

Seamless Integration of Tactical Radios into Multi-Access 5G Systems

Pouyan Ebrahimbabaie, Nathan Prakopetz, Mathias Becquaert
Department of Communications, Information, Systems and Sensors (CISS)
Royal Military Academy (RMA)
Brussels, Belgium

{pouyan.ebrahimbabaievarnosfaderani, nathan.prakopetz, mathias.becquaert}@mil.be

Abstract—The 3rd Generation Partnership Project (3GPP) Release 15 introduced 5G technology, offering significant operational advantages for military communications. However, its radio access technology, 5G New Radio (NR), remains vulnerable to a range of threats. The Multi-Access (MA) connectivity feature enables 5G services over both 5G NR and non-3GPP access networks. In Release 16, MA connectivity is enhanced through Access Traffic Steering, Switching, and Splitting (ATSSS), ensuring seamless service continuity across heterogeneous networks. Recognizing MA connectivity as a mitigation measure, this paper presents a standards-compliant, open-source implementation of ATSSS using Multipath TCP (MPTCP) in an MA 5G system integrating tactical radios as non-3GPP access alongside 5G NR. Validation using over-the-air 5G NR and L3Harris AN/PRC-152A tactical radios demonstrates seamless failover and load balancing, confirming the operational relevance of MPTCP-based ATSSS for military applications.

This paper was originally presented at the International Conference on Military Communication and Information Systems (ICMCIS), organized by the Information Systems Technology (IST) Scientific and Technical Committee, IST-224-RSY – the ICMCIS, held in Bath, United Kingdom, 12-13 May 2026.

Index Terms—5G, ATSSS, MPTCP, N3IWF, Tactical radios.

I. INTRODUCTION

The fifth generation of mobile technology (5G) has received significant attention from defense organizations since its early standardization. Unlike prior generations, it was designed from the outset to support mission-critical use cases, making it of particular interest to military stakeholders [1]–[6]. 5G technology offers solutions that meet the demanding requirements for data throughput, latency, reliability, and connectivity in complex military scenarios [1], [2], [5]. A notable example of such scenarios is Multi-Domain Operations (MDO), which requires seamless orchestration across land, maritime, air, space, and cyberspace domains [4], [7].

A. 5G in Military Applications: Opportunities and Challenges

Recognizing 5G as a key enabler of MDO, NATO considers it a cornerstone of its Next Generation Networks (NGN) strategy and one of its priority Emerging Disruptive Technologies (EDTs), alongside Artificial Intelligence and Quantum Technologies [4]. Accordingly, NATO has launched research and standardization initiatives to both explore the operational opportunities of 5G and assess the risks associated with its applications in military contexts [1]–[3], [8].

A major effort in this area is NATO Research Task Group (RTG) IST-187 (5G Technologies Application to NATO Operations), which examined the application of 5G features, such as network slicing, multi-access edge computing, and massive MIMO, across a wide range of military use cases [1]. The study highlighted the potential of 5G to enable novel or improved military capabilities. In parallel, it conducted a comprehensive threat assessment, identifying vulnerabilities against 16 attack types, including hardware attacks, jamming, spoofing, eavesdropping, and others [8].

Building on the results of IST-187, RTG IST-220 (NATO Wireless Communications Standards Project) aims to develop NATO-specific 5G standards (e.g., STANAG 5665) to ensure interoperability and consistent implementation among member nations [1]. The effort also seeks to identify operational requirements not addressed by current 5G standards and submit these gaps to relevant standardization forums for future releases [1].

B. 5G Vulnerabilities Observed in a Military Field Deployment

While 5G offers notable operational advantages, its civilian-oriented design poses challenges when deployed in contested or combat environments [1]. As outlined in the IST-187 technical report (Annex E: Security Mechanisms), electronic warfare (EW) threats, particularly jamming and network disruption, are expected in future combat scenarios, and existing 5G security mechanisms provide limited mitigation [1]. Similar conclusions are reported in U.S. Department of Defense (DoD)–commissioned RAND studies, which note that although 5G can significantly enhance military capabilities, it remains vulnerable to EW threats, especially jamming [5], [6].

As 5G systems are increasingly deployed in military environments, evaluating their security under realistic field conditions becomes essential. To this end, the Royal Military Academy (RMA), in collaboration with Belgian Defence, conducted a practical study of a 5G Standalone (SA) system deployed at Beauvechain Air Base (ICAO: EBBE) [9].

A structured threat analysis is applied, classifying attacks as *active* or *passive*. Active attacks directly disrupt or interact with the system, whereas passive attacks rely on eavesdropping without affecting ongoing communications. Representative attacks were selected from each category: jamming, fuzzing, and

overshadowing for active attacks, and traffic fingerprinting, bandwidth monitoring, and localization for passive attacks [9].

Each attack was first implemented and evaluated in the laboratory, followed by field testing. Vulnerabilities were assessed using established risk assessment methodologies, including the Factor Analysis of Information Risk (FAIR) framework [10].

Fig. 1 illustrates the spectrograms of two selected attacks recorded during field testing: downlink jamming and a False Base Station (FBS) attack [9].

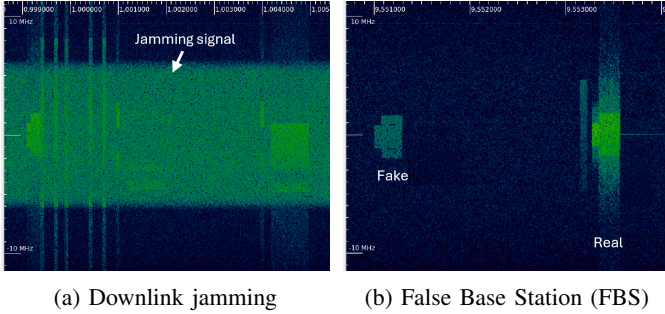


Fig. 1: Spectrograms captured during field testing.

In the jamming scenario, a directional interference signal caused the Signal-to-Noise Ratio (SNR) at the UE to drop sharply to -15 dB, leading to a disconnect. During the FBS attack, the UE intermittently connected to a malicious base station at a nearby frequency, demonstrating potential for eavesdropping, network reconnaissance, or Denial-of-Service (DoS) attacks.

A review of studies conducted by IST-187, RAND, and RMA reveals that the 5G air interface, known as 5G New Radio (NR), is particularly vulnerable to a wide range of attacks [1], [5], [6], [8], [9]. Therefore, it is essential to develop, evaluate, and implement robust mitigation techniques to enable the reliable use of 5G in military applications.

C. Multi-Access Connectivity as a Standard-Driven Mitigation Technique

NATO terminology defines *mitigation* as “actions to reduce the probability of a *risk* occurring and to reduce its impact if it occurs” [11]. Recognizing *communication disruption* and *eavesdropping* as the primary risks associated with 5G NR, IST-187 mitigation measures focus on preventing these events, that is, *reducing the probability* of a successful attack [1].

For instance, IST-187 technical report (Annex C.5: Jamming and Jamming Mitigation Techniques) recommends mitigating jamming by (1) using the beam-steering capabilities of massive MIMO (mMIMO) to suppress interference, or (2) employing millimeter-wave (mmWave) frequencies, which require an adversary to transmit jamming signals at higher power [1]. These approaches align with mitigation measures that focus on reducing the likelihood of a successful attack.

The present research investigates the application of the *Multi-Access* (MA) connectivity feature as a mitigation measure to reduce the potential impacts of communication disruption and eavesdropping in 5G NR. This mitigation approach

focuses on the second part of NATO’s definition of mitigation, namely *reducing the impact* of a successful attack on the air interface.

MA connectivity is a native 5G feature that allows a UE to maintain simultaneous connections to the 5G Core (5GC) through the 5G radio access and other *access networks*, while leveraging key 5GC services [12], [13]. Although MA connectivity was not originally designed as a security mitigation mechanism, its primary purpose is to ensure seamless and uninterrupted service when a UE transitions between access networks, such as between indoor Wi-Fi (WLAN IEEE 802.11) and 5G [14]–[16].

The MA connectivity feature is further enhanced in Release 16 through the introduction of Access Traffic Steering, Switching, and Splitting (ATSSS) [17], [18]. ATSSS enables precise control of ongoing traffic by allowing the data flow to be steered, switched, or split across multiple access networks. This capability supports seamless traffic transfer between the 5G access network and other access networks without service interruption [18]. The standard defines several approaches for implementing ATSSS, which are described in the following sections.

MA connectivity has increasingly attracted interest for military applications because of its potential to enhance resilience against communication disruption and eavesdropping [19]. This is particularly relevant when a tactical access network is available as an additional access. In the event of a communication disruption, MA connectivity provides a secure backup connection, allowing data to continue flowing seamlessly if the 5G link fails. With respect to eavesdropping, data flows can be split across access networks so that, even if an adversary intercepts traffic on the 5G link, only a portion of the message is exposed.

This paper presents a detailed implementation of ATSSS based on the Multipath Transmission Control Protocol (MPTCP) [17], [20], [21] in a multi-access 5G system. The implementation is demonstrated in a practical setup, where L3Harris Falcon III AN/PRC-152A tactical radios serve as an additional access network [22]. To the best of our knowledge, this work is the first to provide an open-source, standards-compliant, MPTCP-based implementation of ATSSS for both the UE and the 5G core.

The structure of this work is as follows. Section II presents the theoretical background of multi-access 5G systems and provides an overview of the ATSSS framework, with a focus on MPTCP. Section III summarizes relevant contributions from the literature and highlights the novelty of the present research. Section IV describes our experimental setup. Section V presents the performance evaluation across multiple scenarios. Section VI concludes the paper, and Section VII discusses future research directions.

II. BACKGROUND

The 3rd Generation Partnership Project (3GPP) Release 15 marked the beginning of the 5G era, introducing substantial

architectural changes and a wide range of new features compared to previous generations [13]. The 5G system architecture consists of two major components: (1) the New Radio Access Network (NG-RAN), which supports the 5G NR, and (2) the 5GC.

The 5G system architecture is RAN-agnostic [23], allowing a UE to connect to the 5GC via both the NG-RAN and Non-3GPP Access Networks (N3ANs), while leveraging a broad set of 5GC services, including Quality of Service (QoS) control and network slicing [12], [14], [24]. 3GPP specifications further allow a UE to be simultaneously registered over both 3GPP and non-3GPP access networks [13].

3GPP specifications define three types of N3ANs [12]: (1) *untrusted* (Release 15), (2) *trusted* (Release 16), and (3) *wired* (Release 16).

For an untrusted N3AN, the Mobile Network Operator (MNO) cannot rely on the security provided by the N3AN. Consequently, all traffic must be protected through secure mechanisms controlled by the operator. In contrast, a trusted N3AN assumes that the operator has full control over the Trusted Non-3GPP Access Point (TNAP) and the radio link [12]. In this case, encryption and other security measures may be managed directly by the operator or delegated to the access network. Wired N3AN refers to a category of UEs that represent stationary devices using wired access technologies to connect to the 5GC [12].

The present research focuses on untrusted N3ANs operating outside the MNO's control. Accordingly, in the following discussion, the term N3AN is used specifically to refer to this untrusted variant.

Additional details regarding other types of N3ANs can be found in [12].

A. Multi-Access 5G Systems

In an MA 5G system, the UE connects to the 5G core simultaneously through both 3GPP and non-3GPP access networks [13]. Fig. 2 illustrates an MA 5G system architecture in which the UE additionally accesses the 5GC via an untrusted N3AN using the Non-3GPP Interworking Function (N3IWF).

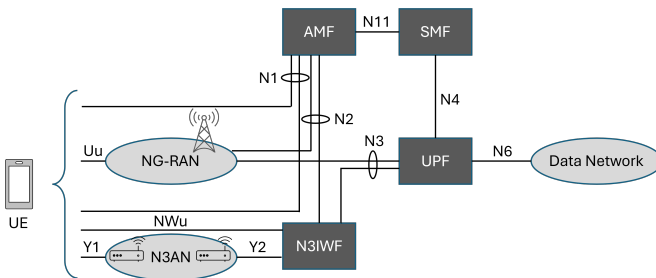


Fig. 2: Multi-Access (MA) 5G system architecture with an untrusted Non-3GPP Access Network (N3AN).

The N3IWF acts as a secure gateway between the N3AN and the 5GC, supporting the N2 interface to the Access and Mobility Management Function (AMF) and the N3 interface to the User Plane Function (UPF). It enables the UE to securely

access the 5GC over the untrusted network by establishing IPsec (IPsec) tunnels, referred to as the NWu interface [12], [13].

NWu tunnels are established using the Internet Key Exchange version 2 (IKEv2) protocol [25], which provides mutual authentication, negotiates Security Associations (SA), and manages cryptographic keys between the UE and the N3IWF. Upon completion of the IKEv2 exchanges, secure IPsec tunnels are created to ensure the confidentiality and integrity of both Control Plane (CP) and User Plane (UP) traffic over untrusted access networks [12].

In addition to securing communications, the N3IWF is responsible for enforcing end-to-end QoS over the N3AN. It maps the QoS flows, based on its policies and the QoS profiles sent by the UE, to the available resources in the N3AN. To achieve this, the N3IWF determines the required number of IPsec Child SAs and dynamically binds each Child SA to the corresponding QoS flow in a Protocol Data Unit (PDU) session. This mapping ensures that different traffic types, such as latency-sensitive or high-throughput services, receive appropriate treatment over the untrusted access network [12]. It should be noted that a PDU session may encompass multiple QoS flows.

Additional details regarding NWu tunnels establishment and QoS mapping can be found in [12], [13].

B. Access Traffic Steering, Switching and Splitting (ATSSS)

3GPP Release 16 introduced the ATSSS feature as an enhancement to the MA 5G system architecture [17]. Technical Report (TR) 23.793 (Study on Access Traffic Steering, Switch and Splitting support in the 5G system architecture) outlines four fundamental concepts that subsequently form the basis of the ATSSS-related Technical Specifications (TSs) TS 24.193 and TS 29.244 [17], [20]. These foundational concepts are [26], [27]:

- *MA PDU session*: A PDU session in which traffic may be carried over NG-RAN, N3AN, or both.
- *Steering*: The procedure that chooses an access network for a new data flow and directs the traffic over the selected access.
- *Switching*: The procedure that transfers all traffic of an ongoing data flow from one access network to another while maintaining continuity.
- *Splitting*: The procedure that distributes the traffic of an ongoing data flow across multiple access networks simultaneously.

Fig. 3 illustrates the high-level architecture of a MA 5G system with the new functionalities introduced to support ATSSS [26], [27].

As depicted in Fig. 3, enabling ATSSS requires enhancements in both the UE and the 5GC. These enhancements begin with extending Policy Control Function (PCF) policy rules to support ATSSS. The PCF delivers the extended policy rules to the Session Management Function (SMF) over the N7 interface. Based on these policy rules, the SMF derives ATSSS rules [27]. The SMF delivers ATSSS rules for uplink traffic

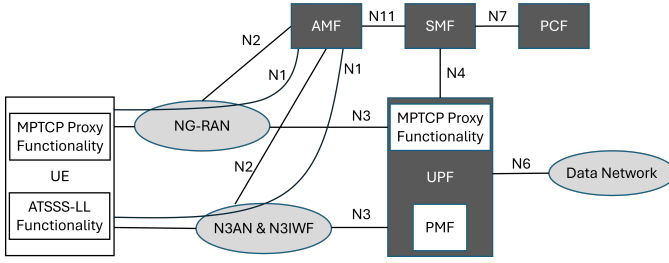


Fig. 3: High-level architecture of a Multi-Access (MA) 5G system supporting Access Traffic Steering, Switching and Splitting (ATSSS).

to the UE via a Non-Access Stratum (NAS) message upon establishment of the MA PDU session. For downlink traffic, the SMF delivers ATSSS rules, referred to as N4 rules, to the UPF over the N4 interface [17], [27].

Additional details regarding the delivery of the ATSSS rules could be found in TS 23.502 (Clause 4.22) [28].

C. Steering Functionality and Steering Mode

ATSSS rules specify the transport mechanisms through two key elements, namely the *steering functionality* and the *steering mode* [27], [29].

Steering functionality enables the steering, switching, and splitting of MA PDU session traffic across 3GPP and non-3GPP accesses. It is divided into two categories according to the protocol layer on which it operates: (1) above the IP layer, referred to as ATSSS High Layer (ATSSS-HL), and (2) below the IP layer, referred to as ATSSS Low Layer (ATSSS-LL) [27].

Release 16 introduced ATSSS-HL through MPTCP, which provides steering functionality at the transport layer by logically combining multiple TCP subflows, as specified in RFC 8684 [21]. Release 17 further expands ATSSS-HL by introducing another HL steering functionality based on the Quick UDP Internet Connections (QUIC) protocol, called Multipath QUIC (MPQUIC), which enables multipath support for UDP connections, as specified in RFC 9000 [30].

Release 16 introduced ATSSS-LL, which relies on a scheduler implemented below the IP layer to steer incoming packets to one of the available access networks based on rules configured in the UE or the UPF [17]. Unlike multipath transport protocols, ATSSS-LL is agnostic to traffic type and supports multi-access transport for UDP, TCP, Ethernet, and other flows. However, it does not provide key functionalities typically offered by multipath protocols, such as packet re-ordering, congestion control, flow control, or delay and loss-rate measurements [18].

Steering mode specifies how traffic belonging to a specific Service Data Flow (SDF) is distributed across 3GPP and non-3GPP access networks [29]. Release 16 outlines the following steering modes [17]:

- *Active-standby*: One access network is designated as active, while the other serves as standby. The standby

network is utilized when the active network becomes unavailable.

- *Smallest delay*: Traffic is steered to the access network with the smallest Round-Trip Time (RTT), commonly referred to as the best-access mode. Future enhancements extend this concept by incorporating additional metrics, such as SNR. This steering mode applies only to non-Guaranteed Bit Rate (non-GBR) SDFs.
- *Load balancing*: Traffic is divided between access networks according to a configured percentage. This steering mode applies only to non-GBR SDFs.
- *Priority-based*: Either the 3GPP or the non-3GPP access is assigned higher priority, and traffic is steered to the prioritized access unless it becomes congested or unavailable. This steering mode applies only to non-GBR SDFs.

The list of steering modes expands with new releases. Each steering functionality may incorporate some or all of the available modes.

Additional details regarding ATSSS rules could be found in TS 24.193 (Clause 6.1.3) [17].

D. ATSSS High Layer Implementation Using MPTCP Proxy

MPTCP is an extension of standard TCP that enables a single logical connection between two *hosts*, rather than connecting individual *interfaces* as in standard TCP. Each host may have multiple interfaces, aka *endpoints*, allowing connections to use multiple network paths simultaneously [31]. Unlike standard TCP, which transmits data over a single path between two IP addresses, MPTCP can create multiple *subflows* across different paths while maintaining a single logical connection. This capability improves resource utilization, enhances resilience to network failures, and ensures uninterrupted service if one path becomes unavailable. MPTCP remains compatible with standard TCP by using the TCP field header called "option" for signaling, with option 30 specifically reserved for MPTCP [31].

Fig. 4 illustrates a comparison between the TCP and MPTCP protocol stacks [32].

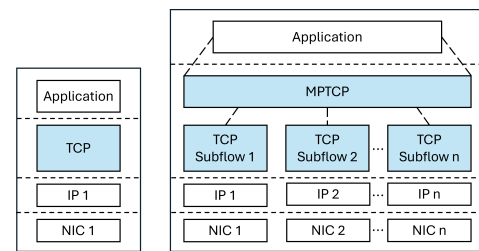


Fig. 4: TCP and Multipath TCP (MPTCP) protocol stacks.

To date, extensive research has been conducted on MPTCP, with a strong focus on minimizing host-side modifications and maintaining transparency for upper-layer applications. However, real-world deployment of MPTCP is still limited. The primary challenge is enabling MPTCP support across all end hosts, as the diversity of devices complicates large-scale deployment [33]. A key question is how to enable hosts to

benefit from MPTCP without imposing significant burdens. One promising solution is to use a network-based MPTCP proxy, which provides support for hosts that do not natively support MPTCP [33].

The MPTCP proxy facilitates conversion between MPTCP and TCP. Fig. 5 illustrates a typical deployment scenario involving an MPTCP-capable client and an MPTCP-incapable server.

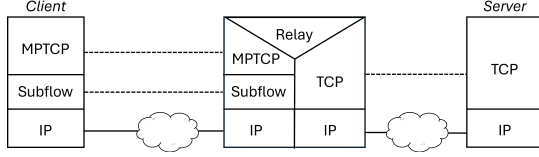


Fig. 5: A typical MPTCP proxy deployment scenario.

Additional details regarding other deployments could be found in [33].

One of the primary use cases envisioned during the early standardization of MPTCP involves mobile devices, such as smartphones, equipped with both cellular and Wi-Fi interfaces [31]. Each interface is assigned a distinct IP address, enabling the device to establish multiple endpoints.

Consistent with the MPTCP standard developments, 3GPP Release 16 introduced ATSSS-HL based on MPTCP for communication across heterogeneous access networks [17], [20]. TS 29.244 (Annex E) specifies the high-level architecture of a 5G system supporting ATSSS based on MPTCP. Figure 6 shows the corresponding system overview [20].

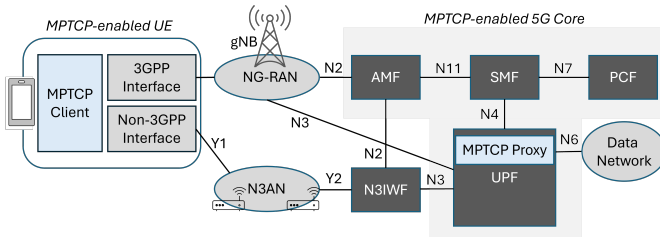


Fig. 6: High-level architecture of a 5G system supporting ATSSS based on MPTCP.

As illustrated in Fig. 6, enabling MPTCP-based ATSSS requires enhancements at both the 5G core and the UE. On the core side, the UPF is extended with an MPTCP proxy server located at the N6 interface. On the UE side, an MPTCP proxy client is deployed, which establishes connections to both 3GPP and non-3GPP access endpoints, each associated with a distinct IP address [34].

On the UE side, each 3GPP and non-3GPP access endpoint may be assigned an operational role, namely *backup*, *non-backup*, or *full-mesh* [31]. An endpoint configured as backup is reserved for *failover* and is activated only when all non-backup subflows become unavailable, for example, due to link failures on other access networks. In full-mesh mode, packets are transmitted concurrently over all available access endpoints. If

one access becomes unavailable, traffic is automatically shifted to the remaining access, thereby ensuring seamless failover.

III. RELATED WORK

Since the introduction of ATSSS in 3GPP Release 16, the topic has received considerable research attention. This section reviews the relevant studies and highlights how the present work addresses existing gaps.

A recent study by MITRE presented a prototype multi-access 5G system [19]. The implementation combines a Silvus radio network as the non-3GPP access network, the open-source free5GC as the 5G core, and open-source UERAN-SIM [35] to emulate the NG-RAN. While Free5GC supports N3IWF functionality, it lacks ATSSS-related enhancements in the core. Since the UE and core did not fully implement 3GPP-defined ATSSS functionalities, the feature was emulated using conventional IP forwarding mechanisms available in Linux and other UNIX-based systems. Consequently, the ATSSS implementation does not comply with the 3GPP specifications [19]. In addition, because UERANSIM is used to emulate the UE and gNB behavior rather than a real 5G NR air interface, the throughput observed in the 3GPP access network does not reflect a true over-the-air 5G NR deployment.

A study conducted by ROMARS investigated the use of Satellite Communications (SATCOM) as N3AN in a multi-access 5G system [34]. The study employed the open-source OpenSand environment to emulate satellite communication. Proprietary UE and 5G core implementations were built upon UERANSIM and free5GC to support MPTCP-based ATSSS. Consequently, the UE and core are not publicly available, limiting their use or experimentation by external researchers. Similar to MITRE's approach, ROMARS used UERANSIM, so the results do not fully represent an over-the-air 5G NR deployment.

Another relevant project is MANTRA [36], which primarily focuses on prototyping a multi-access LTE system and providing non-3GPP access support for 5G Non-Standalone (NSA) deployments. The architecture combines the N3IWF from free5GC with another open-source core, Open5GS. MANTRA employs a USB dongle that provides both WiFi and LTE connectivity and introduces a custom transport converter that functions as an MPTCP proxy. However, the UE implementation is fully proprietary, and the absence of a publicly available core limits its accessibility for independent research. Furthermore, MANTRA also considers a so-called *real-world deployment* option in which the non-3GPP access network bypasses the 5G core and connects directly to the proxy. In this configuration, traffic does not traverse the N3IWF, and IPsec security associations are not established. As a result, this deployment option does not comply with the 3GPP specifications as detailed in Section II. In addition, it does not implement a 5G NR over-the-air deployment.

The present research delivers an open-source ATSSS implementation based on MPTCP, compliant with 3GPP specifications [20]. Unlike prior studies that use UERANSIM to emulate the UE and NG-RAN [19], [34], this study introduces

a testbed that closely reflects real-world conditions, employing the srsRAN open-source project [37], [38] with a pair of SDRs (Ettus USRP B205mini-i [39]) for the NG-RAN and L3Harris Falcon III AN/PRC-152A tactical radios as the N3AN [22].

Table I compares the implemented features across the relevant studies and the present work.

TABLE I: Comparison of implementation features in MITRE [19], ROMARS [34], MANTRA [36] studies, and the present work.

Feature / Study	MITRE	ROMARS	MANTRA	Present Work
ATSSS compliant with 3GPP	No	Yes	No	Yes
Open-source UE and core	Yes (Free5GC)	No	No	Yes
Over-the-air 5G NR	No (UERANSIM)	No (UERANSIM)	No (LTE via dongle)	Yes (srsRAN + USRP)
Over-the-air N3AN	Yes (Silvus radio)	No (OpenSand)	Yes (WiFi via dongle)	Yes (L3Harris radios)

IV. EXPERIMENTAL SETUP

Section II-D introduced the ATSSS-HL implementation based on an MPTCP proxy. In this section, we detail the step-by-step realization of the architecture illustrated in Fig. 6. Fig. 7 shows the experimental setup, which consists of two Linux-based laptops acting as the UE and the 5G core. These devices are interfaced with USRP platforms and L3Harris radios, providing 3GPP and non-3GPP radio access connectivity.



Fig. 7: Experimental setup for the MPTCP-based ATSSS implementation.

3GPP Access Network: The 5G NR deployment is implemented using the open-source srsRAN project [37], [38] together with a pair of software-defined radios (Ettus USRP B205mini-i [39]). The USRPs are synchronized using an external 10 MHz reference clock provided by an Ettus OctoClock-G CDA-2990. The srsRAN gNB operates in NR band 3 with a subcarrier spacing of 15 kHz and a channel bandwidth of 20 MHz, corresponding to 106 Physical Resource Blocks (PRBs).

N3AN: In parallel with the USRP-based setup, a pair of L3Harris Falcon III AN/PRC-152A tactical radios [22]

are connected to the laptops to provide non-3GPP access. The radios are configured in a point-to-point topology using the Communications Planning Application (CPA). The radios operate using the ANW2C waveform at a carrier frequency of 230 MHz with a channel bandwidth of 1.2 MHz. Depending on the selected modulation scheme (WF1–WF6), the achievable data rate ranges from 49 kbps to 1.37 Mbps.

N3AN dialer: Establishing the NWu interface between the UE and the N3IWF requires a dialer to handle signaling and securely set up CP and UP communication. In this study, we used N3IWUE [40], introduced by the free5GC project in 2024, which provides full compatibility with current free5GC releases without requiring any modifications to the core network.

5GC: Several open-source 5G core implementations exist, including Open5GS [41] and free5GC [42], both of which are compatible with the srsRAN project. In the present work, we use free5GC (v4.0.1), which is implemented in the Go programming language and provides N3IWF functionality to support N3AN. In contrast, Open5GS does not currently provide N3IWF.

MPTCP enhancements: As detailed in Section II-D, enabling ATSSS through MPTCP requires enhancements on both the UE and the 5GC. As depicted in Fig. 6, these enhancements include extending the UPF with an MPTCP proxy server on the N6 interface and deploying an MPTCP proxy client on the UE side, which manages the established IPs for both 3GPP and non-3GPP access networks as client “endpoints”.

Several open-source projects implement MPTCP proxies for general-purpose use [43], [44]. In this work, we use the MPTCP proxy implementation in [43], which is written in the Go programming language and is compatible with our Linux environment (Ubuntu 22.04 LTS). We deployed the proxy client from [43] on the UE side and the proxy server on the core network as an extension to the UPF. Additional details on deploying the MPTCP proxy client and server can be found in [31], [43].

V. PERFORMANCE MEASUREMENTS

As described in Section II-D, once the UE successfully registers with the core over both 3GPP and non-3GPP access, it is assigned two distinct IP addresses, one for each access network. In our experimental setup, described in Section IV, two separate network interfaces appear on the UE laptop upon successful registration: `i_5G` for the 3GPP access network and `i_ANW2C` for the non-3GPP access network.

From the perspective of the MPTCP client, these interfaces serve as separate endpoints for transmitting and receiving traffic, effectively creating two distinct paths. By configuring these endpoints differently, we can test both active-standby (switching) and load-balancing (splitting) modes. In the following subsections, we evaluate the performance of each mode in terms of per-access throughput, overall MPTCP throughput, and latency across MPTCP subflows. All experiments are conducted using iperf3, with the client and server running on

the UE and core laptops, respectively, targeting a bandwidth of 5 Mbps.

A. Active-standby (switching): 5G NR as active access and L3Harris radios (ANW2C) as backup

In this configuration, the i_5G endpoint is configured as active and the i_ANW2C endpoint as backup, corresponding to the 5G NR and ANW2C accesses, respectively. Fig. 8 shows the throughput of each access as well as the overall MPTCP throughput across both paths.

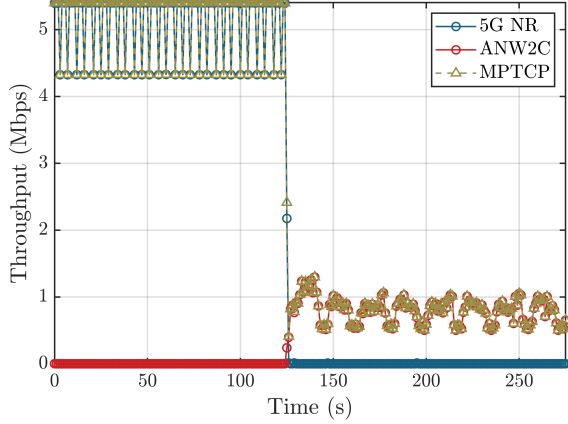


Fig. 8: Active-standby mode (switching): 5G NR as the active link and ANW2C as the backup.

As depicted in Fig. 8, when the 5G NR throughput drops sharply to zero after approximately 125 seconds, the ANW2C link takes over as part of the failover process and its throughput increases accordingly to compensate for the loss of the 5G NR access. As a result, the overall MPTCP throughput converges to the throughput achievable via the ANW2C.

B. Active-standby (switching): L3Harris radios (ANW2C) as active access and 5G NR as backup

In this configuration, the i_ANW2C endpoint is configured as active and the i_5G endpoint as backup. As a result, ANW2C operates as the primary access, while 5G NR serves as the backup access. Fig. 9 illustrates the throughput on each access and the overall MPTCP throughput across both accesses.

As shown in Fig. 9, when the ANW2C throughput drops to zero at approximately 36 seconds, the failover mechanism activates, and the 5G NR link assumes the primary role. Its throughput increases accordingly, compensating for the loss of the ANW2C link. Consequently, the overall MPTCP throughput converges to the target rate.

C. Load balancing (splitting): 5G NR and L3Harris radios (ANW2C) accesses are active simultaneously

In this configuration, both i_5G and i_ANW2C are configured as active MPTCP endpoints. Traffic is distributed across the 5G NR and ANW2C links, and if one link fails, traffic seamlessly fails over to the remaining link. Fig. 10

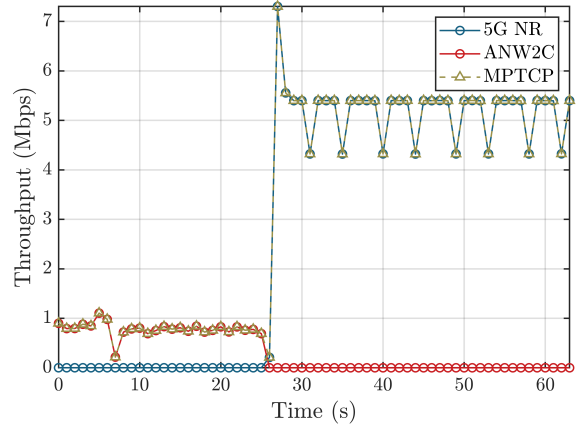


Fig. 9: Active-standby mode (switching): L3Harris radios (ANW2C) as the active link and 5G NR as the backup.

illustrates the throughput on each access and the overall MPTCP throughput across both accesses.

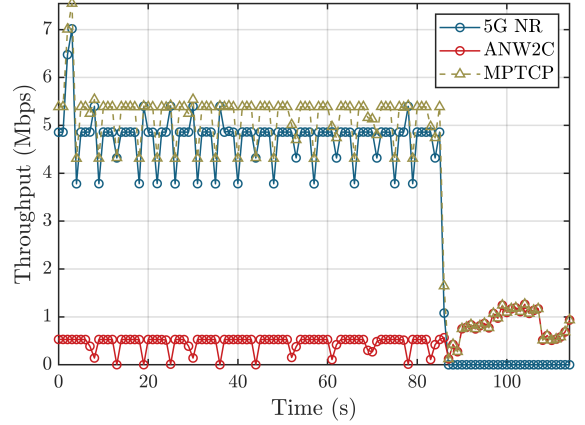


Fig. 10: Load-balancing mode (splitting): 5G NR and ANW2C operating as active links.

As shown in Fig. 10, traffic is distributed across the 5G NR and ANW2C accesses. When the 5G link fails, the ANW2C link takes over through the failover mechanism, and its throughput increases to reach the maximum achievable rate.

D. Comparison of Average Throughput

In this section, we compare the average throughput of individual access networks with the throughput achieved when both accesses are available and MPTCP is enabled. The throughput is measured over 60 seconds for three cases: 5G NR only, ANW2C only, and both accesses with MPTCP. Fig. 11 shows the resulting average throughput.

As depicted in Fig. 11, the average MPTCP throughput is approximately equal to that of the best-performing path, 5G NR. This behavior is consistent with the objectives of MPTCP's coupled congestion control mechanism [45]–[48], which follows the principle that “the total capacity that MPTCP occupies should equal the capacity that the best path

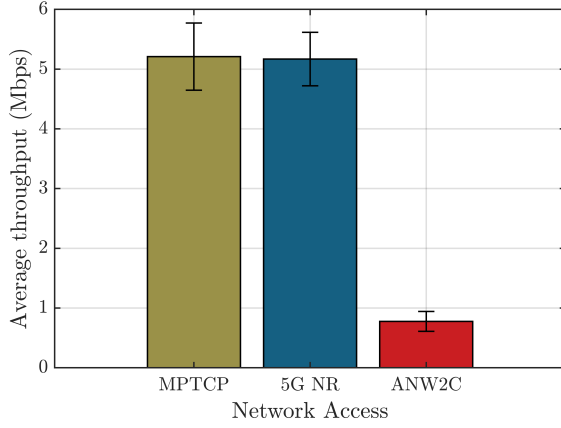


Fig. 11: Average throughput: MPTCP 5.21 ± 0.56 Mbps, 5G NR 5.17 ± 0.45 Mbps, and ANW2C 0.78 ± 0.17 Mbps.

can transport [48].” Another immediate observation is that the 5G NR access easily reaches the target throughput of 5 Mbps, whereas the ANW2C access achieves an average throughput of only about 0.78 Mbps.

Additional information regarding different MPTCP congestion control mechanisms and their objectives can be found in [46]–[48].

E. Latency Analysis of MPTCP Subflows

In this section, we analyze the latency experienced by MPTCP segments on each subflow when both 5G NR and ANW2C accesses are active. We monitored traffic using Wireshark on the *i_5G* and *i_ANW2C* endpoints and extracted the per-segment round-trip time (ACK RTT), calculated as $RTT_{Ack} = t_{ACK\ received} - t_{segment\ sent}$ for each MPTCP segment. Fig. 12 illustrates the ACK RTT of each MPTCP segment versus capture time.

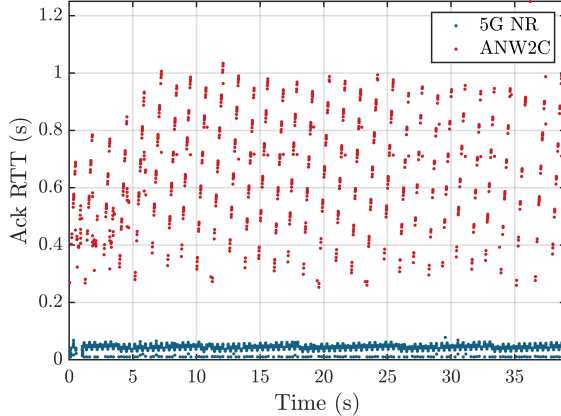


Fig. 12: ACK RTT of MPTCP segments: 43.8 ± 8.8 ms over 5G NR and 654.9 ± 185.4 ms over ANW2C.

As shown in Fig. 12, MPTCP segments transmitted over 5G NR exhibit significantly lower ACK RTT than those sent over ANW2C. This difference is consistent with the inherently lower latency of the 5G NR compared to ANW2C.

VI. CONCLUSIONS

This paper presented a practical and standards-compliant implementation of ATSSS based on MPTCP within a multi-access 5G system. The proposed architecture integrates tactical radios as an untrusted non-3GPP access network alongside a 5G NR access, enabling resilient multi-access connectivity for operational scenarios. Unlike prior studies that rely on emulation frameworks such as UERANSIM, the presented work employs a real over-the-air 5G NR deployment using the srsRAN open-source project and software-defined radios, combined with L3Harris tactical radios operating as the non-3GPP access.

The implementation extends the 5G core with an MPTCP proxy server integrated at the UPF and deploys a corresponding proxy client on the UE, aligned with 3GPP Release 16 specifications for ATSSS high-layer operation. Experimental results demonstrate expected ATSSS behavior across multiple steering modes, including active-standby and load-balancing. In active-standby scenarios, seamless failover is observed when the active access becomes unavailable, ensuring service continuity. In load-balancing mode, traffic is distributed across both access networks, while the aggregate throughput remains close to the capacity of the best-performing path, in accordance with the principles of MPTCP coupled congestion control. Latency measurements further highlight the heterogeneous characteristics of the integrated access networks, with substantially lower round-trip times over 5G NR compared to the tactical radio access.

The results confirm that MPTCP-based ATSSS can effectively enhance communication resilience by mitigating the impact of access-specific disruptions, such as those caused by jamming or link degradation. By combining open-source 5G technologies with tactical radio systems in a realistic deployment, this work demonstrates the feasibility and operational relevance of multi-access 5G architectures for defense applications.

VII. FUTURE WORK

As described in Section III, in addition to the standards-compliant architecture presented in this work, alternative architectures exist for implementing MPTCP-based ATSSS in real-world deployments. An alternative deployment model allows the non-3GPP access network to bypass the N3IWF and the 5G core and connect directly to the MPTCP proxy. As future work, we plan to conduct a comprehensive comparison of these architectures with respect to implementation complexity, service availability, scalability, security implications, performance, latency, and overall operational applicability for military deployments.

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] L. Bastos, G. Capela, A. Koprulu, and G. Elzinga, “Potential of 5G technologies for military application,” in *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1–8.
- [3] M. Damrath and A. Birutis, “Exploring the potential of 5G for maritime military communications,” in *2025 International Conference on Military Communication and Information Systems (ICMCIS)*, 2025, pp. 1–8.
- [4] NCIA. (2025) Technology Strategy towards 2030. Accessed: 2025-12-23. [Online]. Available: https://www.ncia.nato.int/resources/site1/General/newsroom/publications/Public_NCIA_Technology%20Strategy_external_v6%20-%20digital.pdf
- [5] 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.
- [6] M. Lee, J. Dimarogonas, E. Geist, S. Manuel, R. A. Schwankhart, and B. Downing, *Opportunities and Risks of 5G Military Use in Europe*. Santa Monica, CA: RAND Corporation, 2023.
- [7] NATO ACT. (2023) Multi-domain operations in NATO – explained. Accessed: 2025-12-29. [Online]. Available: <https://www.act.nato.int/article/mdo-in-nato-explained/>
- [8] J. M. Batalla, K. Wrona, D. Brown, F. Wiacek, U. Ruoto, and T. Wichary, “Threat assessment of 5G networks for military applications,” in *2024 International Conference on Military Communication and Information Systems (ICMCIS)*, 2024, pp. 01–10.
- [9] N. Prakopetz, “Security audit: 5G standalone installation at Beauvechain air base,” Royal Military Academy (RMA), Brussels, Belgium, Technical Report, 2025.
- [10] J. Freund and J. Jones, *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.
- [11] NATO NSO, “NATO glossary of terms and definitions (English and French),” Terms and Definitions AAP-06, 2020.
- [12] M. T. Lemes, A. M. Alberti, C. B. Both, A. C. D. O. Júnior, and K. V. Cardoso, “A tutorial on trusted and untrusted non-3GPP accesses in 5G systems—first steps toward a unified communications infrastructure,” *IEEE Access*, vol. 10, pp. 116 662–116 685, 2022.
- [13] S. Rommer, C. Mulligan, P. Hedman, M. Olsson, L. Frid, and S. Sultana, *The Core Network for 5G Advanced*. Academic Press, 2025.
- [14] 3GPP, “Access to the 3GPP 5G core network (5GCN) via non-3GPP access networks,” Technical Specification TS 24.502, 2018.
- [15] 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-ItCom)*, 2024, pp. 19–24.
- [16] A. K. Salkintzis, “A vision for multiaccess HTTP in 6G networks,” in *2025 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2025, pp. 1779–1784.
- [17] 3GPP, “Access traffic steering, switching and splitting (ATSSS),” Technical Specification TS 24.193, 2018.
- [18] A. K. Salkintzis, M. Kühlewind, S. Rommer, and R. Liebhart, “Multipath QUIC for access traffic steering switching and splitting in 5G advanced,” *IEEE Communications Standards Magazine*, vol. 7, no. 1, pp. 48–56, 2023.
- [19] 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.
- [20] 3GPP, “Interface between the control plane and the user plane nodes,” Technical Specification TS 29.244, 2018, Annex E: Procedures Related to MPTCP Functionality.
- [21] Internet Engineering Task Force (IETF), “RFC 8684: TCP extensions for multipath operation with multiple addresses,” RFC 8684, 2020. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc8684>
- [22] L3Harris Technologies. (2025) An/prc-152a wide-band networking handheld radio. Accessed: 2025-12-30. [Online]. Available: <https://www.l3harris.com/all-capabilities/falcon-iii-an-prc-152a-wideband-networking-handheld-radio>
- [23] S. Abdallah, F. Xie, I. Chen, and V. Ramaswamy, “Connecting first responders via a 5G access-agnostic network,” in *2024 IEEE World Forum on Public Safety Technology (WFPST)*, 2024, pp. 211–214.
- [24] 3GPP, “Technical specification group services and system aspects; system architecture for the 5G system,” Technical Specification TS 23.501, 2018.
- [25] 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>
- [26] 3GPP, “Study on access traffic steering, switch and splitting support in the 5G system architecture,” Technical Report TR 23.793, 2018.
- [27] Y. Kang and C. Kim, “A multi-access session management for ATSSS support in 5G network,” in *2019 25th Asia-Pacific Conference on Communications (APCC)*, 2019, pp. 409–412.
- [28] 3GPP, “Procedures for the 5G system (5GS),” Technical Specification TS 23.502, 2020.
- [29] —, “Policy and charging control framework for the 5G system (5GS),” Technical Specification TS 23.503, 2020.
- [30] Internet Engineering Task Force (IETF), “RFC 9000: Quic a udp-based multiplexed and secure transport,” RFC 9000, 2021. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc9000>
- [31] O. Bonaventure. (2022) Multipath TCP (MPTCP). Accessed: 2026-01-05. [Online]. Available: <https://mptcp-apps.github.io/mptcp-doc/index.html#>
- [32] S. Lee and K. Chung, “A multipath congestion control scheme for high-quality multimedia streaming,” *KSII Transactions on Internet & Information Systems*, vol. 11, no. 1, 2017.
- [33] J. Han, K. Xue, W. Wei, Y. Xing, Y. Liu, and P. Hong, “Transparent multipath: Using double MPTCP proxies to enhance transport performance for traditional tcp,” *IEEE Network*, vol. 35, no. 5, pp. 181–187, 2021.
- [34] 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.
- [35] A. Güngör. (2023) UERANSIM. [Online]. Available: https://gitlab.com/lin_public_group/UERANSIM
- [36] 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.
- [37] srsRAN. (2025) srsRAN Project. [Online]. Available: https://github.com/srsran/srsRAN_Project
- [38] —. (2023) srsRAN 4G. [Online]. Available: https://github.com/srsran/srsran_4g
- [39] Ettus. (2025) Ettus USRP B205mini-i. [Online]. Available: <https://www.ettus.com/all-products/usrp-b205mini-i/>
- [40] free5GC. (2024) Non-3GPP InterWorking UE. Accessed: 2026-01-09. [Online]. Available: <https://free5gc.org/guide/n3iwue-installation/>
- [41] Open5GS. (2026) Open5GS quickstart. Accessed: 2026-01-09. [Online]. Available: <https://open5gs.org/open5gs/docs/guide/01-quickstart/>
- [42] free5GC. (2024) free5GC user guide. Accessed: 2026-01-09. [Online]. Available: <https://free5gc.org/guide/>
- [43] N. MATSUMOTO. (2022) MPTCP proxy. Accessed: 2026-01-09. [Online]. Available: <https://github.com/naoki9911/MPTCP-Proxy>
- [44] M. Broner. (2023) LENS 5G-transport-converter. Accessed: 2026-01-09. [Online]. Available: <https://github.com/LENS5G-Transport-Converter>
- [45] Internet Engineering Task Force (IETF), “RFC 6356: Coupled congestion control for multipath transport protocols,” RFC 6356, 2011. [Online]. Available: <https://www.ietf.org/rfc/rfc6356.txt>
- [46] Ł. P. Łuczak, P. Ignaciuk, and M. Morawski, “Evaluating MPTCP congestion control algorithms: Implications for streaming in open internet,” *Future Internet*, vol. 15, no. 10, p. 328, 2023.
- [47] B. Y. L. Kimura and A. A. F. Loureiro, “MPTCP Linux kernel congestion controls,” *arXiv preprint arXiv:1812.03210*, 2018.
- [48] free5GC. (2023) Introduction of mptcp. Accessed: 2026-01-13. [Online]. Available: <https://free5gc.org/blog/20231004/20231004/>