UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

SVILUPPO DEL SOFTWARE DI ACQUISIZIONE ED ELABORAZIONE DELLE MISURE DELL'INQUINAMENTO DELL'ARIA DI DRONI PROGETTO A.R.I.A.

Relatore: Prof. Carlo Bettanini Fecia di Cossato

Laureando: Giacomo Favaron

ANNO ACCADEMICO: 2020-2021

Data di laurea: 15/11/2021

Abstract

In the recent years, awareness of the issue of Environmental Pollution has increased, and research shows that not enough has been done, until now, to reduce pollution. In this domain, the monitoring of air quality is fundamental to provide data which can be used to most effectively guide our efforts to reduce air pollution. At this time the monitoring of air quality is usually performed via stationary ground-mounted air pollution stations. However, research(??) has shown that air pollution can vary greatly at different heights, for this reason the *Air Pollutants Monitoring Using UAVs* (ARIA) project is aiming to develop a system to measure vertical gradients of air pollutants using vertical swarms of drones. The ARIA project solution is a low-cost monitoring system based on *Commercial off-the-shelf* (COTS) sensors and on multiple cheap drone platforms. The system is equipped with $PM_2.5$ and PM_10 sensors to monitor the particulate concentration and several other gas sensors (such as NO, NO_2, CO, etc.) and the use of *Unmanned Aerial Vehicles* (UAVs) allows to build a 3D map of pollutants in a specific area. This could prove very useful around buildings in urban areas and possibile polluting plants in industrial areas. In this thesis are presented the system platform, the software implementation and a test flight.

Contents

List of Figures

List of abbreviations

AKA *Authentication and Key Agreement.*

AMF *Access and Mobility Management Function.*

ARIA *Air Pollutants Monitoring Using UAVs.*

AuC *Authentication Center.*

AUSF *Authentication Server Function.*

AUTN *Authentication Token.*

BS *Base Station.*

BSS *Base Station Subsystem.*

COTS *Commercial off-the-shelf.*

DDOS *Distributed Denial Of Service.*

DOS *Denial Of Service.*

ECIES *Elliptic Curve Integrated Encryption Scheme.*

EIR *Equipment Identity Register.*

EPA Environmnetal Protection Agengy.

FACH *Forward Access Channel.*

FDMA *Frequency Division Multiple access.*

GGSN *Gateway GPRS Support Node.*

GPRS *General Packet Radio Service.*

GSM *Global System for Mobile Communications.*

GUTI *Globally Unique Temporary Identifier.*

HLR *Home Location Register.*

HSS *Home Subscriber Server.*

IK *Integrity Key.*

IMEI *International Mobile Equipment Identity.*

IMSI *International Mobile Subscriber Identity.*

IOT *Internet Of Things.*

IP *Internet Protocol.*

LTE *Long Term Evolution.*

MITM *Man In The Middle.*

MME *Mobility Management Entity.*

MS *Mobile system.*

MSC *Mobile Switching Center.*

MTSO *Mobile Telephone Switching Office.*

NEF *Network Exposure Function.*

NFV *Network Functions Virtualization.*

NRF *Network Repository Function.*

NSS *Network Switching Subsystem.*

NSSF *Network Slicing Selector Function.*

PCF *Policy Control Function.*

PCRF *Policy Control and Charging Rules Function.*

P-GW *Packet data network - Gateway.*

PTSN *Public switched telephone network.*

RAN *Radio Access Network.*

SBA *Service Base Architecture.*

SDN *Software Defined Network.*

SDSF *Structured Data Storage Network Function.*

SEAF *Security Anchor Function.*

S-GW *Serving - Gateway.*

SGSN *Serving GPRS Support Node.*

SIM *Subscriber Identity Module.*

SMF *Session Management Function.*

SMS *Short Message Service.*

SNN *Serving Network Name.*

SRES *Signed Response.*

SUCI *Subscription Concealed Identifier.*

SUPI *Subscription Permanent Identifier.*

TMSI *Temporary Mobile Subscriber Identity.*

TPS *Transation Per Second.*

UAVs *Unmanned Aerial Vehicles.*

UDM *Unified Data Management.*

UDSF *Unstructured Data Storage Network Function.*

UMTS *Universal Mobile Telecommunications System.*

UPF *User Plane Function.*

VLR *Visitor Location Register.*

W-CDMA *Wideband Code Division Multiple Access.*

WSN *Wireless Sensor Network*.

Chapter 1

Introduction

Air pollution is caused by different typologies of gas pollutants that are present in the first meters (¡150 m) of the atmosphere and cause therefore damages to humans and environment. As air pollution is becoming the largest environmental health risk, the monitoring of air quality has drawn much attention in both laboratory studies and specific field tests and data collection campaigns. Government agencies and local administrations have, generally, provided and used monitoring stations on dedicated sites in cities and urban areas. Usually the studies have been conducted using fixed stations that are very reliable but produce only coarse-grained 2D monitoring, with several kilometers between two monitoring stations; or the stations monitor the same local area for long periods. Other approaches show that applications using simple system of sensors have been developed to monitor the fine-grained air quality using densely deployed sensors [?], [?]. In any case, the fixed sensor station may achieve high precision, but have high cost and require maintenance and suffer especially for lack of mobility. Furthermore, these approaches don't account for the vertical gradients of air pollution levels. As shown in research (?, ?) the concentrations of air pollutants can vary greatly at different heights and this is a sensitive factor in circumstances such as buildings in urban areas and possible polluting plants in industrial areas. The usage of Unmanned Aerial Vehicles (UAVs) has been particularly rich in the latest years due to their flexibility, mobility and affordable cost. Current monitoring systems are not able to satisfy every need of modern cities and industrial areas and UAVs are valuable supporting elements in this scenario. In terms of urban conditions, which is the main subject of the present study, UAVs can be used to measure environmental parameters such as illumination, wind speed, temperature, humidity, air quality [?] and much more. In any case, for a complete analysis, both ground sensing and aerial sensing are necessary to provide 3D mapping and gas profiling. In our ARIA project, we equipped with the same set of sensors the devices that execute sensing on the ground, and the systems that execute aerial sensing on board the UAVs. The fixed ground sensing suite is able to collect data in a continuous way, but the air quality of the higher levels of air off the ground cannot be detected, so the contemporary use of drones is mandatory. Aerial sensing, on the contrary, is able to sense the air quality off the ground, but it cannot be executed for very long periods due to the high consumption of battery power and human time. By merging the potentialities of these two systems of sensing suites, a better set of data can be collected [?]. A trade off on the possible sensors and UAVs has been performed and quadcopters are the preferred platform for monitoring because of their simplicity, low cost and hovering capabilities. On the contrary a possible bias of data is due to the the influence of air jets created by the rotor rotation or by the electromagnetic field generated by the antennas present on board. The problem of choosing the best location

of the sensors is examined in [?] based on the physical structure of the drones. Our approach is to use an extension on which we fix the sensors in order to suck the air away of the main air jets.

ARIA project was created by a group of students from the Department of Industrial Engineering, University of Padova, under the suggestion and guidance of personnel staff of the Center for Space Studies and Activities (CISAS) of the same University. The core motivation that brought together these students was the desire of researching new fields of application for drone technology. ARIA project has been carried on figuring this scenario: air quality monitoring.

1.1 Related works and state of the art

1.1.1 Air Pollution

Air pollution is extremely complex to evaluate and there are many polluting substances in the atmosphere. The Environmnetal Protection Agengy (EPA) (of United States) takes these 6 in consideration in its studies:

Chemical symbol	Substance	Characteristics
CO	Carobon Monoxide	Colorless, odorless gas
NO_2	Nitrogen Dioxide	Highly reactive gas
O_3	Ozone	Pale blue gas
SO_2	Sulfur Dioxide	Colorless, irritating smell gas
$PM_2.5$ and PM_10	Particulate Matter	Inhalable particles
Pb	Lead	Metal particles

1.1.2 Low-cost sensors

The EPA also provides the Air Sensor Guidebook[**williams2014-air**] which gives extensive information on air quality and low-cost sensors.

[1], [2], [3] propose different implementation of a *Wireless Sensor Network* (WSN) using UAVs. The differentiating factor of the ARIA project solution is the use of vertical swarms to monitor pollution at different heights, which is not a popular topic.

1.2 Dissertation structure

This dissertation describes the ARIA project solution for the monitoring of air pollution. It is divided into 6 chapters:

- Chapter 1 describes the introduction, an overview on the topic of air pollution, the motivation to approach the problem, the motivation of the proposed solution, related works, the state of the art and the dissertation objective.
- Chapter 2 describes the system architecture, that is the UAVs that are being used, their design, specifications and functionality.
- Chapter 3 describes the sensor payload, the motivation of the adopted sensors and their use.

- Chapter 4 describes the software implementation for the data collection of the sensors and the communication of the UAVs.
- Chapter 5 shows the results of a test flight using the proposed solution.
- Chapter 6 presents what conclusions can be taken after all the developed work, and what improvements can be done in the future.

1.3 Dissertation objective

The objective of this dissertation is to describe the solution proposed by the ARIA project for air pollution monitoring, in particular the software impelementation, to show preliminary results and discuss their revelance in future applications.

Chapter 2

ARIA: System architecture

Chapter 3

Generazioni cellulari

Nel corso degli anni, si sono susseguite diverse generazioni di tecnologie cellulari che hanno apportato notevoli cambiamenti alla loro architettura e infrastruttura per consentire il raggiungimento di prestazioni migliori[4].
Di seguito verranno presentate le principali caratteristiche delle diverse generazioni cellulari, in modo tale da rendere di facile comprensione l'analisi dei meccanismi di autenticazione che verranno approfonditi nelle prossime sezioni.
Oltre ad elencare le principali caratteristiche di ogni generazione verranno analizzate nel dettaglio le specifiche delle architetture.

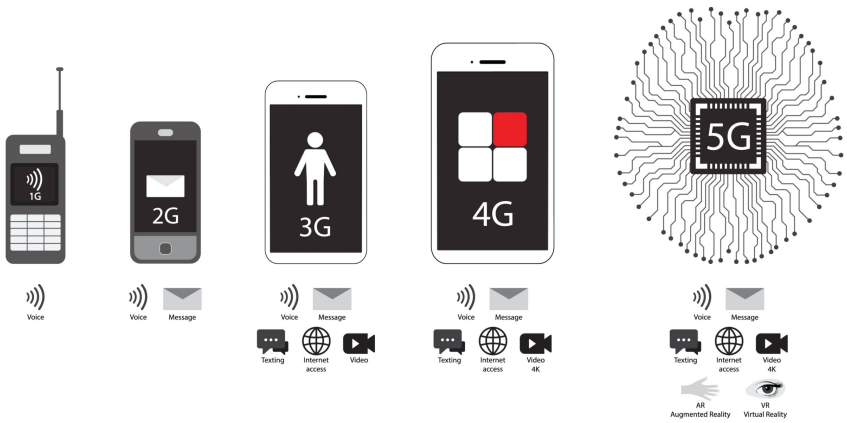

Figure 3.1: Schema delle generazioni cellulari

3.1 1G

La generazione 1G è uno dei primi standard di comunicazione cellulare. Il suo funzionamento era completamente analogico e ormai è stata rimpiazzata totalmente dalle generazioni digitali successive.
L'architettura di questa generazione è molto semplice, è composta da tre componenti principali:

- Antenne per la trasmissione
- *Mobile Telephone Switching Office* (MTSO)
- Unità mobile (cellulare)

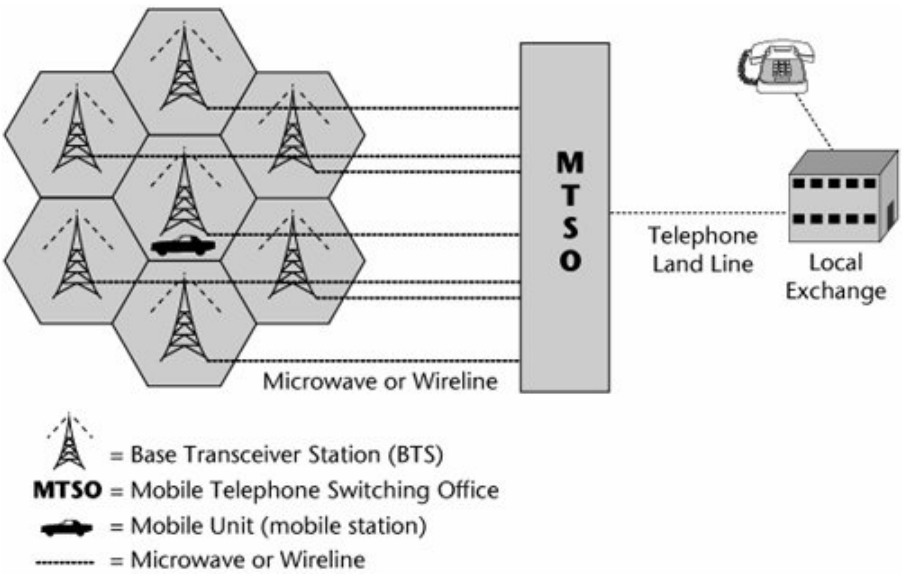

Figure 3.2: Architettura 1G

Si basava sulla *Frequency Division Multiple access* (FDMA) in cui ogni dispositivo che si connetteva alla stazione radio aveva assegnata una specifica sotto banda[5].

3.2 2G

A differenza della prima generazione, la seconda introuduce per la prima volta una rete completamente digitale. Questa tecnologia cellulare è composta da diverse versioni che si sono susseguite nel corso degli anni aggiungendo nuove funzionalità. Anche la sua architettura subisce delle modifiche, per questo verranno trattate separatamente in seguito.

GSM

Il *Global System for Mobile Communications* (GSM)[6] è uno standard di seconda generazione che introuduce importanti novità.
Le principali caratteristiche introdotte sono:

- Maggiori velocità di trasmissione
- Cifratura della comunicazione
- Introduzione di nuovi servizi come gli *Short Message Service* (SMS)

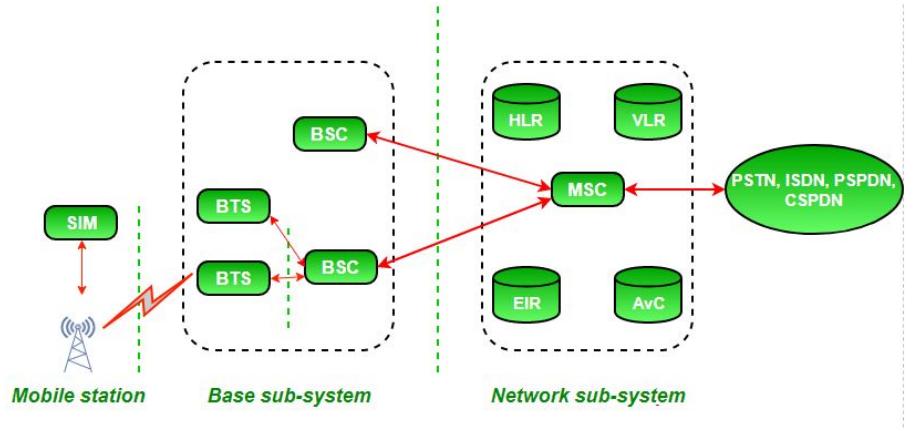

Figure 3.3: Architettura GSM

La sua architettura è composta da due macro aree: La *Base Station Subsystem* (BSS) e la *Network Switching Subsystem* (NSS). Il BSS è l'insieme delle antenne ricevitori che rappresentano il primo collegamento con il *Mobile system* (MS), mentre il NSS rappresenta il *core network* del GSM.
Il NSS è formato dai seguenti componenti:

- *Mobile Switching Center* (MSC) è l'elemento centrale dell'atchitettura GSM, si occupa di interfacciare le *Base Station* (BS) con la rete telefonica *Public switched telephone network* (PTSN).
- *Home Location Register* (HLR) *database* centrale che contiene informazioni inerenti a tutti i *subscribers*, molte delle informazioni che contiene sono dei puntatori agli archivi seguenti.
- *Visitor Location Register* (VLR) *database* che memorizza la posizione degli utenti.
- *Equipment Identity Register* (EIR) *database* degli *International Mobile Equipment Identity* (IMEI) dei dispositivi. Grazie a questo archivio è possibile creare delle *blacklist* per evitare l'accesso a determinati terminali.
- *Authentication Center* (AuC) *database* delle informazioni di sicurezza associate agli utenti registrati.

3.2.1 GPRS

La rete *General Packet Radio Service* (GPRS)[7] introduce per la prima volta un trasferimento dati a commutazione di pacchetto per rendere possibile l'utilizzo dei servizi *internet* con il proprio dispositivo cellulare[8]. La sua architettura è la stessa di quella del GSM ma con dei componenti aggiuntivi che consentono la trasmissione dei pacchetti. Per esempio, il *Serving GPRS Support Node* (SGSN) è un componente per la gestione dei dispositivi connessi alla rete.

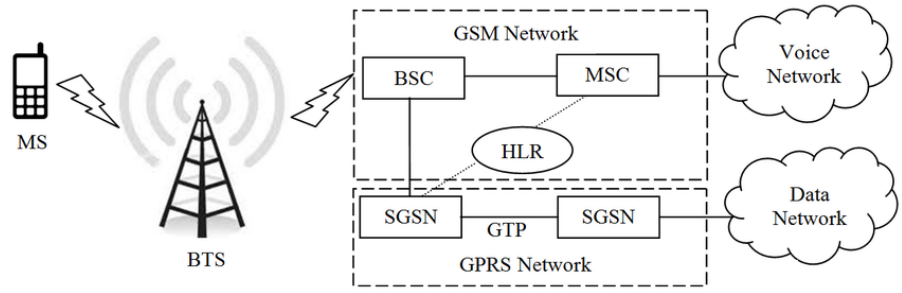

Figure 3.4: Architettura GPRS

3.2.2 EDGE

Evoluzione del GPRS che consente maggiori velocità, l'architettura resta invariata[7].

3.3 3G

L'architettura della terza generazione riprende quella già vista nella seconda. Infatti, questa generazione ha avuto come principale obbiettivo quello di consolidare l'integrazione della rete internet nei sistemi cellulari ed aumentare la velocità di trasmissione per consentire l'utilizzo di nuovi servizi.
L'accesso al canale radio avviene con la tecnologia *Wideband Code Division Multiple Access* (W-CDMA) con canale di banda 5 MHz.

3.3.1 UMTS

Lo *Universal Mobile Telecommunications System* (UMTS) è il primo standard di terza generazione. La sua architettura è composta dai seguenti elementi principali:

- MSC, componente che ha la stessa funzione di quello in 2G. Questa volta il VLR è integrato al suo interno.
- HLR/AuC e EIR
- SGSN e *Gateway GPRS Support Node* (GGSN) ovvero dei componenti ripresi dalla rete GPRS per la commutazione a pacchetto.

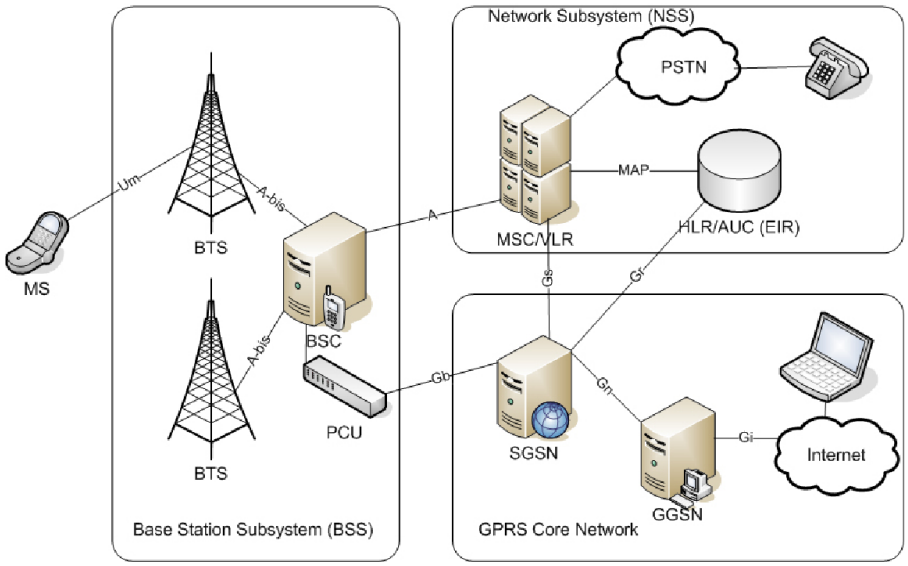

Figure 3.5: Architettura UMTS

3.3.2 HSPA/HSPA+

Evoluzione del UMTS per consentire velocità maggiori apportando modifiche nella trasmissione del segnale. Con questo nuovo standard si riescono a raggiungere velocità di 42 Mb/s[9].

3.4 4G

La quarta generazione è al momento quella più utilizzata, permette di avere dei servizi basati su velocità molto alte. A differenza delle precedenti generazioni che dovevano gestire due *core network*: uno per la rete telefonica e un altro per *internet*, per la prima volta il 4G introduce un unico *core network* basato su *Internet Protocol* (IP).
Per consentire un aumento consistente della velocità, le maggiori modifiche di questa generazione sono state apportate nella *radio interface*, mentre l'architettura rimane con una struttura simile a quella precedente.

3.4.1 LTE

la *Long Term Evolution* (LTE) è uno standard di quarta generazione che ha i seguenti componenti architetturali[10]:

- *Home Subscriber Server* (HSS) è il *database* centrale dei *subscriber* come l'HLR del GSM/UMTS.
- *Mobility Management Entity* (MME) è il corrispettivo del VLR in GSM/UMTS.
- *Serving - Gateway* (S-GW) è un componente che svolge il ruolo di *router* indirizzando i dati dalla *base station* al P-GW.
- *Packet data network - Gateway* (P-GW) è il componente per interfacciare il *core network* con *internet*.
- *Policy Control and Charging Rules Function* (PCRF) è un componente responsabile delle regole di gestione per il flusso di informazioni.

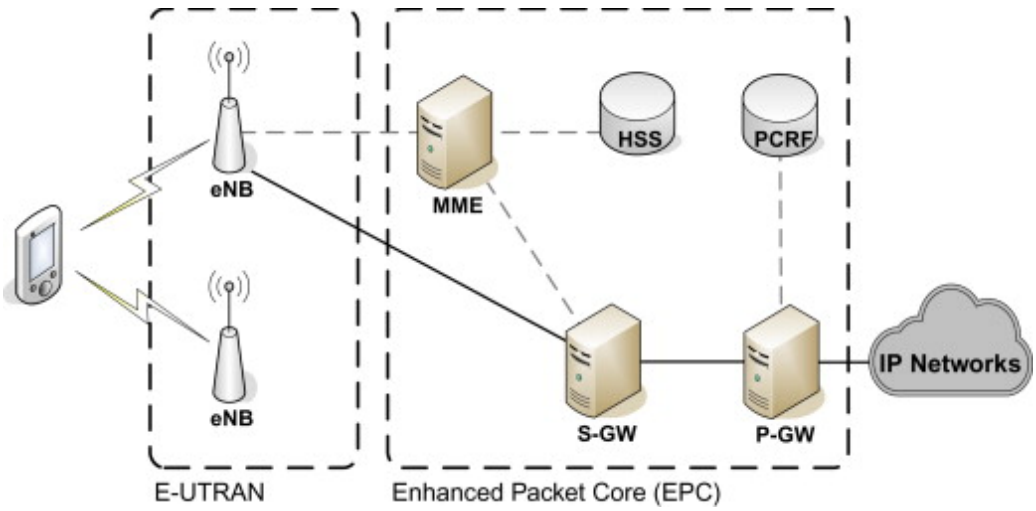

Figure 3.6: Architettura LTE

3.5 5G

Il 5G, ovvero lo standard di quinta generazione rappresenta l'ultima frontiera della tecnologia cellulare. Il suo principale scopo è consentire lo *Internet Of Things* (IOT) massivo, ossia un *network* che sia in grado di gestire la connessione di molti dispositivi con latenze molto piccole. Per consentire velocità fino a 10 Gb/s si sono dovute apportare importanti modifiche strutturali che rendono la sua architettura molto diversa da quelle viste fin'ora.
L'architettura implementata prende il nome di *Service Base Architecture* (SBA). La SBA consiste nel dividere tutti i componenti architetturali in una serie di *microservices*[11]. Questa nuova struttura è stata introdotta per garantire la scalabilità del sistema, migliorare le prestazioni (velocità) e per permettere la gestione simultanea di molti dispositivi.
I principali elementi che la compongono sono:

- *Access and Mobility Management Function* (AMF) responsabile dell'autenticazione e localizzazione del dispositivo.
- *Session Management Function* (SMF) per la gestione della sessione di ogni MS.
- *Policy Control Function* (PCF) per la gestione delle *policy*.
- *Unified Data Management* (UDM) per la gestione dell'identità dell'utente, questo compito era precedentemente svolto da HSS o HLR.
- *Authentication Server Function* (AUSF) per effettuare l'autenticazione dell'utente.
- *Structured Data Storage Network Function* (SDSF) è un helper per la memorizzazione di dati strutturati.
- *Unstructured Data Storage Network Function* (UDSF) è un helper per la memorizzazione di dati non strutturati.
- *Network Exposure Function* (NEF) per esporre determinate funzionalità a servizi di terze parti.
- *Network Repository Function* (NRF) per scoprire tutti i servizi disponibili.
- *Network Slicing Selector Function* (NSSF) per selezionare una determinata partizione di *network*.
- *User Plane Function* (UPF) trasporta il traffico dal *Radio Access Network* (RAN) all'internet.

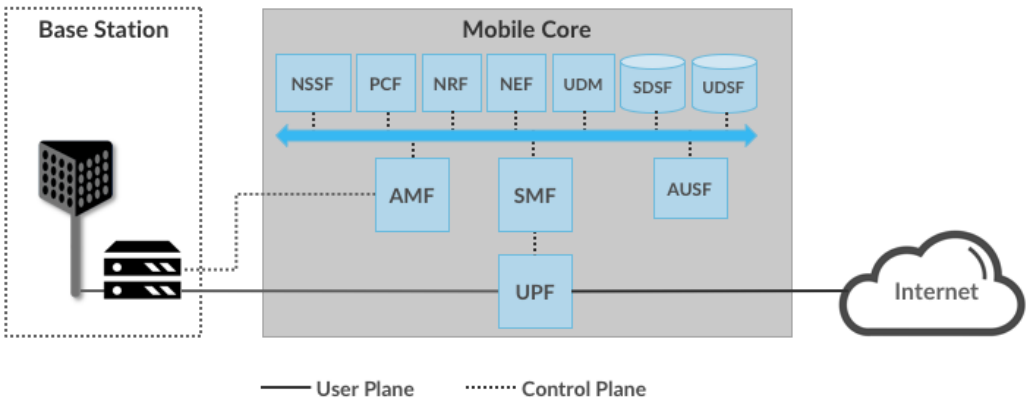

Figure 3.7: Architettura 5G[11]

3.5.1 Network Slicing

Il *Network Slicing* rappresenta una delle caratteristiche più importanti del 5G. Con questo termine si intende il partizionamento della rete in diversi "piani" ciascuno con caratteristiche e requisiti particolari, indipendente e autonomo. Questo risulta fondamentale nella realizzazione dell' IOT massivo, infatti in questo modo la gestione del traffico terrà conto dell'applicazione che viene utilizzata nel dispositivo per decidere di quali prestazioni di rete ha bisogno.

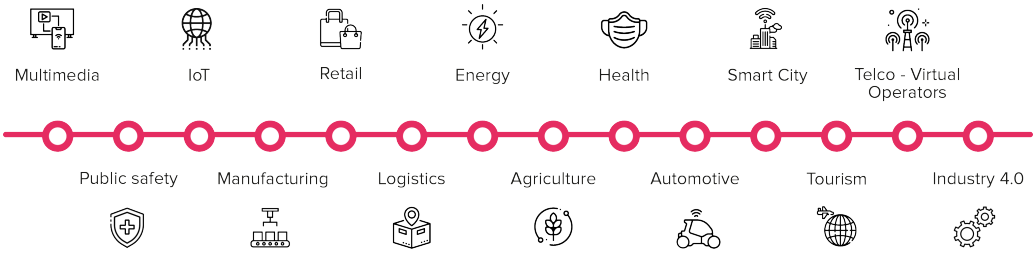

Figure 3.8: Esempi di applicazioni per il 5G

Ogni segmento virtuale del *network* ha uno specifico identificativo che deve essere indicato nella fase di autenticazione come verrà illustrato nella sezione 5.3. Per ogni *slice* sono richieste delle prestazioni differenti, per esempio il settore delle *critical communication* deve avere delle latenze molto basse.

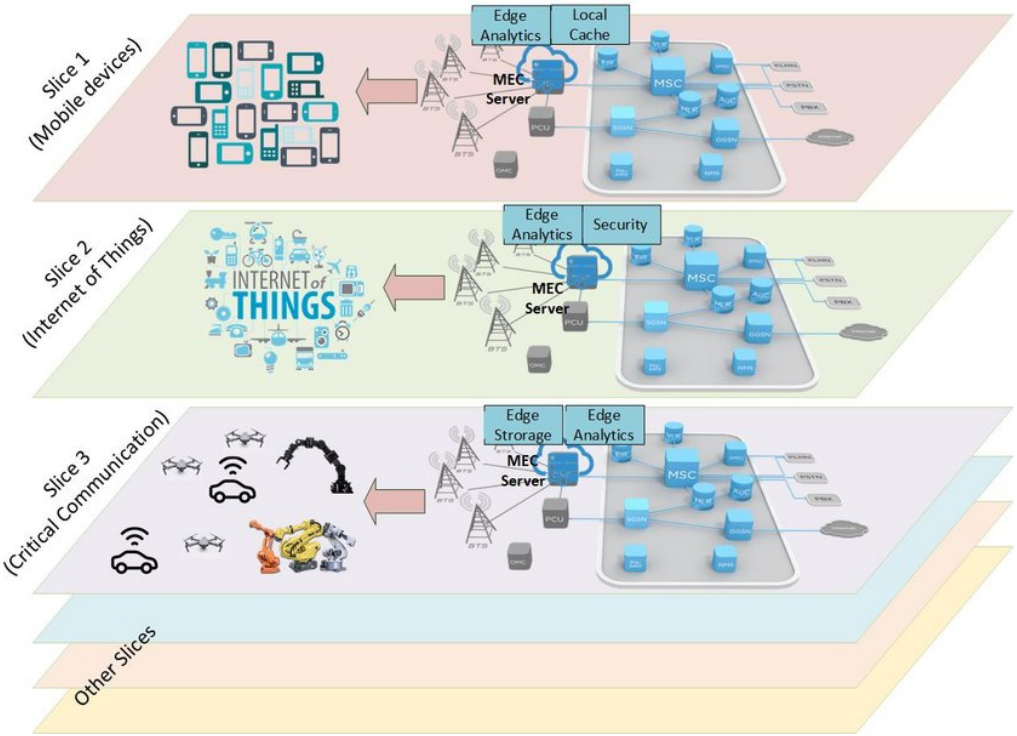

Figure 3.9: *Network slicing* nel 5G

La realizzazione del *Network Slicing* avviene tramite il paradigma del *Software Defined Network* che nella prossima sezione verrà approfondito.

3.5.2 *Software Defined Network* e *Network Functions Virtualization*

Il *Software Defined Network* (SDN) è un paradigma per gestire il *network* in modo efficace. In questo caso il *network* è definito da *Network Functions Virtualization* (NFV), dove intere classi di funzioni sono virtualizzate. Questi sono necessari per interfacciarsi a livello applicativo con i dispositivi cellulari in modo da gestire il traffico della rete in modo efficace[12].

Chapter 4

Attacco Denial of Service

L'attacco di tipo *Denial Of Service* (DOS) consiste nel rendere non disponibili servizi offerti da computer o altri dispositivi [13]. Questo avviene esasperando di richieste la macchina o l'infrastruttura che viene scelta come vittima.

4.1 Vulnerabilità nelle reti cellulari

Le reti cellulari non sono esenti da questo tipo di attacchi, anzi, sono uno degli obiettivi più ambiti poichè essenziali per la vita quotidiana. Sono diversi i componenti che possono essere vulnerabili a un attacco DOS in una rete cellulare. Gli obiettivi identificati come ottimi sono quelli che comportano un maggior utilizzo delle risorse computazionali della rete.
Nelle prossime sezioni verranno illustrate le principali metodologie per fare un attacco di tipo DOS alle reti cellulari[14].

4.1.1 Radio Jamming

Il *Radio Jamming* è una tipologia di attacco DOS che consiste nel disturbare il segnale cellulare emettendo delle onde radio. La realizzazione di questo tipo di attacco è molto semplice, basta procurarsi un trasmettitore che invia segnali ad alta energia nella banda cellulare di riferimento.
Un miglioramento del classico *radio jamming* è lo *smart jamming* che consiste nel saturare uno o più canali di comunicazione della rete. Questo fa sembrare il *network* non disponibile a tutti gli utenti collegati a quella determinata cella.

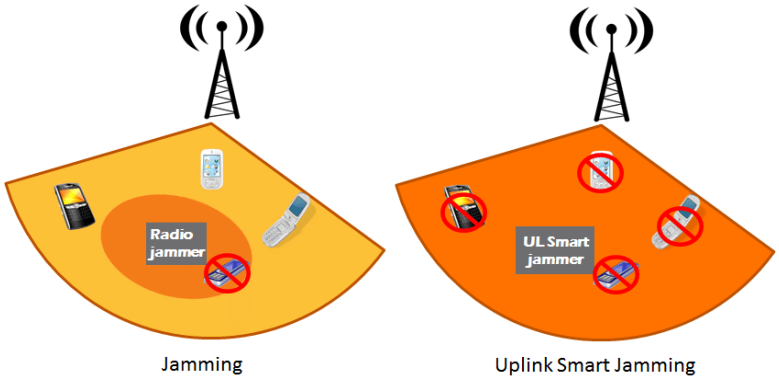

Figure 4.1: *Radio* e *smart jamming*[14]

4.1.2 Vulnerabilità di sistema

Un altro classico modo per creare un interruzione di sistema in una rete cellulare è sfruttando le classiche vulnerabilità che si presentano spesso in qualsiasi tipo di computer. Questo ovviamente perchè tutta l'architettura di una rete cellulare non è altro che *server* con specifiche particolari.

4.1.3 Botnet

La *botnet* è sicuramente una delle tipologie più diffuse, ed è il modo con cui si realizzano i *Distributed Denial Of Service* (DDOS). L'attaccante, in questo caso, dispone del controllo di un grande numero di dispositivi infettati da *malware* che li rendono essere controllabili da remoto per esasperare di richieste un determinato servizio.

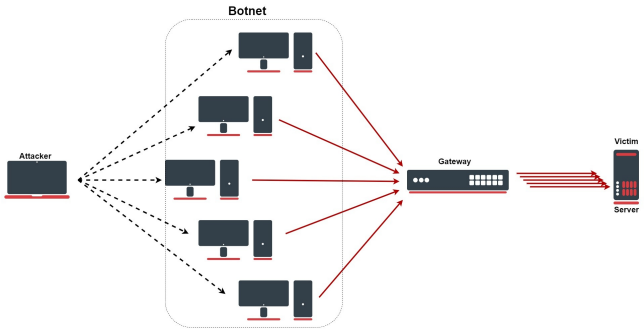

Figure 4.2: *Distributed denial of service*

4.1.4 Autenticazione

Questo è uno degli attacchi più pericolosi poichè le vulnerabilità che sfrutta sono molto difficili da risolvere dato che sono intrinseche nell'architettura del sistema. È la tipologia di vulnerabilità che è stata scelta per confrontare la sicurezza dell'architettura 5G con quelle precedenti. Il suo funzionamento si basa sull'esasperare di richieste di autenticazione i sistemi identificativi delle reti cellulari, che solitamente sono gli elementi con più traffico della rete come la HLR nelle reti 2G/3G.
Questa vulnerabilità si trova nel meccanismo di autenticazione dei dispositivi denominato *Authentication and Key Agreement* (AKA) dove un dispositivo non autenticato forza delle computazioni all'interno del *core network* che consumano più risorse della richiesta stessa[15]. Ad aumentare la pericolosità di questa vulnerabilità vi è la possibilità di creare computazioni nel *core network* senza disporre di una *Subscriber Identity Module* (SIM) valida. Questa tipologia di attacchi, definiti come SIM-less, verranno presi come riferimento per effettuare un attacco DOS alle reti GSM[16] e UMTS[15].

4.2 Misurazione

Per capire quale componente della rete sia il più vulnerabile a un attacco DOS si devono fare delle misurazioni sui vari componenti del *network*. In questo modo è possibile capire in quale punto si possono creare dei rallentamenti o *bottleneck* dovuti a un sovraffollamento di richieste.
In [17] vi è una dettagliata spiegazione di come procedere con queste misurazioni e soprattutto come quantificare il numero di dispositivi che servono all'attaccante per completare l'attacco con successo.
Solitamente le statistiche riguardo alle prestazioni dei componenti del *network* non sono direttamente fornite dagli operatori telefonici quindi bisogna basarsi sui tempi di risposta delle misurazioni. Per esempio, l'immagine seguente mostra i tempi di risposta della HLR in una rete UMTS al comando *location updates*.

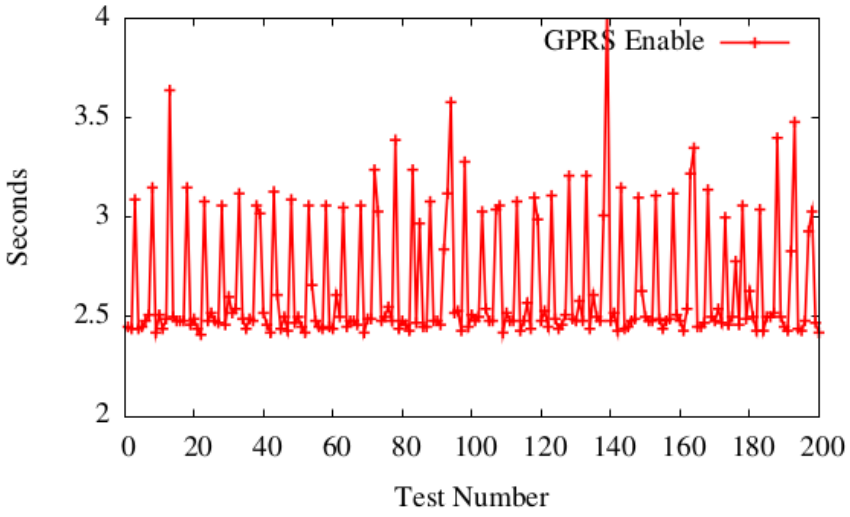

Figure 4.3: Misurazione tempi di risposta HLR con *location updates*[17]

Chapter 5

Sistema di autenticazione

Il meccanismo di autenticazione è la procedura per verificare che un determinato dispositivo sia abilitato a connettersi alla rete. Questo procedimento avviene tramite l'AKA, procedimento in cui il *core network* abilita un dispositivo a connettersi.
In questo capitolo verranno trattate le procedure di autenticazione[18] per le generazioni dal 2G al 5G, il 1G è stato escluso poiché ha un funzionamento completamente analogico.

5.1 2G

Il sistema di autenticazione di seconda generazione utilizza principalmente due codici univoci della SIM e del MS:

- *International Mobile Subscriber Identity* (IMSI) ovvero un codice identificatvo della SIM.
- IMEI ovvero un codice identificativo del MS.

Questi due codici saranno necessari anche per le prossime generazioni fino al 4G.
La procedura di autenticazione di un MS segue questi passaggi:

1. Il MS invia l'IMSI alla BS di riferimento che lo inoltra al *core network*, questo avviene ogni volta che il MS vuole connettersi al *network* e non risulta già registrato presso la rete di riferimento. In caso lo fosse, verrà utilizzato il *Temporary Mobile Subscriber Identity* (TMSI) per preservare il suo anonimato.
2. L'AuC cerca la chiave Ki associata all'IMSI e insieme a un numero casuale RAND genera un codice *Signed Response* (SRES) che verrà salvato nel VLR.
3. Viene inviato al MS il RAND generato.
4. La stessa procedura viene fatta dal MS, che genera quindi il suo SRES e lo invia al VLR.
5. Il VLR confronta se l'SRES ricevuto corrisponde a quello generato dall'AuC, se corrispondono l'autenticazione risulta effettuata con successo.

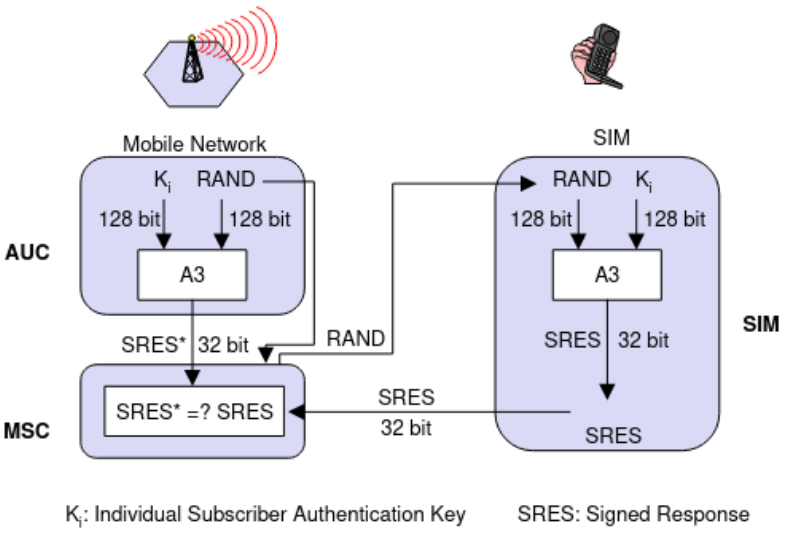

Figure 5.1: Autenticazione nelle reti 2G

5.2 3G e 4G

Dato che l'autenticazione nelle reti 3G e 4G è molto simile, verranno trattate insieme in questa sezione. L'autenticazione nell'architettura di terza e quarta generazione è molto simile a quella della seconda salvo i seguenti miglioramenti:

- Viene introdotta l'autenticazione mutua per prevenire l'autenticazione a false *base stations*.
- La lunghezza della chiave Ki viene incrementata da 64 a 128 bit.
- Viene implementato un flag per verificare se le comunicazioni vengono compromesse durante la trasmissione chiamato *Integrity Key* (IK).

Il procedimento di autenticazione è il seguente[19]:

1. Il MS invia l'IMSI alla BS di riferimento che lo inoltra al *core network*.
2. L'AuC cerca la chiave Ki associata all'IMSI e insieme a un numero casuale RAND genera un codice SRES che verrà salvato nel VLR.
3. Viene trovata la chiave Ki corrispondente all'IMSI dall'AuC, dopodichè viene generato un codice SRES con l'utilizzo di un numero randomico RAND. Inoltre, viene generato un codice *Authentication Token* (AUTN) per permettere al MS di autenticare il *network*.
4. Viene inviato al MS il RAND e AUTN.
5. Il MS autentica il *network* confrontando il valore di AUTN ricevuto. Se il *network* è valido, prosegue con la generazione del SRES.
6. Il VLR confronta se il SRES ricevuto corrisponde a quello generato dall'AuC, se corrispondono l'autenticazione risulta effettuata con successo e viene attribuito il TMSI al MS.

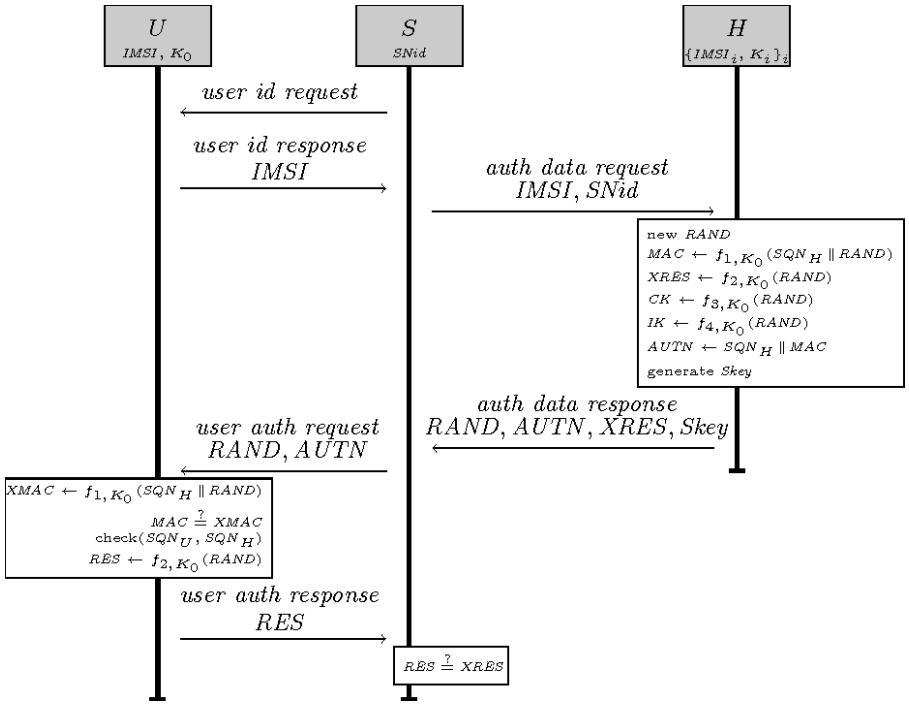

Figure 5.2: Autenticazione nelle reti 3G e 4G

5.3 5G

L'autenticazione della generazione 5G è molto diversa dalle precedenti poichè, come illustrato nella sezione 3.5, l'architettura è completamente rivista diventando una ramificazione di microservizi. Sono definiti tre protocolli di autenticazione:

- 5G-AKA: 5G-*Authentication and Key Management.*
- EAP-AKA: *Extensible Authentication Protocol – Authentication and Key Management.*
- EAP-TLS: *Extensible Authentication Protocol – Transport Layer Security.*

Rispetto alle generazioni precedenti ci sono stati i seguenti miglioramenti di sicurezza[20]:

- L'IMSI non viene mai comunicato in chiaro ma sempre criptato.
- I componenti del *network* coinvolti sono dei servizi.

L'autenticazione è divisa in due parti: La prima è l'inizializzazione dell'autenticazione e la scelta del metodo di autenticazione. La seconda è invece l'autenticazione mutua come avviene nelle generazioni precedenti. Lo schema di autenticazione è il seguente[21]:

1. Il MS invia il *Subscription Concealed Identifier* (SUCI) o 5G-GUTI alla BS di riferimento che lo inoltra al AMF o *Security Anchor Function* (SEAF), il *Globally Unique Temporary Identifier* (GUTI) è un identificativo temporaneo simile al TMSI delle generazioni precedenti, invece il SUCI è un identificatore criptato permanente.
2. il SEAF manda l'identificatore del dispositivo (SUCI o 5G-GUTI) e il *Serving Network Name* (SNN) all'AUSF. Il SNN è una concatenazione di codici identificativi di servizi e il codice identificativo del *serving network*. Serve per capire a quale *slice* vuole connettersi il dispositivo.
3. L'AUSF controlla che la richiesta dal SEAF sia autorizzata a utilizzare il SNN, in caso non lo fosse risponde con un apposito messaggio di errore.
4. L'AUSF reperisce la chiave associata all'identificativo nell'archivio UDM e genera il rispettivo SRES con un numero randomico RAND.
5. Viene inviato all'MS il RAND e AUTN (per l'autenticazione mutua).
6. Il MS procede con la creazione del SRES e lo invia al SEAF.
7. Il SEAF inoltra il SRES all'AUSF che si occupa di controllare se corrispondono e in caso confermare l'autenticazione.

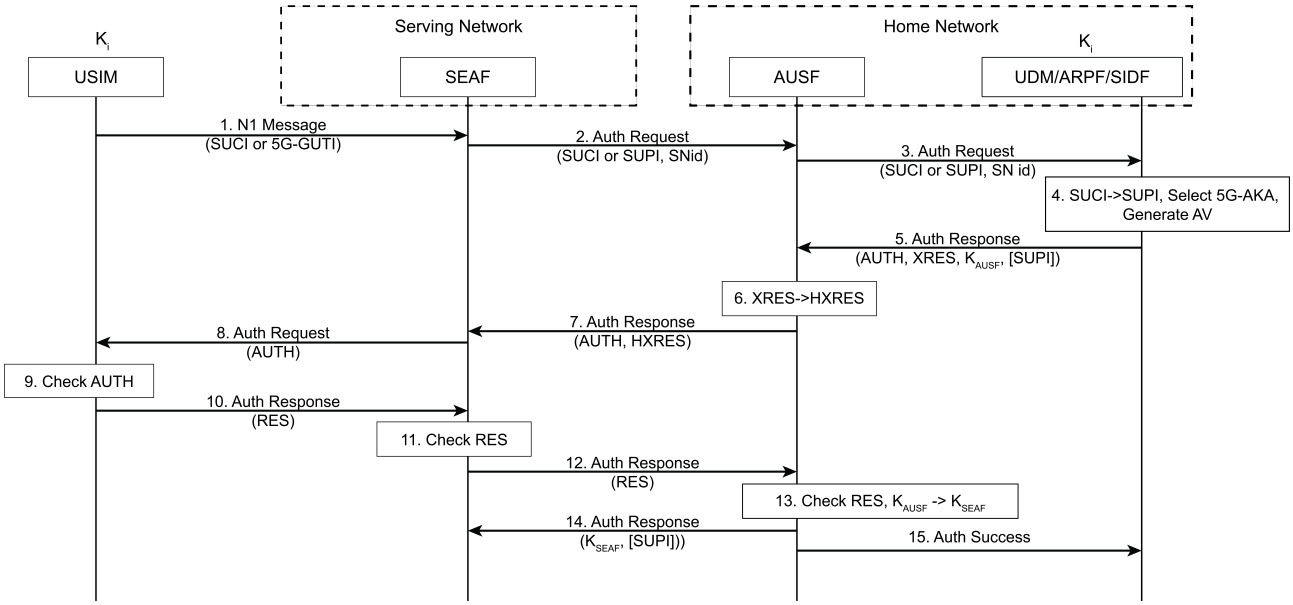

Figure 5.3: Autenticazione nelle reti 5G

Chapter 6

Attacco all'autenticazione delle reti 2G-4G

Le reti cellulari dal 2G al 4G condividono lo stesso schema architetturale, per questo gran parte delle vulnerabilità che vengono utilizzate negli attacchi di tipo *denial of service* sono comuni. Ci sono numerosi modi per effettuare un attacco DOS all'autenticazione, alcuni già accennati nella sezione 4.1.4, in questo capitolo verranno messe in pratica nelle reti 2G fino al 4G.
Fondamentalmente, in modo da creare un *denial of service* nel *core network* di una rete cellulare tramite una richiesta di identificazione bisogna forzare la computazione dei vettori di autenticazione in modo tale da fare sprecare risorse computazionali all'infrastruttura cellulare. Nel momento che un dispositivo si collega alla rete cellulare si possono verificare le seguenti casistiche:

- Se il dispositivo ha una SIM valida inizio la procedura di autenticazione.
- Se il dispositivo non ha una SIM valida inizio la procedura di autenticazione ma senza consumare abbastanza risorse del *network*.
- Se il dispositivo non ha una SIM la procedura di autenticazione non viene iniziata.

Quindi, è chiaro che per effettuare un DOS al sistema di autenticazione degli utenti è necessario disporre o simulare dei dispositivi con delle SIM valide. La validità della SIM è in primo luogo controllata dalla presenza di un IMSI valido come spiegato nella sezione precedente. Di seguito verranno trattate le principali metodologie per effettuare un DOS al sistema di autenticazione.

6.1 Botnet

Il metodo più conosciuto per creare un *denial of service* a una rete cellulare è tramite una *botnet*. In questo modo, l'attaccante ha a disposizione un elevato numero di dispositivi con SIM valida che hanno la possibilità di effettuare massivamente una procedura di autenticazione causando delle dispendiose computazioni all'interno del *network*.
In [17] è descritto come effettuare un DDOS a una rete cellulare di tipo 2G/3G in modo da esasperare di richieste il suo componente più critico: l'HLR. Con 11750 dispositivi infettati è possibile degradare le performance della HLR del 93%[17], garantendo quindi un quasi totale malfunzionamento dell'infrastruttura.
Questa tipologia di attacco è molto pericolosa, e spesso anche la più comune, non è pero esente da diverse problematiche: prima di tutto risulta facilmente rilevabile da un sistema di monitoraggio della rete. Inolte, è richiesto un numero molto elevato di dispositivi, sopratutto se si tiene presente che questi devono appartenere alla stessa zona di competenza della HLR.

6.2 IMSI *catching*

Un metodo alternativo all'utilizzo di una *botnet* è avere a disposizione un *database* di IMSI rubati per effettuare un *flooding* di richieste di autenticazione.
Dato che nelle reti 2G-4G l'IMSI viene trasmesso in chiaro al momento dell'autenticazione, riuscire a ottenerli è abbastanza semplice. In [22] vengono citati i modi più comuni per appropriarsene per poi utilizzarli in un attacco.

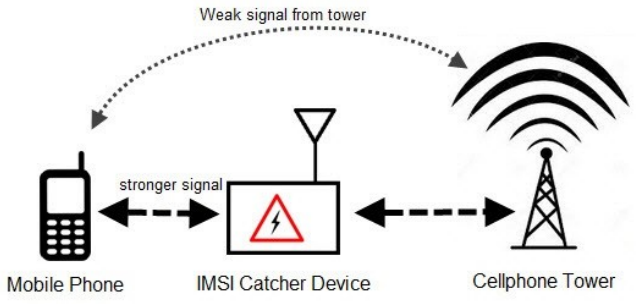

Figure 6.1: Strumento per rubare IMSI

Per rubare l'IMSI si mette in pratica un attacco di tipo *Man In The Middle* (MITM), intromettendosi nella comunicazione fra il MS e la BS.
Nelle reti di seconda generazione questo risulta molto semplice poichè, come spiegato nella sezione 5.1, l'IMSI viene trasmesso in chiaro se il MS è la prima volta che si connette al registro di quella specifica zona. Inoltre, dato che nel GSM l'autenticazione non è mutua è possibile creare una *fake basestation* e collezzionare tutti gli IMSI dei dispositivi che si connettono. Sono stati introdotti diversi identificativi temporanei come il TMSI per fare in modo che l'IMSI non debba essere inviato in ogni procedura di autenticazione, ma sono tutti facilmente raggirabili poichè cambiano con una frequenza troppo bassa.
In [23] viene illustrato un metodo per ottenere gli IMSI di qualsiasi dispositivo nello standard UMTS nonostante l'autenticazione mutua. Infatti viene spiegato come basti mandare al MS una *user identity request* impersonan-

dosi la VLR e il MS risponderà con il proprio IMSI in chiaro.

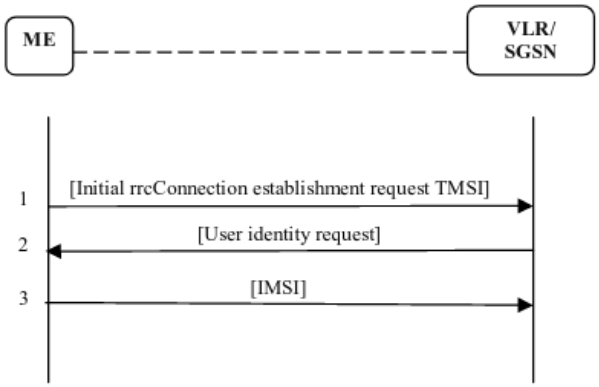

Figure 6.2: IMSI *catching* nelle reti UMTS[23]

6.3 Attacco alle reti con dispositivi SIM-less

In [15] e [16] sono descritti degli attacchi all'autenticazione degli utenti utilizzando dispositivi senza una SIM commerciale, ma bensì delle interfacce di comunicazione programmabili. Questo è stato fatto perchè utilizzare dei MS come dispositivi per effettuare un attacco DOS rappresenta un fattore limitante in termini di prestazioni. Infatti, i sistemi operativi dei MS impongono degli intervalli di tempo fra una richiesta e un'altra.
Entrambi gli attacchi dimostrano che è possibile causare un DOS con un numero di dispositivi senza SIM molto minore rispetto allo stato dell'arte.

6.3.1 GSM

É stato necessario analizzare la rispettiva *air interface* del GSM per valutare quale è il numero massimo di richieste di autenticazione che possono essere inviate al secondo a una *base station*. Questa misurazione risulta di fondamentale importanza poichè riesce anche a fornire il numero necessario di dispositivi per raggiungere il massimo delle *Transation Per Second* (TPS). Nell'immagine seguente vengono illustrati i messaggi e i canali in cui viaggiano durante l'autenticazione alla rete GSM.

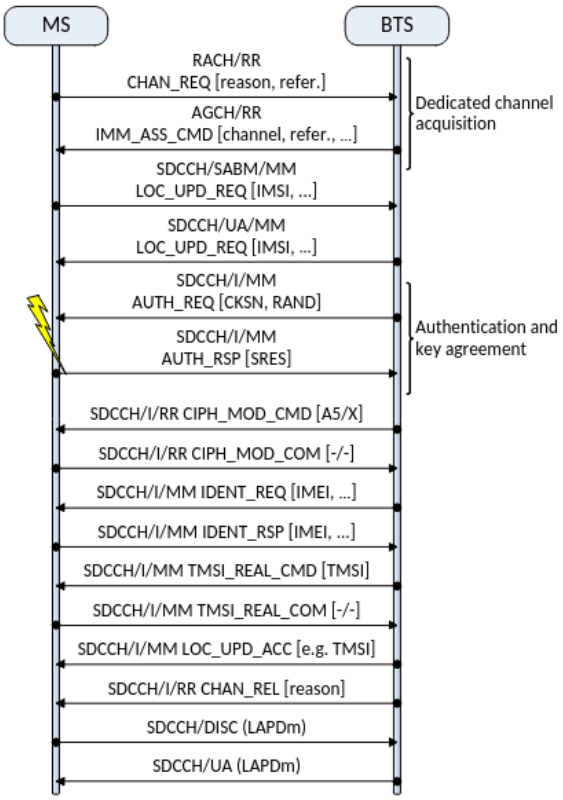

Figure 6.3: Messaggi scambiati durante l'autenticazione in una rete GSM[16]

6.3.2 UMTS

L'immagine seguente rappresenta un semplice schema del dispositivo con SIM programmabile per effettuare un DOS a una rete UMTS[15].

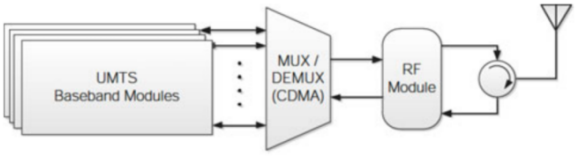

Figure 6.4: Dispositivo per l'attacco DOS alle reti UMTS[15]

Come è stato fatto per la rete GSM, è stato necessario analizzare l'*air interface* dell'UMTS per valutare il numero di TPS. Nell'immagine seguente vengono illustrati i messaggi e i canali in cui viaggiano durante l'autenticazione alla rete UMTS.

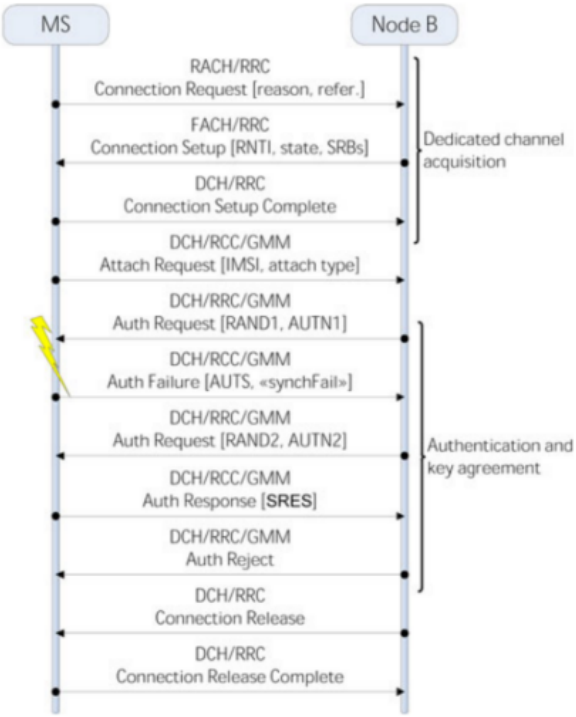

Figure 6.5: Messaggi scambiati durante l'autenticazione in una rete UMTS[15]

Nelle reti UMTS è stato calcolato che il limite più stringente di TPS durante la comunicazione con la *base station* è dato dal canale *Forward Access Channel* (FACH) con 28 TPS. Questo, ha portato a concludere che bastano 446 dispositivi per effettuare una notevole degradazione del sistema, molti di meno rispetto degli 11K necessari per una *botnet*[23].

Nello stesso articolo è spiegato come è possibile duplicare le prestazioni dell'attacco usando delle SIM valide. In questo modo infatti, i vettori di autenticazione vengono generati una seconda volta se si segnala al *network* che l'AUTN calcolato non risulta corretto.

Chapter 7

Attacco all'autenticazione delle reti 5G

In questa sezione verranno trattate le vulnerabilità riguardo un attacco di tipo DOS all'autenticazione delle reti 5G. Questa generazione ha risolto alcune delle probematiche legate all'autenticazione, come per esempio a differenza del 4G, l'identificatore del MS viene criptato con la chiave pubblica prima di essere inviato al *core network*, evitando così di poter essere intercettato e rubato[20]. Però, con il grande aumento di dispositivi connessi nel mondo dell' IOT, gli attacchi DOS saranno senz'altro più semplici da realizzare.
I SDN e NFV, componenti fondamentali per garantire le eccezionali prestazioni del 5G, potrebbero essere un efficace strumento di monitoraggio per identificare possibili attacchi come spiegato in [24].
Allo stesso tempo però, la centralizzazione del controllo del *network* con un SDN e NFV crea le condizioni ottimali per effettuare un attacco DOS con successo[25].
Questa tipologia di attacchi, che ha lo scopo di creare una interruzione del servizio, assume una pericolosià maggiore in questa generazione. Infatti, il mondo dell'IOT e delle *smart cities* comprendono ambiti molto sensibili come per esempio la telemedicina.

7.1 IMSI *catching*

Come anticipato, l'avanzamento più importante in termini di sicurezza che questa nuova generazione ha apportato è sicuramente la trasmissione dell'identificativo del MS in forma criptata. Questa innovazione ha reso molto più difficile la pratica dell'IMSI *catching* trattata nella sezione 6.2, fondamentale per effettuare un attacco DOS.

Realisticamente però bisogna sottolineare che questa pratica non risulta completamente debellata. Infatti, tutte le nuove reti 5G, come è stato anche per le generazioni precedenti, devono essere retro compatibili, e quindi per un non determinato lasso di tempo devono essere supportate le procedure degli *standard* precedenti che, come spiegato nel capitolo precedente, soffrono di questa vulnerabilità.

In [26] viene illustrato un metodo per effettuare un attacco *Man In The Middle* (MITM) nelle reti 5G in modo da ottenere l'IMSI criptato dell'utente: il SUCI. Questo metodo però non sarebbe applicabile per effettuare una raccolta di identificativi per poi effettuare un attacco DOS poichè il SUCI viene rigenerato dopo ogni utilizzo.

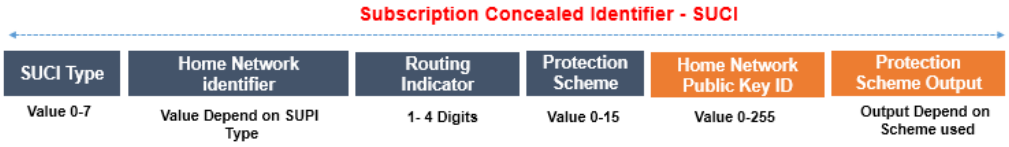

Figure 7.1: Composizione del SUCI nel 5G

7.2 Replicazione dell'attacco SIM-less

Alla base degli attacchi trattati nella sezione 6.3 vi è la costruzione di un *database* di IMSI. Questo *database* può essere agevolmente costruito nelle generazioni precedenti al 5G tramite le tecniche di IMSI *catching* trattate in 6.2. Nel 5G risulta molto più difficile creare un archivio di IMSI poichè questi viaggiano in forma criptata nella rete, ovvero comunicando il SUCI.

Tuttavia, se si riuscisse a ottenere comunque un *database* di IMSI rubati si potrebbe ottenere un attacco dello stesso tipo di [16] e [15] con prestazioni migliori perchè il nuovo protocollo 5G NR[27] per l'*air interface* è stato progettato per supportare il *Massive Machine Type Communications* ovvero l'IOT massivo che richiede latenze molto basse e capacità molto alte. Per questo, sicuramente le capacità dei canali di comunicazione durante la procedura di autenticazione avrebbero un valore di TPS molto alto, sufficiente a causare un notevole degradamento delle prestazioni.

7.3 Nuove vulnerabilità

L'implementazione del SUCI e *Subscription Permanent Identifier* (SUPI) ha risolto, o quantomeno reso molto più complicata la pratica dell'IMSI *catching*. Allo stesso tempo però ha incrementato il dispendio di risorse durante l'autenticazione di un dispositivo. Infatti, prima della generazione dei vettori di autenticazione vengono innestate delle procedure per decriptare il SUCI con un algoritmo detto *Elliptic Curve Integrated Encryption Scheme* (ECIES). Questa procedura aumenta inevitabilmente la creazione di possibili DOS all'autentcazione. In [28] è descritto un protocollo che permetterebbe di controllare fin dal primo momento se il MS ha un SUCI valido senza incorrere nella decriptazione.

Chapter 8

Conclusioni

In questo documento sono state analizzate le più comuni vulnerabilità che consentono di effettuare un attacco di tipo *denial of service* alle reti cellulari. In particolare, sono state analizzate le vulnerabilità nelle autenticazioni di tutte le generazioni.
Dopo un'attenta analisi dei meccanismi di autenticazione e delle classiche vulnerabilità che vengono usate nelle generazioni 2G-4G, si può finalmente fare un confronto fra la sicurezza dell'ultima generazione 5G e quelle precedenti.
Il 5G ha sicuramente apportato dei consistenti miglioramenti di sicurezza, come ampiamente trattato riguardo la cifratura dell'IMSI.
Nonostante ciò, è innegabile che in questa ultima generazione gli attacchi DOS saranno molto più semplici da realizzare, ma sopratutto più pericolosi dati i compiti sensibili che alcuni dispositivi connessi a questa rete dovranno svolgere.

Bibliografia

[1] Orestis Evangelatos and José DP Rolim. "An Airborne Wireless Sensor Network for Ambient Air Pollution Monitoring". In: *SENSORNETS* (2015), pp. 231–239.

[2] Zhiwen Hu et al. "UAV Aided Aerial-Ground IoT for Air Quality Sensing in Smart City: Architecture, Technologies, and Implementation". In: *IEEE Network* 33.2 (2019), pp. 14–22. DOI: 10.1109/MNET.2019.1800214.

[3] Qijun Gu and Chunrong Jia. "A Consumer UAV-based Air Quality Monitoring System for Smart Cities". In: *2019 IEEE International Conference on Consumer Electronics (ICCE)*. 2019, pp. 1–6. DOI: 10.1109/ICCE.2019.8662050.

[4] Massimo Condoluci and Toktam Mahmoodi. "Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges". In: *Computer Networks* 146 (Sept. 2018). DOI: 10.1016/j.comnet.2018.09.005.

[5] Fredrick Njoroge and Lincoln Kamau. "A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G". In: (Nov. 2018).

[6] 3gpp. *Global System for Mobile Communications*. URL: https://www.3gpp.org/specifications/gsm-history.

[7] 3gpp. *General Packet Radio Service / Enhanced Data rates for Global Evolution*. URL: https://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge.

[8] M. Rahnema. "Overview of the GSM system and protocol architecture". In: *IEEE Communications Magazine* 31.4 (1993), pp. 92–100. DOI: 10.1109/35.210402.

[9] 3gpp. *High Speed Packet data Access*. URL: https://www.3gpp.org/technologies/keywords-acronyms/99-hspa.

[10] 3gpp. *Long Term Evolution*. URL: https://www.3gpp.org/technologies/keywords-acronyms/98-lte.

[11] Larry Peterson and Oguz Sunay. *5G Mobile Networks: A Systems Approach*. URL: https://github.com/SystemsApproach/5G.

[12] Alcardo Alex Barakabitze et al. "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges". In: *Computer Networks* 167 (2020), p. 106984. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2019.106984. URL: https://www.sciencedirect.com/science/article/pii/S1389128619304773.

[13] Kevin Hattingh et al. "DoS! Denial of Service". In: ().

[14] Roger Piqueras Jover. "Security attacks against the availability of LTE mobility networks: Overview and research directions". In: (Jan. 2013), pp. 1–9.

[15] Alessio Merlo et al. "A Denial of Service Attack to UMTS Networks Using SIM-Less Devices". In: *IEEE Transactions on Dependable and Secure Computing* 11.3 (2014), pp. 280–291. DOI: 10.1109/TDSC.2014.2315198.

[16] Nicola Gobbo, Alessio Merlo, and Mauro Migliardi. "A Denial of Service Attack to GSM Networks via Attach Procedure". In: (Sept. 2013). DOI: 10.1007/978-3-642-40588-4_25.

[17] Patrick Traynor. "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core". In: (2009).

[18] Prajwol Kumar Nakarmi. "Cheatsheets for Authentication and Key Agreements in 2G, 3G, 4G, and 5G". In: (2021). arXiv: 2107.07416 [cs.CR].

[19] Cristina-Elena Vintilă, Victor-Valeriu Patriciu, and Ion Bica. "Security Analysis of LTE Access Network". In: Jan. 2011.

[20] *A Comparative Introduction to 4G and 5G Authentication.* URL: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication.

[21] David Basin et al. "A Formal Analysis of 5G Authentication". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Jan. 2018). DOI: 10.1145/3243734.3243846. URL: http://dx.doi.org/10.1145/3243734.3243846.

[22] Hamad Alrashede and Riaz Ahmed Shaikh. "IMSI Catcher Detection Method for Cellular Networks". In: (2019), pp. 1–6. DOI: 10.1109/CAIS.2019.8769507.

[23] Muzammil Khan, Attiq Ahmed, and Ahmad Raza Cheema. "Vulnerabilities of UMTS Access Domain Security Architecture". In: (2008), pp. 350–355. DOI: 10.1109/SNPD.2008.78.

[24] Mathias Kjolleberg Forland et al. "Preventing DDoS with SDN in 5G". In: (2019), pp. 1–7. DOI: 10.1109/GCWkshps45667.2019.9024497.

[25] M Awais Javed and Sohaib khan Niazi. "5G Security Artifacts (DoS / DDoS and Authentication)". In: (2019), pp. 127–133. DOI: 10.1109/COMTECH.2019.8737800.

[26] Merlin Chlosta et al. "5G SUCI-Catchers: Still Catching Them All?" In: WiSec '21 (2021), pp. 359–364. DOI: 10.1145/3448300.3467826. URL: https://doi.org/10.1145/3448300.3467826.

[27] Erik Dahlman and Stefan Parkvall. "NR - The New 5G Radio-Access Technology". In: (2018), pp. 1–6. DOI: 10.1109/VTCSpring.2018.8417851.

[28] Ikram Gharsallah, Salima Smaoui, and Faouzi Zarai. "A Secure Efficient and Lightweight authentication protocol for 5G cellular networks: SEL-AKA". In: (2019), pp. 1311–1316. DOI: 10.1109/IWCMC.2019.8766448.