Slice specific authentication and access control for 5G

Shanay Behrad

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2020IPPAS007

Thèse de doctorat

Slice Specific Authentication and Access Control for 5G

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à Télécom SudParis

École doctorale n°625 Institut Polytechnique de Paris (IP Paris)
Spécialité de doctorat: Informatique et Réseau

Thèse présentée et soutenue à Châtillon, le 24/02/2020, par

Shanay Behrad

Composition du Jury :

Bijan Jabbari Professeur, George Mason University, ETATS-UNIS	Rapporteur, Président
Samia Bouzefrane Professeur, CNAM, FRANCE	Rapporteuse
Stuart Clayman Principle research fellow, University College London, ROYAUME-UNI	Rapporteur
Müge Sayıt Professeur associé, Ege University, TURQUIE	Examinatrice
Barbara Martini Ingénieur de Recherche, CNIT, ITALIE	Examinatrice
Noel Crespi Professeur, Télécom SudParis, FRANCE	Directeur de thèse
Emmanuel Bertin Professeur associé, Orange Labs, FRANCE	Co-Directeur de thèse

Doctor of Philosophy (PhD) Thesis

Institut-Mines Télécom, Télécom SudParis

& Institut Polytechnique de Paris (IP Paris)

Specialization

COMPUTER SCIENCE AND NETWORKS

presented by

Shanay BEHRAD

SLICE SPECIFIC AUTHENTICATION AND ACCESS CONTROL FOR 5G

Commitee:

Bijan Jabbari	Reviewer	Professor, George Mason University – United States
Samia Bouzefrane	Reviewer	Professor, CNAM - France
Stuart Clayman	Reviewer	Principle Research Fellow, College London University - United Kingdom
Müge Sayıt	Examiner	Associate Professor, Ege University - Turkey
Barbara Martini	Examiner	Research Engineer, CNIT - Italy
Noel Crespi	Advisor	Professor, Institut-Mines Telecom, Telecom SudParis - France
Emmanuel Bertin	Supervisor	Associate Professor, Orange Labs - France

Orange Labs

Février 2020

Thése de Doctorat (PhD) de
Institut-Mines Télécom, Télécom SudParis
et l'Institut Polytechnique de Paris (IP Paris)

Spécialité

INFORMATIQUE ET RESEAUX

présentée par

Shanay BEHRAD

AUTHENTIFICATION ET CONTRÔLE D'ACCÈS SPÉCIFIQUES AUX SLICES POUR 5G

Jury composé de:

Bijan Jabbari	Rapporteur	Professeur, George Mason University – ETATS-UNIS
Samia Bouzefrane	Rapporteuse	Professeur, CNAM - FRANCE
Stuart Clayman	Rapporteur	Principle Research Fellow, College London University - ROYAUME-UNI
Müge Sayıt	Examinatrice	Professeur associé, Ege University - TURQUIE
Barbara Martini	Examinatrice	Ingénieur de Recherche, CNIT - ITALIE
Noel Crespi	Directeur de thèse	Professeur, Institut-Mines Telecom, Telecom SudParis - FRANCE
Emmanuel Bertin	Co-Directeur de thèse	Professeur associé, Orange Labs - FRANCE

Orange Labs

Février 2020

To

the lost student passengers of Ukraine Airlines PS752

who will not defend their thesis forever…

God, exists in every seed that shows the courage to crack,

in every soul that afflicts pain to feel beyond what it sees,

and in every thought that shows braveness to try;

Experiences itself fearlessly and naturally.

Φ

Fi, Akilah Azra Kohen

Acknowledgements

My dearest Sahand;
Thank you for choosing to experience this life with me, for protecting me from myself and for helping me to stay steady and balanced. Your patience, understanding and faith in me were my wings to explore this way.

My Momy and Dady;
Thank you for your unrequited love that I feel it in the deepest part of my soul. This love empowered me to break my limits and experience the life freely and fearlessly.

My true friend Okhtay;
When it comes to goodness, you are the first to come to my mind. You are a proof of the universe's superiority in every sense. I am very lucky to be your sister.

My brother Babak;
Your courage, intelligence and your love for your profession always inspired me. So glad that I have you.

Dr. Emmanuel Bertin;
The lessons I learned from you brightened my way and helped me to overcome all the obstacles. Thank you for your confidence and mentorship over the years and for sharing your extensive knowledge with me.

Prof. Noel Crespi,
Thank you for believing me at the beginning of this journey and for providing me valuable opportunities. Being a part of your team, was an honor for me.

Dear Stéphane Tuffin;
Thank you for being a great critic, for your valuable ideas and for numerous insightful discussions about finding solution for challenges. Working together was a great pleasure for me. I hope our paths always crossed.

Dear Marc Mazoué;
Words cannot even express my thanks for your supports and friendship. I wish the life to unfold you beautiful and valuable people just like you.

Orange Labs family;
Being a part of this family, was a priceless experience for me. Thank you.

My dear friends;
Fariba, Marziyeh, Yasir, Praboda, Hamza, Dina, my little family in TSP and my colleagues, thank you for your humor and support. I am grateful for each one of you.

My committee members;
Prof. Bijan Jabbari, Prof. Samia Bouzefrance, Dr. Stuart Clayman, Dr. Müge Sayıt and Dr. Barbara Martini, I appreciate your interest in and feedback on my research work. Your suggestions have made this work better.

My favorite writer Azra Kohen,
I am grateful for the inspiration you gave me and the awareness created in me. Meanings that you hide between your lines, touched my life, fed my soul.

Finally, thanks to all the scientists who were the real artists of life and who released us from the prison of our minds and the boundaries of our planet.

Abstract

The fifth generation of mobile cellular networks, 5G, is designed to support a set of new use cases and requirements, e.g. concerning quality of service or security. Using the virtualization technologies and the concept of network slicing, the 5G network operators will be able to provide specific connectivity capabilities in order to support these various use cases. Each network slice can be designed by enabling or disabling certain network functions to satisfy a specific type of usage. It can be dedicated to a 3rd party (i.e., any business actor that is not the network operator), and be designed to fit the 3rd party's requirements.

However, although network slices add flexibility to the network, the architectural logic of the network remains the same as the physical networks (the physical entities are converted to the virtual functions only). Consequently, the network components are still tightly coupled even with the network slicing concept and some mechanisms remain the same for all slices. Authentication and Access Control (AAC) of the end users (or devices) in the network is one of these mechanisms. That means despite the different security requirements of each network slice, the same AAC mechanism are applied for all network slices to allow end users access the slices' provided services.

This thesis proposes 5G-SSAAC (5G Slice-Specific AAC), as an initial step to introduce a more loosely coupled design into the whole 5G network architecture. The purpose of 5G-SSAAC is to delegate the AAC of devices to the 3rd parties providing these devices. With this approach, on the one hand the 3rd parties are able to choose their own AAC mechanism according to their security requirements (they are not restricted to use a certain AAC mechanism). On the other hand, the Mobile Network Operator (MNO) is not responsible for AAC of all devices in the network, which decrease the signalling load on the operator's network. The focus of 5G-SSAAC approach is on the Radio Access Network (RAN) part. The objective is to enable the RAN routes devices attachment requests to the corresponding network slice before the AAC phase of the devices. Therefore, the AAC of the devices is done inside the network slice according to the AAC mechanism that is chosen by the 3rd party for that slice. To assess this innovative mechanism, the thesis analyses the consequences of using the 5G-SSAAC on the security of the whole 5G system. The feasibility of the 5G-SSAAC is also presented with the implementation of a fully virtualized mobile network through an OAI (Open

Air Interface) based testbed. This work finally evaluates the impact of 5G-SSAAC mechanism on the network load considering the anticipated number of AAC signalling messages compared to the existing AAC mechanisms in cellular networks.

Keywords:

5G Networks, 5G Radio Access Network, Virtual Network Functions, Authentication and Access Control, Open Air Interface

Resumé

La cinquième génération de réseaux cellulaires mobiles, 5G, est conçue pour prendre en charge un ensemble de nouveaux cas d'utilisation et exigences, par exemple concernant la qualité de service ou la sécurité. En utilisant les technologies de virtualisation et le concept de découpage de réseau, les opérateurs de réseaux 5G seront en mesure de fournir des capacités de connectivité spécifiques afin de prendre en charge ces différents cas d'utilisation. Chaque tranche de réseau (network slice) peut être conçue en activant ou désactivant certaines fonctions réseau pour satisfaire un type d'utilisation spécifique. Il peut être dédié à un tiers (c'est-à-dire tout acteur commercial qui n'est pas l'opérateur de réseau) et être conçu pour répondre aux exigences du tiers.

Cependant, bien que les tranches de réseau ajoutent de la flexibilité au réseau, la logique architecturale du réseau reste la même que les réseaux physiques (les entités physiques sont converties uniquement en fonctions virtuelles). Par conséquent, les composants du réseau sont toujours étroitement couplés même avec le concept de découpage du réseau et certains mécanismes restent les mêmes pour toutes les tranches. L'authentification et le contrôle d'accès (AAC) des utilisateurs finaux (ou appareils) du réseau sont l'un de ces mécanismes. Cela signifie qu'en dépit des exigences de sécurité différentes de chaque tranche de réseau, le même mécanisme AAC est appliqué à toutes les tranches de réseau pour permettre aux utilisateurs finaux d'accéder aux services fournis par les tranches.

Cette thèse propose 5G-SSAAC (5G Slice-Specific AAC), comme première étape pour introduire une conception à couplage plus lâche dans l'ensemble de l'architecture de réseau 5G. Le but de 5G-SSAAC est de déléguer l'AAC des appareils aux tierces parties fournissant ces appareils. Avec cette approche, d'une part les tiers peuvent choisir leur propre mécanisme AAC en fonction de leurs exigences de sécurité (ils ne sont pas limités à utiliser un certain mécanisme AAC). En revanche, l'opérateur de réseau mobile (MNO) n'est pas responsable de l'AAC de tous les appareils du réseau, ce qui diminue la charge de signalisation sur le réseau de l'opérateur. L'approche 5G-SSAAC se concentre sur la partie Réseau d'accès radio (RAN). L'objectif est de permettre au RAN de router les demandes de connexion des appareils vers la tranche de réseau correspondante avant la phase AAC des appareils. Par conséquent, l'AAC des périphériques se fait à l'intérieur de la tranche de réseau selon le mécanisme AAC choisi

par le tiers pour cette tranche. Pour évaluer ce mécanisme innovant, la thèse analyse les conséquences de l'utilisation du 5G-SSAAC sur la sécurité de l'ensemble du système 5G. La faisabilité du 5G-SSAAC est également présentée avec la mise en œuvre d'un réseau mobile entièrement virtualisé via un banc d'essai basé sur OAI (Open Air Interface). Ce travail évalue enfin l'impact du mécanisme 5G-SSAAC sur la charge du réseau compte tenu du nombre prévu de messages de signalisation AAC par rapport aux mécanismes AAC existants dans les réseaux cellulaires.

Mots clés :

Réseaux 5G, Réseau d'accès radio 5G, Fonctions de réseau virtuel, Authentification et contrôle d'accès, Open Air Interface

Publications

This thesis is the ground of the following original articles, which are referred to in the text by their numerical code:

Conferences :

[P1] S. Behrad, E. Bertin, and N. Crespi, *"Securing authentication for mobile networks, a survey on 4G issues and 5G answers"*, 21st Conference on Innovation in Clouds, Internet and Networks (ICIN), 2018.

[P2] S. Behrad, E. Bertin, S. Tuffin and N. Crespi, *"5G-SSAAC: Slice-specific Authentication and Access Control in 5G"*, IEEE Conference on Network Softwarization (NETSOFT), 2019.

[P3] S. Behrad, S. Tuffin, E. Bertin, and N. Crespi, "Network Access Control for the IoT: A Comparison Between Cellular, Wi-Fi and LoRaWAN", 22st Conference on Innovation in Clouds, Internet and Networks (ICIN), 2019.

Journals:

[P4] S. Behrad, E. Bertin, and N. Crespi, *"A survey on authentication and access control for mobile networks: from 4G to 5G"*, Annals of Telecommunications, pp. 1–11, 2019.

[P5] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Generation Computer Systems*, vol. 108, pp. 46–61, 2020.

Book chapters:

[P6] Behrad, S., Bertin, E. and Crespi, N. (2020). Security and Access Control for 5G. In Wiley 5G Ref (eds R. Tafazolli, C.-L. Wang and P. Chatzimisios). doi:10.1002/9781119471509.w5GRef261

Contents

List of Figures

List of Tables

Nomenclature

3GPP	3rd Generation Partnership Project
3GW	3rd party provided GateWay
5G-SSAAC	5G Slice-Specific Authentication and Access Control
5G-PPP	Fifth Generation Public Private Partnership
AC	Access Control
AS	Access Stratum
ABP	Activation-by-Personalization
AF	Application Function
AAC	Authentication and Access Control
AKA	authentication and key agreement
AuC	Authentication Centre
AC	Authentication Confirmation
AIA	Authentication Information Accept
AIR	Authentication Initiation Request
AMF	Core Access and Mobility Management Function
ARPF	Authentication Repository and Processing Function
AUSF	Authentication Server Function
AUTN	Authentication Token
AV	Authentication Vectors
B2B2C	Business to Business to Consumer
CN	Core Network

DN	Data Network
DoS	Denial of Service
DDoS	Distributed Denial of Service
eMBB	Enhanced Mobile Broadband
eNodeB	evolved Node B
ePDG	Evolved Packet Data Gateway
UTRAN	Evolved Universal Terrestrial Radio Access Network
GUMMEI	Globally Unique Mobility Management Entity Identifier
GFR	Gateway Function Repository
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identifier
HLR	Home Location Register
HN	Home Network
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
LTE	Long Term Evolution
LPWA	low-power, wide-area
MitM	man-in-the-middle attacks
MIoT	Massive Internet of Things
MCC	Mobile Country Code
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
MME	Mobility Management Entity
MIMO	multiple-input and multiple-output
NAI	Network Access Identifier
NEF	Network Exposure Function

NF	Network Function
NFV	Network Function Virtualization
NSSF	Network Slice Selection Function
NRF	NF Repository Function
NAS	Non-Access Stratum
OAI	Open Air Interface
ONAP	Open Network Automation Platform
OTA	Over-the-Air
P-GW	Packet Data Network Gateway
PCRF	Policy and Charging Rules Function
PCF	Policy Control Function
PKI	Public Key Infrastructure
RAN	Radio Access Network
RRC	Radio Resource Control
RAND	random number
RCP	RRC Connection endPoint
SEAF	Security Anchor Function
SOA	service-oriented architecture
S-GW	Serving Gateway
SN	Serving Network
SNid	Serving Network
SMF	Session Management Function
SDR	software defined radio
SDN	Software-defined Network
SDSF	Structured Data Storage network function
SDM	Subscriber Data Management
SIM	Subscriber Identity Module

SUPI	Subscriber Permanent Identifier
SUCI	Subscription Concealed Identifier
SIDF	Subscription Identifier De-concealing Function
SGSN	Serving GPRS Support Node, responsible for mobility management
TMSI	Temporary Mobile Subscriber Identity
TAU	Tracking Area Update
TLS	Transport Layer Security
URLLC	Ultra-Reliable and Low Latency Communications
UDM	Unified Data Management
UDR	Unified Data Repository
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications system
USIM	Universal Subscriber Identity Module
UDSF	Unstructured Data Storage network function
UE	User Equipment
UE	User Equipment
UPF	User plane Function
V2X	Vehicle to Everything
VLR	Visitor Location Register
WPA	Wi-Fi Protected Access

Chapter 1 Introduction

1.1 Motivation

The fifth generation of mobile networks will integrate virtualization technologies to support a set of new use cases and requirements, e.g. concerning quality of service or security. These virtualization technologies offer cost-effective and flexible infrastructures to cellular systems, allowing them to provide services in a dynamic manner, by converting the physical entities of the network into virtual network functions [1]. With the concept of network slicing, virtualization technologies are also enabling customized usages of cellular systems for 3rd parties (i.e., any business actor that is not the network operator). Indeed, network slices are logical networks composed of different network functions providing specific connectivity capabilities. Each network slice can be allocated to a general requirement or use case (such as an IoT-dedicated slice) or it can be dedicated to a 3rd party to address its own specific requirements (e. g, a set of quality-of-service parameters such as throughput, latency, etc.) [2-6]. However, despite this flexibility, the architectural logic of 5G remains partly similar to that of previous physical networks: different parts of the network remain strongly coupled and dependent upon each other [7-9]. This monolithic architecture forces cellular system to have a common set of interfaces between the RAN (Radio Access Network) and the CN (Core Network) for all network slices. It also forces cellular systems to use some common network procedures. Authentication of the devices and controlling their access to the network is one of these common procedures. Therefore, the authentication of the devices is done before the slice selection phase (outside of the slice) and is common for all of the network slices, despite their very different specifications [10, 11].

In 3G and 4G, AAC(Authentication and Access Control) of subscribers are done through AKA (authentication and key agreement) protocols. These protocols (UMTS-AKA protocol in 3G

and EPS-AKA in 4G) are based on the unique identities of subscribers and symmetric cryptographic algorithms [12, 13]. The system subscribers' identities and the secret keys (that are used in symmetric cryptographic algorithms) are provisioned in secured elements(e.g., SIM cards or embedded SIM) and stored in cellular system's database as well. Executing these AKA protocols to establish a secure connection with the cellular system is mandatory for each UE (composed of a mobile device and a secured element) to obtain its cellular connectivity [12, 13]. However, by emerging the fifth generation of mobile networks (5G), using the AKA based protocols as the only way for AAC of the devices in 5G systems encounters the following issues:

- These well-established AKA based principles may prevent cellular systems from supporting the connectivity of a massive number of devices [14], in particular when considering the context of the IoT– where a high growth rate of connected devices is anticipated [15-17]. On one hand, most devices are constrained in terms of energy supply and computational capacities preventing them from running complex security protocols like EPS-AKA [1, 18]. On the other hand, the tremendous number of attachment requests from these devices may induce signalling congestion by increasing the connectivity provider's CN load [19, 20]. According to [21], the "Attach" procedure, that includes AAC, is indeed one of the most expensive procedures in terms of load on the CN. Considering this pattern, adversaries could be able to cause the denial of service attacks by generating traffic or emphasizing the natural traffic of these devices. This could result in authentication failure and connectivity loss of devices [22].
- These AAC mechanisms provide a certain level of security for the cellular networks. On one hand, some use cases do not need such level of security, e.g., a smart entertainment system in a smart home. On the other hand, security plays a vital role in some other use cases, e.g., smart health system [23]. But the current AKA-based AAC mechanisms suffers from some security leaks and they are no able to protect the cellular networks against all kind of attacks (e.g., the attacks related to use of the symmetric cryptographic algorithms and the leakage of the shared secret key that are explained in chapter 2).

While the 3GPP proposes some modifications (mainly for protecting user's privacy) for authentication and access control procedures (5G-AKA, EAP-AKA') of the devices in 5G systems (release 16) [10, 11, 24], these are still performed almost in the same manner as those of previous cellular system (EPS-AKA), along with the associated flaws for supporting a massive number of devices.

Figure 1.1, depicts an overview of the AAC procedure defined by 3GPP for 5G (release 16). In the first step, the device is authenticated in the network. The slice selection procedure is performed during the second step based on the first step's result (based on the subscription information of the device stored in the 5G system). Finally, the device gets access to the network slice in step three.

This work proposes a new approach called 5G-SSAAC (5G Slice-specific Authentication and Access Control) to solving the mentioned restrictions of using only the AKA based protocols for AAC of the devices in 5G systems. It is intended as an initial step to introduce a more loosely coupled design into the whole 5G network architecture. The purpose of the 5G-SSAAC is to open network functions to 3rd parties, through a new kind of interface between access network and 3rd parties' network slices and the aim is notably to maximize the decoupling between them and increase the flexibility of the network to address various use-cases.

In this work, we assume that each 3rd party has subscribed to a dedicated network slice for providing services to its devices and it has a wholesale agreement with the network operator. The "3rd party network" term and the "3rd party's slice" term have the same meaning and they are used interchangeably within this work. The term "3rd party's devices" refers to devices provided by the 3rd party and that should attach to the 3rd party slice. The 3rd party may

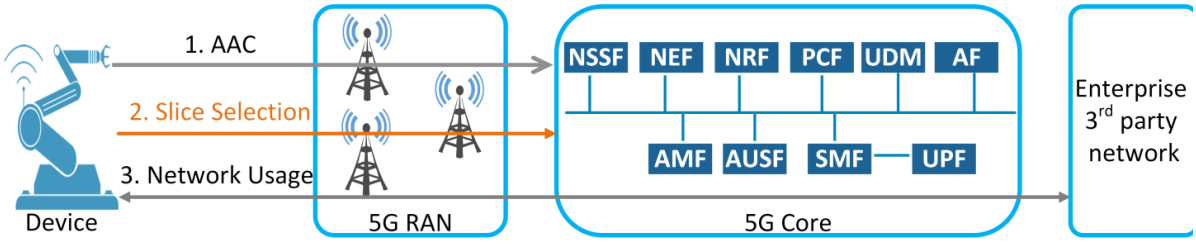


Figure 1.1– AAC procedure for 5G in 3GPP release 16.

produce its own devices or it may purchase them from another enterprise that will provision them with the 3rd party identities and credentials.

1.2 Slice Specific Authentication and Access Control

5G-SSAAC focuses on maximizing the decoupling between the RAN and the CN, by delegating the AAC of devices for a specific network slice to the 3rd party that uses this slice (in this case, the 3rd party is responsible to manage the identities of its devices). Thus, the AAC procedure is mainly done inside the 3rd party's network and not outside of it.

In order to do the AAC delegation, three network functions are defined in the 5G RAN. This allows 3rd parties to choose their own AAC method according to their security requirements which means that SIM based AAC mechanisms might only be used wherever they are needed (e.g., for Mobile Broad Band access). For example, they may not be used in cases of IoT applications running on constrained devices (where SIM based AAC mechanisms are not fully suitable). From the 5G network operator's perspective, this possibility to delegate users' AAC to 3rd parties appears as an interesting tool for enabling wholesaling wireless connectivity. In addition, this would prevent the network from managing the subscriptions of a huge amount of devices from different 3rd party organizations.

This work is defining a new RAN architecture that can:

- Host AAC functions specific to the 3rd parties; and
- Route the AAC requests to the corresponding 3rd party network

Figure 1.2 depicts the general architecture of 5G-SSAAC. It should be first noted that the attachment and AAC of MBB users remains unchanged (arrow 1'), and only new 3rd party IoT devices are impacted. When a 3rd party device requires connectivity, it mentions its corresponding slice in its attachment request as the first step. The RAN processes the device's request and routes it to the right network slice (or to the CN in case of a MBB user). In the second step, the RAN establishes a direct connection between the device and the corresponding network slice. Finally, the device is able to use the network. If the device is an

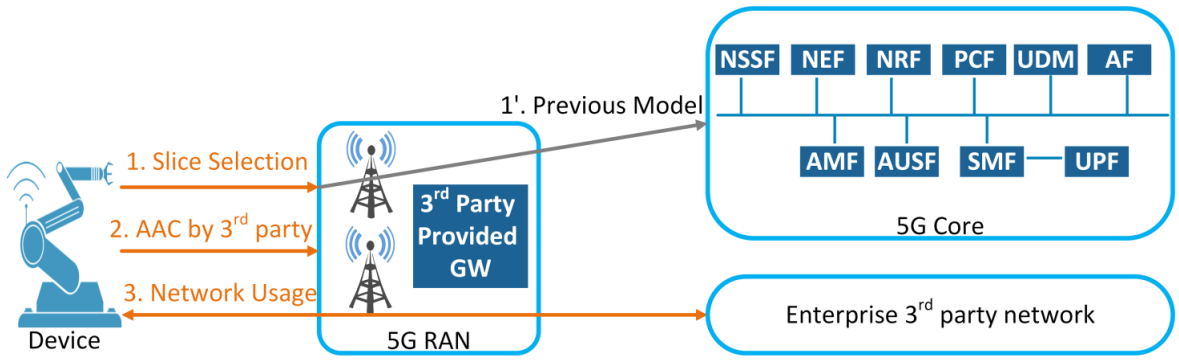


Figure 1.2– The general architecture of the proposed 5G-SSAAC approach.

MMB UE, the RAN routes the attachment request to the 5G CN and the AAC is done with the 5G AAC protocols (e.g. 5G-AKA).

In addition to reducing the connectivity provider's network load, 5G-SSAAC addresses some other new use cases and requirements raised for 5G systems:

- Opening the network functions to 3rd parties allows verticals (such as in the industry sector) to use their pre-existing AAC infrastructure and credentials to manage the AAC of their devices in the 5G environment [25-28]. They do not have to obtain 5G specific credentials for their devices (i.e., user identities and cryptographic keys) and can choose any AAC mechanism (or their pre-existing AAC) other than the AKA-based ones according to the security requirements of their proposed services and the abilities of their devices (in terms of computational power and energy supply). This will allow the 3rd parties that provide constrained devices to manage them by using suitable ACC methods. They can also control the lifecycle of its devices, from installation to de-installation in the AAC level.
- In the 5G-SSAAC, 3rd parties hold the responsibility of managing the identities and AAC of their provided devices. Thus, if a 3rd party wants to change its wholesale agreement from one network operator to another network operator, it has not to do a mass-migration of per-device subscription information from the first operator to the second one.
- In Order to obtain business confidentiality, the 3rd party is able to shield device identities and their credentials' privacy from the 5G network operator (the current

network layout forces the 3rd parties to depend on network operators for managing the identities and credentials of their provided devices).

- Finally, it gives 3rd parties the opportunity to embed connectivity in the devices they provide to their customers, to ensure a better customer experience. In this case, the customer (i.e., the device user) does not have to set up an additional subscription and an accounting plan with a network operator, as the device provider (3rd party) has already set up a subscription for all of its devices.

Besides all the advantages coming from the flexibility of 5G-SSAAC mechanism, there are some concerns we have to pay attention to:

- 5G-SSAAC is a distributed approach and each 3rd party has its own dedicated network function for AAC of its provided devices. Consequently, the security monitoring in this approach is more challenging than the security monitoring in a centralized approach (with one AAC function for all the devices in the network).
- 5G-SSAAC changes the network design in the RAN. The operators needs the participation of the standardization bodies to have a suitable ecosystem for using 5G-SSAAC approach.
- With 5G-SSAAC mechanism, some 3rd party slices may apply very simple and permeable AAC mechanism for their provided devices. Therefore, securing the isolation of the 3rd parties' slices requires more attention to prevent other network slices from the possible attacks against one network slice with a low security level. The connectivity provider (MNO) also has to oblige the 3rd parties to apply AAC mechanisms with a certain level of security. The control of the MNO over the level of security from 3rd party may be done by contractual agreements and audits.

1.3 Contributions

This work makes the following novel contributions, which are mainly disseminated in the original publications:

1. An analysis of security vulnerabilities in the AAC mechanisms proposed by 3GPP for 5G release 16 and possible attacks against them in order to study their suitability for the high security-sensitive use cases. A detailed study on the security flaws in the AAC mechanisms of the 3G and 4G networks is proposed and it is depicted that most of these security flaws remain in the AAC mechanisms of 5G.
2. An analysis of AAC models in the different communication technologies (cellular, Wi-Fi and LoRaWAN) considering the new use cases in 5G and deriving the new requirements from these use cases in order to study the compatibility of the AAC mechanisms in these different systems with the derived requirement as well as the "wholesale wireless connectivity" concept. According to this concept, connectivity providers sell connectivity to 3rd parties, which in turn provide it to their own devices. However, this concept brings also new architecture and security requirements that are not fully addressed by the state of the art.
3. A new way of AAC in 5G system to enable it supports different AAC mechanisms, which are suitable with the security requirements of different use cases. To do so, relying on the virtualization technologies and considering the new requirements in 5G and the "wholesale wireless connectivity" concept, this work defines new network functions in a 5G RAN to delegate the AAC of devices to the 3rd parties providing those devices. It also assesses the feasibility of the proposed network functions and the evaluation of their impact on existing RAN by implementing a fully virtualized mobile network through a testbed based on the OAI (Open Air Interface) open-source product. This work provides an analysis of the security aspects of the proposed approach in comparison with the AKA-based AAC mechanisms and a description and assessment of the signalling flows that have an impact on the network signalling load by focusing on the attachment and authentication signalling.

Table 1.1 depicts the more details about the research articles based on which this work builds the contributions.

Table 1.1 – Thesis contributions and research articles

Contribution	Chapter	Research articles
1	2	[P1], [P4], [P6]
2	3	[P2], [P3]
3	4, 5	[P2], [P5]

1.4 Organization

The remainder of this work is organized as follows:

Chapter 2 is the ground of our papers P1 [29], P4 [30] and P6 [134] and describes the challenges of AAC procedure for 4G systems and the new needs coming from the new 5G use cases, as well as the way, standards are currently evolving. The security flaws of the proposed AAC procedures in the standards are also provided in chapter 2. Chapter 3 is partially the basis of the previous work P3 [31], gives an overview of the AAC mechanisms in cellular, Wi-Fi and LoRaWAN systems to see if they are in line with the new requirements and use cases raised in 5G systems. Chapter 4, as the ground of our previous paper P2 [32], introduces the 5G-SSAAC approach and its detailed call flow and shows how it can support different AAC mechanisms in 5G systems. Chapter 5, as the basis of our recent paper P5 [33], extends the approach in chapter 4 and depicts its feasibility through the implementations on the OAI platform. Chapter 5 also performs the security analysis and the performance analysis of the 5G-SSAAC approach. Chapter 6 concludes this work and describes how 5G-SSAAC can enable the future research.

Chapter 2 Authentication and Access Control in Cellular Networks

2.1 Introduction

Authenticating users and controlling their access to network services is one of the first procedures in cellular networks. This procedure is mandatory for providing suitable connectivity services to the network's subscribers, preventing the network from being abused, and protecting the subscribers' privacy and their information. In other words, the AAC mechanisms provide secure network services for network subscribers. Despite the progress of the cellular networks in each generation to fulfil a broader range of requirements and use cases, the similar progress has not been made in the way of their AAC mechanisms.

The first generation of cellular networks (1G, Nordic Mobile Telephony in Europe and Advance Mobile Phone System in United States) was based on analog technologies and supports only voice call services. Due to its analog nature, its radio links did not support any encryption and an attacker just needed a radio scanner to intercept the calls.

The second generation of cellular networks, GSM (2G, Global System for Mobile Communications) was introduced in 1991 as the first digital communication system. In addition to provide messaging services, it also introduces AAC for its users. The AAC is done through the SIM (Subscriber Identity Module). A SIM card is a well-known secure element that is provided by the operator to its subscribers and contains the subscriber's permanent identity calls IMSI (International Mobile Subscriber Identity) and a long-term secret key used for encryption and establishing a secure connection between the subscriber and the network. However, its lack of mutual authentication has led to active attacks against subscribers (e.g., an attacker can impersonate itself as a valid network to subscribers) [29, 30].

In UMTS (3G, Universal Mobile Telecommunications system), the data application and mobile internet services were introduced. In terms of AAC, the 3GPP (3rd Generation Partnership Project) defined AKA-based (Authentication and Key-agreement) protocols [12] with mutual authentication feature to address the security issues raised in 2G.

In 2010, LTE (4G, Long Term Evolution) system was introduced to support higher data transmission speed (up to 100 Mbps at the early stage) all-IP architecture. In LTE, the AKA-based protocols are used for the AAC purpose as in the 3G systems. The AKA mechanism in LTE (EPS-AKA) is a complementary form of the AKA mechanism in 3G (UMTS-AKA), with a few differences [13].

In the fifth generation of the cellular networks, 5G, the aim is not only to fulfil the increasing demand for the higher throughput, the low latency and the better quality of service. Some additional concepts have also been included in the scope of 5G, such as handling the connectivity for the massive number of IoT devices, providing network slices to specific customers or vertical sectors, and managing heterogeneous network access (e.g., addressing Wi-Fi and cellular access networks from a converged network) [10]. All of these requirements and concepts affect the whole network and the associated security needs. Although the different security requirements of the new use cases, the way of AAC and main protocols provided to fulfil its requirements (e.g., 5G-AKA), still remains the same as the two previous generations [11]. The standards enhance the AAC mechanisms in 5G from the security point of view only with the central role of the connectivity provider (operator). The main focus is on detecting the shortcomings of the pre-5G generation's AAC methods (e.g., EPS-AKA) and solve their security issues in designing the AAC methods for 5G. The need of more open and flexible network in presence of new actors in the 5G environment is not considered in the mentioned enhancements.

This chapter reviews the challenges of the AAC procedure for 4G and 5G systems and discusses the new needs arising from the new 5G use cases, as well as how standards are currently evolving. The primary contributions of this chapter are:

1. An analysis of the vulnerabilities of the AAC mechanism in 4G and the clarification of their goals in section 2.6.

2. An analysis of the possible attacks against the proposed AAC mechanism in 5G in section 2.11.

Section 2.2 explains the basics of the AAC mechanisms. Section 2.3 gives an overall view of the AAC mechanisms in the recent 3 cellular network generations and the main entities evolving in these mechanisms. Section 2.4 details the functionalities of the main nodes in 4G networks. Section 2.5 explicates the EPS-AKA's call flow as the main method for AAC in 4G. Section 2.7 is an introduction of the new concepts and issues raised in 5G and depicts the reasons of why the enhancements just in the security part of the AAC is not enough in the 5G systems. Section 2.8 details the networks functions of the 5G architecture. Section 2.9 explains the 5G-AKA's call flow as the main method for AAC in 5G and its enhancements compared to EPS-AKA.

2.2 Basics of Authentication and Access Control

Authentication and access control architectures and their associated entities may vary in different contexts but the general concepts remain similar. The main objectives are always to protect the subscribers and the resources and to apply billing rules for network usage [34, 35]. Authentication means verifying the user's identity by checking its credentials. Its purpose is to know who the user is [36]. Authentication enables authorization which means defining rules to access to specific types of resources and services [37]. Its purpose is to specify what a user can do [36]. Access control is the method to control and enforce the access rights of users on the resources such as data, or even to IoT objects [38].

AAC architecture usually consists of two main functional entities; an AC (Access Control) server and an AC client. An AC server includes a database containing the users' data and it is responsible for managing the AC processes according to this database. An AC client is responsible for querying the AC server when users try to access the network through this entity [39]. The responsibilities of these two functional entities may be distributed in different physical entities for different systems. In some AC mechanisms, users are referred to by the 'peer' term. Figure 2.1 shows a typical network AAC system. In the first step the user/peer sends its access request to the AC client. In the second step the authentication is done

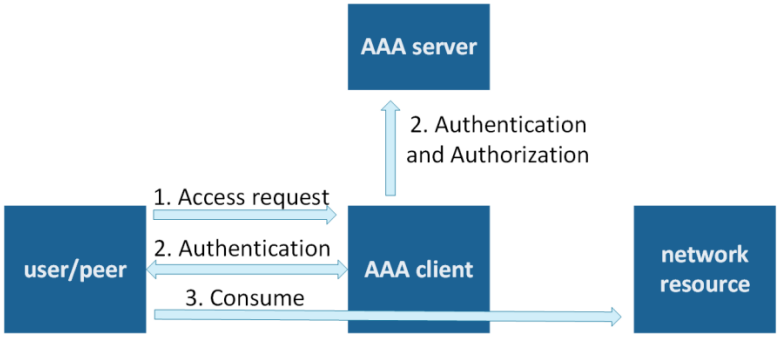


Figure 2.1– Functions of an AAC systems

between the user/peer and the AC client with the help of the AC server. Finally in the third step the user/peer gains accesses to the network resources.

2.3 Overall Architecture of the AAC in 3G, 4G and 5G

From the AAC perspective, a cellular network (e.g., 3G, 4G and 5G) consists of three main parts: UEs (User Equipment) or devices, a SN (Serving Network) and a HN (Home Network). The home network is the network which the UEs have subscriptions with. The serving network is the network which the UEs served at and it is changed in the roaming scenarios. Considering the AAC entities described in section 2.2, the UEs are the peers, the SN is the AC client and the HN is the AC server. Figure 2.2, depicts the AAC model in the cellular networks.

Following is the summary of the AAC systems used in the cellular networks (the details of the architectural entities and the AAC protocols of the 4G and 5G are described in sections 2.4, 2.5, 2.7 and 2.10 respectively). These AAC systems rely on a long-term secret key shared between:

- A hardware security module in the form of an UICC (Universal Integrated Circuit Card) running an USIM application (Universal Subscriber Identity Module, the counterpart of the SIM in 2G) inside the UE.

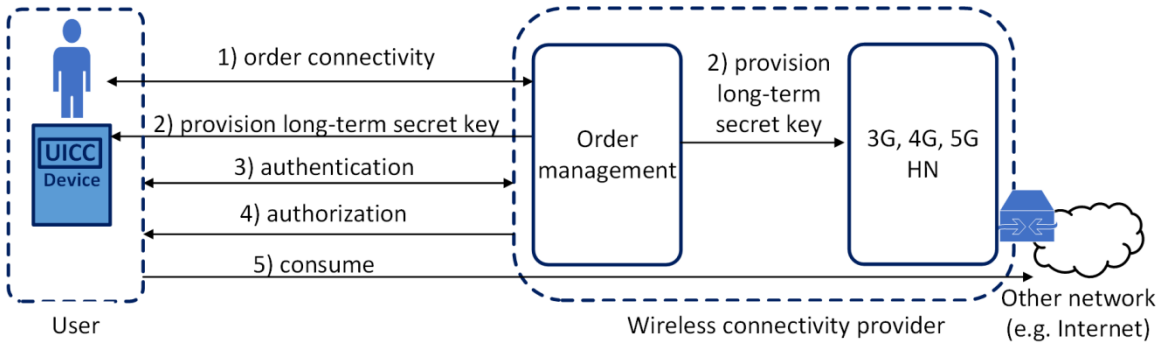


Figure 2.2– AAC model in the cellular networks.

- A database holding the UEs subscriptions data: the HLR (Home Location Register) in 3G, the HSS (Home Subscriber Server) and the UDM/ARPF (Unified Data Management / Authentication Repository and Processing Function) in 5G, which is capable of authenticating the UICC.

Mobile networks use SDM (Subscriber Data Management) systems that consolidate previous silos of subscriber data (e.g., multiple HLR/HSS) into a single system. The authentication of the UICC by the core network of the operator (the connectivity provider) confirms the identity of the UICC at the cellular network provider level. The cellular network provider can then retrieve the subscription information which had previously been associated with this UICC identity at ordering time. The retrieved subscription information is then used by the cellular network provider to authorize which cellular service can be used and to bill the subscriber for the services consumed.

The main methods that are implemented in 3G, 4G and 5G networks to fulfil AAC requirements are UMTS-AKA, EPS-AKA, EAP-AKA, EAP-AKA' and 5G-AKA (Authentication and Key Agreement Protocols). They are all challenge– response authentication protocols with mutual authentication feature (the network authenticates the subscribers and the subscribers authenticate the network). The UMTS-AKA, the EPS-AKA and the 5G-AKA are used to authenticate the subscribers connected across 3GPP access networks to the core network of 3G, 4G and 5G respectively. The UMTS-AKA involves the USIM in the subscriber's mobile equipment, the VLR/SGSN (Visitor Location Register/Serving GPRS Support Node, responsible for mobility management) in the SN, and the HLR in the core network (HN). Authentication of the subscribers is based on their unique

identity, IMSI and a shared secret key K that is stored both inside the USIM and the HLR. This identity is provisioned by an order management module from the mobile network operator Information System while the subscriber buys a UICC from the operator (figure 2.2) [12].

As with the UMTS-AKA, the EPS-AKA operates between the USIM, the MME (Mobility Management Entity, the main control node of the network) in the SN and the HSS in the HN. EPS-AKA is also based on IMSI and a shared secret key (symmetric key cryptography approach) between the USIM and the HSS (previously provisioned by the order management module). One of the important differences between the EPS-AKA and the UMTS-AKA protocols is that the EPS-AKA uses the serving network's identity in deriving the further keys in the key hierarchy (from the shared secret key K), to secure the connections between the network elements. The binding of the keys to the serving network identity reduces the probability of a serving network impersonation fraud. The details of the 4G network entities and the EPS-AKA are explained in sections 2.4 and 2.5 respectively [13].

The 5G-AKA is also based on symmetric key cryptography approach (as the UMTS-AKA and the EPS-AKA) operates between the UEs and the network (details are in section 2.10) with the same AAC manner as the AAC in the pre-5G cellular network generations [11].

The EAP-AKA and the EAP-AKA' are responsible for the authentication of subscribers when they try to access a 3GPP core network via a non-3GPP access network (e.g., via a public or private Wi-Fi network). These two protocols belong to the EAP framework (Extensible Authentication Protocol). In this framework, we have 'authenticators' (the AC client) and 'EAP servers' (the AC server). In the EAP-AKA and the EAP-AKA', the authentication process is based on NAI (Network Access Identifier, derived from IMSI) and a shared secret key as in UMTS-AKA, EPS-AKA and 5G-AKA. It is performed between USIM or any other application with a similar functionality (this part is left unspecified in 3GPP specifications because of the use of non-3GPP access networks) and the network. The EAP-AKA' is more secure than the EAP-AKA as it uses serving network identity in key derivation processes like the EPS-AKA [11, 13].

2.4 4G Network Architecture

4G uses a completely IP-based packet-switched architecture. This means, in contrast to its predecessors, all the transmissions offered as IP-based services (e.g., VoIP, Voice over IP) [30]. The 4G architecture combines many functional entities to ensure AAC. The 4G network consists of the operator's IP network and all of the entities that are connected to this IP network. This means that all the entities have the same IP protocol and communicate with each other via a typical IP network (through logical interfaces).

The 4G network consists of three main components: the UE (User Equipment), the E-UTRAN (Evolved Universal Terrestrial Radio Access Network) and the EPC (Evolved Packet Core).

The E-UTRAN is the access network of the 4G and handles the radio communications between the UE and the EPC. The EPC is the core network of the 4G and it contains all the entities for handling the UE's connectivity and mobility. The main entities of each part are described below and summarized in Figure 2.2 [40]:

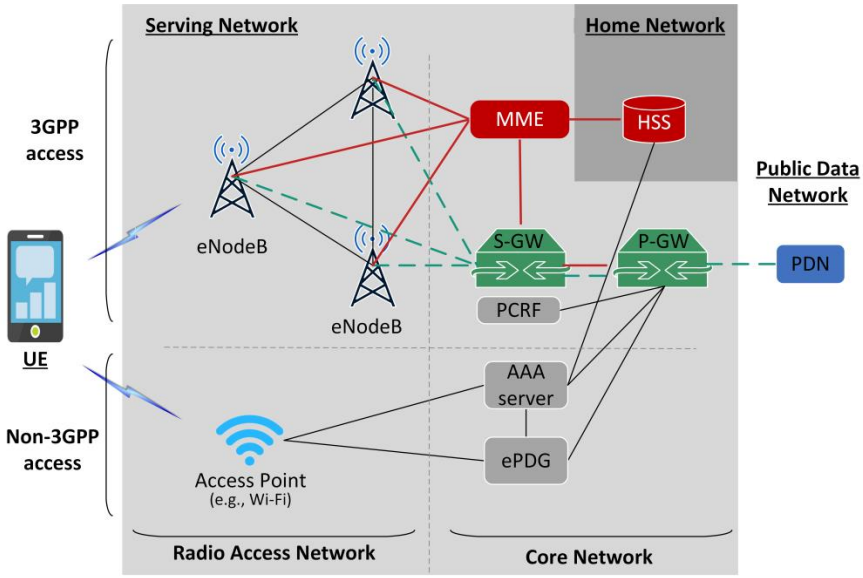


Figure 2.3– 4G network architecture. The MME and the HSS are in the control plane and the S-GW and the P-GW are in the user plane. The solid lines show the control plane links and the dashed lines show the user plane links.

- UE: a mobile device that includes a UICC (Universal Integrated Circuit Card) integrated with the USIM (Universal Subscriber Identity Module, the counterpart of the SIM in 2G). The USIM stores user-related information, such as the IMSI that is used to identify each UE in a unique way and the subscriber's Secret key (which is pre-shared with the AuC part of the HSS and never leaves these two elements). The IMSI uniquely identifies a subscriber and consists of three parts: an MCC (Mobile Country Code), an MNC (Mobile Network Code) that specifies the subscriber's carrier network, and an MSIN (Mobile Subscriber Identification Number) that identifies the subscriber in the mobile network. The USIM participates in the subscriber authentication process.
- eNodeB (evolved Node B): the main component of the E-UTRAN. Each eNodeB consists of an antenna and a set of transceivers. The eNodeBs can be directly linked together; compared to 3G this flatter architecture promotes lower latency and better connection performance in comparison with 3G [41, 42].

The main entities of the EPC are:

- MME (Mobility Management Entity): the main control node of the network. The MME performs authentication by getting the subscription information from the HSS and is mainly responsible for the attachment process, bearer handling (in collaboration with the P-GW), the tracking of UE locations and selecting the gateways (deciding the pathways of the data packets).
- HSS (Home Subscriber Server): a database that stores the subscriber's data (including their identities, rights and subscription profiles) and the secret keys. HSS contains the AuC (Authentication Centre) that holds and generates all the needed cryptographic material. It provides authentication data to the MME.
- S-GW (Serving Gateway): anchors the data bearer and routes data packets to the UE.
- P-GW (Packet Data Network Gateway) connects the packet core network to the external networks, such as the internet, and provides IP addresses to the UE. It is also responsible for policy enforcement, billing, and charging based on the rules provided by a PCRF.

- PCRF (Policy and Charging Rules Function): manages the bandwidth and network resources usage and controls the QoS of the sessions for each subscriber according to the subscription information, the provided services, and the peak usage times.

The 4G network architecture is designed to separate the entities that manage the control (Control Plane) from the entities that take care of traffic (Data Plane). All of the data plane packets in the (public) packet data network that are destined for 4G network subscribers (UEs) are routed to the P-GW of the operator's network. The P-GW sends the data plane packets to the S-GW, the S-GW sends them to eNodeB and the eNodeB delivers them to the intended UE. S-GWs act as intermediary entities. Each is responsible for a specific geographic area. The movements of UE are usually within the same S-GW. Therefore, thanks to these S-GWs, there is no need to bother the P-GW for UE location updates.

In addition to data plane packets, a set of control functions and signalling messages (control plane packets) are also transmitted in the network to manage network access or the tracking of the UEs when they move. The Subscribers' authentication and access control processes belong to this category. The MME and the HSS only take care of control plane packets and do not manage data plane packets. The control messages' path (that is related to the subscribers' authentication and access control) is between the UEs, the eNodeB, the MME, and the HSS. The MME is designed to prevent the HSS from being disrupted by the millions of UE requests for each of their activities needing access control (e.g. location update). Each MME manages a very large region. The number of MMEs in a PLMN (Public Land Mobile Network) depends on the operator's decision (e.g. the size of the area that is under the responsibility of the operator). At the first attachment of a UE, the MME obtains the UE's profile and all the security information from the HSS. Then, for all further accesses, the MME will be able to verify the UE's access rights.

The 4G architecture supports multiple access technologies (trusted and untrusted access networks). The operator decides which non-3GPP access networks are trustworthy and which are not. The handling of non-3GPP accesses involves two other entities:

- AAA Server: responsible for the authentication and authorization of the UE in the case of non-3GPP access; and

- ePDG (Evolved Packet Data Gateway): responsible for the establishment of an IPsec tunnel between the operator's core network and the UE in the case of untrusted non-3GPP access

2.5 EPS-AKA Protocol

Without loss of generality, we focus on the EPS-AKA protocol and its vulnerabilities as it is the main authentication and key agreement protocol to fulfil the AAC requirements in 4G. In the 5G specifications (release 16), this protocol is reused (5G-AKA), with some differences [11]. EPS-AKA is based on the symmetric key cryptography. Figure 2.4 depicts the EPS-AKA procedure. As indicated in figure 2.4, the EPS-AKA procedure starts by sending the *Attach request* message from the UE to the MME after it finds its operator's eNodeB (each eNodeB broadcasts the operator's identity via a beacon channel). This message contains the UE's IMSI or GUTI (Globally Unique Temporary Identifier) if it is not the initial attach request [43]. GUTI is a temporary identifier that the MME allocates to a UE after the initial attachment procedure and after the activation of the radio channel encryption, thereby protecting the IMSI from eavesdropping (i.e., it is used instead of the IMSI in the further attachments of the UE to the network to avoid the IMSI having to be transmitted frequently). A GUTI consists of a TMSI (Temporary Mobile Subscriber Identity) that is allocated by the UE's current MME, and the MME's identifier. If the MME cannot recognize the GUTI (e.g., the UE exits the MME's territory), it sends an *Identity request* message to the UE, which then sends its IMSI in the *Identity response* message. The rest of the EPS-AKA procedure is as follows [13, 45]:

- The MME sends an authentication information request that contains the UE's IMSI and the SNid (Serving Network Identifier to the HSS). The UE trusts the home network about the verification of the serving network's identity (the home network uses the SNid to compute the serving network's specific K_{ASME} key that we will describe below).
  The HSS generates a random number RAND. To authenticate the UE, the network needs to be sure about the presence of the secret key in the UE. As explained in subsequent steps, to indicate this presence, the HSS sends this random number (RAND) to the UE. Then, the HSS and the UE will do the same calculation with RAND, and if

the results are the same, the presence of the secret key in the UE will be approved. The HSS also finds the UE's secret key K (according to the UE's IMSI) and then inputs the RAND and the K into cryptographic functions to generate AVs (Authentication Vectors). AVs consist of the RAND, an XRES (the MME checks if XRES is equal to the RES from the UE to authenticate the UE), a local master key K_{ASME} (computed by a key derivation function with the SNid as one of its inputs) and an AUTN (Authentication Token). The AUTN is the result of another calculation with the random number and the secret key. The AUTN will be used by the UE to authenticate the network. The UE will also calculate it and if it gets the same amount, it will trust the network. The other input of the cryptographic functions is SQN (a counter) that is increased with each new authentication. The HSS keeps this counter for each UE, using it to prevent an attacker from impersonating itself to the UE by stealing the AVs and reusing them. Indeed, SQN guarantees the freshness of the AVs.

- The HSS sends the AV to the MME that stores the K_{ASME} and XRES parts of the AV, and sends the RAND and AUTN to the UE.
- The USIM inside the UE retrieves the SQN from the AUTN by using the secret key K and the RAND; next, it computes the $AUTN_{UE}$ by using the same cryptographic functions as the HSS. The UE authenticates the HSS by comparing the $AUTN_{UE}$ with the AUTN (the HSS is authenticated if the $AUTN_{UE}$ and the AUTN are equal). Then, the UE checks if the SQN is in the right range (the USIM has its own SQN, and so it checks if the SQN from the HSS is not too far from its own SQN, to ensure synchronization between the HSS and the UE). Next, the USIM computes the K_{ASME}, so that both the UE and the MME have the same key with which to establish secure connections. The USIM also computes a RES and sends it to the MME. If the SQN is not in the expected range, the UE sends a synchronization failure message, and if $AUTN_{UE}$ is not the same as AUTN, the UE sends a authentication failure message to the network.
- The MME checks if XRES and RES are equal and then completes the authentication and key agreement process.

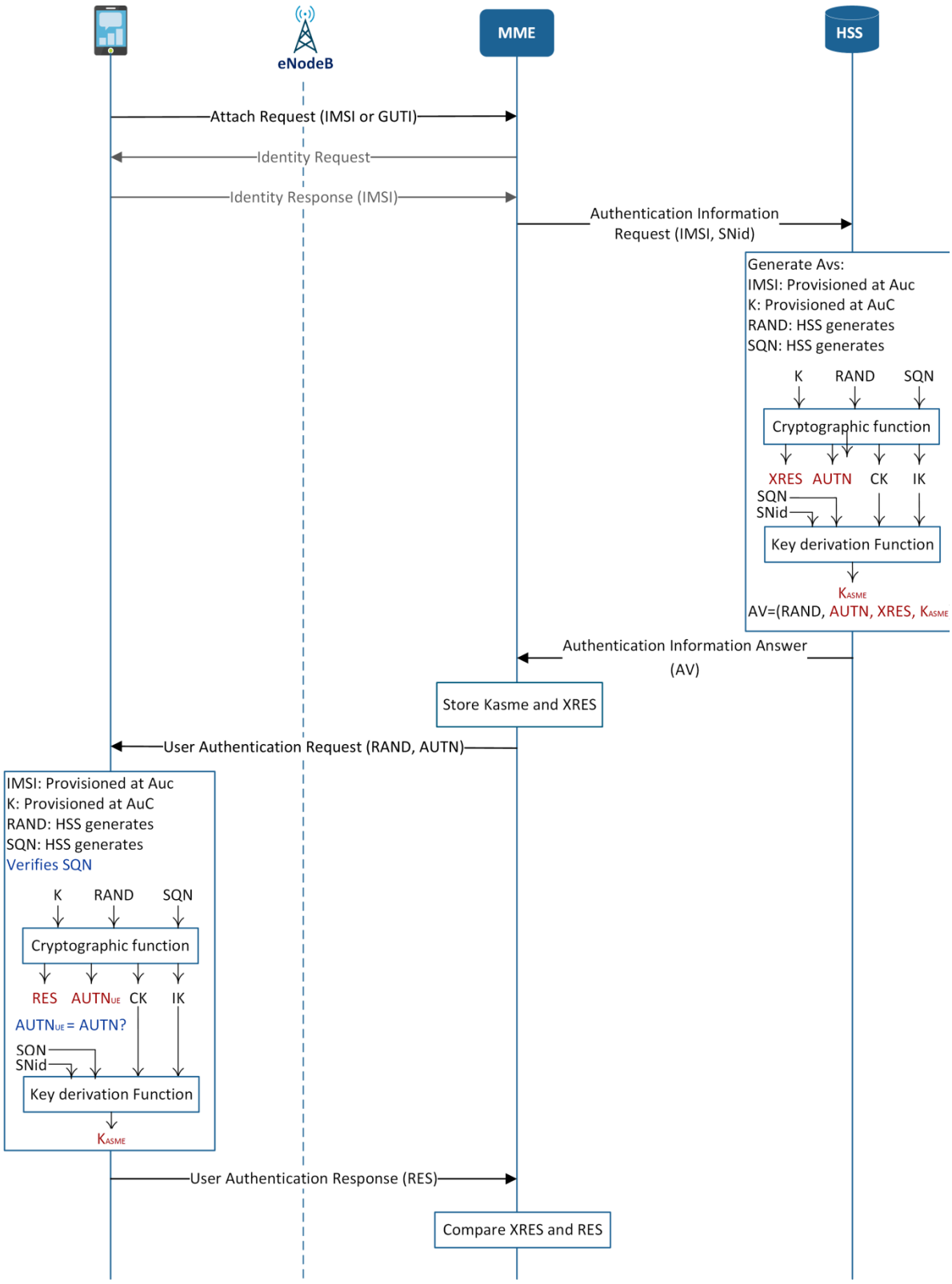


Figure 2.4– The EPS-AKA procedure.

After the mutual authentication is done between the UE and the network through the EPS-AKA procedure and the UE's network access authorization is determined, the NAS (Non-Access Stratum) security procedure and the AS (Access Stratum) security procedure are performed. NAS security is to provide ciphering and integrity protection for the signalling between the UE and the MME. AS security is to provide ciphering and integrity protection for the signalling between the UE and the eNodeB as well as the ciphering for the user traffic between them. While NAS messages are transmitted via the eNodeBs, their content is not analysed by the eNodeBs, but the AS messages are analysed by the eNodeBs. The required keys for the NAS and AS security procedures are derived from the K_{ASME} key. After the execution of the EPS-AKA and the NAS security procedures, the MME proceeds to the creation process of the sessions for the UE via the SGW and the PGW. In the session creation process, the PGW assigns an IP address to the UE and this IP address is delivered to the UE at the end of the attachment process. Finally the AS security procedure is done after the successful attachment of the UE to the network.

2.6 Security flaws in EPS-AKA

There are various security concerns with LTE security. In the scope of this work, we only focus on the authentication and access control; and so we mainly consider EPS-AKA protocol vulnerabilities. Table 2.1 summarizes these vulnerabilities and their effects on the security of the LTE system. These vulnerabilities and attacks are also depicted in figure 2.5. As a general principle, authentication of UEs is needed to avoid the fraudulent use of the network (e.g. by stealing other UEs' IMSIs).

The first vulnerability is IMSI disclosure (IMSI catching), which affects user confidentiality. As mentioned in the previous section, the UE sends the IMSI to the MME in clear text during the first attachment procedure. Furthermore, the IMSI is transmitted in paging messages that are sent from the MME to eNodeBs and from eNodeBs to UEs, in order to locate a specific UE (for example, when a UE has an incoming call). An attacker can trigger a paging procedure without alerting the user, e.g. by using social network applications, and then sniff the paging messages between eNodeB and a UE to decode them

Table 2.1 – Summary of the EPS-AKA vulnerabilities and attacks, the goal of these attacks and the current solutions

Vulnerability	Attacks	Attacks Goals	Proposed Solutions
- IMSI disclosure - GUTI persistence	- Impersonating UEs [42, 50, 53, 73] - MitM	- Weaken subscriber confidentiality - DoS attacks against the HSS and the MME - Theft of service	- public key-based solutions [55-60]
- SNid disclosure	- Rogue eNodeB [45, 52, 53, 65]	- Disclosure of the subscriber's location - Weaken UE's data security - Intercepting connections between the UE and the network - DoS against the MME	- public key-based solutions [57, 61]
- Acceptance of TAU reject, Service reject, Attach reject messages without integrity protection	- DoS attack	- DoS against a UE [45]	- public key + digital signature [45]
- UE's network and security capabilities disclosure	- Bidding down attack	- DoS against a UE	- public key + digital signature [45]
- Synchronization failure	- Replay attack - Impersonating UEs	- Disclosure of the subscriber's location - DoS against UEs	

and acquire the IMSI [45, 46]. In handover cases between MMEs, if a synchronization failure occurs, the new MME or the previous one request the UE's IMSI, which is then transmitted in clear text again [42, 47-49]. In these cases, an attacker can simply eavesdrop the connection to capture IMSIs.

One of the problems of IMSI disclosure is the theft of services with session mix-up attacks. This can be an inside attack, where the attacker is a subscriber of the network but impersonates itself as another subscriber to use the services that the victim should get from the network [47, 50, 51]. It could also be an outside attack, in which the attacker is not a network subscriber network and swaps services between network subscribers network [51]. Theft of service attacks can also happen between the UE and the IMS parts of the network (IP multimedia subsystems that provide multimedia services such as voice calls) and thus affect the operator's revenue [52]. It is also possible for an attacker to force a UE to repeatedly send

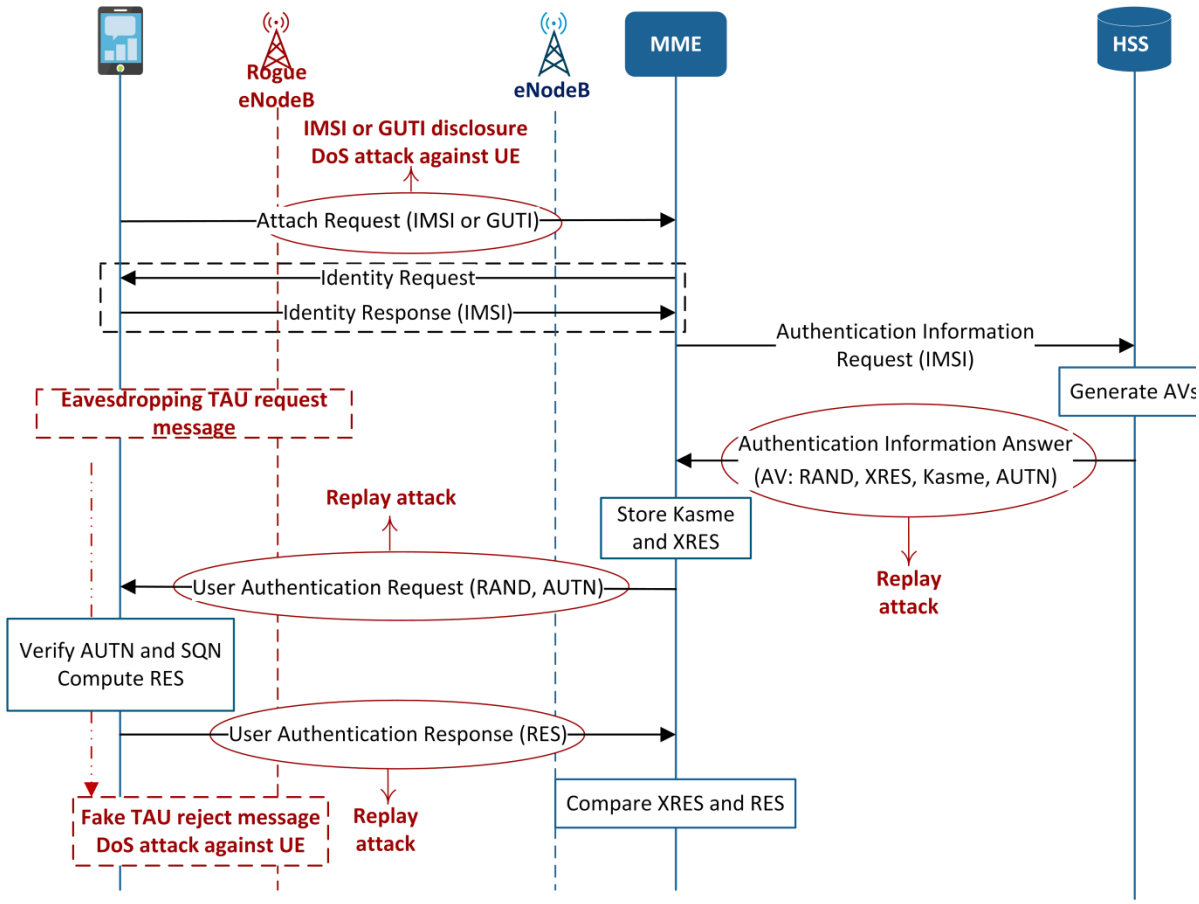


Figure 2.5– The EPS-AKA vulnerabilities and attacks.

IMSIs, thereby expending both the computational power of the HSS and the memory of the MME [53, 54]. In addition to the above problems, IMSI disclosure can cause a service disruption for the UE. As mentioned in the previous section, the UE checks the SQN range after getting the AV. If a malicious UE sends attach requests several times by using a victim UE's IMSI, the SQN amount increases in an uncounted way on the HSS side. Then, if the victim UE sends a real attach request to the network, it will get an AV with an out of range SQN and so the UE will face a synchronization failure.

To solve the IMSI disclosure problem, some solutions based on public key cryptography have been proposed [55-62]. Some of these encrypt all the messages between the UE and the network, and some only encrypt the IMSIs. Most of the public key-based solutions increase the computational and communication costs for UEs (with limited capabilities and energy) and for network elements. Pseudonym-based solutions to the IMSI disclosure problem were also

proposed [49, 63], but these require additional capabilities in UEs or additional entities in the network [42, 56, 61, 63].

As mentioned in section 2.5, GUTI is a temporary identifier and should be fresh. The main purpose of using this temporary identity is to have a protection against the UE's location disclosure (if a UE sends its IMSI to the network frequently, an attacker can detect it and determine that the UE is nearby). However, in reality, GUTIs are not changed frequently (the operator does not configure its network to refresh the GUTI frequently), and so their disclosure may cause the same problems as IMSI disclosure [45, 61, 64]. An attacker can also change GUTIs. In this scenario, the server cannot recognize GUTIs and so requests UEs to send their IMSIs [60].

One of the most severe types of attacks is to use a rogue eNodeB that pretends to be a legitimate eNodeB. By operating with high power, a false eNodeB can force UEs to connect to it [45, 52, 53, 65, 66]. A rogue eNodeB can redirect UEs to another network that provides weak data encryption instead of the UE's home network [47]. It can cause man-in-the-middle attacks (MitM, where the attacker impersonate itself to the network as a legitimate UE) [47] and also the disclosure of a UE's location. A rogue eNodeB can compromise session keys during handover processes as well (de-synchronization attacks) [42, 48], or hijack the paging channel (blocking the UE's incoming calls or creating paging messages with a victim UE's IMSI and forcing it to disconnect from the current legitimate eNodeB and send and attach request to the rogue eNodeB). Leakage of the SNid, because of clear transmission from the MME to the UE, may also cause rogue eNodeB attacks [48, 57]. SNid disclosure may cause traffic on the MME as well, as an attacker can force UEs to attach to an MME [61]. Furthermore, LTE systems support femtocells and HeNodeBs and operators do not control them, so an attacker can use them as rogue eNodeBs to collect IMSIs [56, 62].

The next type of vulnerability is related to the TAU (Tracking Area Update) procedure. Mobile operators divide their service area into tracking areas and each tracking area consists of a number of cells. UEs, inform the MME about their locations by sending TAU messages. Some network services are not accessible in some tracking areas, or some UEs are not authorized to access them; as a result, the network sends TAU reject message to UEs. This

message is not encrypted and integrity protected (if the UE performs the TAU procedure after changing location in idle mode, it does not contain the keys for the encryption and the integrity protection purposes). In this case, an attacker can cause DoS (Denial of Service) attacks against a UE by getting TAU request messages from a UE via a rogue eNodeB and sending TAU reject message to the UE with "LTE services not allowed" or "LTE and non-LTE services not allowed" content [45, 54, 66]. It is also possible for an attacker to use the location information of a UE to find a link between its IMSI and GUTI and then trace the UE across the network [56].

DoS attacks against UEs can also happen during an attachment procedure when the UE sends its network and security capabilities to the network. An attacker can change this message, causing the MME to reject some of the UE's requests [45, 47].

Unprotected AVs' vulnerability can be used to determine if a specific UE is in a particular area or not and thus track its movements. AVs are sent in clear text between the HSS and the MME and between the MME and the UE [57]. If an attacker gets these AVs (using User Authentication requests) by eavesdropping the connection between the MME and the UE, it can replay them. The attacker will then send these AVs to the UEs in a specific area. The UE that the AVs belong to will send synchronization failure message and the other UEs will send MAC failure messages, allowing the attacker to determine the presence of the UE in that location [46, 52, 60, 61, 67- 69].

Finally, EPS-AKA is based on symmetric key cryptography, and all the keys that are used to prevent data integrity are derived from the secret key (in the key hierarchy), therefore, the leakage of this key would cause serious problem to the whole network [47, 57].

In addition to the aforementioned vulnerabilities, some security issues are due to the interworking with non-3GPP access networks. The UE uses EAP-AKA and EAP-AKA' as the authentication and key agreement protocol when trying to access the LTE core network via a non-3GPP access network, as well as during handover procedures between 3GPP access networks and non-3GPP access networks [43]. These protocols are similar to the EPS-AKA protocol (instead of MME, they work with an AAA server; the needed keys are driven from the AVs that the AAA server gets from the HSS) and so they have similar vulnerabilities as

EPS-AKA, such as attacks against UE privacy and location, DoS attacks, UE impersonation and billing mechanism attacks [70- 72].

2.7 5G Network

The fifth generation of mobile communications has a number of goals, such as achieving low latency, high data rates, increased convergence, accessibility and dense connectivity. 5G will also support IoT (Internet of Things) services and address the needs of different vertical markets, such as healthcare, automotive and transport. The 5G-PPP (Fifth Generation Public Private Partnership) has defined several different use cases for 5G, including enhanced mobile broadband and critical communications [74].

These different goals and use cases have important impacts on the security aspects of the system, and service-specific security requirements should be considered when designing appropriate authentication and access control mechanisms for 5G networks (e.g., fast communications need fast AKA procedures) [75]. As another example, in the IoT, numerous devices may access the network at the same time, and so the network should have the ability to control this large amount of signalling traffic and authenticate the devices correctly to avoid DDoS (Distributed Denial of Service) attacks. The IoT devices have low power capacity and cannot support strong authentication procedures. In addition, they are usually able to connect to the network via non-3GPP access options (some of them will not have 5G radio access and will use Wi-Fi or Bluetooth) [76]. In light of these limitations, some solutions based on group-based authentications with an IoT gateway have been proposed to decrease the number of full AKA procedure executions [77, 78]. But these group-based AKA solutions have their own weaknesses. While some of these include the traditional AKA weaknesses mentioned in the previous section, some are specific to the group-based nature of these approaches. For example, an attacker can pose as a member of a group and get access to the network [79].

The aforementioned requirements of 5G have also produced new concepts, and thus new security issues:

- Network slicing, which is a solution to meet heterogeneous requirements from different vertical markets [2]. Networks slices are logical networks relying on a single physical network [80]. Each network slice is composed of various network functions to provide specific capabilities and to satisfy a specific type of usage [80]. For example, in some IoT cases (e.g., a smart factory), mobility will not be very high, so it may not need mobility handling functions [80]. There can be different approaches in providing network slicing (for example, we can have a slice per service or a slice per vertical market). Different technologies like SDN (Software-defined Network), NFV (Network Function Virtualization) and automation as with ONAP (Open Network Automation Platform) will be used to deploy slicing. [4], [81] and [82] present some proposals for network slicing architecture and implementations. Concerning security, network slicing also adds some issues such as slice isolation to prevent threat propagation through slices, authentication and integrity protection of input data, and access control between slices [76].
- Heterogeneous network access, as different radio technologies might be used to access 5G networks. As we mentioned before, one of the 5G goals is to provide a better accessibility to users, therefore when users do not have 5G connectivity, they may connect to 5G network through other types of accesses, e.g., satellite access. In IoT case, devices may also use different radio access technologies. In these situations, the enterprises or satellite providers may have their own AAA servers and the management of the connection between different AAA servers, especially in roaming scenarios is very important [76, 83]. It is also important to prevent the network against unauthorized access in this heterogeneous infrastructure [84].

2.8 5G Network Architecture

3GPP has provided a technical specification to define the architecture of 5G systems and to specify the main nodes and their responsibilities [10]. In this architecture, control planes and user planes are separated as much as possible to achieve more flexible and scalable deployment. Instead of Network Entities grouping many functions, 3GPP attempted to define NFs (Network Function) with more atomistic roles (i.e., one specific responsibility per function). However,

most of these NFs are somehow a mapping of existing 4G entities. Two representations are possible for NF interactions; one of them is based on the SOA (service-oriented architecture) viewpoint and the other is based on traditional reference points. In service-based representation, an NF exposes a set of services it offers to other NFs, and it uses the services provided by other NFs. All interactions are carried by the same protocol for API invocations. Each time a new NF needs to be plugged in, only its new API should be declared to the other components. In the reference point representation, specific protocol links are kept between pairs of network functions. Figure 2.6 shows the 3GPP provided 5G architecture and its network functions [10].

The two first defined NFs can be seen as an evolution of the HSS:

- AUSF (Authentication Server Function) provides a unified framework for authentication issues (for 3GPP access as well as non-3GPP access); and
- UDM (Unified Data Management) contains data that is related to the HSS (i.e., user data). The UDM stores only some part of the data (such as a user's subscription data) and not all of it. It also supports authentication credential processing, user identification handling and access authorization.

Indeed, we should observe that the concept of the data in 5G is a little bit different than it is in 4G, with the differentiation between structured data and unstructured data. Structured data is exchanged between NFs in a standardized way, to enable communication between equipment from different vendors. Unstructured data is vendor-specific data that can be hidden from other network functions. Three new functions are defined in this context:

- SDSF (Structured Data Storage network function);
- UDSF (Unstructured Data Storage network function); and
- UDR (Unified Data Repository), which is responsible for storing or retrieving subscription and policy data

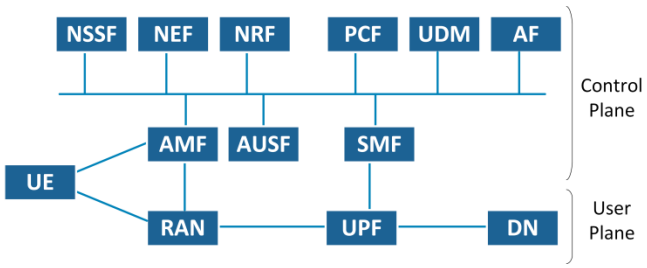


Figure 2.6– 5G.architecture and its main network functions. All of the NFs can connect to the UDSF, the NEF and the NRF; therefore they are not shown in the figure.

Two other NFs can be seen as a division of the 4G MME:

- AMF (Core Access and Mobility Management Function) has different functionalities, including access authentication and authorization, registration management and mobility management. Since different access technologies will be used, 5G needs a common framework for access management, as well as for handling mobility between different types of access. Therefore, the AMF will support both 3GPP access networks and non-3GPP access networks. Unlike 4G (where the MME is used for 3GPP access and the AAA server for non-3GPP access), the structure of the core network will be common for 3GPP access and non-3GPP access in the 5G system
- SMF (Session Management Function) is responsible for session management and some other functionality, such as the allocation of IP addresses and the control of the policy enforcement and QoS (establishment of a session is totally separated from mobility management in 5G).

A function is also dedicated to policy management, as the PCRF (Policy and charging rules function) in 4G was:

- PCF (Policy Control Function) is related to policy framework and provides policy rules to NFs in the control plane.

New functions are introduced to manage the instantiation of network functions and the interactions between them:

- NEF (Network Exposure Function) handles all the information and services that can be exposed by NFs, for example, to 3rd parties, and the information exchanges between different NFs in the control plane
- NRF (NF Repository Function) stores the NFs available in the system and informs other NFs about new NFs. In the service-based representation, each time a new NF is added to the system, it needs to be discovered by all the other NFs.

A new function is also dedicated to network slicing:

- NSSF (Network Slice Selection Function) determines the serving AMF for the UE and selects network slice instances for it (in addition to the network slicing concept, network slice instances provide specific services to different enterprises).

Finally, generic functions represent the application plane, transfer plane and external data network:

- AF (Application Function) provides services to 3rd parties (e.g., it establishes the QoS and some charging aspects for a service in IMS)
- UPF (User plane Function) is responsible for everything related to user data and acts as a high-performance forwarding engine for user traffic. It can be located closer to end users to allow for local processing.
- DN (Data Network) handles internet access or services from operators and 3rd parties.

2.9 Authentication and Access Control in 5G

The 5G architecture comes with some new design choices for the authentication and access control, but also brings much continuity. The most important continuity concerns the symmetric key-based authentication through a secure element. In 5G specifications release 16, it is decided to keep a secure element in the UE or device (like the UICC in 4G and 3G and the SIM card in 2G) to process subscription credentials [11], which could also be an ESIM (Embedded SIM) provided by device makers and with which operators can provision their

profile over-the-air at the subscription time. The authentication methods introduced in 5G specifications are 5G-AKA, EAP-AKA' and EAP-TLS (Transport Layer Security).

5G introduces a new type of identifier, the SUPI (Subscriber Permanent Identifier), which is somehow equivalent to the IMSI but with a more global footprint, as it can be used not only for cellular service subscribers but for different environments like the IoT. The SUPI can have different formats: IMSI and NAI (Network Access Identifier). The NAI is more flexible than the IMSI and it can include different identifiers (including the IMSI). To protect user privacy, the MSIN part of the identifier will be encrypted with the public key of the subscriber's home network (limiting the IMSI disclosure vulnerability). This choice can be justified as follows: if all parts of the identifier were encrypted, the decryption would have to be done in the serving network in order to route the messages to the right home network. This would impose the need for a global mechanism to distribute and manage certificates as well as to control multiple public keys for different serving networks. The SUCI (Subscription Concealed Identifier) contains the concealed SUPI. The public key of the home network could be stored in the secure element of the UE. The 5G-GUTI is also used as the temporary identifier, like the GUTI in the 4G systems. Sending the SUCI as the encrypted form of the SUPI over the radio links is the major security improvement of 5G in comparison with the former generations. It prevents the UEs' or devices' permanent identifiers to be sent in a clear text over the radio [11].

2.10 5G-AKA Protocol

Without loss of generality, we focus on the 5G-AKA protocol (and its differences with the EPS-AKA protocol) as it is the main authentication and key agreement protocol to fulfil the AAC requirements in 5G. Figure 2.7 depicts the detailed message flow in 5G-AKA procedures [11]. As mentioned in section 2.9, the authentication mechanisms in 5G systems will be done along with the same principle as in 4G systems with some minor differences. These differences in AKA mechanisms will be from the network perspective only, and not from the UE perspective. AKA mechanisms in 5G systems, like those in 4G systems, use a

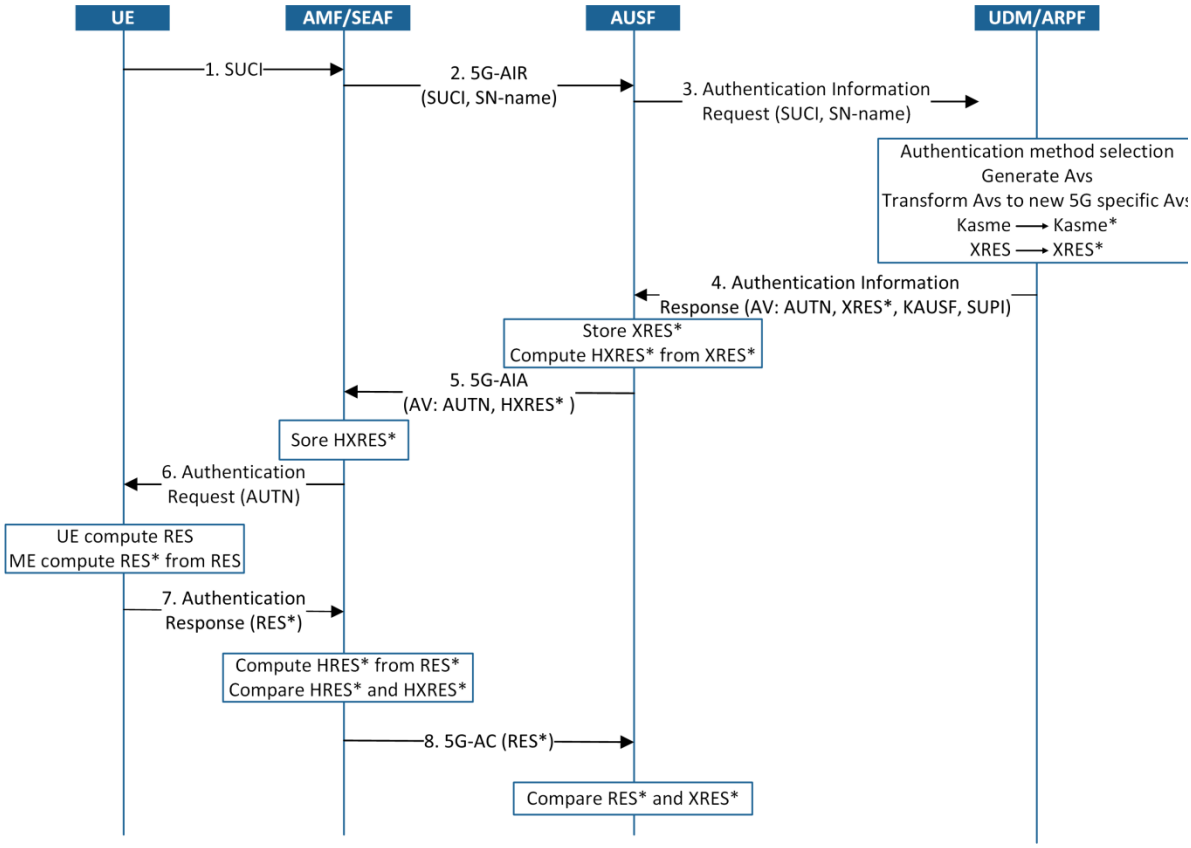


Figure 2.7– The 5G-AKA procedure. The computation of the RES* in the ME (Mobile Equipment) is in the same way as the computation of the XRES* in the ARPF. The computation of the HRES* in the SEAF is in the same way as the computation of the HXRES* in the AUSF.

"serving network name" (like SNid in 4G) to derive the anchor key (K_{SEAF}), thus, the anchor key will belong to the specific serving network and this serving network cannot pretend to be another serving network. Different from the EPS-AKA; there are 4 actors in the 5G-AKA which are explained further in this section. Another difference in AKA mechanisms for 5G systems is that the anchor key (K_{SEAF}), that is derived in a 3GPP access, can also be used in a non-3GPP access without a new authentication process. As mentioned in section 2.4, the 4G systems use EPS-AKA for 3GPP access and EAP-AKA for non-3GPP access, but in 5G systems both 5G-AKA and EAP-AKA' can be used in 3GPP access and non-3GPP access. The NAS context (e.g., K_{AMF} which is derived from K_{SEAF}) is needed for 5G-AKA, which is not present for non-3GPP access, and so, at the beginning of non-3GPP access, only EAP-AKA' is foreseen [85].

The authentication process will involve the UE, the SEAF (Security Anchor Function) in the serving network, the AUSF in the home network and the UDM/ARPF (Authentication Repository and Processing Function) also in the home network [86]. The SEAF will be included in the AMF, and interact with the AUSF to obtain authentication data from the UDM. It accomplishes UE authentication for different access networks. The ARPF stores subscribers' profiles and the information related to security. It also selects an authentication method (e.g., 5G-AKA, EAP-AKA', EAP-TLS) based on the subscriber's identity and computes the keying materials for the AUSF. According to figure 2.7, the call flow of the 5G-AKA is as follows [93]:

1. At the beginning of the authentication process, the UE sends its SUCI to the SEAF.
2. After receiving the signalling message from the UE, the SEAF sends the 5G-AIR (Authentication Initiation Request) message to the AUSF. The 5G-AIR contains the SUCI or SUPI of the UE and the name of the serving network. This message also indicates that the UE using a 3GPP access or a non-3GPP access.
3. After verifying the authorization of the serving network that asks for the authentication service, the AUSF sends the Authentication Information Request message to the UDM/ARPF. If the AUSF sends the SUCI in this message, the SIDF (Subscription Identifier De-concealing Function) which is collocated with the UDM/ARPF decrypts the SUCI to obtain the SUPI. After receiving the authentication information request from the AUSF, the UDM/ARPF generates an AV as in 4G, and then transforms them to new AVs that are specific to 5G systems. This transformation will be different according to the chosen authentication method.
4. The UDM/ARPF sends the AVs containing the AUTN, XRES*, K_{ASUF} and the decrypted SUPI to the AUSF in the Authentication Information Response message. Upon receiving this message, the AUSF computes the HXRES* which is the hash of the XRES* and stores the K_{AUSF}.
5. The AUSF sends the 5G-AIA (Authentication Information Accept) including the HXRES* to the SEAF. This message does not include the SUPI and the AUSF (in the home network) sends the SUPI to the SEAF (in the serving network) only after the successful UE authentication.

6. After storing the HXRES*, the SEAF sends the AUTN token in the Authentication Request message to the UE. The UE checks the validity of the AUTN (using its secret key shared with the home network). If the AUTN is valid, the network authentication in the UE is successful. If the AUTN is not valid, the UE sends the MAC Failure message to the SEAF (Message Authentication Code). Next, as in the ESP-AKA procedure, the UE checks the SQN derived from the AUTN to control the freshness of the AUTN. If this verification fails, the UE sends the Synchronization Failure message to the SEAF. The UE also computes the RES*.
7. The UE sends the RES* to the SEAF in the Authentication Response massage. The SEAF checks the validity of the RES* by computing the HRES* and comparing it with the HXRES*.
8. For making the final decision about the UE's authentication by the home network, the SEAF sends the 5G-AC (Authentication Confirmation) message including the RES* to the AUSF. The AUSF checks the validity of the RES* by comparing it with the XRES*. Sending the 5G-AC message from the SN to the HN is a prevention against the possible billing cheat raised by the SN [94]

In terms of success, the AUSF computes the K_{SEAF} and sends it to the SEAF along with SUPI. The further keys for securing the radio connections are derived from the K_{SEAF}. In addition to use of the encrypted form of the UEs or devices' permanent identifies, 5G-AKA differs from the EPS-AKA in the following areas:

- In the 5G-AKA, the AUSF, which is a part of the home network, makes the final decision on the UE's authentication. But in the EPS-AKA, the HN (HSS) only generates the authentication vectors and does not make decision on the UE's authentication. This property in 5G-AKA, reduces the level of trust the 5G system has to put into the SNs. Thus, the SN cannot send fake authentication information requests to the HN for the UEs not attached to one of its gNBs (5G base station).
- The key hierarchy in the 5G-AKA is different from the key hierarchy in the EPS-AKA. In addition to the K_{SEAF} which operates like the K_{ASME} in EPS-AKA (the anchor key), the 5G-AKA also introduces the K_{AMF} as another intermediate key.

The 5G system also supports the EAP-AKA' and the EAP-TLS methods. The EAP-AKA' method is also based on the symmetric cryptography and it has the same security characteristics as the 5G-AKA with some differences related to the message flows, the role of the SEAF and the derivation of the K_{AUSF}. The EAP-TLS method is different from the 5G-AKA and EAP-AKA' and it can be used in some private networks and IoT use cases. The mutual authentication in this method is based on the certificates. Although the EAP-TLS eliminates the need of storing the long-term keys in the home network, it increases the overhead of the system as it has to manage the certificates '[87].

2.11 Security flaws in 5G-AKA

Although the 5G-AKA is not in the operational stage yet, some security flaws have already been recognized. This section summarizes the 5G-AKA vulnerabilities found so far. As in the 4G network, the communications between the network functions within the 5G core network is done through the secure channels (the communications between the AMF/SEAF, AUSF and UDM/ARPF) [11, 85]. But the communications between the UEs or devices and the AMF/SEAF is subject to passive and active attacks [85, 88]. The vulnerabilities of the 5G-AKA and the possible attacks against it are as follows:

- According to step 6 of the 5G-AKA procedure in section 2.10, the UE or device sends the failure messages in clear text. This vulnerability can cause the "Linkability Attack". The attacker can capture the authentication request message which is sent from the SEAF to the UE (or device) and replay it after. If the UE (or device) answers with the Synchronization Failure message, the attacker determines the presence of the target UE (or device) in a particular area [88-91]. The "Linkability Attack" is the same as the replay attack in the EPS-AKA procedure which is explained in section 2.6 (the last row in table 2.1). In [92] the authors introduce the "Location Confidentiality Attack" which is against the user location confidentiality but as it is mentioned in [93]. This attack is an extension of the "Linkability Attack". The proposed solutions for addressing the mentioned vulnerability and the attacks are based on the encryption of the failure messages with the public keys of the connectivity providers (operators). But in this case

there is a need for a global PKI (Public Key Infrastructure) among all the operators which is not feasible [89]. The authors in [92] also introduce another attack called "Activity Monitoring Attacks" which is also caused by the transmission of the Synchronization Failure message in clear [90]. They claimed that an attacker can break the confidentiality of the SQN and monitor the activity of the target UE or device and learn its typical service consumption from the difference between the SQNs at two different times. But as it is mentioned in [93], the prerequisite of this attack is the compromise of the identity confidentiality and the location confidentiality of the target UE which is difficult to obtain (especially with using the SUCI instead of the SUPI).

- The pre-authentication messages such as the RRC (Radio Resource Control) messages (e.g., RRC Connection Request), the NAS messages (e.g., Attach Request) and some other messages (e.g., Paging) are transmitted in clear. All the following procedures between the UEs or devices and the network are based on these messages that may come from fake base stations or fake UEs [94, 95]. This vulnerability is also exist in the EPS-AKA procedure and can cause the same attacks in 5G (section 2.6) such as the DoS attacks against UEs or their location confidentiality. In 5G-AKA only the disclosure of the UE's permanent identity which is related to this vulnerability is addressed.

2.12 Summary

In this chapter the development of the cellular networks in the different generations is presented. By explaining the AAC models in the last three generations (3G to 5G), it is concluded that although there is a high progress in the used technologies in each generation, the AAC models remain the same since 3G. Considering the new requirements that the 5G aims to address, its AAC procedure cannot be an incremental advancement to the AAC mechanisms in the pre-5G generations. In order to show how standards are currently evolving from the AAC point of view, the details of the AAC procedure in the 4G and 5G systems are provided. By reviewing the vulnerabilities of the AAC procedures in the last two generations, it is explained that the enhancements in these procedures are only from the security point of view. The proposed AAC protocols (e.g., 5G-AKA) for 5G, only address some security

vulnerabilities of the AAC protocols in 4G (e.g., EPS-AKA) which is not enough considering the broad requirements raised in 5G.

Chapter 3 AAC Mechanisms for 5G-Specific Use Cases and Requirements

3.1 Introduction

The fifth generation of mobile cellular networks, 5G, is designed to support a set of new use cases and requirements. The purpose of addressing these use cases and the derived requirements not only involves the 5G network operators (connectivity providers) and the end users, but also brings different 3rd parties in the 5G environment. By emerging the different 3rd parties and business actors in the 5g environment, the concepts like "wholesale wireless connectivity" is gaining more and more attention. With wholesaling wireless connectivity, network operators (connectivity providers) sell connectivity to different 3rd parties which in turn provide them to their own users, in a B2B2C business model (Business to Business to Consumer). Therefore, the wholesaling of wireless connectivity appears as a key issue, especially for the IoT use-cases targeting vertical sectors that are involving end-users (e.g. connected car occupants).

The connectivity providers are trying to address these different use cases and their requirements by using network slicing architecture. The standards categorized the different use cases in 4 groups and defined 4 types of slices for each of them in the 5G specifications release 16: eMBB (Enhanced Mobile Broadband), URLLC (Ultra Reliable and Low Latency Communications), MIoT (Massive Internet of Things) and V2X (Vehicle to Everything). But these network slices only consider the different QoS requirements (e.g., bandwidth, latency and etc.) of the use cases while they have other types of requirements as well. As it is mentioned in chapter 2, the standards provide the same AAC model for the different use case although their different AAC requirements.

In this chapter we introduce the new use cases in the 5G and the derived requirements (section 3.2). The primary contributions of this chapter are:

- An analysis of the models of the proposed AAC mechanisms for cellular networks and a study of their compatibility with the derived requirements from the new use cases in section 3.3.
- An analysis of the models of the AAC mechanisms in the communication technologies used for IoT and a study of their compatibility with the derived requirements from the new use cases in section 3.4.

3.2 Use Cases and Requirements

Three typical use cases, which have been inspired from 5G Ensure Project [26], are described below for deriving the requirements to address on the end users' side, on the 3rd party organizations' side and for the 5G network operators [32].

3.2.1 Motivating Use Cases

1) Alice buys a device with cellular connectivity to stay connected everywhere (e.g., a connected vehicle). She wants to have wireless connectivity embedded inside her device. That means she does not want to have an additional subscription with a wireless carrier and the need to set up an accounting plan with that carrier.
2) Alice lives in a smart home with a smart light system, a smart energy usage control system, a smart entertainment system and a smart lock system. The IoT devices of these systems are connected to the outside world through a 5G network. The security of the data issued by the different elements of Alice's smart systems is important to her, but the leakage of some of them would cause more serious problems to her than the others' (malicious access to the smart lock system is more dangerous that malicious access to the entertainment system) [96]. On the other hand, most of her devices are constrained devices with low energy and processing power and they are not able to support strong security algorithms [1].

3) Alice works as factory manager at Acme Corporation. She wants to better automate the production of her factory. Alice subscribes to a 5G network slice, so her factory robots can access this slice through 5G connectivity. Acme only trusts itself to provide security policies, accounting and configurations data for its factory robots [83]. So Alice wants to manage the identities and credentials of the robots, as well as their life cycles (from enrolment to decommissioning). She does not want to rely on the 5G network operator for installing each new robot or for uninstalling and eliminating a robot's profile and credentials from the network.

3.2.2 Derived Requirements

As it can be inferred from the use cases, there are a number of requirements for slice-specific AAC mechanisms. R1 is derived from the motivating use case 1, R2 and R4 are derived from the motivating use case 2, R3 is derived from the motivating use case 3 and R5 is a general requirement, which is, related to all of the mentioned motivating use cases. These requirements are summarized as follows:

- R1: *Provide embedded connectivity inside devices.* Future connected devices such as connected vehicles and future things for automation and assisted living are now believed to be best retailed when connectivity is directly commercialized with the device (e.g., iPad+ cellular, Kindle readers etc.), for a better customer experience (the customer does not want to have an additional subscription with a wireless carrier and the need to set up an accounting plan with that carrier). In these cases, a connectivity provider (i.e., the 5G network operator) sells connectivity to different verticals which in turn provide them to their own users in a B2B2C business model (Business to Business to Consumer). The 3rd parties (verticals) should then be able to manage the identities and credentials of their provided devices in order to control their subscriptions and connectivity usage.
- R2: *Allow 3rd parties to choose their own AAC methods.* The security requirements in each of the use cases are distinct. In other words, the sensitivity of the signalling and data messages between the devices and the network is not the same for all types of devices (nor for all use cases). Therefore the network should have the ability to allow

the 3rd parties to choose the appropriate AAC mechanisms according to the security requirements of their proposed services.

- R3: *Allow 3rd parties to manage the lifecycles of their devices.* The fleet of devices belonging to a specific 3rd party is not static. New devices are regularly added to this fleet and old one uninstalled. The network should offer 3rd parties the ability to control the whole lifecycle from their devices, from enrolment to disenrollment processes.
- R4: *Provide AAC mechanisms for constrained devices.* The devices involved in each use case are different in terms of computational power and restricted in their energy supply. The network should give 3rd parties the ability to apply the most suitable AAC mechanisms for each type of constrained devices.
- R5: *Support for a massive number of devices.* A massive number of devices attempting to simultaneously connect to the 5G network operator's core network (by sending attachment and AAC requests) may cause congestions in the core network and bring latency. Therefore the network should be able to give the ability to the 3rd parties to manage the AAC of their provided devices to avoid the congestions in the 5G network operator's core.

3.3 AAC Proposals in Cellular Networks

Authentication and access control of UEs (devices) in cellular networks (from 2G to 4G) is based on a secure element, i.e. a SIM card: a globally unique identifier calls IMSI and a secret key shared between the UE and the network are physically provisioned on the card for each new subscription (chapter 2, section 2.3) [12]. As for 5G release 16 specifications, 3GPP decides to keep working with such a secure element in the device and with the AKA (authentication and key agreement) protocols for the UEs AAC as well (e.g., 5G-AKA protocol) [8].

Today, the use of eSIM (more precisely, eUICC) that means an embedded SIM instead of a plastic SIM card, is gaining more and more attention. Through eSIMs, users can choose which operators they would like to subscribe to. Over the air activation methods are proposed to provision the needed credentials to the eSIMs in a secure manner [97]. Although it is possible

to add embedded connectivity features to some devices through the eSIMs, identity management and connectivity usage control of these devices are still done under the responsibility of the operator and not of the device providers (3rd parties). Therefore, the 3rd parties are not able to choose their AAC mechanisms according to their security requirements and manage the lifetime of their devices (They rely on the connectivity provider in the AAC level). The AAC mechanisms in eSIMs is also based on the AKA protocols. However, AKA protocols used in cellular networks (e.g., 5G-AKA) are not fully suitable for constrained devices, as these devices may not be able to compute with the required cryptographic algorithms. Moreover, when a massive number of devices is simultaneously attaching to the network, these protocols increases the computations overhead on the operator's network side as well [19, 20].

To overcome the shortcomings of AKA protocols in the presence of massive constrained device, group-based AAC mechanisms have been proposed [98]. The general process of these mechanisms is the following one:

- to form a group of devices based on their local communication areas, applications or behaviours;
- to choose a leader device for the group based on its computational and battery capacity;
- to forward the signalling messages (authentication requests) of the group members to the network through this group leader [20, 77, 99, 100].

In [101], the devices form a group also, but they do not choose a group leader. The authentication is done between the first device who attempt to connect to the network and then continued locally with the remaining members of the group (more precisely, the remaining devices and the serving network). These group-based AAC mechanisms address the requirements of constrained devices and solve the network congestion problems caused by a massive number of authentication requests. However, as the management of joining and leaving the devices in the group is done locally in the serving network, the core network is not aware of each individual device's behaviour. It means that, although the core network provides services to each member of the groups, it is not able to control their connectivity usage and security issues [79]. For example, it is also not possible to provide different services to each member of the group (including AAC services) although their requirements would be different.

There are also some AAC mechanisms designed for preserving the privacy of the UEs (devices) when trying to connect to a service provider network, or foreign serving networks in the roaming scenarios. In [102] the authors propose an authentication procedure between the UEs and the IoT service providers, in addition to the existing 5G-AKA between the UEs and the 5G network provider. They try to protect the service data and UEs' privacy (UEs are able to anonymously ask for services) against the intermediate nodes like gNBs (i.e., 5G base station) and inhibit them to capture sensitive information about UEs. [103] and [104] also provide anonymity when the UEs visit a serving network that is different from its home network. Although these mentioned papers show that it is possible to design AAC mechanisms based on the service providers or the visited serving networks security requirements, the network does never provide the ability of choosing the AAC mechanisms in a dynamic way. They are not suitable for authenticating the massive number of constrained devices as well.

The different AAC methods proposed for cellular networks and their compatibilities with the different requirements mentioned in section 3.2.2 are summarized in the table 3.1. As we can see in this table, cellular AKA and service oriented and anonymity based methods fully meet none of the requirements; eSIM method just addresses embedded connectivity inside the device; while group-based AAC methods address the AAC requirements of the constrained devices and the mass number of devices' simultaneous connectivity request.

Table 3.1 – Different AAC mechanisms and their compatibility with the different requirements

AAC method	**R1**	**R2**	**R3**	**R4**	**R5**
Cellular AKA	-	-	-	-	-
eSIM (AKA)	+	-	-	-	-
Group based (AKA)	-	-	-	+	+
Service oriented and anonymity based (AKA + service provider's AAC)	-	+/-	-	-	-

3.4 AAC in the Other Communication Technologies

As it is mentioned in section 3.1, 3GPP defines 4 general slice types for the 5G network: eMBB, URLLC, MIoT and V2X. Among these 4 slice types and their related use cases, different communication technologies other than the cellular one are used for the MIoT in the literature. We can consider them as two categories: Long-range networks like LoRaWAN and short-rage networks like Wi-Fi. In this section we review the AAC mechanisms in these communication technologies and study their compatibilities with the 5G new requirements mentioned in section 3.2.2.

3.4.1 AAC in Wi-Fi

Wi-Fi networks are one of the most widely spread networks. The main security mechanisms that are applied to these networks are WPA (Wi-Fi Protected Access) and WPA2 [105]. The entities that participate in the users' authentication process and establish secure connections are user devices, access points (acting as AC client) and an authentication server (acting as AC server).

The WPA protocol uses IEEE 802.1x standard for users' authentication. In home or small networks, it utilizes the personal mode in which a key is pre-shared between the users and the access point – anyone who holds the key can access the network. In this mode, the access points have the responsibilities of both AC client and AC server [106]. In a business network, the WPA protocol utilizes the enterprise mode in which there is no pre-shared key between the users and access points. It uses an EAP type protocol (choosing an EAP protocol is based on the existing authentication system) with an AC server (EAP server) as a separate entity of the access point. WPA2 was introduced to replace WPA. The users' authentication process is almost the same as in WPA. It improves the level of security by adding the requirement of proving an access point's identities with the authentication server (this part is out of our paper's scope). Figure 3.1 is the general workflow of a Wi-Fi AAC system. After the devices provide their identities (user names) to the access point, they negotiate with the authentication server through the access point, about the type of EAP authentication method they want to use.

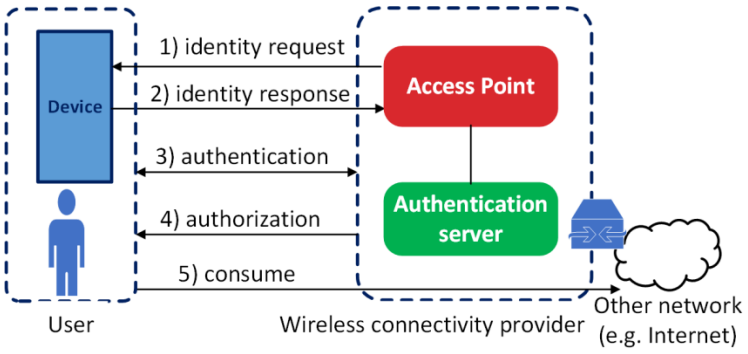


Figure 3.1– AAC model in Wi-Fi.

3.4.2 AAC in LoRaWAN

LoRaWAN networks are based on LPWA (low-power, wide-area) technologies that are suitable for transmitting low amounts of data through a wide area with low power consumption [107]. LoRaWAN network's architecture has a star topology and contains: End-Devices (sensors that are connected to the gateways to have access to the network, this connection is a single-hop LoRa connection), Gateways (forwards received data from end-devices to the network server through an IP backhaul), a Network Server (the intelligent part of the network and the center of the star topology), a Join Server (manages end-device activation and connection to the network) and an Application Server (for application-specific processing) [108].

There are two types of end-device activation processes for connecting them to the network: ABP (Activation-by-Personalization) and OTA (Over-the-Air) [108]. Therefore, there are two types of AAC in LoRaWAN. In the OTA activation process, the end-devices should introduce themselves to the network to obtain the necessary information to establish secure connections with the network (e.g. the session key between the end-device and the application server to encrypt the application-specific data messages). Each end-device in this process should have two unique identifiers and an AppKey, a shared secret key between the end-device and the joint server that controls the end-device. The AppKey is never sent to the other servers and is used to derive the further session keys with which to encrypt the communications and data [109]. As for identifiers, one of them, the DevEUI identifies the end-device (like a MAC address of a TCP/IP device) and the other, the JoinEUI (known as the AppEUI in the previous specifications of LoRa), identifies the join server that the end-device should refer to (the service provider of

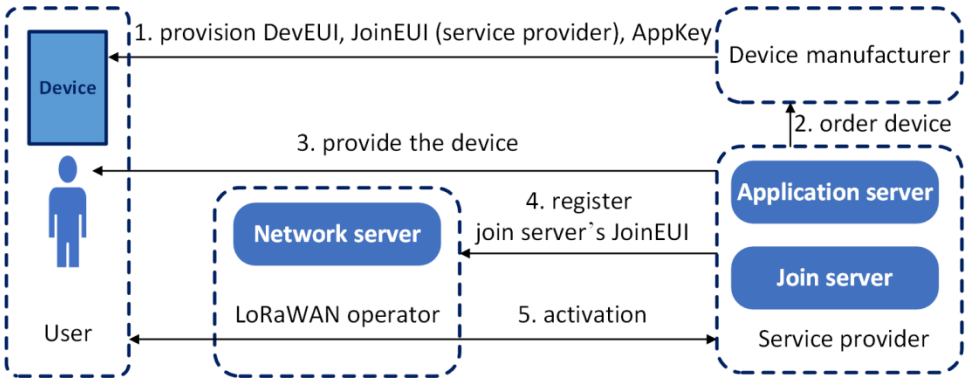
the device). An end-device should have an address, DevAddr that identifies it in the current network. The join server should contain the devices' AppKey and DevEUI.

There are two scenarios for provisioning the identities in an end-device. In the first, the device manufacturer allocates the DevEUI and the AppKey to the end-device and sets the value of the JoinEUI to the service provider's join server identifier. In this scenario, the end-device belongs to the service provider but it can work in different networks in different countries because the service provider can register its join server identifier (JoinEUI) in different network operators (figure 3.2.a). In the second scenario, as with the first, the device manufacturer allocates the DevEUI and the AppKey to the end-device but the device's JoinEUI is set to the identifier of a join server belonging to a trusted third party (and which knows the end-device's DevEUIs and its AppKeys). Therefore, the end-device can work with any service provider in the various networks (figure 3.2.b). In this scenario, end users buy these end-devices from any retail channel (they do not get the end-devices from the service providers).

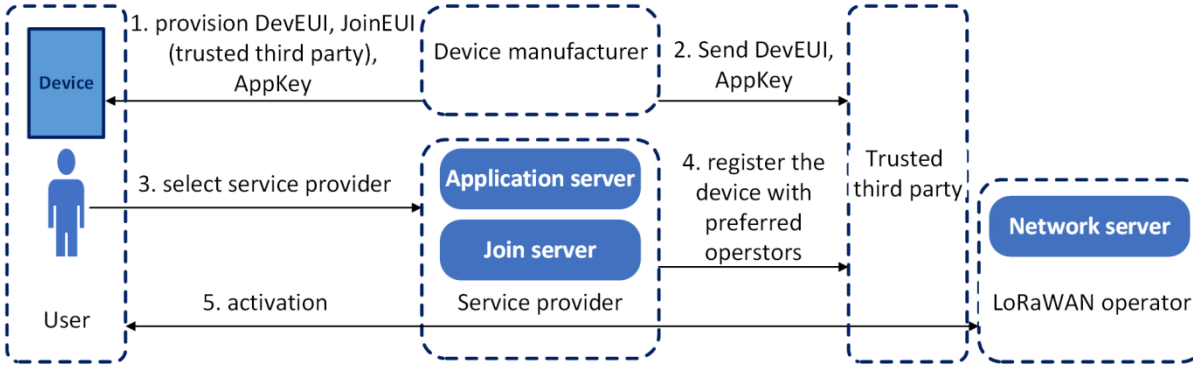
In the ABP activation process, unlike the OTA activation process, the join server plays no role. Devices are personalized to work with a specific LoRaWAN network. All the necessary information and session keys required to establish a secure connection between the end-device and the network have already been configured in the end-device, the network server and the application server (figure 3.3). Therefore there is no need for remote authentication and access control and the end-device can exchange data with the network immediately.

3.4.3 Comparison of AAC Models in Wi-Fi and LoRaWAN

The AAC model in Wi-Fi networks is relatively simple, and appears to not be very helpful for elaborating the mentioned requirements in section 3.2.2. There is no contract (free or per user) and the authorization may be unrelated to the authentication. It does not fit to wholesale connectivity concept as well. As there is no AAC method with high computational overhead in Wi-Fi, it is suitable for constrained devices. But the AAC model do not compatible with the remaining requirements mentioned in section 3.2.2.



a –scenario 1 in the OTA activation process. The device belongs to a specific service provider.



b –scenario 2 in the OTA activation process. The device does not belong to a specific service provider and a user can buy it from any retail channel.

Figure 3.2– AAC model in LoRaWAN

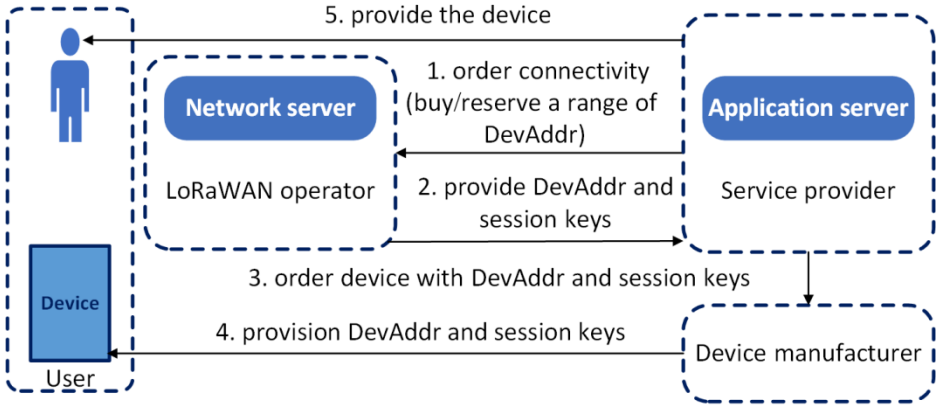


Figure 3.3– LoRaWAN AAC model with the ABP activation process.

The AAC system in LoRaWAN however, it does allow for several business models quite distinct from the retailing of cellular network subscriptions to end-users. As noted in section 3.4.2, by providing different possibilities to allocate the necessary information such as identities and keys to the end-devices, LoRaWAN could have different scenarios for the different actors' connections.

In the OTA activation process, the end-devices work with a specific application provider on any network or they work with any (compatible) application provider on any network (through the mediation of an undefined Trusted Third Party player at device activation time). LoRaWAN does not give a central role to network based AAC systems. Instead the main players regarding authentication and authorization are recognized by the system architecture to be the device manufacturers and the application providers: in all the business cases considered the network provider is involved in the commissioning process, either by the application provider or by a yet-undefined trusted third party player (Considering the potential ecosystem evolutions where multiple Trusted Third Parties might attempt to take a central position in device activation and where the number of application provider and device provider could explode, this is probably a weak point of the LoraWAN architecture.). Moreover, endpoint/application keys are learned by the network provider the usage phase (i.e. involving an "ordering" process in the information systems similar to traditional SDM based systems) only in the ABP activated end-devices case. Otherwise, the network (i.e. the network server, not a subscription management system) learns about endpoint/application at first use-time i.e. during over-the-air activation. Considering the requirements in section 3.2.2, the AAC model in LoRaWAN is compatible with R3, R4 and R5 requirements. Table 3.2 depicts the compatibilities of the AAC models used in the Wi-Fi and the LoRaWAN communication technologies.

3.5 Summary

In the multi actor environment of 5G, the purpose is to cover a broad range of use cases. In this chapter the new use cases raised in 5G and the associated requirements are introduced. A survey on the different AAC mechanisms and models proposed for the cellular, Wi-Fi and

Table 3.2 – AAC models in Wi-Fi and LoRaWAN and their compatibility with the different requirements

AAC method	R1	R2	R3	R4	R5
AAC in Wi-Fi	-	-	+	-	-
AAC in LoRaWAN	-	-	+	+	+

LoRaWAN communication technologies in the literature shows that none of them is compatible with all of the derived requirements. It can be concluded that giving the central role to the connectivity provider in the AAC model disables the network to address all the requirements in the different use cases. Assigning specific network slice to the 3rd parties and giving just an intermediate player role to them for obtaining connectivity orders from the users is not enough for addressing the mentioned requirements. The AAC model in scenario can be an AAC model depicted in figure 3.4. Such an evolution (deforming the current AAC systems) is however questionable. It would generate redundancies at the intermediate player and at the wholesale connectivity provider (5G network operator), because each must manage end-users/subscribers in their own information systems; while the wholesale connectivity provider would have no business incentive to do so (the wholesale connectivity provider is selling to the intermediate player, not to individual subscribers). Furthermore both the intermediate player and the connectivity provider have to authenticate the end-users/subscribers at their own level. The intermediate player could use any means relevant to its own business while the connectivity provider would be restricted to authenticating an UICC and its assumed ownership by the end-user/subscriber that it does not directly know. These redundancies could generate extra costs and a lack of agility.

On the other hand, it is expected that, the next generation of mobile networks, 5G, will support heterogeneous and non-3GPP networks accesses like LoRaWAN and Wi-Fi. By these non-3GPP networks accesses, devices are not always equipped with an UICC and the connectivity provider doesn't always have a-priori knowledge (i.e. pre-provisioned in its information system) about the person/organization responsible for the network consumption

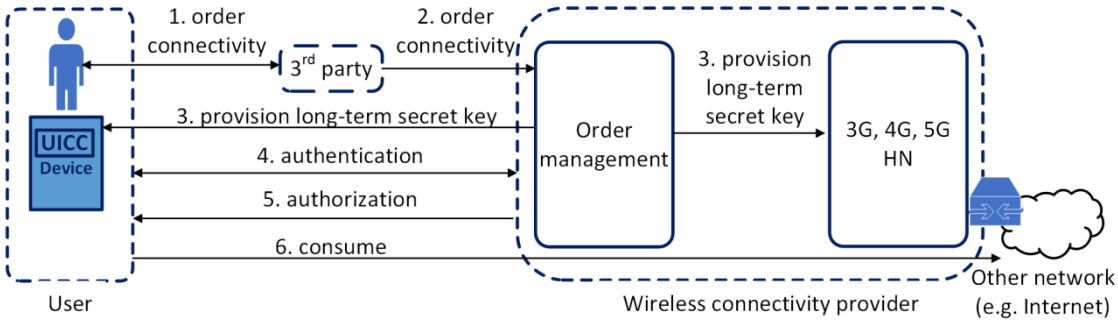


Figure 3.4– Deformation of current mobile network AAC model for addressing the requirements.

of a given device. The connectivity provider still needs to provide ciphering and/or integrity protection keys to the device but this is done when the device is about to use a given network (e.g. activated) and without relying on long-term secret keys stored in the UICC and pre-provisioned in the information system. As 5G's core network will have to cope with heterogeneous access types, devices and business-cases, one cannot assume that a UICC-SDM based system is the panacea. Therefore, the best way to address all the different requirements in the use cases is not only assigning specific network slices to the 3rd parties but also to delegate them the AAC responsibilities of the their provided devices and release the connectivity provider from this responsibility. The details of this proposal are explained is chapters 4 and 5.

Chapter 4 Slice Specific Authentication and Access Control

4.1 Introduction

Virtualization technologies are being progressively incorporated into cellular network architectures, as a mean to offer cost effective and flexible infrastructures and to provide services in a dynamic manner [1]. Classically, the design of cellular networks strongly distinguishes between the access network and core network. That means there is a clear border between the RAN and the CN. The main functions of the RAN are first to assign the radio resources to the UEs or devices; and second to forward signalling and data messages between devices and the CN, with all service level procedures such as AAC being performed in the CN. However, virtualization technologies make these borders more blurred. With these technologies it is possible to execute network functions in the best suitable location (e. g. executing some CN functions in a proximity data centre or some RAN functions in a central data centre) [110-112]. Choosing the location of each function might then be done according to technical (ex., low-latency requirements) and business criteria (hosting costs in a proximity datacentre are higher than in a centralized datacentre).

Virtualization technologies are also enabling a greater openness of 5G network to 3rd parties (i.e., any business actor that is not the network operator), with the concept of network slicing. Each network slice addresses a specific set of quality of service parameters (throughput, latency, etc.) and could be dedicated to a 3rd party according to its requirements [2, 113]. It might therefore be considered by the 3rd party as a virtually dedicated network. Although network slices can be designed by enabling or disabling certain network functions (according to 3rd parties' requirements), the functions of the 5G radio access network and the interfaces between the radio access network and the core network are common for all network slices.

Some network functions, like authentication and user access control, are done outside the network slices; these are the same for all of the network slices despite the different specifications of these slices [10, 11]. This means that, in 5G, the authentication and access control of the users is done before the slice selection phase, which is then performed based on this common authentication phase.

However despite the introduction of such virtualization techniques, cellular network architectures should still be considered as monolithic: the different parts of the network remain strongly coupled and dependent to each other. The network slicing concept is adding here flexibility, but still remains in the same architectural logic as the physical networks, with tightly coupled network components; there is no customization at the network level of the provided services [7].

In this context, this work provides a new approach called 5G-SSAAC (5G Slice-Specific Authentication and Access Control) as an initial step to have a more loosely coupled network architecture. Focusing on the AAC, this approach intends to maximize the decoupling between the RAN and the CN, by delegating the AAC of the devices for a specific network slice to the 3rd party that uses this slice (in this case, the 3rd party is responsible to manage the identities of its devices). This allows 3rd parties to choose their own AAC method according to their security requirements. In other words, the AAC is done inside the 3rd party's slice and not outside of it. Using this approach, the 5G network will have the required flexibility to support various AAC mechanisms for the different 3rd parties, alongside the AKA-based AAC mechanisms. The possibility of delegating users' AAC mechanisms to the 3rd parties is an interesting tool for enabling the wholesaling of wireless connectivity for the network operators as well.

This chapter introduces a new way of AAC for the 5G. The contributions are:

- A definition of three new network functions for the 5G RAN in order to delegate the AAC of devices to the 3rd parties providing these devices in section 4.2.
- A detailed call flow of the attachment process of the devices to the network and their AAC with the 5G-SSAAC approach in section 4.4.

4.2 Network Functions for 5G-SSAAC

While the current cellular RAN is mainly intended for forwarding signalling and data messages between the core network and the UEs (devices) and providing them the radio resources, we propose here to design a new RAN function that is able to host an AAC function from a 3rd party. The main challenge is to intercept the dependencies between the RAN and the core network in terms of the AAC of the devices and route the AAC requests to the corresponding 3rd party network (network slice).

More precisely, to enable the RAN for hosting different AAC functions of the different 3rd parties or routing the attachment requests of the devices to the right AAC functions, we introduce three network functions (three main network functions, each of them is a set of sub functions) in the RAN to enable a more loosely coupled architecture. One of them is developed and provided under the 3rd party's responsibility and the other two are under the responsibility of the MNO. These functions are in the form of a software code executable in the proximity datacentre located at the level of the 5G base station (gNB). By using these functions, the access network can register 3rd parties' slices and connect each UE to the adequate 3rd party's slice. These three network functions are explained in the following sub sections and they are called during the execution of the gNB's main code (section 5.4.4).

4.2.1 3GW, 3rd party provided GateWay virtual function

In 5G-SSAAC approach, first, we consider a dedicated AAC function for each 3rd party's network slice, then we enable the RAN to communicate with that AAC function for the AAC processes of the devices provided by that slice. The AAC function of each 3rd party's network slice is called 3GW function (3rd party provided GateWay virtual function). It is under the responsibility of the 3rd party and the 3rd party may design this function according to its own security requirements (it could be a simple password based authentication mechanism or a complex authentication mechanism with post-quantum cryptography TLS). The 3rd party may also decide to design this function as a simple routing function to its slice and in this case, there is an AAC function inside the 3rd party's network that manages the AAC of the 3rd party's devices.

The 3GW function is dedicated to a specific 3rd party's network slice and its software code may differ from the software code of the other 3GW functions belonging to the other 3rd party network slices. In this case, as it will be mentioned further in chapter 5, section 5.5, a software attack against one 3GW function will not be efficient for the other 3GW functions. There is also no AAC function (e.g., AMF and AUSF in the current 5G architecture) as a single point of failure in the system (detailed explanations are provided in section 5.5).

4.2.2 GRF, Gateway Function Repository

In order to introduce different 3GW functions to the 5G-RAN, and enable the 5G-RAN to communicate with these functions, another network function is needed to store the information of the 3rd partys' 3GW functions. This function is called GFR ((Gateway Function Repository) is under the responsibility of the MNO. A 3rd party has to first registers the code of its 3GW function through this GFR function (the details of this registration is explained further in sections 5.4.1 and 5.4.2). After this registration, the GFR keeps the information of the 3GW. The modality of this information depends on the convention between the MNO (connectivity provider) and 3rd party and on the execution infrastructure (e. g. NFV-MANO [114]).

4.2.3 RCP, RRC Connection endPoint

RCP (RRC Connection endPoint) is the termination point of the signaling messages with the devices on the MNO's side. This function is the main part of the 5G-SSAAC approach. The RCP function gets the attachment requests from the devices first, and then according to the information it obtains from the GFR function, it routs the requests to the right 3GW function. In addition to the functionalities of the 5G-RAN, it consists of three sub functions as follows:

- RCP1 function: The RCP1 function gets the message from the device and according to the information in this message (slice ID), it selects the right 3GW function. As it is mentioned in chapter 1, the attachment of the mobile broadband devices to network remains the same as it is in the current 5G architecture. If the RCP1 function gets an attachment request from a mobile broadband device, it routs the request to the 5G core network.

- RCP2: The RCP2 function waits for the response from the 3rd party's 3GW function or the 5G core network. It creates appropriate structures for the further steps according to the obtained response. In order to have the ability to support different AAC mechanisms, the RCP2 function has to create different structure types according to requirements of the 3rd party's AAC mechanism. If the RCP2 function receives a response from the 5G core network, it creates an structure with the fields corresponding to the secret key and the security algorithms related to the AAC mechanism in 5G (e.g., 5G-AKA). If it receives a response from a 3GW function, it creates a structure with the fields related to the information it gets from the 3GW function.
- RCP3: The RCP3 function calls the appropriate security functions according to the fields of the structure, which is created by the RCP2 function. It is responsible for securing the connection between the gNB and the device.

Indeed, the RCP acts as an anchor point between the 5G network operator domain and the 3rd party domain. It is an API through which the different types of AAC mechanisms can be interfaced with the OAI-RAN.

4.3 5G-SSAAC General view

In the proposed 5G-SSAAC approach, the needed information for AAC of the devices (which are not MMB UEs) is provisioned by the 3rd party before providing the devices to the end users. This information contains the 3rd party's Slice ID (slice identifier, corresponding to the slice subscribed by the 3rd party to the MNO) and the devices identifiers which identify each device in the 3rd party's slice. These identifiers may differ from the globally unique identifier that is used in the current cellular systems context and in 3GPP specifications for 5G (IMSI for 4G and SUPI for 5G). The provisioned information to the devices may also contain some security credentials as well, according to the AAC mechanism that is chosen by the 3rd party. The 3rd party decides the format of the subscription identifiers, and these identifiers do not have to be 5G-specific.

Figure 4.1 is a detailed view of the slice selection phase of our proposal (the first step of figure 1.2 in chapter 1). This figure shows the execution order of the proposed network

functions by the 5G RAN. We assume that the registration of the 3GW in the RAN and the storage of its address in the GFR are already completed. As the first step the devices send their identities and the identifier of the slice (Slice ID) they want to attach, in the "Attach Req" message to the RAN (step 1). Upon receiving the "Attach Req" message from the devices, the RCP function sends the slice information request message (2. Slice Info Req) to the GFR by mentioning the Slice ID. The GFR finds the slice information related to this Slice ID and sends this information to the RCP through the slice information response message (3. Slice Info Res). After receiving the "Slice Info Res" message, the RCP has the needed information to establish the connection with the 3GW. Therefore, it routes the device's attachment request to the 3GW through the "Attach Req Reroute" message (4. Attach Req Reroute). We provide the details of each operation in section 2.4. At the end of this stage, the slice connection is established between the device and the 3GW and the AAC can be done between the device and the 3rd party slice. For example, if the 3rd party is an automated factory with a pre-existing AAC infrastructure and database for its devices, it is able to use the mentioned slice connection for authenticating its devices and controlling their access to its network without depending on the connectivity provider.

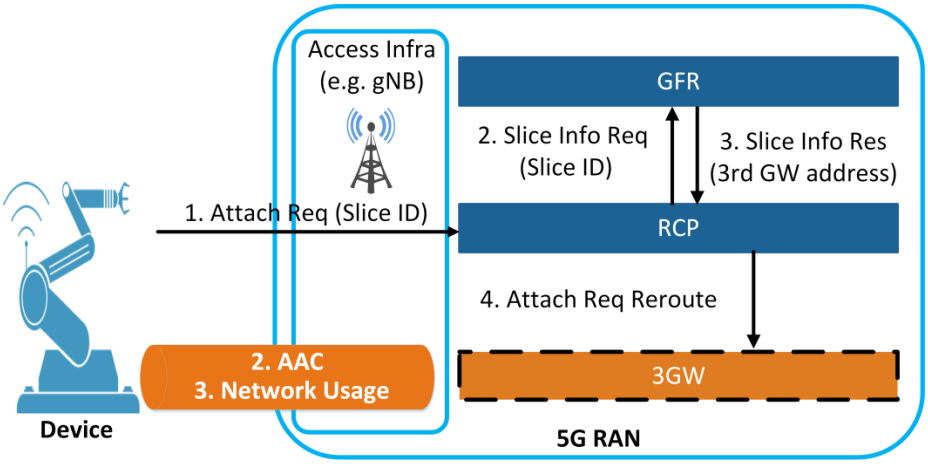


Figure 4.1– A detailed view of the slice selection phase in the proposed 5G-SSAAC.

4.4 5G-SSAAC Call Flow

Here, the detailed call flow of the proposed SSAAC procedure is explained, from the 3rd party's slice registration phase to the slice connectivity establishment phase. Without losing the generality of the work, the focus is on the first attachment procedure of the device in the network. Figure 4.2, presents this call flow, which contains four main phases and their associated sub-phases:

1. 3rd Party's slice registration and devices' information provisioning: In this phase and before starting the attachment procedure of the devices in the network, the 3rd party designs its 3GW function and registers it in a 5G network operator (MNO). The 5G network operator saves the information of this 3GW (e. g. the 3GW function's address) in the GFR of its RAN. This registration ensures that the gNB is configured with the 3rd party slice's information. The 3rd party also has to provision the information required to AAC of its devices' (the Slice ID and the device's subscription identifiers) in them.
2. Radio Link Synchronization: During this procedure, the devices get the necessary information for establishing radio connections with the gNB. The Radio Link Synchronization procedure is out of the scope of this paper (see the Random Access procedure in [115]).
3. Slice Connection Establishment: This phase contains three sub-phases according to the figure 4.2:
   3.1. RRC Connection Establishment: To establisha connection between the device and the corresponding network slice, we need to establish one connection between the device and gNB (RAN) that calls RRC Connection, and another connection between the RCP and the 3GW (the RCP acts as an interface between the 3rd party's slices and the associated devices). The RRC Connection establishment procedure consists of two steps, the same as the RRC connection establishment procedure in LTE (i.e., 4G) [115]. The device sends an RRC Connection Request to the RAN. The 5G RAN part of the RCP gets this message and sends the RRC Connection Setup message to the device, establishing the RRC Connection

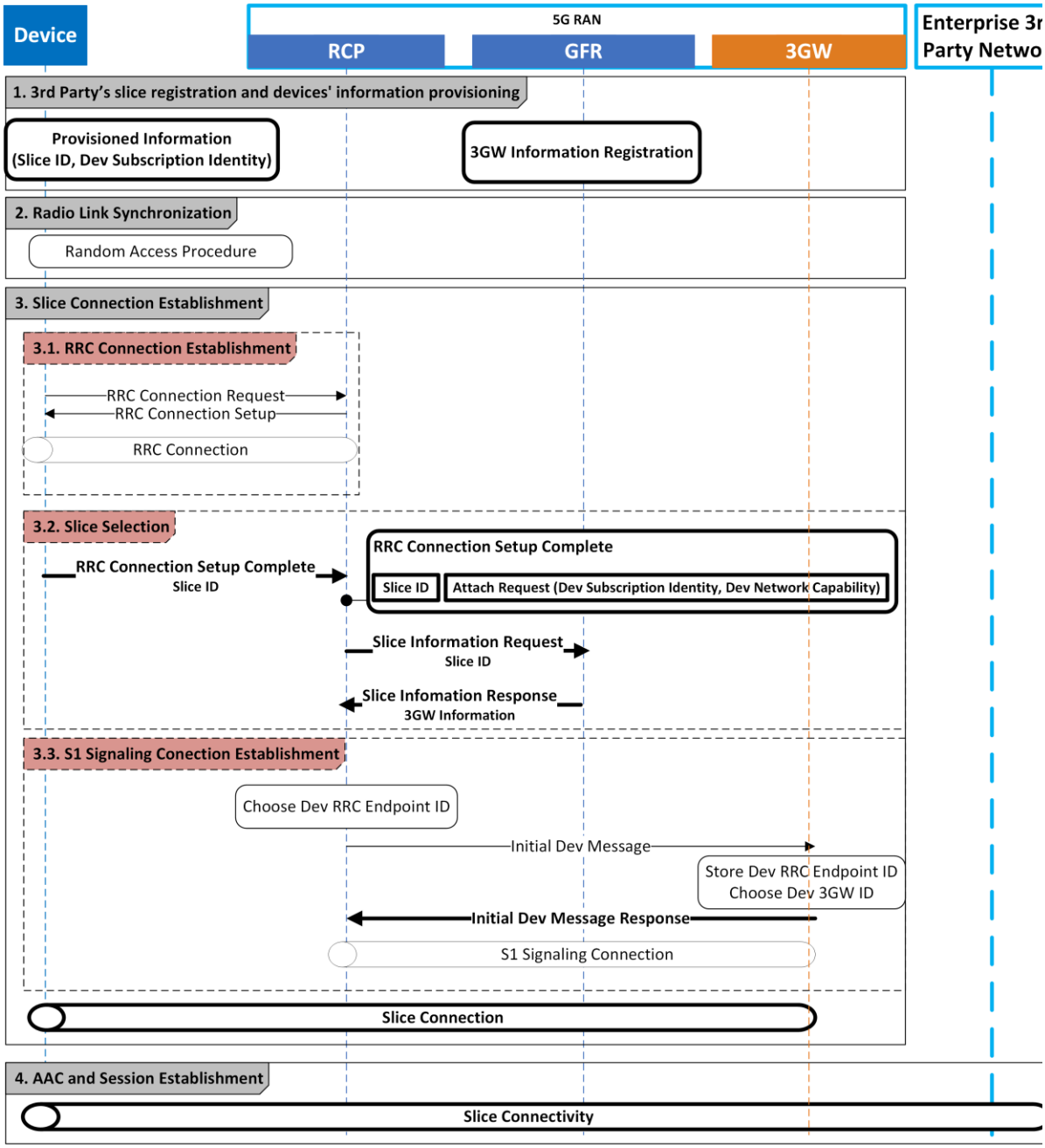


Figure 4.2– The detailed call flow of the proposed 5G-SSAAC. The entities in bold, represent the new parts that are added to the current 4G call flow.

between the device and the RCP. After these two steps, the device can use the radio resources allocated through the RRC Connection Setup message.

3.2. Slice Selection: The RRC Connection Setup Complete message is sent from the device to the RAN. This message contains the Attach Request. The Attach Request consists of the device's subscription identity and the device's network capabilities

(the device's network capabilities' content depends on the security requirements of the 3rd party slice. In LTE, these capabilities consist of the device's algorithms for the 4G AAC procedures). The RRC Connection Setup Complete message also includes the slice's ID. The device informs the RAN about the slice that it wants to connect to by using this ID (In LTE, the device sends the PLMN ID in the RRC Connection Setup message during the first attachment to the network, and in 5G, as mentioned in [115], the device sends the NSSAI in this message). Upon receiving the RRC Connection Setup message from the device, the RCP gets the 3GW information from the GFR to then forward the device's attach request to the right slice. It obtains this information by sending the Slice Information Request message to the 3GW, specifying the Slice ID (the RCP extracts the Slice ID from the attach request embedded in the RRC Connection Setup Complete message). The GFR sends the slice information related to this Slice ID to the RCP through the Slice Information Response message. The RCP is now able to establish a connection with the 3GW Function. This connection is called an S1 Signalling Connection. If the RCP does not find its intended 3GW information from the GFR, it releases all the connections related to that device (the RRC Connection and theS1 Signalling Connection).

3.3. S1 Signalling Connection Establishment: For each device that belongs to the 3rd party's slice, there is one S1 Signalling Connection dedicated to that device. These connections must have an identifier for each of their endpoints. Therefore, the RCP chooses an identifier for this connection on its side (the Dev RRC Endpoint ID) and sends it to the 3GW in the Initial Dev Message. The Initial Dev Message also contains the Attach request. After receiving this message, the 3GW chooses an identifier for the S1 Signalling Connection on its side (Dev 3GW' ID) and informs the RCP about this identifier by sending the Initial Dev Message Response to the RRC Connection End Point. This completes the Slice Connection Establishment procedure and the device is connected to the 3rd party's slice.

4. AAC and Session Establishment: All the AAC processes of the device in the network and the session establishment for providing network services to the device are done inside the corresponding 3rd party's slice. The 3rd party organization selects which

AAC mechanism to use according to its own security requirements and the security requirements of its subscribers and informs the RCP about the selected AAC mechanism (through the "Initial Dev Message Response" messaged in the previous step). If the AAC of the device in the 3rd party's slice is not successful, the 3GW informs the RCP by sending it an authentication failure message. Upon receiving the authentication failure message from the 3GW, the RCP releases all the connections related to that device.

4.5 Summary

In this chapter, an original slice specific AAC approach is proposed by designing a new kind of RAN for 5G mobile networks. Taking advantage of virtualization technologies, three virtual network functions (in addition to their sub functions) are defined in 5G RAN in order to enable the delegation of the AAC of the devices to the 3rd parties who provide these devices. To do so, a connection between the device and the corresponding 3rd party slice is stablished before the device's AAC procedure. Therefore, managing the AAC of these devices may be fully under the responsibility of 3rd parties. Via these network functions, it is possible to have different AAC mechanisms in 5G according to the 3rd parties and their provided devices' security requirements as well as to keep the previous AAC mechanisms for mobile broadband UEs (e.g. 5G-AK). The details of the defined network function and their implementations are explained in chapter 5.

5G-SSAAC can be seen as a first step towards a more loosely-coupled design for 5G network architecture. It enables the connectivity providers to address the new requirements brought by the wholesales connectivity concept. This approach also offers embedded connectivity to the 3rd parties' customers inside their produced devices.

Chapter 5 Evaluations

5.1 Introduction

Different ways and mechanisms for authenticating the users and devices and controlling their accesses to the network have different impacts on the security aspects of the network. In the multi-actor environment of 5G, 5G-SSAAC mechanism gives this opportunity to the 3rd parties to have their own AAC mechanism for their provided devices. On the one hand, the security of the 3rd parties' network (slice) and their provided devices depends on the AAC mechanisms that they choose according to their requirements. On the other hand it depends on the security of the whole 5G system. Therefore the security analysis of the 5G-SSAAC and the study of its impacts on the whole 5G systems is necessary.

Different AAC mechanisms also affect the load on the network (e.g., the signalling and the traffic loads). Considering the increasing number of devices that demand connectivity (e.g., IoT devices), analysing this load become even more important to prevent the network from disruption. Different approaches are proposed to manage the AAC of this massive number of devices like the group-based authentication schemas for the IoT devices. The shortcomings of these mechanisms are discussed in chapter 3 section 3.3. Unlike the group-based AAC mechanism, with 5G-SSAAC each device is authenticated separately through its corresponding 3rd party network slice that protects the network and the devices against potential threats. It is also possible to manage the requirements of each device separately and do not limit their services to the common requirements of the group. As it is mentioned in chapter 1, it is important to note that the 5G-SSAAC approach is suitable for the use cases with the presence of massive number of IoT devices. For the mobile broadband devices, the attachment and AAC procedures remain the same as the current procedures in 5G.

In this chapter, we focus on the implementation of the proposed approach and studying its impacts on the 5G network from the security and signalling load points of view. The primary contributions of this chapter are:

- Assessing the feasibility of the defined network functions in 5G-SSAAC mechanism and evaluating their impact on existing RAN by implementing a fully virtualized mobile network through a testbed based on the OAI (Open Air Interface) open-source product.
- Analysing the security aspects of the proposed approach in comparison with the AKA-based AAC mechanisms and emphasising the necessary arrangements in the network in order to have a secure system while using the 5G-SSAAC.
- Describing and assessing the signalling flows in 5G-SSAAC and the AAC mechanisms used in 4G and 5G networks that have an impact on the network signalling load by focusing on the attachment and authentication signalling.

5.2 Related Works

This section briefly reviews the related literature. It focuses on the works that model the CN load for different purposes and on efforts to analyse the signalling performance of different AAC mechanisms. The purpose of this section is to depict the different ways that are used in the literature for assessing the load of the network and explain the reason of choosing the signalling cost as the evaluation criteria in this work.

5.2.1 CN Load Modelling

There are several proposals that address the modeling and calculating of the CN load in different manners and for different purposes.

M. M. Rahman and S. S. Heydari [116] model the number of messages generated at the MME to recover failed sessions in order to evaluate the performance of the self-healing schemes for the failed elements in the CN. J. Prados et al [117], model the control plane traffic of the CN as a G/G/m queue and then calculate the response time of the CN entities in order to

resource dimensioning for providing network slice planning. In [118] the authors focus on the MME load and model it with a queuing network. They also estimate the overall system delay considering the different traffic models. A. S. Rajan et al [119] consider the MME capacity as the number of NAS messages (from the devices that want to have connectivity) it can handle in one second and model the CN as a D/D/K queue. Their purpose is to quantify the performance bottlenecks in virtualizing the CN. In [120] G. Foddis et al consider the network load or overhead as the number of bytes that are needed or transmitted through the CN to complete the intended procedures. The objective is to balance the devices' energy consumption and the network overhead. I. Widjaja et al [121] analyze the MME signaling load by counting the number of input and output signaling messages that belong to different procedures. They compare the MME signaling load in different CN architectures (centralized or distributed MME) and in the different paging scenarios. While all of these works propose theoretical models for evaluating the CN load in the different scenarios, we validate the 5G-SSAAC through the implementation of a fully virtualized mobile network. Therefore, all the evaluations can be done in a real environment. The focus of the evaluations is on the AAC signaling load on the network.

5.2.2 AAC Signalling Performance Analysing

There are some works that provide new AAC mechanisms for cellular networks. In [14], J. Cao et al design a lightweight group-based AAC scheme for a massive number of devices in 5G systems. They analyze the performance of their proposal considering the authentication signaling cost on the CN, the authentication bandwidth consumption, the authentication transmission cost, and the authentication computational cost. They compare their proposed approach's performance with the performance of the existing AAC mechanisms for cellular networks (e.g. EPS-AKA). The authors in [122-124], propose group-based AAC mechanisms for cellular systems and analyze their proposal in terms of signaling cost, bandwidth consumption, computation cost, and storage overhead. In [125], Y.L. Huang, proposes an AAC mechanism for UMTS and evaluates the proposal considering the signaling cost, and the bandwidth consumption. We refer to these works in calculating the AAC signaling load on the network.

5.3 Testbed

In order to evaluate the feasibility of the 5G-SSAAC mechanism and assess its impact on the RAN, we studied its possible implementation with OAI (Open Air Interface). OAI is open source software that implements cellular network functions of the RAN (OAI-RAN) and the core (OAI-CN). These functions are executable on general purpose processors (such as x86 and ARM). We demonstrate our proposal in this 4G environment due to unavailability of 5G devices and networks. But it will be feasible to demonstrate it in a 5G environment soon because of the fast open source developments for 5G.

Figure 5.1 shows a schematic view of our testbed and the protocol stacks of the control plane and the user plane. The RAN part of the proposed solution is implemented based on the OAI-RAN code. The 3rd parties' slices (enterprise 3rd party networks) are launched based on the OAI-CN code, but it is also possible to define new network functions in these slices according to the 3rd parties' requirements. In OAI, the 4G terms are used, like eNB. But, as we target 5G, we will use the term gNB instead.

Our main purpose is focused on the RAN and on adding the proposed network functions to it. To build the radio access part (the base station), the OAI-RAN (master branch release v1.1.0) was executed on a PC with an Intel Xeon W-2102 quad-core at 2.9 GHz, 16 GB memory; USB3 and Gigabit Eth. We use a USRP B210 board for radio communications. This SDR (software defined radio) supports 2*2 MIMO (multiple-input and multiple-output) and connects to the PC through the USB3 interface. The operating system is a 64-bit Ubuntu 16.04 with a low latency kernel. To support the network slices, the OAI-CN was installed on Ubuntu 16.04 virtual machines (with kernel 4.7). We used Samsung Galaxy S4 and programmable sim cards, sysmocom for the device. We programmed them using a Gemalto IDBridge K30 as card reader/programmer hardware.

The OAI-RAN source tree consists of five main parts: Openair1, Openair2, Openair 3, Targets and Common. Openair 1 is the physical layer implementation of the RAN. Openair 2 is the implementation of the MAC, RLC, PDCP and RRC layers of the control plane and the data plane of the RAN. Openair 3 is the implementation of the UDP, GTP, SCTP, S1AP and

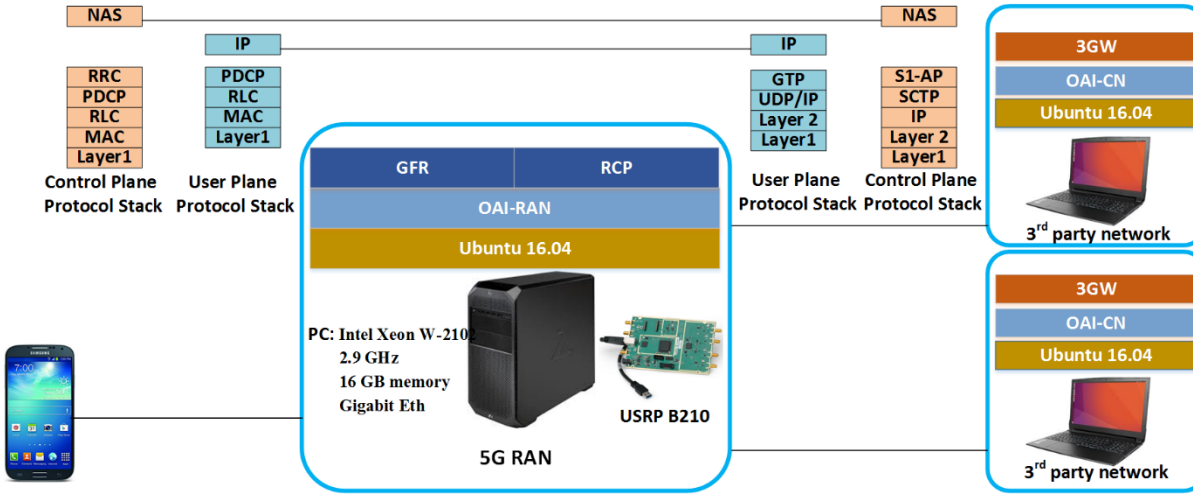


Figure 5.1– Schematic view of the testbed. The GFR and RCP functions are implemented on the OAI-RAN.

NAS layers of the control plane and the data plane of the RAN. The hardware specific codes (drivers, tool, etc) and the main function of the OAI-RAN is in the Targets. The Common is dedicated to the common services. The OAI-RAN handles the execution of its processes though multiple threads related to different tasks (e.g. SCTP task, S1AP task, etc.). The management of these threads is done through a middleware called itti (interthread interface) and the connections between the threads are done through different types of itti messages. The different functions are designed in OAI-RAN for handling these messages such as itti_receive_msg for receiving a message from a task.

As the AAC procedure is one of the control plane procedures and it is mainly related to the RRC, S1AP and NAS layers, the modifications were done in the RRC, S1AP and the NAS layers of the control plane protocol stack to implement our proposal. Table 5.1 is a summary of the modified network functions of the OAI-RAN related to the different phases of the proposed 5G-SSAAC mechanism's call flow introduced in chapter 4 (section 4.4 and figure 4.2). The second phase of the attachment process in the proposed 5G-SSAAC mechanism's call flow (Radio Link Synchronization) does not require any changes. As depicted in the last row of the table, 6 OAI functions from 5 different OAI-RAN files, representing 650 lines of code are impacted, which shows the limited impact of such modifications.

Table 5.1 – The OAI-RAN files and functions that are affected by applying the 5G-SSAAC. The first column "P" represents the phase number in the 5G-SSAAC and the fourth column "N" represents the number of lines of code per function. The last row represents the total number of OAI-RAN files, the functions and the number of lines of code that are modified. T means the total of previous items.

P	OAI-RAN file	OAI-RAN function	N
1	Openair 3/S1AP/s1ap_eNB.c	s1ap_eNB_register_MME	82
	Openair 2/ENB_AP/enb_app.c	RCconfig_S1	70
2			
3	Openair3/S1AP/s1ap_eNB_nas_procedures.c	s1ap_eNB_handle_nas_first_req	100
	Openair3/S1AP/s1ap_eNB_handlers.c	s1ap_eNB_handle_initial_context_request	150
	Openair2/RRC/LITE/rrc_eNB_S1AP.c	rrc_eNB_send_S1AP_NAS_FIRST_REQ	117
4	Openair2/RRC/LITE/rrc_eNB_S1AP.c	rrc_eNB_process_S1AP_INITIAL_CONTEXT_SETUP_REQ	131
T	5	6	650

5.4 Implementations

As it is explained in chapter 4, the 5G-SSAAC introduces three main virtual network functions for 5G RAN: the 3GW function which contains the AAC mechanism of the 3rd party and is under responsibility of the 3rd party, the GFR function which contains the 3rd party's 3GW function's registration information, and the RCP function which is the termination point of the signalling messages and gives the ability to the RAN to support different AAC mechanisms. Our implementations consist of two main parts: the implementation of the GFR function and the implementation of the RCP function as these two functions are under the responsibility of the connectivity provider (mobile network operator). In this section, first we describe the configuration of the gNB and the device. Then, we explain the detailed implementations of the proposed network functions as well as the execution of the gNB's main function.

We launched two OAI-CNs on two systems as two network slices and considered the MME functions of these two OAI-CNs as the 3GW functions of the assumed network slices. In this assumption, the 3rd party slice carries the full features of a cellular core network but the 3rd party enterprise can customize the different network functions, including the MME network function, according to its specific requirements. We also considered the PLMN IDs of these cores as the Slice IDs of the corresponding slices. Since we used a commercial UE with a sim card as our device, we have assumed the IMSI of the sim card as the Dev Subscription Identity

of the device, but the Dev Subscription Identity can be different if another type of device is used.

5.4.1 RAN gNB and Device Configuration

The OAI-RAN, uses a configuration file to configure the gNB. This configuration file consists of several parameters including the parameters required to set up the physical channels, the PLMN list that stores the PLMN IDs which the gNB belongs to, the MME IP addresses the gNB can connect to and the network interface information related to the gNB. By adding several PLMN IDs (Slice Ids) and the MME IP addresses (3GW IP addresses) to the gNB configuration file, the gNB is able to connect to multiple MMEs (multiple core networks). This mechanism that enables multiple core networks to share the same RAN is called S1-flex. One of the purposes of the S1-flex technology is to provide load sharing between MMEs.

Figure 5.2 is a part of the configuration file that we have changed according to our setting. We have added the PLMD IDs (Slice Ids) of our two OAI-CNs (two network slices) and the MME IP addresses (3GW IP address) of these two cores to the configuration file. This configuration is the prerequisite of the phase 1 in figure 4.2, chapter 4 (3rd party's slice registration and devices' information provisioning) as we give the Slice Id of the enterprises' slices and their addresses to the gNB. It is also possible to add a new field specific to the Slice Ids to the configuration file and to use a different format than the PLMD ID format for the Slice Id. The GFR function reads this information and registers it according to the gNB configuration file (we explain the GFR function in section 5.4.2).

For provisioning the Slice Id and the Dev Subscription Identity in the device, we have programmed two sim cards according to the PLMN IDs (Slice Ids) of the OAI-CNs (network slices). We programmed one sim card with the IMSI equal to 208920000000001 and the other one with the IMSI equal to 208930000000001. Therefore the provisioned Slice Id in the first device is 20892 and it is 20893 in the second device. The Dev Subscription Identity of both devices is 0000000001 (as they belong to different slices, they can have the same Dev Subscription Identity).

```
tracking_area_code  =  1;


plmn_list = ( { mcc = 208; mnc = 92; mnc_length = 2; };
              { mcc = 208; mnc = 93; mnc_length = 2; });


////////// MME parameters:
  mme_ip_address     = (  { ipv4      = "10.193.203.33";
                            ipv6      = "192:168:30::17";
                            active    = "yes";
                            preference = "ipv4";
                           };
                           { ipv4      = "10.193.203.182";
                            ipv6      = "192:168:30::17";
                            active    = "yes";
                            preference = "ipv4";
                           };
                        );
```

Figure 5.2– RAN gNB configuration. The MME has the IP address 10.193.203.33 is correlated with the mnc equals to 92 and the MME with has the IP address 10.193.202.182 is correlated with the mnc equals to 93.

5.4.2 GFR Function Implementation

The GFR function reads the configuration file of the gNB and verifies if the format of the Slice Id is identical to the Slice Id format of the 3rd party. In the case of using PLMN IDs instead of Slice Ids, it checks the ranges of the PLMD IDs. Function 5.1 is the definition of the GFR function. It gets a pointer to an itti message of the S1AP type. The structure of this message consists of the list of Slice Ids, the list of the 3GW IP addresses and the number of SCTP streams used for a 3GW (MME) association. The GFR function configures the different fields of this itti message's structure according to the information it obtains from the gNB configuration file.

Function 5.1	
1:	**function** GFR(parameters: pointer to ittiMessage)
2:	**READ:** gNB Configuration File
3:	**CHEACK:** Slice Id Format
4:	**CONFIGURE:** ittiMessage
5:	**end function**

5.4.3 RCP Implementation

The RCP function is the combination of three sub-functions called RCP1, RCP2 and RCP3, as well as the gNB functionalities. This function acts as an API through which the different types of AAC mechanisms can be interfaced with the OAI-RAN. The RCP's main functionality consists of two parts. The first part gets the Slice Id from the "RRC Connection Setup Complete" message (figure 4.2, section 4.5, chapter 4), fetches the slice information (3GW information) from the GFR function according to this Slice Id, and sends the "Initial Dev Message" to the proper 3GW function (the 3rd phase in Fig.4). The second part receives the "Initial Dev Message Response" from the 3GW and configures the connection between the device and the 3GW (slice) according to the information in that message. The RCP function also has to initialize the security mechanisms related to the 3rd party's AAC method using the "Initial Dev Message Response" message.

The RCP1 function gets the "RRC Connection Setup Complete" message from the device and acts accordingly as depicted in function 5.2. If the device wants to connect to the network operator's core, it provides the GUMMEI, MME code or the PLMD ID in the "RRC Connection Setup Complete" message. If it wants to connect to a 3rd party's 3GW, it provides the Slice Id. In our setup, since we use the PLMD ID as the Slice Id, we consider a specific range for the PLMD IDs of the network operator. If the provided PLMD ID in the "RRC Connection Setup Complete" message does not belong to the network operator's PLMN ID range, it means that the device wants to connect to a 3rd party's network slice. The RCP1 function gets a pointer to an itti message of type S1AP and a structure of type s1ap_gNB_mme_data (described in the main function of the gNB in section 5.4.4) as the inputs. It also chooses the Dev RRC Endpoint Id for the S1 connection (sub-phase 3.3 in figure 4.2, section 4.5, chapter 4).

The RCP2 function obtains the "Initial Dev Message Response" from the 3GW (MME) and creates appropriate structures for the further steps according to this message's type. In order to have the ability to use different AAC mechanisms, we have to define different structures according to the requirements of the 3rd party's AAC mechanism. If the message

Function 5.2

```
1:  function RCP1(parameters: pointer to ittiMessage, struct)
2:      structure mme_desc
3:          unsigned short plmn id
4:          int association id
5:      end structure
6:      if ittiMessage->id == GUMMEI then
7:          mme_desc = Select MME with GUMMEI (struct)
8:      end if
9:      if mme_desc == NULL then
10:         if ittiMessage->id == S-TMSI then
11:             mme_desc = Select MME with S-TMSI (struct)
12:         end if
13:     end if
14:     if mme_desc == NULL then
15:         mme_desc = Select MME with PLMN ID (struct)
16:     end if
17:     if mme_desc == NULL and ittiMessage->PLMN ID ∈ 5G core then
18:         mme_desc = Select MME with Highest Capacity (struct)
19:     else
20:         Discard Connection
21:     end if
22:     SET: Dev RRC Endpoint ID
23: end function
```

comes from the network operator' core (e.g. 5G core), the RCP2 function creates the S1AP_INITIAL_CONTEXT_SETUP_REQ_5G_CORE structure with the security key and security algorithms fields. Then, the RCP2 sets the fields of this structure according to the keys and algorithms resulted from the AKA procedure (5G-AKA). The gNB uses these keys and security algorithms to establish a secure connection with the device. If the "Initial Dev Message Response" message comes from a 3rd party's slice, the RCP2 function creates another structure accordingly. For example, if the 3rd party would like to fully shield the devices' identities from the operator, it has to use digital certificates and asymmetric encryption based AAC mechanism as the gNB is controlled by the network operator. Function 5.3 is the definition of the RCP2 function. It waits for an itti messages of type S1AP

Function 5.3

```
1:  function RCP2(parameters: pointer to ittiMessage)
2:      if ittiMessage->type == 5G Core then
3:          structure pointer to S1AP_INITIAL_CONTEXT_SETUP_REQ_5G_CORE
4:              unsigned short type
5:              unsigned char key
6:              unsigned short encryption_algorithm
7:              unsigned short integrity_algorithm
8:          end structure
9:      end if
10:     if ittiMessage->type == Slice x then
11:         structure pointer to S1AP_INITIAL_CONTEXT_SETUP_REQ_SLICEx
12:             unsigned short type
13:             //define fields according to the slice x AAC mechanims
14:         end structure
15:     end if
16: end function
```

from the 3GW (MME) and then based on to this message, it greats and configures the right type of structure.

The RCP3 function is responsible for calling the appropriate security functions and securing the connection between the gNB and the device. Function 5.4 defines the RCP3 function showing how it gets an itti message of type RRC. The structure of this message is different depending on the required AAC mechanism. It has a fixed field calls type that clarifies the type of the AAC mechanism.

5.4.4 gNB Execution

The gNB functionalities of RCP operate in the main body of the gNB, therefore, we do not consider separate function names for them. Function 5.5 is the main function of the program and it clarifies how to call Function 5.1 to Function 5.4. When we boot up the gNB, it makes a structure called S1AP_REGISTER_gNB_REQ that contains the 3GW IP addresses (MME IP address) and the Slice Id (PLMN ID) fields. The GFR function fills this structure according to the gNB configuration file. Considering this structure, the gNB makes SCTP

Function 5.4

```
1:  function RCP3(parameters: pointer to ittiMessage)
2:      switch ittiMessage->type
3:          case 5G_CORE:
4:              //Calls 5G Core related security functions
5:              break
6:          case Slice_X:
7:              //Calls Slice_X related security functions
8:              break
9:      end switch
10: end function
```

associations with all the 3GWs (or MMEs) recorded in the configuration file and assigns an association Id for each of these associations. It then creates and configures a structure called s1ap_gNB_mme_data. This structure contains the PLMD ID and the association ID fields and it keeps the data of the SCTP associations.

After the device has been turned on, the gNB establishes the RRC Connection (according to the 3.1 sub-phase in figure 4.2, section 4.5, chapter 4) and waits for the "RRC Connection Setup Complete" message from the device. Upon receiving this message, the gNB creates a structure called S1AP_NAS_FIRST_REQ and fills the PLMD ID field of this structure with the PLMD ID it fetches from the "RRC Connection Setup Complete" message. Then the gNB calls the RCP1 function. This function chooses the right 3GW (MME) and forwards the device attachment request to that 3GW (MME). The gNB waits for the "Initial Dev Message Response" message from the 3GW (MME). Upon receiving this message, the gNB calls the RCP2 function. Based on the type of the Initial Dev Message Response message, the RCP2 creates and configures a proper S1AP_INITIAL_CONTEXT_SETUP_REQ structure. Finally the gNB calls the RCP3 to run the proper security algorithms according to the S1AP_INITIAL_CONTEXT_SETUP_REQ structure.

Function 5.5

```
1:  function main
2:      structure pointer to S1AP_REGISTER_gNB_REQ
3:          char MME IP address[number of MMEs]
4:          unsigned short plmn id[number of MMEs]
5:          unsigned short SCTP streams
6:      end structure
7:      call: GFR(arguments: pointer to S1AP_REGISTER_gNB_REQ)
8:      CREAT: SCTP Association(pointer to S1AP_REGISTER_gNB_REQ)
9:      structure pointer to s1ap_gNB_mme_data
10:         unsigned short plmn id
11:         int association id
12:     end structure
13:     CONFIGURE: s1ap_gNB_mme_data
14:     GET: RRC Connection Setup Complete
15:     structure pointer to S1AP_NAS_FIRST_REQ
16:         unsigned short id
17:     end structure
18:     S1AP_NAS_FIRST_REQ->id <- Connection Setup Complete. plmn id
19:     call: RCP1(arguments: pointer to S1AP_NAS_FIRST_REQ, pointer to
        s1ap_gNB_mme_data)
20:     //wait for the Initial Dev Message Response
21:     call: RCP2(arguments: pointer to Initial Dev Message Response)
22:     call: RCP3(arguments: pointer to S1AP_INITIAL_CONTEXT_SETUP_REQ)
23: end function
```

5.5 Security Analysis

In this section we analyse our proposal from the security perspective. First we provide a summary of the security flaws related to the AAC mechanism in 3G, 4G and 5G networks considering the content of chapter 2, and then we explain how our proposal can address some of these flaws. We represent the security concerns in our proposal at the end of this section.

5.5.1 AKA-based AAC Flaws

As it is explained in chapter 2, the architecture of 3G, 4G and 5G networks consists of three parts: UE, SN (serving network) and HN (home network) which contains a database of the subscribers. The main AAC mechanisms used in these networks are based on the AKA protocol. The purpose of these AAC mechanisms is to establish mutual authentications between the UE and its corresponding HN and to set session keys in the UE and SN to secure the connections between them. Despite the evolutions to the AKA protocol made in each generation, the nutshell of the AAC mechanism stays the same and is based on symmetric cryptography and a secret key shared between the UE and the HN [126]. In 3G and 4G, the identity of the UE (IMSI) is sent in a clear text in the identity request part of the AKA protocol, which allows privacy attacks against the UE [29, 30]. To address this problem, in 5G, the UE sends its identity protected by asymmetric encryption using the HN's public key. Although this evolution prevents attackers from obtaining the UE's identity, the use of asymmetric encryption is just for concealing the UE's identity and the AAC mechanism itself is still based on symmetric key cryptography.

The security flaws of the AKA-based AAC mechanism used in cellular networks, the different attacks against them and their formal security analysis were studied in several researches [88, 92, 94, 110, 127, 128] and are explained in chapter 2. For example in [92], authors explain a new class of attacks calls activity monitoring attacks against the privacy of the UE. The target of the attacker is to catch the sequence number used to synchronize the UE and the HN (used to prevent the network against replay attacks) and learn the service consumption pattern of the UE using fake base stations. As another example, the authors in [94], discuss about the importance of pre-authentication messages' security in cellular networks (e.g. RRC Connection Request) and explain how exchanging them in clear texts provides the possibility of establishing fake base stations. They also propose to use digital certificates in order to confirm the legitimacy of the base stations.

The mentioned problems steam from the fact that the cellular networks are consistent with the logic of their used AAC mechanism (AKA-based AAC mechanisms with symmetric key encryption algorithms). All the required keys to secure the connection between the devices and

the network are derived as the result of AKA protocols (the network design and implementation are limited to rely on only AKA-based AAC mechanisms to derive security keys). Our proposal gives the ability to the network to provide session keys for the device and the access network to secure the communications between them without relying on only an AKA-based protocol. It means that the 3rd parties can use any AAC mechanism according to their requirements and the keys for securing the connection between the devices and the network are derived according to the used AAC mechanism.

In our proposal, the security of each 3rd party network slice and its provided devices are under the responsibility of the 3rd party itself and it depends on the AAC mechanism that the 3rd party chooses to use. If the 3rd party uses an AKA-based protocol (e.g., 5G-AKA), the security level of its network slice will be the same as the security level of the current cellular networks. But as we mentioned in the paper, using our proposal, the 3rd parties can provide lightweight AAC mechanisms for their constrained devices [19] or they can also provide more secure AAC mechanisms (e.g. with asymmetric encryption) to prevent their own networks and devices from the shortcomings of the AKA-based protocols. For example, a 3rd party network slice may use longer keys in the cryptographic functions during the AAC of the devices or even it can use a post-quantum cryptography TLS in order to protect its devices and network slice against the attacks that can break the security of both symmetric asymmetric algorithms using quantum computers. As another example, a 3rd party can use Kerberos authentication protocol for its Windows devices connecting to its company in case of remote working.

5.5.2 Security Advantages and Concerns in 5G-SSAAC

One of the main network functions in the proposed 5G network architecture from 3GPP is AMF (core Access and Mobility Management Function). Not only it plays a central and vital role in the AAC mechanism, but also it acts as an interface between the devices and the other network functions because of its responsibility in the network slice selection process. Therefore, several attacks can target AMF itself and the other network functions through the AMF. Although the AMF is a virtual network function and there can be several AMFs in the network, it is a potential single point of failure. Especially with the presence of massive number of IoT devices, the AMF can be the target of intentional and unintentional DoS attacks (if a

device maker wants to update the firmware of its devices at the same time which generates a lot of attach and detach messages). This DoS attack affects the AMF functionalities, the devices and the slices linked with this AMF and the other network functions such as AUSF (Authentication Server Function) that AMF sends messages to it in the AAC process. In our proposal, no network function of the connectivity provider has a central role in the attachment and the AAC of all the devices in the network. The 3GW function of each 3rd party's network slice is responsible for managing the attachment and the AAC of the devices in that slice (each 3rd party is responsible for its own devices). Therefore, the attacks such as the DoS attacks against a 3rd party's network slice (or any network function in that slice such as its 3GW function), only affect that slice and do not compromise the whole network (the other 3rd parties' network slices and the connectivity provider's network and services).

The central role of the AMF in the network makes it the target of software attacks as well which causes further attacks against the other network functions (in the whole network) just like the DoS attacks. These attacks are because of sending invalid or incomplete messages to the network functions that disturb the correct behavior of the target network function or cause software crashes. In our proposal, although the RCP and the GFR network functions are shared between the 3rd parties' network slices, the 3GW function with the central role in the AAC of the devices in the slice is a dedicated network function to the specific 3rd party's network slice. Thus, a software attack against a 3GW function which provides a specific AAC mechanism, only affects that 3GW function and the corresponding 3rd party's network slice (the network functions responsible for the AAC of the devices are not shared between all the devices in the network, such as the AMF function in the current 5G network architecture).

In addition to address the problems related to the AMF as the single point of failure in the current 5G architecture, our approach enables the 3rd party enterprise to conceal its provided devices' identities and their credentials' from the 5G network operator. It brings business confidentiality to the whole 5G system (as it is mentioned in the introduction section).

Despite all the advantages coming from the flexibility of our proposal, there are some points we have to pay attention to. Securing the isolation of the 3rd parties' slices requires more attention. On the one hand, different slices can provide different security mechanisms

according to our proposal. In this context, an attack against a slice with a lower security level should not have an impact on the other slices [128]. On the other hand, there are common resources between the multiple slices (e.g. the spectrum; the computing resources in the gNodeB; the bandwidth on the link connecting the gNB to the 3rd party's slice) and it is important to avoid denial of service attacks against the network slices by exposing one slice and thereby risking the exhaustion of the common resources [128]. To secure the isolation of the 3rd parties' slices, it is important to have careful management rules and the enforcement of limits in the consumption of resources that are shared by multiple slices. If the network operator can provide secure isolation between the different slices it has wholesaled to the different 3rd parties, the misconfiguration of a 3GW function in one slice, cannot affect the other slices. In this case, well-defined security SLAs (Service Level Agreement) between the connectivity provider and the different 3rd parties, proper implementations of them and forcing all the actors to respect these SLAs, can prevent the attack and vulnerability diffusion between 3rd parties' network slices. Of course, the mentioned attacks and vulnerabilities are related to the virtualization technologies and the infrastructure which already exists in the current 5G architecture as well.

Finally, it is important to consider that our proposal is a distributed approach (each 3rd party's network slice owns a dedicated network function for AAC of its provided devices). Consequently, the security monitoring in this approach is more challenging than the security monitoring in a centralized approach (e.g., the AMF(s) is responsible for the AAC of the all devices in the network). In the centralized approach, the connectivity provider is the only responsible for monitoring the network functions in the AAC processes of all devices. Therefore, it can monitor the signaling traffic of the different network functions and detect the attacks (e.g., DoS attacks) against them. While in our approach the 3rd party has to monitor its own network functions and protect them from the attacks.

5.6 Performance Analysis

In this section, we compare the performance of the AAC mechanism in 4G and 5G cellular networks with our SSAAC proposal, focusing on the signalling cost (signalling load) [14, 101].

For 4G, we consider EPS-AKA [13, 29, 130] and for 5G, we consider three authentication methods from release 16: 5G-AKA, EAP-AKA' and EAP-TLS [10, 11, 21]. For sake of simplicity, we only consider the initial AAC for each of these mechanisms which contain the attachment of the UE or device to the network too as the attachment process totally dependent to the authentication methods. We assume that the number of devices is n.

5.6.1 EPS-AKA Signalling Cost

According to [13], the number of CN signalling messages in the EPS-AKA procedure is 5. The CN entities involved in this procedure are the MME (Mobility Management Entity) and HSS (Home Subscriber Server). These messages are depicted in table 5.2. Among these messages, the "Attach request", the "User authentication request" and the "User authentication response" are exchanged between the devices and the CN through the RAN (eNB, 4G base station). The "Attach request" message is sent through the "RRC connection setup complete" message from the device to the eNB and through the "Initial device message" from the eNB to the MME. Therefore; the "Attach request" message consists of two signalling messages on the RAN side. In this case, the number of signalling messages go through the RAN is 4 (the "User authentication request" message and the "User authentication response" message are just forwarded through the eNB). Thus, the total signalling cost of the EPS-AKA procedure on the network for n devices is 9n (5n for CN and 4n for RAN).

5.6.2 5G-AKA Signalling Cost

5G-AKA is used when UEs connect to the network through a 3GPP access network. According to [11], the number of CN signalling messages in the 5G-AKA procedure is 9. The CN functions involved in this procedure are the SEAF (Security Anchor Function) which is included in the AMF (core Access and Mobility management Function), the AUSF (Authentication Server Function) and UDM/ARPF (Unified Data Management/ Authentication Repository and Processing Function). These messages are depicted in table 5.3.

Table 5.2 – The EPS-AKA procedure messages exchanged between CN entities.

	Message	Source	Destination
1	Attach request	UE	MME
2	Authentication information	MME	HSS
3	Authentication information answer	HSS	MME
4	User authentication request	MME	UE
5	User authentication response	UE	MME

Table 5.3 – The 5G-AKA procedure messages exchanged between CN functions.

	Message	Source	Destination
1	N1 messages	UE	AMF/SEAF
2	Nausf_UEAuthentication_Authenticate Request	AMF/SEAF	AUSF
3	Nudm_UEAuthentication_Get Request	AUSF	UDM/ARPF
4	Nudm_Authentication_Get Response	UDM/ARPF	AUSF
5	Nausf_UEAuthentication_Authenticate Response	AUSF	AMF/SEAF
6	Authentication Request	AMF/SEAF	UE
7	Authentication Response	UE	AMF/SEAF
8	Nausf_UEAuthentication_Authenticate Request	AMF/SEAF	AUSF
9	Nausf_UEAuthentication_Authenticate Response	AUSF	AMF/SEAF

Among these messages, the “N1 message”, the “Authentication request” message and the “Authentication response” message are exchanged between the UEs and the CN through the RAN (gNB). The “N1 message” in this procedure consists of two signalling messages on the RAN side (as with the “the “Attach request” message in the EPS-AKA procedure). Therefore, the number of signalling messages that go through the RAN is 4 and the total signalling cost of the 5G-AKA procedure on the network for n devices is 13n (9n for the CN and 4n for the RAN).

5.6.3 EAP-AKA’ Signalling Cost

The EAP-AKA’ is used when UEs connect to the network through a non-3GPP access network. According to [11], the number of CN signalling messages in the EAP-AKA’ procedure is 11. These messages are depicted in table 5.4. The “N1 message” (from the UE to the AMF/SEAF and from the AMF/SEAF), the “Authentication request” message and the “Authentication response” message are exchanged between the UEs and the CN through the RAN (gNB). As in the 5G-AKA, the “N1 message” which is sent from the UE to the AMF/SEAF, consists of two signalling messages on the RAN side. Therefore, the number of

Table 5.4 – The EAP-AKA' procedure messages exchanged between CN functions.

	Message	Source	Destination
1	N1 messages	UE	AMF/SEAF
2	Nausf_UEAuthentication_Authenticate Request	AMF/SEAF	AUSF
3	Nudm_UEAuthentication_Get Request	AUSF	UDM/ARPF
4	Nudm_Authentication_Get Response	UDM/ARPF	AUSF
5	Nausf_UEAuthentication_Authenticate Response	AUSF	AMF/SEAF
6	Authentication Request	AMF/SEAF	UE
7	Authentication Response	UE	AMF/SEAF
8	Nausf_UEAuthentication_Authenticate Request	AMF/SEAF	AUSF
9	Optional exchange of further EAP messages	between UE, AMF/SEAF, and AUSF	
10	Nausf_UEAuthentication_Authenticate Response (EAP success)	AUSF	AMF/SEAF
11	N1 message (EAP success)	AMF/SEAF	UE

signalling messages that go through the RAN is 5 and the total signalling cost of the EAP-AKA' procedure on the network for n devices is 16n (11n for the CN and 5n for the RAN).

5.6.4 EAP-TLS Signalling Cost

The EAP-TLS can be used for private networks or with the IoT devices in isolated deployment scenarios (without roaming). It is an additional EAP method for primary authentication in private networks [130]. These messages are depicted in table 5.5. According to [11], the number of the CN's signalling messages in the EAP-TLS procedure is 18. The messages exchanged between the UEs and the CN through the RAN (gNB) are as follows: the "Registration request", the "Authentication Request (EAP request, EAP-TLS)", the "Authentication Response (EAP response, EAP-TLS)", the "Authentication Request (EAP-TLS, EAP request, TLS certificate request)", the "Authentication Response (EAP response, TLS certificate verify)", the "Authentication Request (EAP request, TLS finished)", the "Authentication Response (EAP response)" and the "N1 message (EAP success)". By considering the two parts of the "Registration request" message, the number of signalling messages that go through the RAN is 9. Therefore, the total signalling cost of the EAP-TLS procedure on the network for n devices is 27n (18n for the CN and 9n for the RAN).

Table 5.5 – The EAP-TLS procedure messages exchanged between CN functions.

	Message	Source	Destination
1	Registration request	UE	AMF/SEAF
2	Nausf_UEAuthentication_Authenticate Request	AMF/SEAF	AUSF
3	Nudm_UEAuthentication_Get Request	AUSF	UDM/ARPF
4	Nudm_Authentication_Get Response	UDM/ARPF	AUSF
5	Nausf_UEAuthentication_Authenticate Response (EAP request, EAP-TLS)	AUSF	AMF/SEAF
6	Authentication Request (EAP request, EAP-TLS)	AMF/SEAF	UE
7	Authentication Response (EAP response, EAP-TLS)	UE	AMF/SEAF
8	Nausf_UEAuthentication_Authenticate Request (EAP response, EAP-TLS)	AMF/SEAF	AUSF
9	Nausf_UEAuthentication_AuthenticateResponse (EAP request, TLS certificate request)	AUSF	AMF/SEAF
10	Authentication Request (EAP-TLS) (EAP request, TLS certificate request)	AMF/SEAF	UE
11	Authentication Response (EAP response, TLS certificate verify)	UE	AMF/SEAF
12	Nausf_UEAuthentication_AuthenticateRequest (EAP response, TLS certificate verify)	AMF/SEAF	AUSF
13	Nausf_UEAuthentication_AuthenticateResponse (EAP request, TLS finished)	AUSF	AMF/SEAF
14	Authentication Request (EAP request, TLS finished)	AMF/SEAF	UE
15	Authentication Response (EAP response)	UE	AMF/SEAF
16	Nausf_UEAuthentication_AuthenticateRequest (EAP response)	AMF/SEAF	AUSF
17	Nausf_UEAuthentication_AuthenticateReSponse (EAP success)	AUSF	AMF/SEAFs
18	N1 message (EAP success)	AMF/SEAFs	UE

5.6.5 5G-SSAAC Signalling Cost

In our proposed 5G-SSAAC procedure, none of the signalling messages related to the devices' AAC go through the MNO's CN (except the mobile broad band subscribers). Thus, only the RAN part of the MNO is affected by the AAC signalling cost. The numbers of messages exchanged between the devices and the RAN and between the network functions inside the RAN are 4 and they are depicted in table 5.6. We do not consider the messages that are related to the ACC between the devices and the 3rd party's slice because these messages are exchanged inside the established slice connectivity (phase 4 of figure 4.2, section 4.5, chapter 4) and they do not involve the network functions which are under the responsibility

Table 5.6 – The signalling messages in the proposed 5G-SSAAC procedure.

	Message	Source	Destination
1	Attach request	Device	RCP
2	Slice information request	RCP	GFR
3	Slice information response	GFR	RCP
5	Attach request reroute	RCP	3GW

of the connectivity provider (e.g., RCP). Therefore, the total signalling cost of the proposed 5G-SSAAC procedure on the MNO's network for n devices is 4n.

5.6.6 Comparison Results

Table 5.7 gives a comparison of the different AAC mechanisms in terms of the total number of signalling messages representing the signalling cost of each protocol. We can see that the signalling costs of the AAC mechanisms used in 5G (5g-AKA, EAP-AKA', EAP-TLS), are higher than the signalling cost of the AAC mechanism that is used in 4G (EPS-AKA). This growth in signalling cost is due to the separation between the 4G's physical entities' functionalities. For example, the functionalities of the MME entity in 4G have been distributed between the AMF, SMF and UDM network functions in 5G [131]. Since the AAC mechanisms need the signalling message exchanges between these network functions, the signalling cost becomes higher than the signalling cost in 4G.

Among the AAC mechanisms for 5G, the EAP-TLS may be suitable for private networks, but it has the highest signalling cost. In our proposed 5G-SSAAC mechanism, the AAC signalling messages do not go through the MNO's CN, and so its signalling cost on the MNO's core network is less than that of the other procedures.

Table 5.7 – A comparison of the different AAC mechanisms' signalling cost on the MNO's CN, MNO's RAN and the MNO's whole network (CN+RAN). "n" is the number of devices.

Protocol	**Signaling cost on CN**	**Signaling cost on RAN**	**Overall signaling cost**
EPS-AKA	5n	4n	9n
5G-AKA	9n	4n	13n
EAP-AKA'	11n	5n	16n
EAP-TLS	18n	9n	27n
SSAAC	0	4n	4n

5.6.7 Concluding Remarks

Figure 5.3 based on table 5.7 shows the comparison results of the signalling cost on the whole network (CN+RAN). From figure 5.3, we can see that by increasing the number of UEs (devices), the signalling costs of all of these AAC procedures increase linearly. Therefore if the network operator takes the responsibility of controlling the AAC of the massive number of devices, e.g., in an IoT environment (each type with different requirements), the load of the signalling on its CN may cause network downtime and/or lead to the inability to meet QoS requirements. Even though 5G provided flexibilities will give network operators the ability to have more than one instance of each network function and to locate them in different locations, the core network function and especially the AMFs are likely to be congested as the single point of access for the control plane [131]. By delegating the AAC of the different devices to their owners' 3rd parties, our proposal isolates the operators' CN from the high volume of the devices' ACC signalling.

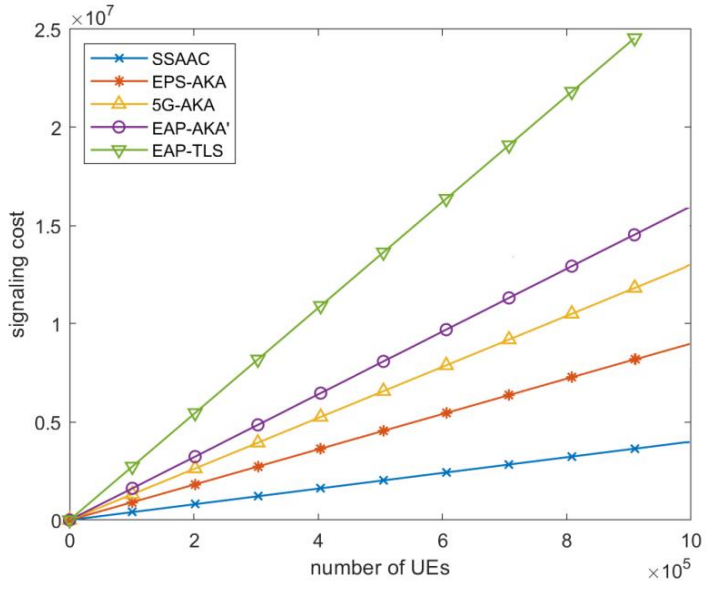


Figure 5.3– Comparison of the different AAC signalling cost on the MNO's network.

5.7 Summary

The proposed 5G-SSAAC approach opens the 5G network to the 3rd parties by defining three network functions in the RAN and delegating the AAC of the devices to the 3rd parties who provide these devices. On the one hand, this approach enables industries (3rd parties) to use their pre-existing AAC infrastructure and credentials (or to choose a specific AAC mechanisms according to their own security requirements) to manage the authentication and the access control of their own devices in 5G. It also gives the ability to the 3rd parties to shield devices' identities and credentials from the operator. On the other hand, it drastically reduces the signalling load on the connectivity provider's (operator) CN by redirecting the devices' AAC signalling to the corresponding 3rd party networks. In this case, the connectivity provider's CN will not be a single point of failure and so it will not have to endure the signalling load that is caused by the AAC requests of a massive number of devices. Table 5.8, shows the compatibility of 5G-SSAAC with the derived requirements that are presented in chapter 3, section 3.2.2, in comparison with the different AAC methods proposed for cellular networks as well as the AAC mechanisms in Wi/fi and LoRaWAN technologies.

Table 5.8 – A comparison between 5G-SSAAC approach with the different AAC mechanisms in Cellular, WiFi and LoRaWAN technologies in terms of addressing 5G-specific requirements.

AAC method	R1	R2	R3	R4	R5
Cellular AKA	-	-	-	-	-
eSIM (AKA)	+	-	-	-	-
Group based (AKA)	-	-	-	+	+
Service oriented and anonymity based (AKA + service provider's AAC)	-	+/-	-	-	-
AAC in WiFi	-	-	+	-	-
AAC in LoRaWAN	-	-	+	+	+
5G-SSAAC	+	+	+	+	+

There are two questions considering the proposed 5G-SSAAC approach: Is it feasible to define new virtual network functions in 5G RAN to do the devices' AAC delegation? What are the impacts of this delegation on the network from the security and the signalling load points of view? We evaluated the feasibility of our approach by implementing it via OAI-RAN and testing its impact on an actual RAN. We then analysed the security aspects of the proposed approach. We also evaluated the impact of our approach on reducing the connectivity provider's CN signalling load by comparing it to the signalling load of the current AAC mechanisms.

Chapter 6 Conclusions and Future Work

6.1 Summary and Discussions

Since 1G, the cellular networks have made a significant progress in technologies used (from the analog communications in 1G to the all-IP networks in 4G) and the use cases addressed (from voice calls in 1G to the high-speed data transmissions in 4G) in the pre-5G networks. This progress in each generation is the continuation of the previous generation in terms of the technologies used and the use cases addressed. However, this is not the case for 5G. The 5G network is not just a continuity of the 4G network and it aims to address much broader use cases in many different vertical domains (than any other pre-5G networks) using the virtualization technologies and providing new virtual network functions.

Considering the use cases that the 5G aims to address, the 5G environment does not only consist of the connectivity providers (operators) and the end users (mobile devices). There are also other business actors such as different 3rd parties (that are not network operators) in the 5G environment to address the broad range of use cases. These different 3rd parties require different connectivity services (e.g., in terms of latency, etc.) and network functionalities from the connectivity providers according to their addressed use cases (e.g., smart home, smart factory, etc.). The security requirements of the 3rd parties are also different and depend on the sensitivity of their provided services, and the predicted effects of the security flaws on their network and customers (the 3rd parties need a trade-off between their required security level and the processing power of their network and provided devices). Consequently, in order to address this broad range of use cases and requirements, the 5G network has to be more flexible and open to the different actors and 3rd parties. Virtual network slices obtain flexibility for the 5G network to provide different connectivity services to the 3rd parties. But currently there is no slicing in the AAC level of the end users (devices) in the network.

Despite the different security requirements in the different use cases, the 5G network only provides one way of AAC of the devices in the network, which is the same as the AAC in the 3G, and 4G networks with few enhancements (AKA-based AAC) and it is not suitable for all the 5G-specific use cases. In the other words, although the expectations from the 5G networks (e.g., in terms of use cases and requirements) are not the continuation of the expectations from the pre-5G networks, the AAC mechanisms as the most important mechanisms in attaching to the network, follow the AAC mechanisms in the pre-5G networks. Even these AAC mechanisms are well-established mechanisms, they suffer from some security vulnerabilities and flaws. These security vulnerabilities and flaws are studies deeply in chapter 2. The contribution of chapter 2 is to explain the few differences of the AAC mechanisms in 5G networks with the AAC mechanisms in the pre-5G networks and to highlight the recognized security flaws in the AAC mechanisms of 5G although they are not in the operational stage yet. Therefore, the lesson learned from chapter 2 is that the AAC mechanisms in 5G (e.g., 5G-AKA) are not suitable for highly security-sensitive use cases (e.g., autonomous driving).

One of the most important feature in the currently used AAC model in cellular networks is that the connectivity provider (operator) plays the central role and it is the only responsible of the devices identities and credentials. The need for supporting the device identities and credentials owned by an entity (3rd party) separated from the connectivity provider (operator) is mentioned as a key issue in the 3GPP technical report, "Study on enhanced support of Non-Public Networks", release 17 [132]. However, in the proposed solution the 3rd party network (the standalone non-public network in this technical report) has to have all the functionalities of the 5G-RAN and the 5G-CN (all the network functions). In another 3GPP technical report, "Study on Security Aspects of Enhanced Network Slicing", release 16 [133], the authentication for access to a specific network slice is mentioned as a key issue. But in the proposed slice specific authentication and authorization solution, it is mandatory to have a primary authentication between the devices and the 5G network (using 3GPP credentials), then doing the slice specific authentication with the corresponding slice as the secondary authentication (using slice specific identities and credentials). The 5G network also proposes the use of EAP-TLS protocol rather than the AKA-based protocols for the private networks and some IoT use cases. Although this protocol provides the opportunity to do the AAC by deploying credentials

in the devices and the network parts and do not use the UICC-based AAC, the 3rd party has to include all the functionalities of the 5G-RAN and the 5G-CN and again the MNO has the central role in the AAC procedure.

In addition to the cellular technologies, there are other technologies such as WiFi and LoRaWAN for addressing the use cases that the 5G network aims to address. The feature of giving central role to the connectivity provider in the AAC procedure also exist in these technologies. Chapter 3 studies the AAC of these technologies. The contribution of chapter 3 is first to introduce some 5G-specific use cases and to derive new requirements from these use cases. Then this chapter analyzes the compatibility of the AAC mechanisms provided in the literature for the cellular, WiFi and LoRaWAN technologies with the 5G-specific use cases and requirements. This analysis shows that none of the AAC mechanisms can address all the requirements derived from the 5G-specific use cases and it highlights that the 5G network has to be flexible enough to support different AAC mechanisms instead of being confined to use only one type of AAC mechanism.

In order to enable the network to support different AAC mechanisms for different 3rd parties (and considering different use cases), this work presents the 5G-SSAAC (5G Slice Specific Authentication and Access Control): a new way of AAC of the UEs and devices in the 5G network. Using the virtualization technologies, new network functions are defined in 5G-RAN to route the attachment requests of the devices directly to the network slices, which provide these devices. The AAC of the devices is then done inside the related slice according to that slice's security requirements. In this approach, the 3rd parties can own and manage the identities and credentials of their provided devices without deploying all the 5G-RAN and the 5G-CN network functions and without relying on the connectivity provider. The defined network functions for 5G-SSAAC is depicted in chapter 4. The contribution of this chapter is to show the interworking of the new defined network functions and the feasibility of the 5G-SSAAC approach with a detailed call flow of the devices' attachment process to the network.

The impact of the 5G-SSAAC on the 5G network is depicted in chapter 5 through the implementation of the defined network functions in a fully virtualized mobile network with a testbed based on the OAI (Open Air Interface). Chapter 5 also analyses the security and

performance (the signalling load on the MNO's network) of the proposed 5G-SSAAC approach. In this chapter, it is shown that with 5G-SSAAC approach, the AAC signalling load on the 5G network is reduced in comparison with the AKA-based and the EAP-TLS protocols. This enables the network to support the connectivity of massive number of devices. Besides enabling the network to support different AAC mechanisms for different 3rd parties (with lower level of security for constrained devices or the higher level of security for sensitive use cases), the 5G-SSAAC also has the following advantages in addition to mentioned ones:

- The 3rd party is able to shield device identities and their credentials' privacy from the 5G network operator.
- The 3rd party can embed connectivity in its provided devices to its customers, to ensure a better customer experience. In this case, the customer (i.e., the device user) does not have to set up an additional subscription and an accounting plan with a network operator.
- The 5G-SSAAC enables the 5G network to support wholesaling connectivity in the AAC level. In this case if the 3rd party wants to change its wholesale agreement from one network operator to another network operator, it has not to do a mass-migration of per-device subscription information from the first operator to the second one.

6.2 Limitations

Beside the advantages of the 5G-SSAAC approach, some limitations remain in the present work:

- The mobility management of devices has not been considered yet in case of handovers and roaming scenarios.
- A malicious device can send its attachment request to a slice which it's not belonging to. Therefore, a group of malicious devices can cause DoS attacks against target 3rd party's network slice.
- Considering the performance analysis, due to the time limitations, we restricted the evaluations to calculating AAC signaling cost in the first attachment of the device to the network and comparing the network load according to the different AAC

mechanisms. However analyzing the traffic models related to the MIoT and computing the amount of traffic which is routed to the connectivity provider's network would give a better view of the 5G-SSAAC impact on the network load.

In addition to the mentioned limitations, despite the 5G-SSAAC decrease the connectivity's provider network load, it also limited the connectivity provider's authority domain. In order to use the 5G-SSAAC approach, the operators needs the participation of the standardization bodies to have a suitable ecosystem and the trust relationships should be clearly defined between the actors (3rd parties and the connectivity providers). Finally it is difficult to make the 5G-SSAAC compatible with the pre-5G generations.

6.3 Future Work

According to the 5G-SSAAC approach, we propose the following promising areas for the future research to progress in this way.

6.3.1 New AAC Mechanisms for 5G

5G-SSAAC mechanism enables the 5G network to support different AAC mechanisms. It opens the way to define 3rd parties slice-specific network functions for the 3rd party's slice according to their AAC requirements as it makes the RAN flexible and compatible with any AAC mechanism. Designing the new AAC protocols for the different use cases such as mass market IoT (sensors) with low processing power or different use cases in the V2X communications like self-automotive which needs the mechanisms executable with very low latency is suggested as the future work.

6.3.2 Customization in Cellular Network Services

As it is mentioned in section 4.1, despite the introduction of virtualization techniques, cellular network architectures should still be considered as monolithic: the different parts of the network remain strongly coupled and dependent to each other and there is no customization at the network level of the provided services. 5G-SSAAC is the initial step to have a more loosely

coupled network architecture and intends to maximize the decoupling between the RAN and the CN. Not only it enables the 3rd parties to use their specific AAC mechanism, but also it enables the designing of the customized network services other than the ACC mechanisms. The future work would be designing new network functions (without using the previously defined network functions) in order to increase the customization rate in the network level according to the 3rd parties service requirements.

6.3.3 Smart Contracts between Different Actors

Having management rules and the enforcement of limits in the consumption of resources, which are shared by multiple slices, are mandatory in the contracts between the connectivity providers and the different 3rd parties. Using the 5G-SSAAC approach, the connectivity providers are able to set their wholesale contracts with the 3rd parties in the AAC level. In this case, as the AAC of the devices is dedicated to the 3rd parties that provide these devices, the connectivity provider has not to set the management rules and enforce limits in the device level and it is possible for connectivity provider to set these rules in the 3rd parties' slice level. The wholesaling connectivity contracts between the connectivity providers and the 3rd parties can be in the form of smart contracts over a block chain. Consequently, the execution of the rules and the consumption of the resources can be done in the form of trusted transactions without a need of central authority (the validity of these transactions is approved in the block chain and the connectivity provider is not the only responsible in controlling the execution of the rules, therefore it is not the single point of failure). In the case of using smart contracts, malicious 3rd parties cannot pretend as legitimate ones and the devices can perform the AAC with the corresponding 3rd party slice in a safe manner.

The UEs and devices can also set smart contracts with 3rd parties according to the services they got from the 3rd parties. For instance, there can be a smart contract between the video playing device and a media service provider company in order to get recent movies. The future work would be designing the mentioned smart contracts and also AAC mechanisms to use these smart contracts.

References

[1] 5G Ensure Project, "Deliverable D2.7 Security Architecture (Final)", 2017.

[2] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[3] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[4] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.

[5] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5G and future mobile networks: mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[6] R. Wen *et al.*, "On robustness of network slicing for next-generation mobile networks," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 430–444, 2018.

[7] A. Boubendir, E. Bertin, and N. Simoni, "Flexibility and dynamicity for open network-as-a-service: From VNF and architecture modeling to deployment," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–6, 2018.

[8] G. Tseliou, F. Adelantado, and C. Verikoukis, "NetSliC: Base Station Agnostic Framework for Network SliCing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3820–3832, 2019.

[9] N. Nikaein *et al.*, "Network store: Exploring slicing in future 5G networks," in *Proceedings of the 10th International Workshop on Mobility in the Evolving Internet Architecture*, pp. 8–13, 2015.

[10] 3GPP,"System Architecture for the 5G System". TS 23.501, Tech. Spec. v16.0.2, 2019.

[11] 3GPP, "Security architecture and procedures for 5G system". TS 33.501, Tech. Spec. v15.4.0, 2019.

[12] 3GPP, "Security Architecture". TS 33.102, Tech. Spec. v15.1.0, 2018.

[13] 3GPP, "Security Architecture". TS 33.401, Tech. Spec. v15.7.0, 2019.

[14] J. Cao, M. Ma, and H. Li, "LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth Generation (5G) cellular networks," *International Journal of Communication Systems*, vol. 32, no. 3, p. e3860, 2019.

[15] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018

[16] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 492–496, 2017.

[17] F. Malandra, L.-O. Chiquette, L.-P. Lafontaine-Bédard, and B. Sansò, "Traffic characterization and LTE performance analysis for M2M communications in smart cities," *Pervasive and Mobile Computing*, vol. 48, pp. 59–68, 2018

[18] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[19] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017

[20] B. L. Parne, S. Gupta, and N. S. Chaudhari, "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network," *IEEE Access*, vol. 6, pp. 3668–3684, 2018

[21] 3GPP,."Non access stratum (NAS) protocol for evolved packet system (EPS)". TS 24.301, Tech. Spec. v16.0.0, 2019.

[22] 5G Ensure Project, "Deliverable D2.3 Risk Assessment, Mitigation and Requirements (draft)"., 2016.

[23] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, 2016.

[24] 3GPP,."Study of enhancement of network slicing". TR 23.740, Tech. Report. v16.0.0, 2018.

[25] 5G Ensure Project, "Deliverable D 3.5 5G PPP enablers technical roadmap (update)" , 2016.

[26] 5G Ensure Project, "Deliverable D 2.1 Use cases", 2016.

[27] 5G Ensure Project, "Deliverable D 2.5 Trust model (final)", 2018.

[28] Y. Zhang, R. Gravina, H. Lu, M. Villari, and G. Fortino, "PEA: Parallel electrocardiogram-based authentication for smart healthcare systems," *Journal of Network and Computer Applications*, vol. 117, pp. 10–16, 2018.

[29] S. Behrad, E. Bertin, and N. Crespi, "Securing authentication for mobile networks, a survey on 4G issues and 5G answers," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 1–8, 2018.

[30] S. Behrad, E. Bertin, and N. Crespi, "A survey on authentication and access control for mobile networks: from 4G to 5G," *Annals of Telecommunications*, vol. 74, no. 9–10, pp. 593–603, 2019.

[31] S. Behrad, S. Tuffin, E. Bertin, and N. Crespi, "Network Access Control for the IoT: A Comparison Between Cellular, Wi-Fi and LoRaWAN," in *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 195–200, 2019.

[32] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "5G-SSAAC: Slice-specific Authentication and Access Control in 5G," in *2019 IEEE Conference on Network Softwarization (NetSoft)*, pp. 281–285, 2019.

[33] S. Behrad, E. Bertin, S. Tuffin and N. Crespi, *"*A new scalable authentication and access control mechanism for 5G-based IoT", Future Generation Computer Systems *(under revision)*.

[34] S. Wong, N. Sastry, O. Holland, V. Friderikos, M. Dohler, and H. Aghvami, "Virtualized authentication, authorization and accounting (V-AAA) in 5G networks," in *Standards for*

Communications and Networking (CSCN), 2017 IEEE Conference on, pp. 175–180, 2017.

[35] M. Koutsopoulou, A. Kaloxylos, A. Alonistioti, L. Merakos, and K. Kawamura, "Charging, accounting and billing management schemes in mobile telecommunication networks and the internet," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 1, 2004.

[36] T. Velte and A. Velte, *Cisco: a beginner's guide*. McGraw-Hill, Inc., 2006.

[37] C. Metz, "AAA protocols: authentication, authorization, and accounting for the Internet," *IEEE Internet Computing*, vol. 3, no. 6, pp. 75–79, 1999.

[38] S. Gusmeroli, S. Piccione, and D. Rotondi, "IoT access control issues: a capability based approach," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pp. 787–792, 2012.

[39] A. E. Yegin and F. Watanabe, "Authentication, Authorization, and Accounting," *Next Generation Mobile Systems 3G and Beyond*, pp. 315–343, 2005.

[40] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access". TS 23.401, Tech. Spec. v16.4.0, 2019.

[41] 3GPP, "Network Architecture," TS 23.002, Tech. Spec. v15.0.0, 2018.

[42] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[43] 3GPP, "Numbering, Addressing and Identification," TS 23.003, Tech. Spec. v16.0.0, 2019.

[44] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE security*. John Wiley & Sons, 2012.

[45] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.

[46] M. S. A. Khan and C. J. Mitchell, "Another look at privacy threats in 3G mobile telephony," in *Australasian Conference on Information Security and Privacy*, pp. 386–396, 2014.

[47] F. B. Degefa, D. Lee, J. Kim, Y. Choi, and D. Won, "Performance and security enhanced authentication and key agreement protocol for SAE/LTE network," *Computer Networks*, vol. 94, pp. 145–163, 2016.

[48] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[49] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Enhancing user identity privacy in LTE," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 949–957, 2012.

[50] J.-K. Tsay and S. F. Mjølsnes, "A vulnerability in the umts and lte authentication and key agreement protocols," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pp. 65–76, 2012.

[51] S. Mjølsnes and J.-K. Tsay, "Computational security analysis of the UMTS and LTE authentication and key agreement protocols," 2012.

[52] D. Bhasker, "4G LTE security for mobile network operators," *Cyber Secur. Inf. Sys. Inf. Anal. Cent.(CSIAC)*, vol. 1, no. 4, pp. 20–29, 2013.

[53] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, "LTE Authentication Protocol (EPS-AKA) Weaknesses Solution," in *Intelligent Computing and Information Systems (ICICIS), 2015 IEEE Seventh International Conference on*, pp. 434–441, 2015.

[54] L. Qiang, W. Zhou, B. Cui, and L. Na, "Security analysis of TAU procedure in LTE network," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on*, pp. 372–376, 2014.

[55] J. B. Abdo, J. Demerjian, K. Ahmad, H. Chaouchi, and G. Pujolle, "EPS mutual authentication and crypt-analyzing SPAKA," in *Computing, Management and Telecommunications (ComManTel), 2013 International Conference on*, pp. 303–308, 2013.

[56] Z. J. Haddad, S. Taha, and I. A. Saroit, "Anonymous authentication and location privacy preserving schemes for LTE-A networks," *Egyptian Informatics Journal*, 2017.

[57] X. Li and Y. Wang, "Security enhanced authentication and key agreement protocol for LTE/SAE network," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, pp. 1–4, 2011.

[58] J. V. Franklin and K. Paramasivam, "Enhanced Authentication Protocol for Improving Security in 3GPP LTE Networks," in *Proc. International Conference on Information and Network Technology (ICINT 2011)*, 2011.

[59] J. B. B. Abdo, H. Chaouchi, and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for EPS," in *Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on*, pp. 73–77, 2012.

[60] P.-A. Fouque, C. Onete, and B. Richard, "Achieving Better Privacy for the 3GPP AKA Protocol," *IACR Cryptology ePrint Archive*, vol. 2016, p. 480, 2016.

[61] K. Hamandi, I. Sarji, A. Chehab, I. H. Elhajj, and A. Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme," in *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 929–934, 2013.

[62] G. Escudero-Andreu, C. P. Raphael, and D. J. Parish, "Analysis and design of security for next generation 4G cellular networks," in *The 13th annual post graduate symposium on the convergence of telecommunications, networking and broad-casting (PGNET)*, 2012.

[63] 3GPP, "Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution," TR 33.821, Tech. Report. v9.0.0, 2009.

[64] K. Hamandi, I. Sarji, I. H. Elhajj, A. Chehab, and A. Kayssi, "W-AKA: Privacy-enhanced LTE-AKA using secured channel over Wi-Fi," in *Wireless Telecommunications Symposium (WTS)*, pp. 1–6, 2013.

[65] J. Cichonski, J. M. Franklin, and M. Bartock, "LTE Architecture Overview and Security Analysis," *NIST Draft NISTIR*, vol. 8071, 2016.

[66] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Security & Privacy*, vol. 11, no. 2, pp. 55–62, 2013.

[67] S. Alt, P.-A. Fouque, G. Macario-Rat, C. Onete, and B. Richard, "A Cryptographic Analysis of UMTS/LTE AKA," in *International Conference on Applied Cryptography and Network Security*, pp. 18–35, 2016.

[68] M. Arapinis *et al.*, "New privacy issues in mobile telephony: fix and verification," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 205–216, 2012.

[69] M.-F. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, "Anonymity guarantees of the UMTS/LTE authentication and connection protocol," *International journal of information security*, vol. 13, no. 6, pp. 513–527, 2014.

[70] S. Othmen, F. Zarai, M. S. Obaidat, and A. Belghith, "Re-authentication protocol from WLAN

to LTE (ReP WLAN-LTE)," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, pp. 1446–1451, 2013.

[71] Y. E. H. El Idrissi, N. Zahid, and M. Jedra, "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA," in *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 137–142, 2012.

[72] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA," in *Wireless Telecommunications Symposium, 2009. WTS 2009*, pp. 1–8, 2009.

[73] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Globecom Workshops, 2007 IEEE*, pp. 1–6, 2007.

[74] N. Alliance, "5G white paper," *Next generation mobile networks, white paper*, 2015.

[75] P. Schneider and G. Horn, "Towards 5G security," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1, pp. 1165–1170, 2015.

[76] 5G Ensure Project, "Deliverable D2.4 Security Architecture (draft)," 2016.

[77] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[78] W.-T. Su, W.-M. Wong, and W.-C. Chen, "A survey of performance improvement by group-based authentication in iot," in *Applied System Innovation (ICASI), 2016 International Conference on*, pp. 1–4, 2016.

[79] R. Giustolisi and C. Gerhmann, "Threats to 5G group-based authentication," in *13th International Conference on Security and Cryptography (SECRYPT 2016), 26-28 July 2016, Madrid, Spain*, 2016.

[80] B. Chatras, U. S. T. Kwong, and N. Bihannic, "NFV enabling network slicing for 5G," in *Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on*, pp. 219–225, 2017.

[81] K. Katsalis, N. Nikaein, E. Schiller, A. Ksentini, and T. Braun, "Network Slices toward 5G Communications: Slicing the LTE Network," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 146–154, 2017.

[82] P. Rost *et al.*, "Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[83] 5G Ensure Project, "Deliverable D2.1 Use Cases," 2016.

[84] 5GPP, "5G PPP Phase1 Security Landscape", white paper, 2017.

[85] M. Dehnel-Wild and C. Cremers, "Security vulnerability in 5G-AKA draft," *Department of Computer Science, University of Oxford, Tech. Rep*, 2018.

[86] 3GPP, "Study of Security Aspects of the Next Generation System," TR 33.899, Tech. Report. v1.3.0, 2017.

[87] J. Zhang, Q. Wang, L. Yang, and T. Feng, "Formal Verification of 5G-EAP-TLS Authentication Protocol," in *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, pp. 503–509, 2019.

[88] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1383–1396, 2018.

[89] F. Liu, J. Peng, and M. Zuo, “Toward a secure access to 5G network,” in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1121–1128, 2018.

[90] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, “Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks,” *IEEE Access*, vol. 7, pp. 64040–64052, 2019.

[91] A. Koutsos, “The 5G-AKA authentication protocol privacy,” in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 464–479, 2019.

[92] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, “New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,” *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 108–127, 2019.

[93] H. Khan and K. M. Martin, “On the Efficacy of New Privacy Attacks against 5G AKA,” 2019.

[94] R. P. Jover, “The current state of affairs in 5G security and the main remaining security challenges,” *arXiv preprint arXiv:1904.08394*, 2019.

[95] R. P. Jover and V. Marojevic, “Security and protocol exploit analysis of the 5G specifications,” *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

[96] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, “Security and privacy issues for an IoT based smart home,” in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on, 2017, pp. 1292–1297, 2017.

[97] GSMA, “Remote Provisioning Architecture for Embedded UICC,” Tech. Spec. V3.1, 2016.

[98] 3GPP, “Service requirements for Machine-Type Communications (MTC),” TS 22.368, Tech. Spec. V14.0.1, 2017.

[99] J. Yao, T. Wang, M. Chen, L. Wang, G. Chen, "GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network", Proc. IEEE Int. Conf. Cloud Comput. Res. Innov. (ICCCRI), pp. 42-48, May 2016.

[100] J. Cao, M. Ma, and H. Li, “A group-based authentication and key agreement for MTC in LTE networks,” in Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 1017–1022, 2012.

[101] C. Lai, H. Li, R. Lu, and X. S. Shen, “SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks,” Computer Networks, vol. 57, no. 17, pp. 3492–3510, 2013.

[102] J. Ni, X. Lin, and X. S. Shen, “Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT,” IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 644–657, 2018.

[103] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, “CPAL: A conditional privacy-preserving authentication with access linkability for roaming service,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46–57, 2014.

[104] J. K. Liu, C.-K. Chu, S. S. Chow, X. Huang, M. H. Au, and J. Zhou, “Time-bound anonymous authentication for roaming networks,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 178–189, 2015.

[105] M. Mathews and R. Hunt, “Evolution of wireless LAN security architecture to IEEE 802.11 i (WPA2),” in *Proceedings of the fourth IASTED Asian conference on communication systems and*

networks, 2007

[106] M. Khasawneh, I. Kajman, R. Alkhudaidy, and A. Althubyani, "A survey on Wi-Fi protocols: WPA and WPA2," in *International Conference on Security in Computer Networks and Distributed Systems*, pp. 496–511, 2014.

[107] LoRa Alliance Technical Committee, "LoRaWAN™ 1.1 Specification", Tech. Spec. V1.1, 2017.

[108] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, no. 1, pp. 14–21, 2017.

[109] LoRa Alliance Technical Committee, "LoRaWAN™ Backend Interfaces 1.0 Specification", Tech. Spec. V1.0, 2017.

[110] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[111] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[112] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, 2018.

[113] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing & softwarization: A survey on principles, enabling technologies & solutions," IEEE Communications Surveys & Tutorials, 2018.

[114] ETSI, "Network Functions Virtualisation (NFV) Management and Orchestration (NFV-MAN)". Tech. Spec. 1.1.1, 2014.

[115] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC)". TS 36.331, Tech. Spec. v15.4.0, 2018.

[116] M. M. Rahman and S. S. Heydari, "Performance evaluation of LTE EPC self-healing solutions," in *2012 IEEE Globecom Workshops*, pp. 813–817, 2012.

[117] J. Prados, A. Laghrissi, M. Bagaa, T. Taleb, and J. M. Lopez-Soler, "A Complete LTE Mathematical Framework for the Network Slice Planning of the EPC," *IEEE Transactions on Mobile Computing*, 2019.

[118] J. Prados-Garzon, J. J. Ramos-Munoz, P. Ameigeiras, P. Andres-Maldonado, and J. M. Lopez-Soler, "Modeling and dimensioning of a virtualized MME for 5G mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4383–4395, 2016.

[119] A. S. Rajan *et al.*, "Understanding the bottlenecks in virtualizing cellular core network functions," in *The 21st IEEE International Workshop on Local and Metropolitan Area Networks*, pp. 1–6, 2015.

[120] G. Foddis, R. G. Garroppo, S. Giordano, G. Procissi, S. Roma, and S. Topazzi, "LTE traffic analysis for signalling load and energy consumption trade-off in mobile networks," in *2015 IEEE international conference on communications (ICC)*, pp. 6005–6010, 2015.

[121] I. Widjaja, P. Bosch, and H. La Roche, "Comparison of MME signaling loads for long-term-evolution architectures," in *2009 IEEE 70th Vehicular Technology Conference Fall*, pp. 1–5, 2009.

[122] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control

(MAC) protocol specification". TS 36.321, Tech. Spec. v15.4.0, 2018.

[123] S. Gupta, B. L. Parne, and N. S. Chaudhari, "SRGH: A secure and robust group-based handover AKA protocol for MTC in LTE-A networks," *International Journal of Communication Systems*, vol. 32, no. 8, p. e3934, 2019.

[124] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Transactions on emerging telecommunications technologies*, vol. 26, no. 3, pp. 414–431, 2015.

[125] Y.-L. Huang, C.-Y. Shen, and S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4509–4519, 2011.

[126] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[127] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193–199, 2017.

[128] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[129] Alliance, N. "5G security recommendations Package# 2: Network Slicing". Ngmn 1–12, 2016.

[130] 3GPP, "Service requirements for the 5G system". TS 22.261, Tech. Spec. v16.7.0, 2019.

[131] I. Alawe, Y. Hadjadj-Aoul, A. Ksentini, P. Bertin, and D. Darche, "On the scalability of 5G Core network: the AMF case," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, 2018.

[132] 3GPP, "Study on enhanced support of Non-Public Networks". TR 23.700-07, Tech. Report. v0.2.0, 2019.

[133] 3GPP, "Study on Security Aspects of Enhanced Network Slicing". TR 33.813, Tech. Report. v0.7.0, 2019.

[134] Behrad, S., Bertin, E. and Crespi, N. (2020). Security and Access Control for 5G. In Wiley 5G Ref (eds R. Tafazolli, C.-L. Wang and P. Chatzimisios). doi:10.1002/9781119471509.w5GRef261