTRA	RMA (Previous)	Present Work
Authentication via UICC	No	No	No	No	Yes
Connectivity via COTS 5G Modem	No	No	No	No	Yes
MA Connectivity with Single Subscription	No	No	No	Yes	Yes
Over-the-air N3AN	Yes	No	Yes	Yes	Yes
COTS Smartphone Implementation	No	No	No	No	Yes

IV. PRACTICAL IMPLEMENTATION

In Section I-C, we outlined five key challenges associated with implementing MA connectivity on COTS Android smartphones. In this section, we progressively describe the proposed solutions addressing these challenges.

A. Enabling APDU-Based Authentication with the USIM

As a baseline, we used the open-source N3IWUE dialer project [9], previously employed in our earlier work [5]. A key limitation of this implementation is that sensitive subscriber credentials (e.g., K , SQN , OP/OPc) are stored in configuration files and used by the dialer to locally execute the MILENAGE functions and derive authentication parameters.

This approach is not standard-compliant, as subscriber credentials should remain protected within the USIM. Instead, the USIM should perform the MILENAGE computations internally and return only the resulting authentication parameters via APDU exchange [20]. To address this limitation, we implemented APDU-based authentication support in the dialer. The required functions were first developed and validated on Ubuntu using a smart-card reader, including support for *AUTS*-based re-synchronization, and were subsequently integrated into the Android-based dialer.

B. Further Dialer Extensions for Android Smartphones

In addition to APDU-based authentication support, the dialer was extended to support both single- and dual-subscription deployments. In the first mode, the 3GPP and non-3GPP accesses share a single subscription hosted on one UICC, while in the second mode, separate subscriptions are used for each access, which is particularly relevant for dual-SIM smartphones.

Furthermore, the original N3IWUE routing architecture was redesigned to accommodate Android networking constraints. As Virtual Routing and Forwarding (VRF) is not natively supported on standard Android devices, the proposed implementation adopts Policy-Based Routing (PBR), which is supported by the Android networking stack.

C. Implementation of the Dialer on the Application Processor

As described in Section II-B, due to the absence of a dedicated processor or hardware block for non-3GPP access, the dialer must be implemented on the application processor. This implementation introduces several significant technical challenges, including the isolation of the dialer runtime environment from the native Android system and secure interaction with the UICC through APDU exchange. Fig. 3 illustrates the runtime environment of the proposed implementation on the application processor. In the following, we describe how the presented architecture addresses each of these challenges.

1) *Environment Isolation*: In the proposed implementation, both the Android OS and the dialer environment operate on top of the same Linux kernel. However, the dialer is isolated from the native Android file system through the use of a *chroot* environment, which provides a separate root file

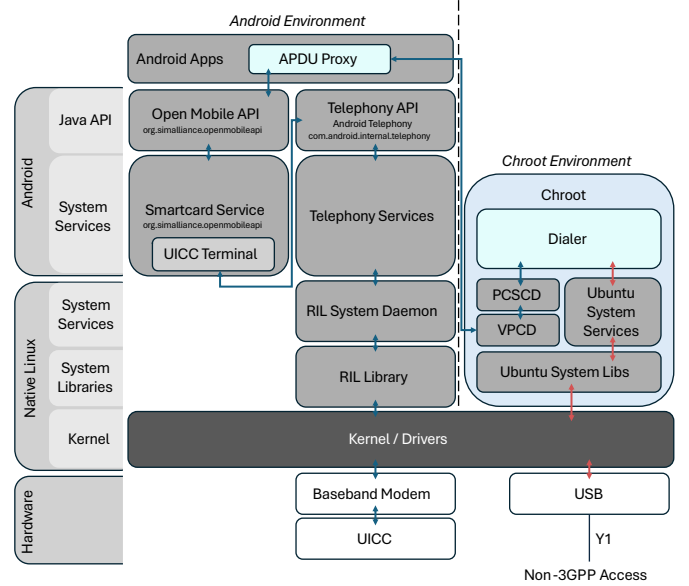


Fig. 3: Runtime environment of the proposed implementation. Blue arrows indicate the APDU-based communication path between the dialer and the UICC, while red arrows indicate the connectivity path toward the non-3GPP access network.

system for the dialer and its associated applications. Unlike a virtual machine, the chroot environment does not instantiate a separate guest operating system or kernel, but instead shares the underlying Linux kernel with Android while providing file-system-level isolation. This file-system separation simplifies the integration of Linux-based networking tools and dependencies while reducing interference with the native Android environment. Consequently, modifications performed within the chroot environment do not affect the Android file system outside the isolated environment.

A key practical consideration is that several networking functionalities required by the dialer, such as routing configuration and tunnel management, require root privileges. Therefore, the smartphone must operate in a rooted configuration.

2) *Secure Element Access*: Access to the secure element is enabled through the Open Mobile API (OMAPI), which provides a standardized Android interface for communication with secure elements such as the UICC [21]. In the proposed implementation, APDU exchange with the UICC is performed through an Android APDU proxy application [22] that interacts with the Radio Interface Layer (RIL) system daemon to forward APDU commands toward the modem and the UICC. The connection between the dialer environment running inside the chroot and the APDU proxy application is established using the *socat* utility, which relays socket-based communication between the Virtual Smart Card Reader (VPCD) operating inside the chroot and the Android APDU proxy application.

Additional details regarding UICC access on Android devices are provided in [21].

V. EXPERIMENTAL SETUP

Section II introduced the MA 5G system architecture with an untrusted additional access network. In this section, we present our smartphone-based implementation of the architecture illustrated in Fig. 1. Fig. 4 illustrates the experimental setup, in which a COTS Android smartphone serving as the UE simultaneously connects to the 5GC via 3GPP access over 5G NR (Band n78) and via non-3GPP access over L3Harris tactical radios.

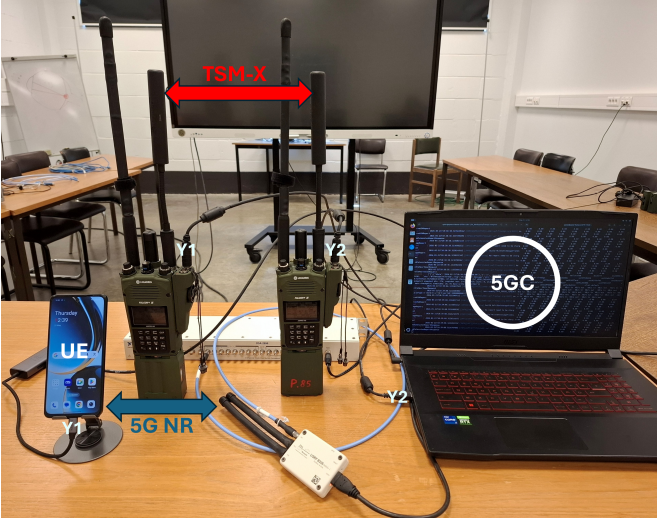


Fig. 4: Experimental setup of the proposed Multi-Access (MA) 5G system using a COTS smartphone and tactical radios.

COTS Smartphones with Integrated Dialer: We tested our implementation on the COTS Android smartphones listed in Table II. After rooting the smartphones, we installed the developed dialer within a chroot environment, as described in Section IV. We used programmable SIM cards to enable realistic authentication and key establishment procedures for both 3GPP and non-3GPP access.

TABLE II: COTS smartphones used in the experiments.

Smartphone	Model	Android Version	System on Chip (SoC)
OnePlus Nord CE 3 Lite	CPH2465	Android 14	Qualcomm Snapdragon 695 5G
OnePlus Nord N10 5G	BE2029	Android 10	Qualcomm Snapdragon 695 5G
Crosscall CORE-Z5	CORE-Z5	Android 14	Qualcomm QCM6490

3GPP Access Network: In this study, we used the standard 5G NR Band n78 spanning 3.3–3.8 GHz, with a channel bandwidth of 20 MHz and a subcarrier spacing of 30 kHz. The gNB was implemented using the open-source srsRAN Project [19] together with an Ettus USRP B205mini-i software-defined radio. An external stable 10 MHz reference clock was provided to the USRP using an Ettus OctoClock-G CDA-2990.

Non-3GPP Access Network: In parallel with the 5G NR access, a pair of L3Harris Falcon IV AN/PRC-163 tactical radios [23] provides the non-3GPP access connectivity between the smartphone and the 5GC. The radios use the protected TSM-X waveform operating at 1.785 GHz with a selected bandwidth of 20 MHz.

5GC: The 5GC is implemented on an Ubuntu 24.04 laptop using the open-source free5GC project (v4.0.1) [9]. free5GC is written in the Go programming language and includes N3IWF functionality to support N3ANs, making it well-suited for testing MA connectivity.

VI. PERFORMANCE MEASUREMENTS

To evaluate the proposed implementation, a programmable UICC was used to enable standard-compliant authentication and key establishment procedures for both 3GPP and non-3GPP access. The experiments were conducted using a One-Plus Nord CE 3 Lite smartphone running the developed dialer. After launching the dialer, signaling messages exchanged between the dialer and the N3IWF over the L3Harris tactical radio link establish secure NWu IPsec tunnels for both CP and UP traffic. These tunnels appear in the Android networking stack as distinct virtual network interfaces (e.g., `gretun-id-*`), used for routing and traffic forwarding over the tactical radio network.

Independently, the cellular modem also establishes additional network interfaces (e.g., `rmnet-*`), associated with the native 5G NR access network.

To evaluate the throughput performance, *iperf* measurements were conducted over a one-minute interval, with the client running on the smartphone and the server hosted on the laptop running the 5GC. Fig. 5 illustrates the measured throughput for each access network evaluated independently.

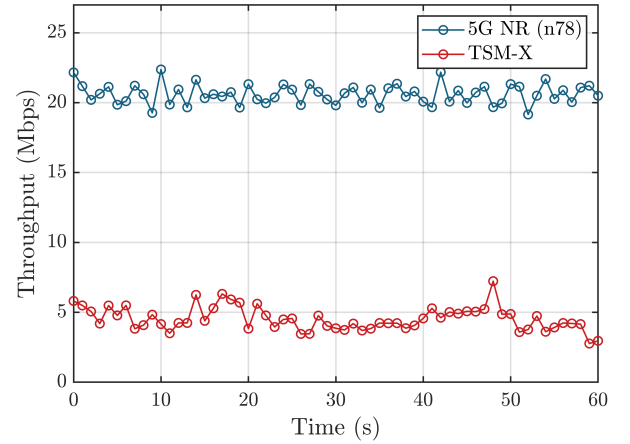


Fig. 5: Measured throughput over the 5G NR and L3Harris tactical radio (TSM-X) links.

We measured the average throughput and delay over each access network during a three-minute interval. The delay was evaluated by sending ICMP *ping* messages toward the N6

TABLE III: Performance Metrics of the Access Networks.

Access Network	Average Throughput (Mbps)	Average RTT Latency (ms)
5G NR	20.60 $\pm$ 0.71	30.32 $\pm$ 5.9
TSM-X	4.15 $\pm$ 0.91	98.59 $\pm$ 26.74

UPF interface. Table III summarizes the observed performance metrics for each access network.

The observed throughput and latency for the 5G NR access are well aligned with the performance values reported by the srsRAN Project for COTS smartphone experiments using the USRP B205mini-i platform [19]. Similarly, the measured performance metrics for the L3Harris radios align with the expected performance characteristics of the selected TSM-X configurations [23].

The same experimental procedures were subsequently repeated on the additional Android smartphones listed in Table II. In all cases, the UE successfully registered to the 5GC through both 3GPP and non-3GPP access networks, while similar performance metrics were observed across all devices.

VII. CONCLUSIONS

This paper presented a standard-compliant implementation of MA connectivity on COTS Android smartphones. The proposed dialer addressed several practical challenges related to enabling non-3GPP access on smartphone platforms. In particular, the dialer was significantly enhanced to support APDU-based USIM authentication, single- and dual-subscription deployments, runtime environment isolation from the Android OS, and secure element access from the application processor.

Experimental results demonstrated successful simultaneous connectivity to the 5GC through both native 5G NR and non-3GPP tactical radio access. The developed dialer successfully established secure NWu IPsec tunnels over the tactical radio network while maintaining 5G NR connectivity through the commercial modem. Throughput and latency measurements further confirmed the practical feasibility of the proposed implementation across multiple Android smartphone platforms.

The presented implementation highlights the potential of MA connectivity to transform commercial smartphones into resilient multi-access 5G communication platforms for contested environments.

VIII. FUTURE WORK

The present implementation enables simultaneous and independent connectivity to the 5GC through both 3GPP and non-3GPP access networks on COTS Android smartphones. As future work, this capability could be extended to support ATSSS, enabling fine-grained traffic management across the available access networks. This would allow traffic flows to be dynamically distributed, switched, or aggregated according to network conditions, application requirements, or operational policies.

ACKNOWLEDGMENT

The authors would like to sincerely thank the Belgian Defence CC V&C—Department of Operational C³ Systems—Tactical Intranet for their valuable support and assistance with tactical radios.

REFERENCES

- [1] NATO STO, “5th generation international mobile telecommunications (5G) technologies application to NATO operations,” Technical Report STO-TR-IST-187, 2025.
- [2] T. M. Bonds, M. Lee, N. A. O’Donoghue, B. F. D. Bruhl, S. Ayuk, T. Hamilton, R. Steeb, and G. J. Briggs, *Harnessing 5G-Era Innovations: Preparations Allies Could Make to Defend Against Attack*. Santa Monica, CA: RAND Corporation, 2025.
- [3] 3GPP, “Access to the 3GPP 5G core network (5GCN) via non-3GPP access networks,” Technical Specification TS 24.502, 2018.
- [4] F. Zampognaro, D. Verde, M. Luglio, and C. Roseti, “Local edge-services through N3IWF in 5G networks,” in *2024 IEEE International Mediterranean Conference on Communications and Networking (Med-NetCom)*, 2024, pp. 19–24.
- [5] P. Ebrahimbabaie, N. Prakopetz, and M. Becquaert, “Seamless integration of tactical radios into multi-access 5G systems,” in *2026 International Conference on Military Communication and Information Systems (ICMCIS)*, 2026.
- [6] I. Chen, S. Abdallah, F. Xie, and V. Ramaswamy, “Using 5G to integrate heterogeneous networks with improved traffic engineering,” in *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 2024, pp. 1192–1197.
- [7] M. Broner, S. Lee, L. Jin, and R. Stoleru, “5G-MANTRA: Multi-access network testbed for research on ATSSS,” in *Proceedings of the 3rd ACM Workshop on 5G and Beyond Network Measurements, Modeling, and Use Cases*, 2023, pp. 8–13.
- [8] M. Quadri, D. Verde, M. Luglio, C. Roseti, and F. Zampognaro, “Implementation and testing of MP-TCP atss in a 5G multi-access configuration,” in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, 2023, pp. 1–6.
- [9] free5GC. (2024) free5GC user guide. Accessed: 2026-01-09. [Online]. Available: <https://free5gc.org/guide/>
- [10] F. Ferraz. (2022) NWu-Non3GPP-5GC client. Accessed: 2026-01-09. [Online]. Available: <https://github.com/fasferraz/NWu-Non3GPP-5GC>
- [11] 3GPP, “Technical specification group services and system aspects; system architecture for the 5G system,” Technical Specification TS 23.501, 2018.
- [12] —, “Security architecture and procedures for 5G system ; release 15,” Technical Specification TS 21.915, 2021.
- [13] Internet Engineering Task Force (IETF), “RFC 5996: Internet key exchange protocol version 2 (IKEv2),” RFC 5996, 2010. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5996>
- [14] 3GPP, “Access traffic steering, switching and splitting (ATSSS),” Technical Specification TS 24.193, 2018.
- [15] 3GPP, “Non-access-stratum (NAS) protocol for 5G system (5GS),” Technical Specification TS 24.501, 2026.
- [16] S. K. Das, *Mobile terminal receiver design: LTE and LTE-Advanced*. John Wiley & Sons, 2017.
- [17] 3GPP, “UICC-terminal interface; physical and logical characteristics,” Technical Specification TS 31.101, 2025.
- [18] A. Güngör. (2023) UERANSIM. [Online]. Available: https://gitlab.com/lin_public_group/UERANSIM
- [19] srsRAN. (2025) srsRAN Project. [Online]. Available: https://github.com/srsran/srsRAN_Project
- [20] 3GPP, “Remote APDU structure for (U)SIM toolkit applications,” Technical Specification TS 31.116, 2025.
- [21] M. Roland and M. Hölzl, “Open mobile api: Accessing the UICC on android devices,” *arXiv preprint arXiv:1601.03027*, 2016.
- [22] Osmocom. (2026) Android APDU proxy. Accessed: 2026-05-10. [Online]. Available: <https://gitea.osmocom.org/sim-card/android-apdu-proxy>
- [23] L3Harris Technologies. (2025) AN/PRC-163 multi-channel handheld radio. Accessed: 2026-05-26. [Online]. Available: <https://www.l3harris.com/all-capabilities/an-prc-163-multi-channel-handheld-radio>