Université Libre de Bruxelles

5G Security Analysis

Students:
Ali khodja Myriam Johana
Hassani Mortaza
Amanor Deborah
Bouta Ali

Supervisor:
Prof. Dricot Jean-Michel

January 5, 2025

Contents

List of Acronyms

Nomenclature

1G First Generation

2G Second Generation

3G Third-Generation

3GPP 3rd Generation Partnership Project

4G Fourth-Generation

5GC 5G Core Network

AN Access Network

AS Application Server

CDMA Code Devision Multiple Access

CN Core Network

FDMA Frequency Devision Multiple Access

IMT-2000 International Mobile Technology-2000

ITU International Telecommunication Union

ITU-R International Telecommunication Union Radiocommunication

LTC Long Term Evolution

MBB Mobile Broadband

MIMO Multiple-Input Multiple-Output

NFV Network Function Virtualization

NG-RAN Next Generation Radio Access Network

NR New Radio

NS Network Slicing

OFDMA Orthogonal Frequency Division Multiple Access

RAN Radio Access Network

SDN Software-Defined Networking

SDOs Standard Development Organizations

TDMA Time Devision Multiple Access

UE User Equipment

1 Introduction

First mobile cellular network deployment take place since 1970s [10]. The first generation (1G) network was designed on principal of frequency devision multiple access (FDMA) and delivered analog voice transfer service to the mobile users. In second generation (2G) network, time devision multiple access (TDMA) was developed after near 10 years from 1G introduction. 2G network introduced digital voice services and supported low data rates. Between the mid-1990s and 2000s, code division multiple access (CDMA) technology was utilized to develop third-generation (3G) networks. CDMA allowed for more efficient multi-user access within the available bandwidth, enabling data rates ranging from several kilobits to several megabits per second, which facilitated faster multimedia transmission. [12]

In mid-2000s, with the rise of ubiquitous data, it pushed to redefine mobile communication services. The increased expectation for data services beyond the capabilities of 3G networks was because of the users demanding expected seamless connectivity. Frequent data transfer happens, and higher data rates are becoming essential. The Users started demanding broadband's speed from their wireless mobile network service. In response, the development of fourth-generation (4G) networks started in 2005, with the target of delivering ubiquitous mobile broadband (MBB) services. The 3GPP introduced Long Term Evolution (LTE), which utilizes Orthogonal Frequency Division Multiple Access (OFDMA) to balance multi-user data rates and system complexity effectively. LTE received widespread industry backing and integrated OFDMA with multiple-input multiple-output (MIMO) technology, significantly reducing system complexity while enhancing performance.

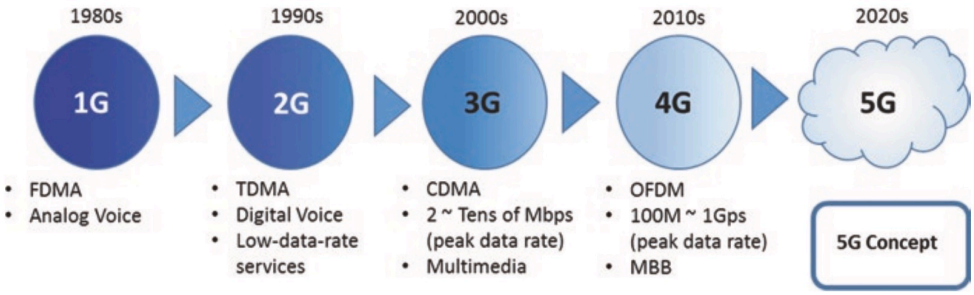

Figure 1: A schematic view of the history of cellular communications

International Telecommunication Union (ITU), especially its Radiocommunication Sector (ITU-R), has been a major role player mobile in mobile network development since 3G. Because of great success of 1G and 2G mobile networks, the industry and research interests were increased exponentially for 3G development. Therefore, many stakeholders were involved in 3G development with respect to previous generation mobile networks. A global standardization was becoming necessary due to the involvement of a variety of network vendors, user terminal manufacturers, and chipset providers. Global spectrum harmonization also becomes a critical issue for the successful development and deployment of the mobile network. In order to harmonize the spectrum use in different regions for appropriate technologies for 3G mobile network, ITU-R established procedures to address the allocation of spectrum for 3G mobile network, and to identify the appropriate radio interface technology that could be deployed on those spectrums globally. In this context, International Mobile Technology-2000 (IMT-2000) was specified by the ITU, where a family of technologies were identified as radio inter- face technologies for 3G mobile network (IMT-2000 system). Such procedures provide fair opportunity

for the proponents that are interested in mobile network development, as well as set the necessary performance requirements to guarantee that candidate technology can effectively meet the requirements. The procedure is further developed and applied to 4G and 5G development in ITU-R. This resulted in the IMT family specification: IMT-2000 for "3G," IMT-Advanced for "4G," and IMT-2020 for "5G."

While ITU-R plays the central role for defining appropriate technology for each generation of mobile network, the technology development is conducted in standard development organizations (SDOs). In 1998, the third generation partnership project (3GPP) was initiated by the key players of the mobile network development, and gains the support from six regional SDOs from europe, China, Japan, Korea, and America. It lays the foundation of global development for mobile technologies, and attracts the participation of a variety of industry and academy players. 3GPP has grown to be the essential standard organization for technology development for mobile networks since 3G.

2 5G Architecture

The 5G communication networks' purpose is to render services that would satisfy the different requirements of vastly mobile systems (high throughput, low latency, and massive connections). The framework of 5G is logical, dynamic, consistent, and flexible of numerous advanced technologies that would be supporting a wide range of applications. In corresponding to the 3GPP NR, the entire architectural system of both the RAN and the Core Network were reassessed, and the functional split amongst the two networks (CN and RAN). Unlike the previous mobile communication networks, the 5G employs a more intelligent architecture that would no longer be constrained by the proximity of base stations (BS). In addition to complex infrastructure constraints. Instead, it has a flexible deployment employing novel concepts like network slicing (NS), software-defined networking (SDN) as well as network function virtualization (NFV). [7] [3]

3GPP defined the 3GPP 5G system architecture in [3], indicating the required features and functionality for the deployment of a commercially operational 5G system. Usually, the technical specifications for mobile communication are constantly evolving due to new features and service demands, making it a continues development process. Typically, mobile system architecture consists of two core components: the Access Network (AN) and the Core Network (CN). The 3GPP has defined the 5G system architecture to be an interaction between the user equipment (UE) and an endpoint, this endpoint could be a server like the Application Server (AS), or it could be an alternative UE [12]. Hence, the 3GPP system consists of the AS, 5G Core Network (5GC), the Next Generation Radio Access Network (NG-RAN), and UE [8], which establishes communication between the DN and UE via AN and CN [3]. Figure 2 illustrates a simple end-to-end architecture of 5GC.

Figure 2: 5G system end-to-end architecture

2.1 Overview of the 5G Core Network

The 5G core network manages all data, voice, and internet connections referred to as the mobile exchange and data network. The basis of the 5G network architecture was expressed based on the service requirements, which started as a preliminary study in [1] and was fully detailed in [3], [4], [6]. Unlike in the EPC, where MME handles the session management and mobility management function, these functionalities and procedures are governed by Session Management Function (SMF) and AMF in 5GS. The control plane connection of AN and UE are terminated at the AMF. The connection link between the UE and AMF via the AN is called the Non-Access Stratum (NAS). The SMF procedures and the session management functionalities are handled as actual user data are transmitted through the UPF. Likewise, the UPF selection/re-selection are handled by the SMF [12]. The AMF can accommodate various ANs (3GPP/non-3GPP) due to the separation of mobility management functionalities and that of the session management. Likewise, specific accesses can be achieved by the SMF. In short, the AMF/UPF/SMF delivers the CP functions primarily from the 5GC. More on the functions of AMF/SMF/UPF can be found in the 3GPP technical reports [2], [3].

3GPP defines the Service-Based Architecture (SBA) as a framework for delivering standard data repositories and control plane (CP) functionalities in the 5G system through interconnected Network Functions (NFs) that are authorized to access each other's services. Unlike the EPC in the 4G Core Network, the 5G Core (5GC) incorporates SBA, offering flexibility for deploying common applications across different sources or suppliers. Figure 3 illustrates a basic standalone (non-roaming) 5G System architecture with interconnected NFs in the 5GC. These NFs provide specific services to others via a unified interface framework, enabling reusability, modularity, and virtualized deployment. The uniform connections among NFs are referred to as Service-Based Interfaces (SBI) [14], [16].

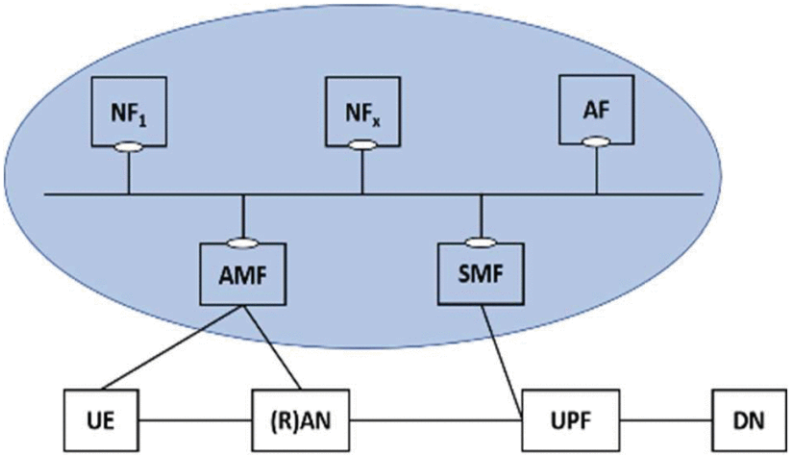

Figure 3: 5G system architecture with a set of interconnected NFs

2.2 Next Generation Radio Access Network (NG-RAN) Overview

The operations of all radio related functions of the network, such as coding, retransmission protocols administration, handling of radio-resource, scheduling, and different multiple antenna structures, are managed by RAN. The 3GPP [5] defined the universal guidelines that navigated the architecture and interfaces of the NG-RAN as follows;

- Mobility of the Radio Resource Control (RRC) protocols is entirely controlled by the NG-RAN
- Logical separation between signaling and data transport networks
- 5G core network functions and the NG-RAN are completely distinguished from that of the transport functions. Hence, the applied addressing scheme of 5GC/NG-RAN and that of transport functions are not tied to each other
- In terms of the NG-RAN interfaces, it has fewer options for the functional division, controls by logical model via an interface and, multiple logical nodes could be implemented by a physical network element

2.3 The RAN and 5GC Functional Split

The separation of RAN and 5GC marks a major design shift in the architecture of the 5G system and allows for greater flexibility, scalability, and modularity in terms of the infrastructure and the operations of the network. In contrast to the tightly integrated architectures in the previous generations, the 5G system adopts a functional splitting approach between the RAN and 5GC using standard interfaces like the NG interface as its boundary. As a result, the RAN unit can concentrate on radio-related functions like resource allocation, scheduling, and mobility management, whereas the 5GC unit handles core network duties such as session and connection management, authentication, and policy control. The interfacing of RAN with 5GC uses the NG interface, which includes N2 control plane and N3 user plane interfaces. This makes possible the interoperability of different vendor's equipment by enabling a multiplicity of network topologies. The decoupling of RAN and 5GC is fundamental of the support of a wide range of 5G use cases, including eMBB, URLLC, and mMTC, by allowing the RAN as well as the core part of the network to be individually optimized.

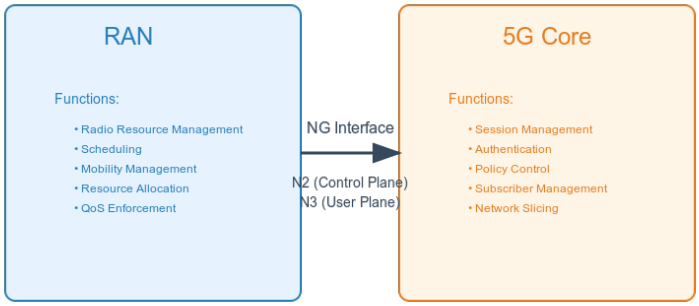

Figure 4: Functional split between RAN and 5GC

The functional split also reflects the Service-Based architecture of the 5GC which divides core network features into independent and modular deployable Network Functions. Specifically, the Access and Mobility Management Function, Session Management Function and User Plane Function are NF deployed to interact with the RAN via the NG interface to provide all round connectivity and service continuity. For example, the AMF ends the control plane connection from the RAN, maintains an interface to the SMF and sends the relevant mobility signaling to manage. The SMF, in turn, manages the session and needed resources in the user plane. The

UPF, however, is in charge of the directing of user data and routing of the traffic. [12] This functional split also allows centralized or distributed RAN architectures to be deployed, as well as more advanced functions, including network slicing in which virtual end to end networks can be created for specific applications or industries. Furthermore, through the decoupling of the RAN and the 5GC, the 5G architecture features a high degree of flexibility, empowering operators to improve network performance and diminish the organizational expenditures while ensuring quick installation of new services. This partition is one of the basic elements of the functionality of the 5G system within a contemporary communication network.

- **Cloud Radio Access Network** Cloud Radio Access Network (Cloud-RAN) is a big step in the way of how radio access network is structured because there is an unbundling and virtualization of the functions performed by the base station to the cloud computing infrastructure. This change in architecture structure adds on a three layer hierarchy which consists of Remote Radio Units (RRUs), Distributed Units (DUs), and Centralized Units (CUs) that are connected by the fronthaul and midhaul interfaces [9] The upgrading of RAN functions to the virtual mode allows for dynamic resource provisioning, a lower CAPEX, and greater flexibility of the network. The architecture of Cloud-RAN aids in the use of more enhanced functionalities such as CoMP transmission as well as reception that boosts the efficiency of cell-edge along with spectrum The Coordination improves network and resource optimization in addition to advanced interference management and load balancing mechanisms. [15]

- **Open Radio Access Network** Open Radio Access Network, or O-RAN, enhances network disaggregation further by adding open interfaces and standardized protocols, allowing for user's several vendor options and reducing reliance upon proprietary solutions. The O-RAN diagram developed by the O-RAN Alliance includes AI and ML components through the RAN Intelligent Controller, RIC, which can function in both near real time and non-real time environments [13]. RIC that functions is divided into RT RIC and Non RT RIC, NT PICS focuses on RRM and MO resources in close time scales while Non RT RIC focuses on policy and network optimization over a period of time. This type of architecture encourages more innovations through its open interfaces, cuts the operational costs OPEX, and makes the networks intelligent in the sense that they may be optimized based on real time information. Combining the O-RAN with NG-RAN takes advantage of the programmable network element together with the 3GPP interfaces to offer even greater network flexibility. This combination gives rise to an ecosystem that is suited for multiple deployment configurations ranging from high density cities to rural areas, all while being able to work with 5G core network functions and services [11].

When paired with the Next Generation RAN, such framework innovations are in tune with the overall core principle of the 5G networks. However, the Next Generation RAN is able to utilize the Cloud-RAN and O-RAN concepts to maximise performance, cost, and flexibility, while still conforming to 3GPP requirements. This means that operators can introduce new functionality like use cases with slicing, MIMO systems, and spectrum sharing without limiting their connection to the core within the 5G ecosystem through the standardized NG interfaces [6].

References

[1] 3GPP. Study on architecture for next generation system (release 14). Technical report, 3rd Generation Partnership Project, 2016.

[2] 3GPP. 5g; nr; overall description; stage-2 (release 15). Technical report, 3rd Generation Partnership Project, 2018.

[3] 3GPP. 5g: System architecture for the 5g system (3gpp ts 23.501 version 15.2.0 release 15). Technical report, 3GPP, 2018.

[4] 3GPP. Policy and charging control framework for the 5g system (5gs); stage 2 (release 15). Technical report, 3rd Generation Partnership Project, 2019.

[5] 3GPP. Ng-ran; architecture description (release 16). Technical report, 3GPP, 2020.

[6] 3GPP. Procedures for the 5g system (5gs); stage 2 (release 16). Technical report, 3rd Generation Partnership Project, 2020.

[7] S. Ahmadi. *5G NR: Architecture Technology Implementation and Operation of 3GPP New Radio Standards*. Academic, New Delhi, India, 2019.

[8] G. Bernini, P. G. Giardina, S. Spadaro, F. Agraz, A. Pages, J. Cabaca, and et al. Multi-domain orchestration of 5g vertical services and network slices. In *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, pages 1–6. IEEE, Jun. 2020.

[9] Aleksandra Checko, Henrik L. Christiansen, Ying Yan, Lara Scolari, Georgios Kardaras, Michael S. Berger, and Lars Dittmann. Cloud ran for mobile networks—a technology overview. *IEEE Communications Surveys and Tutorials*, 17(1):405–426, 2015.

[10] Illinois Bell Telephone Co. Trial development cellular system in the chicago area, 1979. Conducted in the Chicago area.

[11] Liljana Gavrilovska, Valentin Rakovic, and Daniel Denkovski. From cloud ran to open ran. *Wireless Personal Communications*, 113, 08 2020.

[12] Wan Lei, Anthony C. K. Soong, Liu Jianghua, Wu Yong, Brian Classon, Weimin Xiao, David Mazzarese, Zhao Yang, and Tony Saboorian. *5G System Design: An End to End Perspective*. Springer, Beijing, China, 2020. ISBN 978-3-030-22236-9 (eBook).

[13] O-RAN Alliance. O-RAN Architecture Description. Technical report, O-RAN Alliance Technical Specifications, 2020.

[14] B. Valera-Muros and P. Merino-Gomez. Is géant testbeds service compliant with etsi mano? In *Proc. IEEE 2nd 5G World Forum (GWF)*, pages 502–507, September 2019.

[15] Jun Wu, Zhifeng Zhang, Yu Hong, and Yonggang Wen. Cloud radio access network (c-ran): a primer. *IEEE Network*, 29(1):35–41, 2015.

[16] C. Zhang, X. Wen, L. Wang, Z. Lu, and L. Ma. Performance evaluation of candidate protocol stack for service-based interfaces in 5g core network. In *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, pages 1–6, May 2018.