République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou (UMMTO)

Faculté de Génie Electrique et Informatique

Département d'Electronique

Mémoire de Fin de cycle

En vue de l'obtention du Diplôme de Master Académique

Domaine : Sciences et Technologies

Filière : Télécommunication

Spécialité : Réseaux et Télécommunications

Thème :

Sécurité des réseaux 4G/LTE

Encadré par : Réalisé par :

MrLAHDIR Mourad **MrDIALLO MamadouLamine**

Mr TAKOUCHE Karim

2017/2018

Remerciements :

Tout d'abord, nous remercions le bon Dieu qui nous a éclairé sur le chemin du savoir et nous a donné la patience, la volonté et le courage nécessaire à la réalisation de ce projet.

Nous tenons aussi, à remercier l'Université Mouloud Mammeri de Tizi-Ouzou, de nous avoir accueillis en son sein pour y passer nos études universitaires.

Nos reconnaissances les plus vifs vont à l'endroit de tous nos enseignants pour leur sérieuse collaboration et leur disponibilité totale et entière pendant tout notre cycle de formation, plus particulièrement ceux du département d'électronique.

Aussi, nous tenons à adresser nos vifs et sincères remerciements à notre encadreur M. **M.LAHDIR Mourad**pour son aide précieuse, ses conseils judicieux, et son implication ainsi que ses remarques objectives.

Nous remercions également les membres du jury pour avoir accepté de juger ce travail, et pour l'attention qu'ils apporteront à sa lecture.

Enfin, nous tenons à remercier toutes les personnes qui nous ont aidées de près ou de loin pour l'élaboration de notre travail.

Dédicace

Je dédie ce projet à :

Mon père qui est ma source d'inspiration illimitée. Celui qui a toujours été là pour moi, tu n'as vraiment ménagé aucun effort pour me permettre d'atteindre mes objectifs. Merci pour ton écoute, ton sacrifice, ta patience, ta persévérance, ton don de soi. Je ne t'oublierai jamais.

Ma chère et tendre mère, qui est la présence dans l'absence. Toi qui ne peux assister, ni partager cette réussite, à cette étape de ma vie. Sache que je te porte au plus profond de mon cœur. Que la lumière divine soit avec toi. Repose en Paix.

A tous les enseignements de l'école fondamentale privée le « Kaarta », et ceux du lycée de Diéma. Merci pour la qualité de vos enseignements.

Mes frères, mes sœurs, mes oncles, mes tantes, mes cousins, mes cousines, et mes amis, ainsi que tous ceux qui de prêt ou de loin m'ont aidé et ainsi contribue à la réalisation de cet objectif.

Pour terminer, une dédicace spéciale à mes amis de cœur **Lasseni COULIBALY**, **Rokia DIALLO**, **Ousmane SOKONA**, d'avoir été toujours là pour moi. Ainsi qu'à mon binôme **Karim TAKOUCHE**pour son implication quant à la réussite de ce projet.

DIALLO Mamadou Lamine

Dédicace

Ce mémoire est dédié à :

Mes parents. Eux qui ont toujours été là pour moi. Sachez que sans vous, rien n'aurait pu être possible. Dieu vous protège toujours.

Mes frères et mes sœurs. Que le tout puissant vous garde unis pour la vie.

Ma famille et mes amis. Merci pour votre présence.

Mon binôme **Mamadou Lamine DIALLO**.

TAKOUCHE Karim

Résumé

Nul n’est sans le savoir que nous nous trouvons dans un monde où, il y a un énorme problème de sécurité dans les systèmes d’information et les réseaux 4G/ LTE. Les chercheurs en sécurité ont découvert un ensemble de vulnérabilités sévères dans le protocole 4G/LTE qui pourraient être exploitées pour espionner les appels téléphoniques et les messages texte des utilisateurs, envoyer de fausses alertes d’urgence, usurper l’appareil et même déconnecter complètement les appareils.

L’objectif recherché dans ce mémoire est de permettre au lecteur, familiarisé avec les systèmes d’information et les réseaux 4G/LET, d’acquérir un ensemble de connaissances sur la sécurité qui lui permettront de mieux comprendre les divers mécanismes permettant de protéger les systèmes d’information et les réseaux 4G/LTE contre les principaux risques de piratage et d’intrusion.

Pour cela, nous traitons les faiblesses de la sécurité EPS et surtout les vulnérabilités du protocole EPS-AKA de 3 GPP qui constitue la pierre angulaire de toute l’architecture de sécurité et qui permet l’accès des abonnés au réseau. Après, nous étudions les protocoles existants dans la littérature qui amélioreront la sécurité en EPS. Pour terminer nous proposons un protocole qui apporte un jeu d’améliorations afin de résoudre tous les problèmes et les faiblesses identifiés dans l’EPS et les autres protocoles étudiés.

Sommaire

Listes des figures

Chapitre 1 :

Chapitre 2 :

Chapitre 3 :

Chapitre 4 :

Liste des tableaux

Liste des sigles

1G 1ère Génération

2G 2ème Génération

3G 3ème Génération

4G 4ème Génération

5G 5ème Génération

3GPP 3rd Generation Partnership Project

A

ACK Acknowledgement.

AKA Authentication and Key Agreement.

APN Access Point Name.

AS Access Stratum.

ASN.1 Abstract Syntax Notation 1.

AUC AUthentification Center.

AUTN AUthentication Token for The Network.

AV Authentication Vector.

B

BG Border Gateway.

BSC Base Station Controller.

BSS Base Station Subystem.

BTS Base Transceiver Station.

C

CDMA Code Division Multiple Access.

CK UMTS Confidentiality Key.

CM Connection Management.

CS Circuit Switched.

D

DL Down Link.

E

EDGE Enhaced Data Rates for GSM Evolution.

EEA EPS Encryption Algorithm.

EIA EPS Integrity Algorithm.

EIR Equipment Identity Register.

EMM EPS Mobility Management.

eNodeB evolved NodeB.

EPC Evolved Packet Core.

EPS Evolved Packet System.

ESM EPS Session Management.

ETSI European Telecommunications Standards Institute.

eUTRAN evolved UTRAN.

F FDD Frequency Division Duplex.

G GEA GPRS Encryption Algotithm.

GGSN Gateway GPRS Support Node.

GMM GPRS Mobility Management.

GMSC Gateway MSC.

GPRS General Packet Radio Service.

GSM Global System for Mobile communication.

GUTI Globaly Unique Tomporary Identity.

H

HLR Home Location Register.

HSDPA High Speed Downlink Packet Access.

HSPA High Speed Packet Access.

HSS Home Suscriber Service.

HSUPA High Speed Uplink Packet Access.

I ID Identifiant.

IEEE Institue of Electrical and Electronics Engineers.

IK UMTS Integrity Key.

IMEI International Mobile Equipement Identity.

IMS IP Multimedia Subsystem.

IMSI International Mobile Subscriber Identity.

IP Internet Protocol.

K

K ASME Access Security Management Entity key.

KC GSM Confidentiality key.

K EnbeNodeB master key.

KI GSM Integrity key.

K NASenc Non-Access Stratum Confidentiality key.

K NASint Non-Access Stratum Integrity key.

K RRCenc Radio Ressouce Control Confidentiality key.

K RRCint Radio Ressouce Control Integrity key.

L

LTE Long Term Evolution.

LTE-A Long Term Evolution Advenced.

M

MAC Message Authentication Code

MCC Mobile Country Code

MCS Modulation and Coding scheme

ME Mobile Equipment

MIMO Multiple-Input Multiple-Output

MME MobilityManagementEntity

MNC Mobile Network Code

MS Mobile Station

MSC Mobile Switching Center

MSISDN Mobile Station Integrated Services Digital Network Number

N

NAS Non-Access Stratum.

NMC Network and Management Center.

NS-2 Network Simulator 2.

NS-3 Network Simulator 3.

NSS Network Sub-System.

O

OFDMA Orthogonal Frequency Division Multiple Access.

OMC Operations and Maintenance Center.

OSS Operation Sub-System.

P

PCI Physical Cell Identity

PCRF Policy Control and Charging Rules Functions

PDCP Packet Data Convergence Protocol

PDN Packet Data Network

PDN GW PDN Gateway

PDU Protocol Data Unit

PEK Permanent Encryption Key

PID Packet Identifier

PIK Permanent Integrity Key

PIM Protocol Independent Multicast

PIN Personal Identification Number

PKH Public Key of HSS

PKI Public Key Infrastructure

PKM Public Key of MME

PKU Public Key of UE

PN Packet Number

PRNG Pseudo Random Number Generator

Q

QoS Quality of Service.

R

RAC Radio Admission Control.

RAND RANDom value.

RES RESponse.

RNC Radio Network Controller.

RNIS Réseau Numérique à Intégration de Services.

RRC Radio Ressource Control.

RTC Réseau Téléphonique Commuté.

RTCP Real-time Transport Control Protocol.

S

SAE System Architecture Evolution.

SAD Security Association Database

SAE System Architecture Evolution

SDO Standards Development Organizations

SE-AKA Security Enhanced-AKA

SEULE Secured EULE

SGW Serving Getway

SGSN Serving GPRS Support Node

T

TAI Tracking Area Identifier

TAU Tracking Area Update

TEK Transient Encryption Key

TIK Temporary Integrity Key

TIK Transient Integrity Key

TK Transient Key

TLKH Two-Tiered LKH

TLS Transport Layer Security

TMSI Temporary Mobile Subscriber Identity

TNK Total Number of Keys

TR Technical Report

TS Technical Specification

TTP Trusted Third Party

U

UE User Equipment

UEA UMTS Encryption Algorithm

UESecCapab UE Security Capabilities

UIA UMTS Integrity Algorithm

UICC Universal Integrated Circuit Card

UK Unique Key

ULE Unidirectional Lightweight Encapsulation

ULE Sec-ID ULE Security Identifier

UMEK UE-MME shared Encryption Key

UMIK UE-MME shared Integrity Key

UMTS Universal Mobile Telecommunications System

UP User Plane

USIM Universal Subscriber Identity Module

V

VID Vendor ID

VLR Visitor Location Register

VOIP Voice Over IP

VPN Virtual Private Networks

XMAC-I Expected MAC-I

XRES Expected Response

Introduction générale

En un laps de temps de deux décennies, les réseaux mobiles et sans fil ont connu un grand envol au cours de ces dernières années. Il s'agit entre autre d'un prolongement de nombreuses générations successives de réseaux de télécommunications totalement dédiés à la téléphonie (2G, GSM), puis plus orientés vers le multimédia (3G, UMTS). Les réseaux locaux sans fil sont rentrés dans la vie quotidienne au travers de standards phares tels que Wifi, Bluetooth, etc.

La future génération de réseaux mobiles sans fil dite de quatrième génération apporte un réel tournant dans le fonctionnement et la disparité des solutions existantes. Les réseaux mobiles LTE (Long Term Evolution) sont également déployés à travers le monde. Ils utilisent la commutation complète de paquets et le protocole IP, contrairement aux itérations précédentes du réseau mobile, ce changement de la commutation de circuit à la commutation de paquet permet de nouvelles attaques qui n'étaient pas possible auparavant.Certaines implémentations de réseaux LTE et d'applications mobiles sont actuellement vulnérables à plusieurs échelles. Ils peuvent entraîner une perte de confidentialité, une facturation incorrecte et une falsification de données. C'est ce qui nous pousse à nous demander comment sécuriser les réseaux LTE à travers les mécanismes de sécurité : l'authentification, le chiffrement et la confidentialité ; permettant de protéger les systèmes d'information et les réseaux 4G/LTE contre les principaux risques de piratage et d'intrusion.

A travers cette problématique en ressort un certain nombre de questions comme :
Quelles sont les différentes générations de téléphonies mobiles ?
Quelles sont les spécificités et les technologies dans les réseaux 4G/LTE ?
Qu'est-ce qui menace la sécurité des réseaux 4G/LTE ?
Comment protéger et améliorer la sécurité des réseaux 4G/LTE ?

Dans le but, de pouvoir apporter des éléments de réponses à ces questions, nous avons répartis notre travail en quatre chapitres.

Dans le premier chapitre, nous introduisons les différentes générations pour mieux comprendre la suite du travail. Le deuxième chapitre est consacré à la présentation de la 4G/ LTE. Vue qu'une grande partie de notre projet est focalisé sur la sécurité du réseau de la quatrième génération (réseau 4G/LTE), nous allons consacrer le troisième chapitre aux mécanismes de sécurité du réseau 4G/LTE. Ensuite dans le quatrième chapitre nousétudions les faiblesses de la sécurité du protocole EPS, dans l'optique de proposer des solutions pour ces différentes faiblesses avec un coût minimal et une meilleure QOS.

Nous terminons notre mémoire par une conclusion ainsi que par des perspectives.

Chapitre 1 : Généralité sur la Téléphonie Mobile

1.1 Historique

Il est important de noter que le développement des réseaux mobiles a eu une forte croissance à travers plusieurs générations (1G, 2G, 3G, 4G). Elles ont doncœuvré pour augmenter le débit afin d'accroitre la bande passante.

En 2005, la technologie de transmission OFDMA (Orthogonal frequency-division multiple Access) est choisi comme candidat pour la liaison descendante HSOPA, rebaptisée plus tard 3GPP Long Term évolution (LTE) de l'aire l'interface E-UTRA. En novembre 2005, KT démontre le service mobile WiMAX à Busan, Corée du sud.

La société japonaise NTT DoCoMo (Nippon Telegraph et téléphone) a testé, en février 2007, un prototype de communication 4G système MIMO 4x4 appelé VSF-OFCDM à 100 Mbit/s tout en se déplaçant, et 1Gbit/s à l'arrêt.

En décembre 2009 sprint a commencé à annoncer ''4G'' de service dans certaines ville des États-Unis, en dépit de la moyenne des vitesses de téléchargement de seulement 3-6 Mbit/s avec un une vitesse de pointe de 10 Mbit/s (pas disponible sur tous les marchés).

Le 25 février 2010, l'Estonie a ouvert EMT LTE ''4G'' travail en réseau dans le régimed'essai.

Le 5 juin 2010 Sprint Nextel a publié le premier smartphone 4G, l'evo HTC 4G.

1.1 Les différentes normes de téléphones mobiles :

Dans cette partie, il sera question de retracer l'évolution des différentes générations. Pour cela, nous allons détailler ci-dessous toutes les différentes générations des téléphones mobiles pour mieux comprendre.

1.2.1La première génération des téléphones mobiles (1G)

Elle est apparue au début des années 80, mais à cette époque sa qualité de service était médiocre et le cout de la communication était très élevé. Elle avait notamment beaucoup de défauts, d'une part les normes incompatibles d'une région à une autre, et d'autre part une transmission analogique qui n'était pas sécurisée.

1.2.2 La deuxième génération des téléphones mobiles(2G)

Le GSM est apparu dans les années 90. C'est n'est autre chose que la norme 2G.

Son fonctionnement est basé sur les transmissions des appels numériques afin de sécuriser les données par un cryptage par exemple. Grâce, à la 2G, il ya la possibilité d'émettre avec succès les minimessages (SMS, limites à 80 caractères). Contrairement à la 1G, il permet de faire le roaming vers l'international.

Devant ce succès, il a fallu proposer de nouvelles fréquences aux opérateurs pour acheminer toutes les communications, et de nouveaux services sont aussi apparus, comme le MMS. Le débit de 9.6 kbps proposé par le GSM est insuffisant, dans ce concept, ils ont pensé à développer de nouvelles techniques de modulations et de codages qui ont permis d'accroitre le débit pour la nouvelle génération.

1.2.2.1Le réseau GSM

Le réseau GSM a pour premier rôle de permettre des communications entre abonnés mobiles (GSM) et abonnés du réseau téléphonique commuté (RTC– réseau fixe). Il se distingue par un accès spécifique appelé la liaison radio.

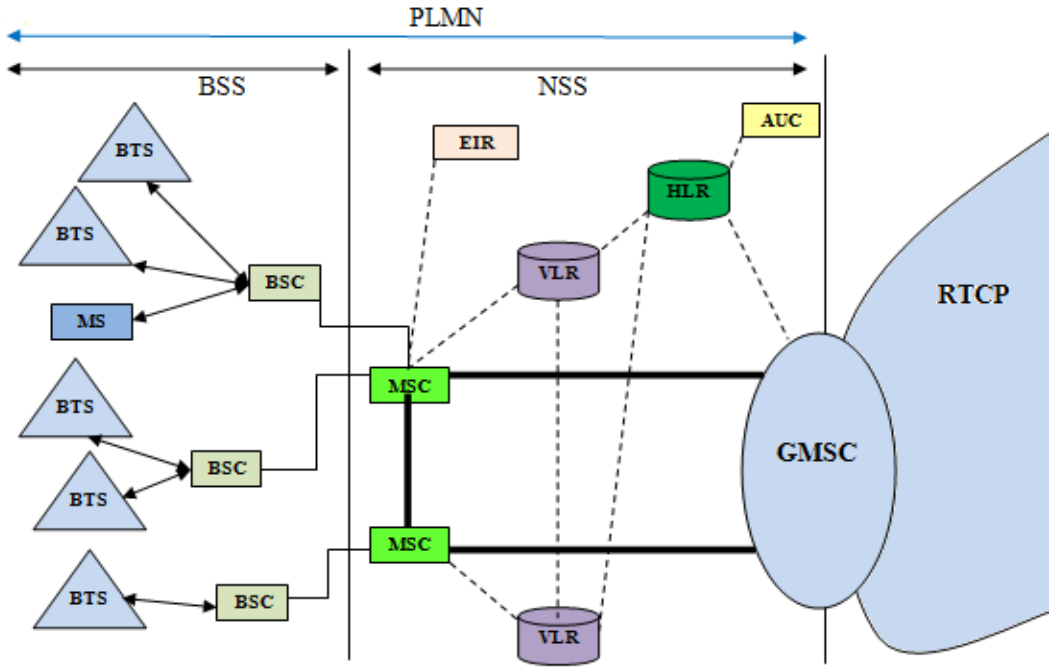

Figure 1 : L'architecture du Réseau GSM.

Technologie 2G :

- ✓ Utilisée pour la première fois en 1990 en Europe.
- ✓ Utilise la modulation numérique GMSK.
- ✓ Divisée en deux normes : TDMA, CDMA
- ✓ Débit de données 270 kbps.

1.2.2.2Le réseau GPRS (2.5G) :

Le réseau GPRS vient ajouter un certain nombre de « modules » sur le réseau GSM sans changer le réseau existant. Ainsi sont but est de conserver l'ensemble des modules de l'architecture GSM, nous verrons par ailleurs que certains modules GSM seront utilisés pour le fonctionnement du réseau GPRS.

La mise en place d'un réseau GPRS va permettre à un opérateur de proposer de nouveaux services de type "Data" à ses clients.

Le GPRS est en mode paquets. La figure suivante présente l'architecture du réseau GPRS.

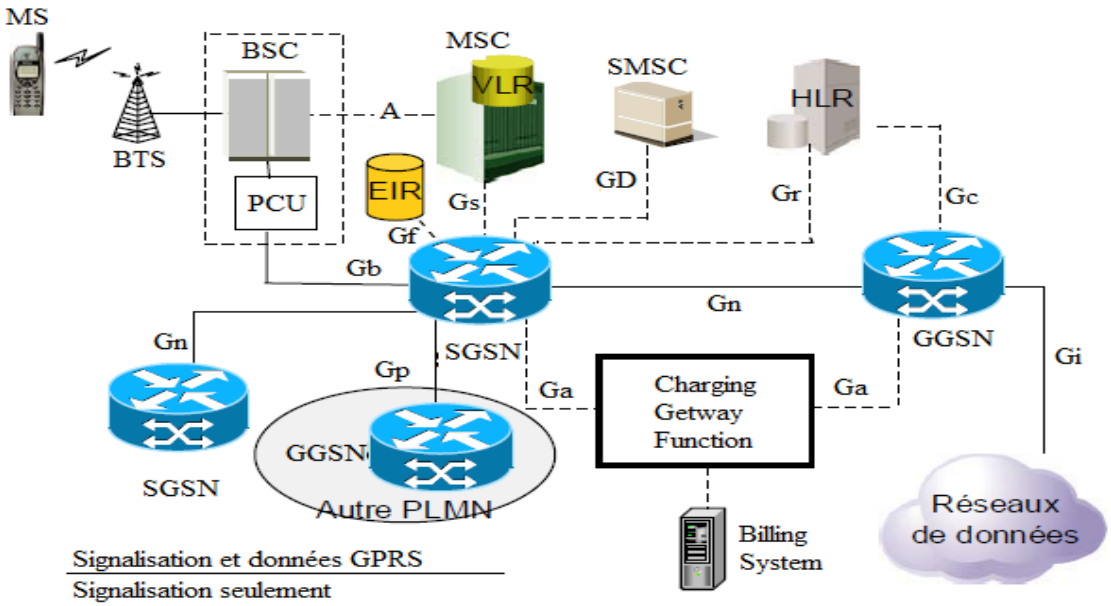

Figure 2 : Architecture du réseau GPRS

Entités GSM/GPRS	Logiciel	Matériel
BTS	Extension requise	Aucun changement
BSC	Extension requise	Interface PCU
MSC/VLR	Extension requise	Aucun changement
HLR	Extension requise	Aucun changement
Nouvelles entités		
MS	Mobile station	
SGSN	Serving GPRS Support Node	
GGSN	Gateway GPRS Support Node	
CGF	Charging Gateway Function	
OMC-G	Operations And Maintenance Centre GPRS	

Tableau1 : Evolution du GSM au GPRS

Un réseau GPRS est un réseau IP. Qui est donc constitué de routeurs IP. L'introduction de la mobilité nécessite par ailleurs la précision de deux nouvelles entités :

A-Le nœud de service (SGSN)

Le nœud de service dénommé SGSN (Serving GPRS Support Node) est relié au BSS du réseau GSM. Le SGSN est en connexion avec l'ensemble des éléments qui assurent et gèrent les transmissions radio : BTS, BSC, HLR ...

Le SGSN joue un rôle de routeur, il gère les terminaux GPRS présents dans une zone donnée. Le SGSN est le « contrôleur » des terminaux GPRS présents dans sa zone de surveillance.

B-Le nœud de passerelle (GGSN)

Le nœud de passerelle dansle GPRS dénommé GGSN (Gateway GPRS Support Node) est relié à un ou plusieurs réseaux de données (Internet, autre réseau GPRS...). Le GGSN est un routeur qui permet de gérer les transmissions de paquets de données :

- ✓ Paquets entrants d'un réseau externe, acheminés vers le SGSN du destinataire.
- ✓ Paquets sortants vers un réseau externe, émanant d'un destinataire interne au réseau.

C-Le module BG pour la sécurité

Les recommandations introduisent le concept de BG (Border Gateway) qui permettent de connecter les réseaux GPRS via un réseau fédérateur et qui assurent les fonctions de sécurité pour la connexion entre ces réseaux. Ces BG ne sont néanmoins pas spécifiés par les recommandations mais elles jouent le rôle d'interface avec les autres PLMN (Public Land Mobile Network) permettant ainsi de gérer les niveaux de sécurité entre les réseaux (par exemple entre deux réseaux de deux opérateurs concurrents).

D-Les équipements GSM utilisés

Le réseau GPRS appuie son architecture sur les éléments du réseau GSM :

- ✓ Les BTS et BSC permettent de couvrir un territoire national pour localiser les terminaux.
- ✓ Le MSC et le VLR permettent également de gérer les problématiques d'itinérance des abonnées sur les réseaux GSM et GPRS.
- ✓ Le SMSC et le GMSC permettent la communication interne au réseau par l'envoi de messages courts à destination du terminal GPRS.
- ✓ Le HLR permet de gérer les problématiques liées à la localisation des individus (en mode GPRS, fournir une carte de la ville où se trouve l'abonné).

- ✓ L'EIR permet de gérer les problématiques liées au terminal visé. Le réseau GPRS est totalement dépendant du bon fonctionnement des infrastructures du réseau GSM. Le réseau GSM constitue donc en effet une base pour la mise en place du réseau GPRS.

  Le tableau 1 se compose de deux partie : la première partie présente les entités utilisées dans les deux réseaux GSM et GPRS et la deuxième partie présente les nouvelles entités ajoutées au réseau GSM ainsi de constituer le réseau GPRS.

- ✓ Le type de transmission dans le réseau GPRS

  Ce standard utilise un mode de transmission par paquet. Lorsque le mobile transmet des données vers un terminal fixe, les données sont transmises via le BSS (BTS + BSC) au SGSN qui envoie ensuite les données vers le GGSN qui les route vers le destinataire.

  Le routage vers des terminaux (terminal mobile vers terminal mobile ou terminal fixe vers terminal mobile) utilise le principe de l'encapsulation et des protocoles tunnels. Les données revues par le GGSN sont transmises au SGSN dont dépend le mobile destinataire.

- ✓ La gestion d'itinérance

  La gestion de l'itinérance reprend les principes du réseau GSM avec le regroupement de cellules en zones. Le terminal GPRS peut se trouver dans trois modes :

  - Etat de « repos », le mobile est éteint.
  - Etat de « surveillance », le mobile est localisé au niveau de la zone de routage. Le mobile peut être appelé par le SGSN.
  - Etat « prêt », le mobile est localisé au niveau de la cellule. Le mobile peut recevoir des informations ; dans cet état le terminal est localisable à la cellule près. Une zone de routage est un regroupement de cellules (cellules réseau GSM). En état de « surveillance » puis de « prêt », le terminal ne monopolise pas de canal radio s'il n'y a pas de transmission ou de réception de données.

1.2.3 La troisième génération des téléphones mobiles UMTS (3G)

Elle propose d'échanger 1.9 mégabits par seconde, soit environ 5 fois plus rapidement que la génération précédente. Elle a permis d'utilisation des applications vidéos sur le mobile et l'amélioration des multimédias. Elle a également permis l'augmentation du débit pour pouvoir passer d'un service de téléphonie (à connexion circuit) vers un service DATA

(connexion par paquets). Elle ajouta des amplificateurs pour amplifier le signal pour qu'il puisse être accueilli par une autre antenne.

1.2.3.1 Architecture de l'UMTS

Le réseau UMTS vient se combiner au réseau déjà existants GSM et GPRS, qui apportent des fonctionnalités respectives de voix et de données, le réseau UMTS apportent ensuite les fonctionnalités multimédia.

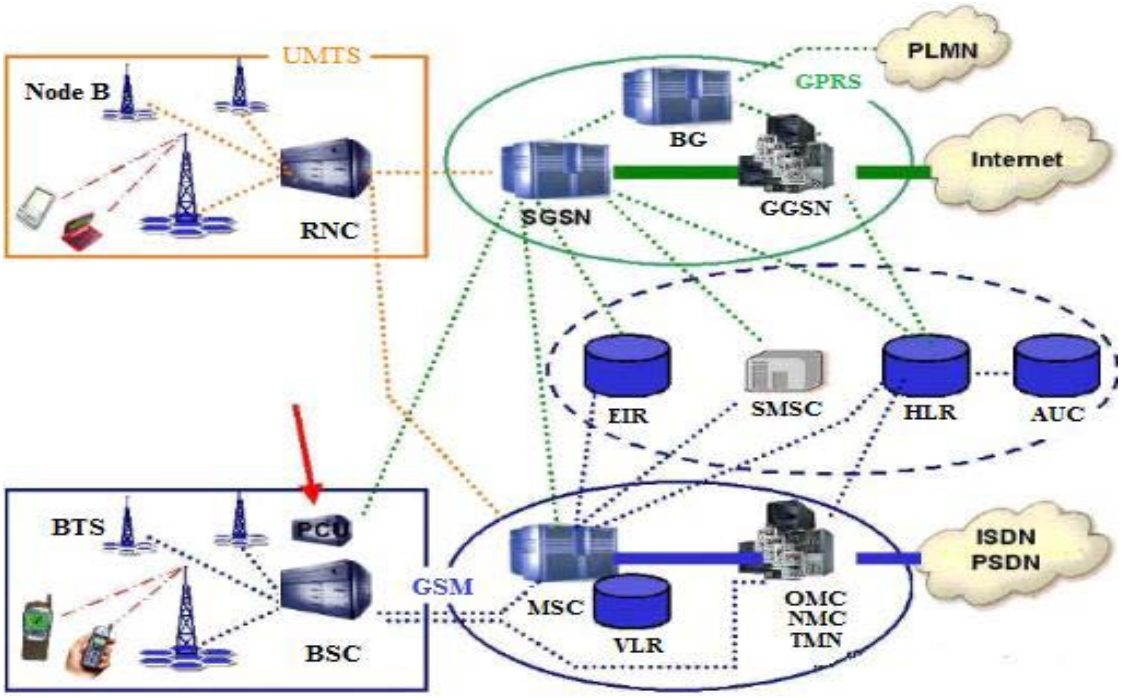

Figure 3 : Architecture de réseau UMTS

Le réseau UMTS constitue de trois entités principales :

1) Le réseau fixe CN (coré network)

   Assure la gestion de la localisation et le contrôle des paramètres du réseau.

2) Le réseau UTRAN (Terrestrial Radio Access Network)

   Assure la gestion de ressource radio (handover, allocation de ressource,…) et L'accès au réseau fixe via l'interface Iut. Les différents constituants de ce réseau D'accès UTRAN sont :

   - Le Node B :

     Son rôle principal est d'assurer les fonctions de réception et de transmission radio pour une ou plusieurs cellules de l'UTRAN.

   - LE RNC :

Son rôle principal est le routage des communications entre le Node B et le réseau cœur.

3) L'équipement d'usager UE (User Equipement)

C'est l'équipement exploité par l'utilisateur afin d'accéder aux différents services fournis par l'UMTS via l'interface radio UTRA

Le 3GPP (3rd generationpartnership Project) qui gère cette norme, est constamment améliorée, notamment pour augmenter les débits et pouvoir prendre en charge un nombre plus important d'abonnés. Les normes associées à cette génération sont :

- La norme HSDPA (High Speed Downlink Packet Access) : Elle offre des Performances dix fois supérieures à la 3G, uniquement sur le flux descendent.
- La norme HSUPA (High Speed UplinkPacket Access) : Elle apporte des améliorations uniquement au flux montant.
- La norme HSPA+ (High Speed Packet Access) : nommée H+, 3GPP, est une norme de téléphonie mobile 3G de la famille UMTS ; c'est une evolution de la norme HSPA permettant d'atteindre des débits de : 42Mb/s (montant) et 11Mb/s(descendent).

1.2.3.2 Le mode de transmission dans le réseau UMTS

Le mode circuit :

Il s'occupera de la bonne gestion des services temps réels dédiés aux conversations téléphoniques (vidéo-téléphonie, jeux vidéo, applications multimédia). Ces applications sont performantes en transfert rapide.

Nous constatons qu'au moment de l'introduction de I'UMTS le débit du mode domaine circuit sera de 384 Kbits/s.

Il est aussi important de noter que son infrastructure s'appuie sur les principauxéléments du réseau GSM : MSC/VLR (bases données existantes) et le GMSC afin d'avoir une connexion directe vers le réseau externe.

Le mode paquet :

Il permettra également de gérer les services non temps réels.

II est question ici, de la navigation sur Internet, de la gestion de jeux en réseaux et l'accès et l'utilisation des e-mails.

La raison pour laquelle les données transiteront en mode paquet, est du au fait qu'elles sont moins sensibles au temps de transfert.

Le débit du domaine paquet sept fois plus rapide que le mode circuit, environ 2Mbits/s.

L'infrastructure s'appuie alors sur les principaux éléments du réseau GPRS : SGSN (bases de

données existantes en mode paquet GPRS, équivalent des MSC / VLR en réseau GSM) et le GGSN (équivalent du GMSC en réseau GSM) qui jouera le rôle de commutateur vers le réseau Internet et les autres réseaux publics ou privés de transmission de données.

Problèmes :

- ➢ La haute bande passante requise
- ➢ Coût élevé du spectre
- ➢ Capacité énorme

1.2.4 La quatrième génération des téléphones mobiles (4G) :

La 4G est la quatrième génération de réseau mobile. Celle qui succède directement la 3G.Elle est la norme des standards de téléphonie permettant des débits ayant 50 fois plus d'importance que la première norme. (Elle sera mieux étudier dans le chapitre suivant).

1.2.4.1 Taux de téléchargement des données

La figure ci-dessousreprésente le taux de téléchargement des données des différentes générations :

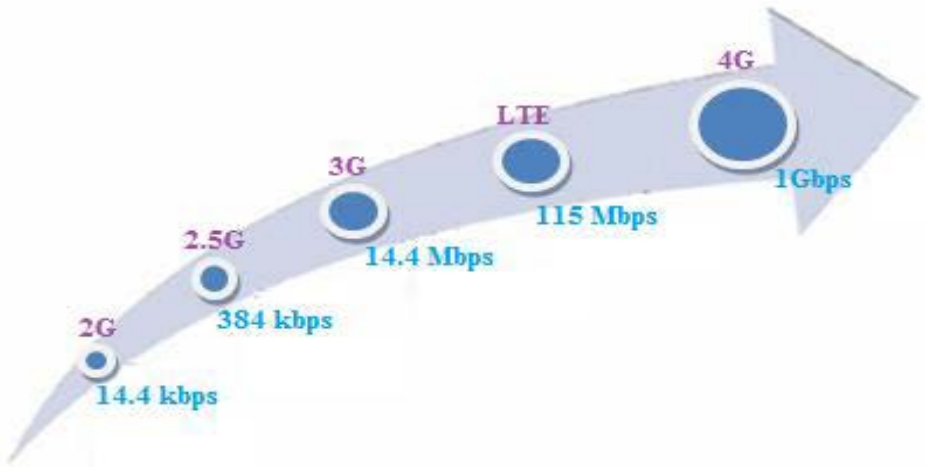

Figure 4 : Taux de téléchargement des données

Nous observons qu'au fur et à mesure le taux de téléchargement des données augmente de génération en génération. Pour les réseaux 4G, le débit à atteint jusqu'à 1Gbps.

1.2.4.2 Comparaison entre différentes générations

Générations	Définitions	peakspeed / real speed	Technologies
1	Analoc	13 kbps	FDMA
2	Digital narrowband circuit data	14.4 kbps / 9.9 Kbps	TDMA -CDMA
2.5	Packet data	180 kbps / 20-40 Kpbs	GPRS
3	Digital narrowband packet data	3.1 Mbps/ 500-700 Kbps	W-CDMA UMTS EDGE
3.5	Digital narrowband packet data	4.4 Mbps/ <3Mbps	HSPA
4	Digital narrowband packet data , All IP	100-300 Mbps / > 100Mbps	LTE

Tableau 2 : Comparaison entre toutes les générations

1.3 Conclusion :

Nous avons présenté dans ce chapitre d'une façon générale les différentes générations de téléphonie mobile. Et aussi les principales caractéristiques d'un réseau cellulaire. En commençant par la 1G qui est née dans les années 80. Etant le point de départ de toutes les générations, elle a montré ses limites ce qui a nécessité la naissance de la 2G. Celle-ci est toujours utilisée jusqu'à nos jours, mais étant plus développée que la précédente. Concernant la 3G, elle est venue avec des nouvelles qualités notamment son haut débit pour l'accès à Internet et le transfert de données.

La naissance de la 4G, qui est le successeur évolué de la 3G, montre d'une manière claire que le développement des réseaux augmente considérablement.

Quant aux réseaux 4G (LTE), nous allons mieux les étudier dans notre prochain chapitre.

CHAPITRE 2 : Description de la 4G/ LTE

2.1 Introduction :

Ce chapitre a pour objectif de présenter la 4G/LTE, les différents éléments importants de notre projet tels que: la stratégie de mise en place par le réseau radio mobile LTE, les spécificités et aussi les technologies de transmission de la qualité de services dans le réseau 4G.

2.2 Définition de la 4G/LTE :

LTE (Long Term Evolutionof UMTS) est un projet mené par la 3GPP (3G) et a été considéré comme une norme de 3^{éme} génération (3,9G) proche de la 4G.Elle permet d'atteindre des débits théoriquesde 100 Mbit/s en voie descendante et 50 Mbit/s en voie montante pour une largeur de bande de 20Mhz, avec une très grande portée, un grand nombre d'appels simultanés, une faible latence et une capacité élevée.

2.3 But de la 4G/LTE :

La 4G vise à augmenter la capacité de gestion du nombre de mobiles dans une même cellule. Elle tente aussi d'offrir des débits élevés en situation de mobilité et à offrir une mobilité totale à l'utilisateur en établissement l'interopérabilité entre différents technologie existantes. Elle vise à rendre le passage entre les réseaux transparent pour l'utilisateur, à éviter l'interruption des services durant le transfert intercellulaire, et à basculer l'utilisation vers le tout-IP.

Les principaux objectifs visés par les réseaux de 4^{éme} génération sont :

- ✓ Assurer la continuité de la session en cours.
- ✓ Réduire les délais et le trafic de signalisation.
- ✓ Fournir une meilleure qualité de service.
- ✓ Minimiser le cout de signalisation
- ✓ Optimiser l'utilisation des ressources
- ✓ Réduire le délai de relève, le délai de bout en bout, la perte des paquets.

2.4 Architecture de la 4G/LTE

La technologie LTE a apporté une efficacité spectrale, amélioration de débit, augmentation de couverture et du nombre d'appels supportés par la cellule.

De même que ces précédentes, elle est caractérisée par son architecture qui comporte :

- L'équipement de l'usager : **UE**
- Un réseau d'accès: **l'E-UTRAN**

- Un réseau cœur : **EPC (Réseau tout-IP).**

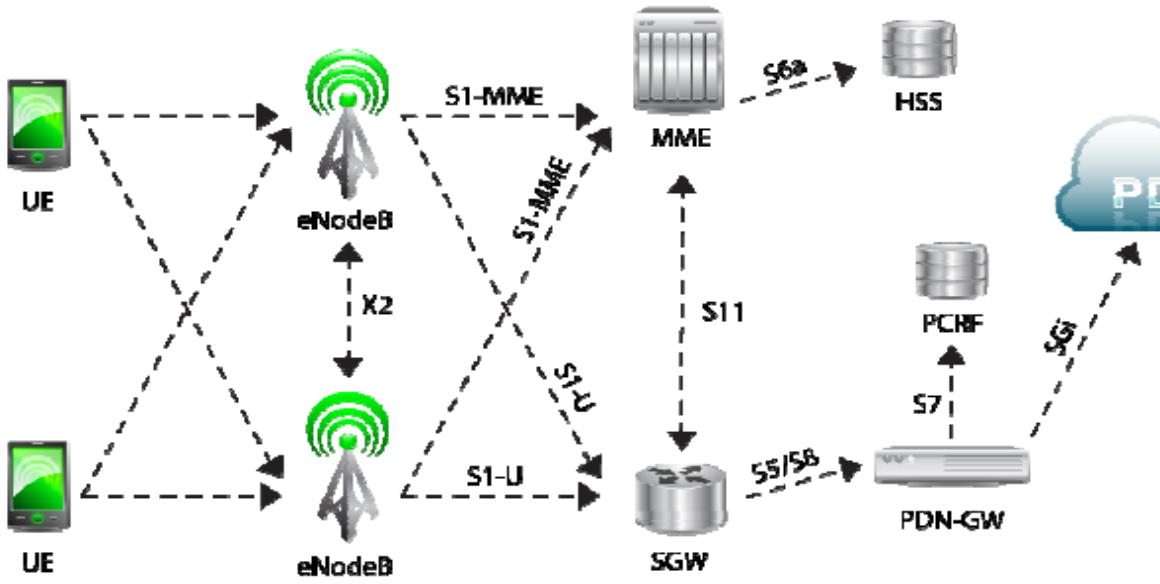

Figure 5: Architecture du réseau LTE

2.2.1 Catégorie d'UE :

La mise en œuvre du réseau LTE nécessite de nouveaux équipements, comme de nouveaux terminaux compatibles avec une nouvelle technologie.

Caractéristiques des catégories d'UE du LTE : Le tableau suivant représente les différentes catégories de l'UE ;

Catégorie D'UE	Débit crête (Mbit/s)		Modulations		Nombre D'antennes De réception	Nombre max De couches Spatiales en DL
	DL	UL	DL	UL		
1	10	5	QPSK, 16QAM, 64QAM	QPSK, 16QAM	2	1
2	50	25			2	2
3	100	50			2	2
4	150	50			2	2
5	300	75		QPSK, 16QAM, 64QAM	4	4

Tableau 3 : Caractéristiques des catégories d'UE du LTE

2.2.2 Réseau d'accès : E-UTRAN

Il ne contient que des eNodeB.

L'eNodeB qui assure l'échange radio avec l'E-UTRAN. A la différence de la 3G, les fonctions supportées par le RNC ont été réparties entre l'eNodeB et les entités du réseau coeur SGW.

Ils sont reliés entre eux par une interface X2.

➢ L’interface X2: c’est une interface logique.

Elle est introduite dans le but de permettre aux eNodeBs d’échanger des informations de signalisation durant le Handover ou la signalisation, sans faire intervenir le réseau coeur.

La partie radio eUTRAN :

La partie radio du réseau, appelée « eUTRAN » est simplifiée par rapport à celles des réseaux 2G (BSS) et 3G (UTRAN) par l’intégration dans les stations de base « eNodeB » avec des liaisons en fibres optiques et des liens IP reliant les eNodeB entre eux (liens X2).
Ainsi que des fonctions de contrôle qui étaient auparavant implémentées dans les RNC (RadioNetwork Controller) des réseaux 3G UMTS. Cette partie est responsable sur le management des ressources radio, la porteuse, la compression, la sécurité, et la connectivité vers le réseau cœur évolué.
L'eNodeB est relié au cœur du réseau à travers l'interface S1.

- ✓ L’interface S1 : C’est l’interface intermédiaire entre le réseau d’accès et le réseau cœur, et elle peut être divisée en deux interfaces élémentaires : Cette dernière consiste en S1-U (S1-Usager) entre l'eNodeB et le SGW et S1-C (S1-Contrôle) entre l'eNodeB et le MME.

Les eNodeB ont offert deux qualités au réseau :

- ✓ La sécurité : en cas de problème d’un relais.
- ✓ Un partage des ressources équitable : partage de ressource en cas de saturation du lien principale.

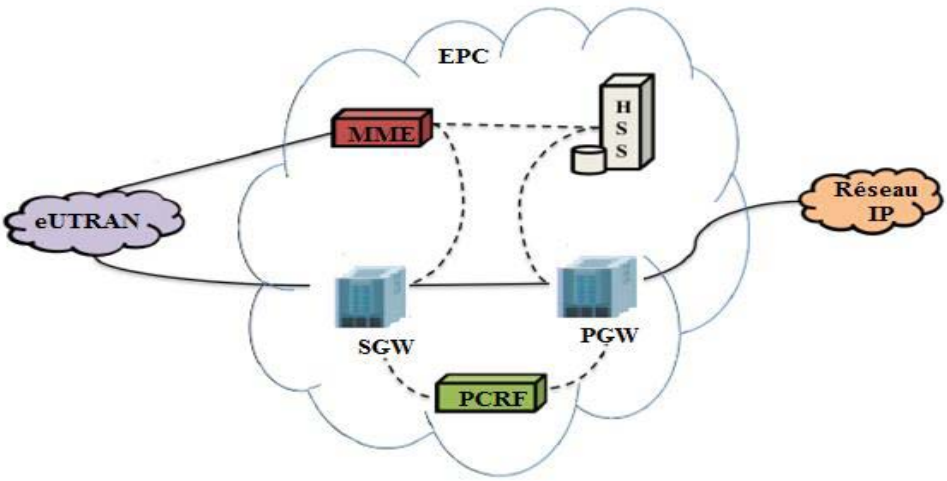

Figure 6 : Architecture du réseau cœur EPC

2.3.3 Réseau Cœur : EPC (Evolved PacketCore) :

C'est le nom du réseau cœur évolué, paquet tout IP. EPC peut aussi communiquer avec les réseaux 2G/3G. Son architecture est simplifiée, comme montre la figure 7, en la comparant à celle de 2G/3G.

Le réseau cœur EPC est décomposé en :

-MME « Mobility Manager Entity » : cette entité est responsable de la location de l'utilisateur, de connaitre son état et gérer les procédures d'authentification et mobilités des UE.

-SGW « Serving GateWay » : cette entité est responsable du transfert d'un relai à un autre, il gère tout l'aspect Handover inter-eNodeB et effectuer ce transfert vers réseau 'w2G ou 3G.

-PGW « Packet data network Gateway » : c'est la passerelle vers les réseaux externes, responsable du routage en assignant une adresse IP au mobile au moment de l'attachement au réseau. PGW est un point pour faire le filtrage des données, il participe aussi à l'opération de taxation.

-HSS « Home Subscriber Server » : cette entité contient le profil de l'abonné pour les réseaux : 2G, 3G et LTE.

-PCRF « Policy ChargingRulesFunction » : cette entité fournit au PGW les règles de taxation nécessaires pour différencier les flux de données et de les taxer d'une façon convenable.

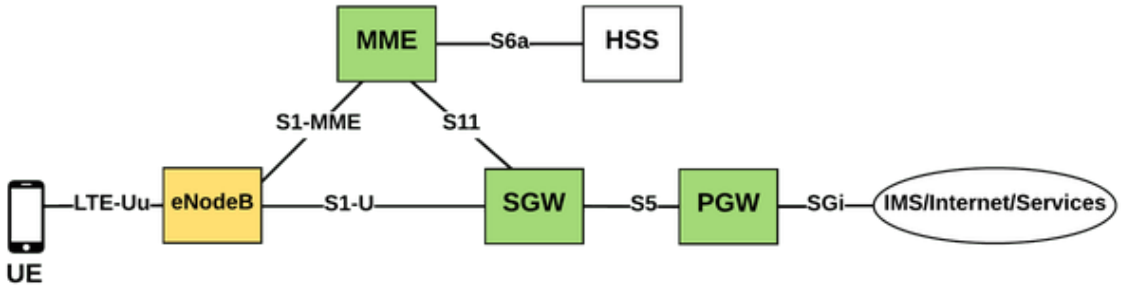

Figure 7: Le réseau cœur EPC.

Remarque :

Lorsque nous comparons l'architecture du réseau LTE avec celle des réseaux précédents, nous constatons que :

- ✓ L'entité MME remplace le dispositif MSC ce qui offre une architecture simplifiée.
- ✓ L'entité SGW remplace le dispositif SGSN
- ✓ L'entité e-NodeB remplace la BTS/NodeB

- ✓ L’entité PGW remplace GGSN.

2.5 Caractéristiques de la 4G/LTE

2.5.1 Les débits : Les objectifs du débit maximale définit pour LTE sont les suivantes :

- ✓ 100Mb/s en voie descendante pour une largeur de bande allouée de 20Mhz
- ✓ 50Mbit/s en voie montante pour une largeur de bande allouée de 20Mhz

Le débit de la cellule doit être atteignable au moins par 95% des utilisateurs.

2.5.2 La latence : C’est la capacité à réagir rapidement à des demandes d’utilisateurs oude service.

On a deux plans :

- ➢ **Latence du plan de contrôle** : Son objectif est d’améliorer la latence du plan de contrôle, par rapports à l’UMTS, avec un temps de transition inferieur à 100ms.
- ➢ **Latence du plan usager** : correspond au délai de transmission d’un paquet IP au sein de réseau d’accès. Le réseau LTE vise une latence du plan usager inferieur a 5ms.

2.5.3 L’agilité en fréquence : Le LTE doit pouvoir opérer sur des porteuses des différentes largeurs afin de s’adapter à des allocations spectrales variées. Les largeurs de bande initialement requises ont par la suite été modifiées pour devenir les suivantes : 1,4Mhz, 3Mhz, 5Mhz, 10Mhz, 15Mhz et 20Mhz.

2.3.4 Codage et sécurité :

L’OFDMA (orthogonal frequency division multiple Access) est une technologie de codage radio de type « Accès multiple par répartition en fréquence). L’OFDMA et sa variante SC-FDMA sont dérivés du codage OFDM (utilisé dans l’ADSL et WiFi), mais contrairement à L’OFDM, l’OFDMA est optimisé pour l’accès multiple, c'est-à-dire le partage simultané de la ressource spectrale (bande de fréquence) entre plusieurs utilisateurs distants les uns des autres.

2.5.5 Multiplexage :

Il existe deux modes du multiplexage de fréquences :

-FFD (frequency division duplexing) : L’émission et la réception se font à des fréquences différentes.

-TDD : L’émission et la réception se transitent à une même fréquence, mais à desinstants différents.

2.5.6 La mobilité :

Le réseau LTE doit rester fonctionnel pour des UE qui se déplacent à des vitesses élevées.

2.6 Conclusion :

Dans ce chapitre, nous avons constaté que l'architecture du réseau 4G/LTE permet de faciliter l'évolution du réseau en intégrant des technologies plus performantes, qui leur permettent de fournir en même temps des services de bonne qualité.

En tenant compte du fait que notre projet est plus focalisé sur la sécurité du réseau de la quatrième génération du réseau4G/LTE, nous étudions la sécurité dans les réseaux 4G/LTE en profondeur dans le chapitre suivant.

CHAPITRE 3 : Sécurité dans les réseaux 4G/LTE

3.1 Introduction

Les réseaux mobiles LTE (Long Term Evolution) offrent des possibilités à la fois riches et nouvelles pour la croissance et le développement commercial et sont actuellement déployés à travers le monde. Ces réseaux LTE mobiles utilisent la commutation complète de paquets et le protocole IP, contrairement aux itérations précédentes du réseau mobile, ce changement de la commutation de circuit à la commutation de paquet permet de nouvelles attaques qui n'étaient pas possibles auparavant.

Certaines implémentations de réseaux LTE et d'applications mobiles sont actuellement vulnérables à plusieurs échelles. Ce qui entraîne une perte de confidentialité, une facturation incorrecte et une falsification de données.

L'objectif recherché dans ce chapitre est de mieux comprendre les composants de la sécurité EPS ainsi que la qualité de service dans les réseaux 4G/LTE.

3.2 La sécurité dans L'EPS

3.2.1 Définition de la sécurité

D'une façon générale :«la sécurité est l'ensemble des mesures permettant d'assurer la protection des biens/valeurs.»

Dans le monde informatique, on distingue deux types de biens à savoir :

- L'information, les données (comme : les offres, les commandes, les contrats, les données clientèles, les données stratégiques…)
- Les systèmes permettant de traiter, véhiculer et stocker l'information (les applications, les serveurs, les stations de travail, les bases de données, les réseaux internes et externes…)

3.2.2 Les composants de la sécurité

3.2.2.1 L'authentification :

L'authentification désigne la procédure par laquelle une entité <A> avec laquelle elle communique est bien autorisée. L'authentification d'un UE consiste donc pour le réseau à s'assurer qu'il est bien en contact avec la personne désirée.

3.2.2.2 La confidentialité :

Une information est dite confidentielle lorsqu'elle ne peut être partagée qu'avec des entités, (individus ou processus autorisés). Le niveau de la confidentialité d'une formation indique la nature et le nombre de ces éléments avec lesquelles elle peut être partagée. En effet le niveau de confidentialité est lié à la sensibilité de l'information.

3.2.2.3 L’intégrité :

La protection de l’intégrité a deux objectifs :

- ✓ La protection de l’intégrité proprement dite : assuré que la donnée n’a pas été altéré par un tiers après son envoi initial.
- ✓ L’authentification de la source : vérifier que la source de cette donnée est bien celle indiqué dans le message.

3.2.3 Les menaces de la sécurité :

La plupart des menaces de sécurité qui forment une source de préoccupation pour l’EPS, comme pour n’importe quel autre système antérieur, peuvent être résumé comme suit :

- ✓ ***Menaces contre l'identité de l'utilisateur*** **(IMSI catchingattack):** Ce type de menace esttrès grave puisqu’il ouvre la voie à différentes attaques et puisqu’il est l’un des pointsfaibles dans la sécurité de l’UMTS.
- ✓ ***Menaces de suivi d’UE*** **(Threats of UE tracking) :** Pour ce type de menaces on peutimaginer le suivi d'un utilisateur en se basant sur l’adresse IP liée à l’identité del’utilisateur (IMSI ou TMSI), ou bien le suivi d'un utilisateur en se basant sur lesmessages de signalisation du transfert intercellulaire (handover).
- ✓ ***Menaces liées à l’eNB*****(Threatsrelated to eNB) :** Comme par exemple la menace decompromettre physiquement la station de base eNB.
- ✓ ***Menaces contre la manipulation des données de signalisation*** **(Threatsagainstmanipulation of control plane data) :** Les informations de contrôle peuvent être très utilespour les attaquants afin de dévoiler l’identité de l’utilisateur.
- ✓ ***Menaces d’accès non autorisé au réseau*** **(Threats of unauthorizedaccess to the network) :** Un pirate non abonné peut utiliser les ressources du réseau dans ce cas.
- ✓ ***Menaces liées à un déni de service*** **(Threatsrelated to denial of service) :** Le brouillage radio, ou le lancement d’une attaque distribuée à partir de plusieurs UE vers certainesparties du réseau, ou une attaque DoS (Denial of Service) contre un UE.
- ✓ ***Menaces contre les protocoles radio*** **(Threatsagainst the radio protocols) :** Un attaquantcompétent peut modifier les premiers messages d’établissement de connexion radiode l’UE.

3.2.4 Concept générale de la sécurité LTE :

La dernière version de la spécification décrivant tous les éléments de la sécurité de l'EPS n'est qu'une amélioration de la sécurité UMTS ou elle garde les éléments de sécurité robustes et nécessaires. Chaque mécanisme de sécurité 3G gardé, doit être adapté au nouveau contexte pour être appliqué à la nouvelle architecture de l'EPS.

Le niveau élevé de sécurité offert par EPS est assuré par l'introduction de nouveaux mécanismes, en particulier dans le domaine de l'accès au réseau. Parmi ces mécanismes :

- ✓ LTE effectue une authentification mutuelle entre un équipement utilisateur et le réseau.
- ✓ NAS sécurité : effectue la protection de l'intégrité (vérification) et chiffrement (cryptage/décryptage) de la signalisation NAS entre l'UE et le MME.
- ✓ AS sécurité :effectue la protection de l'intégrité (vérification) et le chiffrement de la RRC signalisation entre l'UE et l'eNB. Effectue également le chiffrement du trafic utilisateur entre l'UE et l'eNB.
- ✓ Une nouvelle hiérarchie des clés.
- ✓ Utilisation d'une nouvelle identité temporaire appelé GUTI.

3.2.5 Procédure EPS-AKA

Elle a pour but de réaliser une authentification mutuelle entre l'utilisateur et le réseau ainsi que l'établissement d'une nouvelle clé maîtresse Kasme commune entre l'UE et le MME.La clé Kasme va servir à dériver des clés multiples utilisées dans les procédures de protection de la signalisation NAS, de la signalisation RRC, et du plan usager.

Le déroulement de la procédure EPS-AKA est présenté dans la figure 8. Cette procédure est initiée par le MME après l'identification de l'utilisateur par son IMSI ou GUTI. Dans une première étape le MME demande au HSS les vecteurs d'authentification AV EPS. Cette demande, appelée Authentication Data Request, doit inclure : l'IMSI, l'identité du réseau de service 'SN id' du MMEdemandeur, et une indication que les données d'authentification sont demandées pour l'EPS. Dans le HSS et comme nous venons de voir, le SN id entre dans le calcul de Kasme.

L

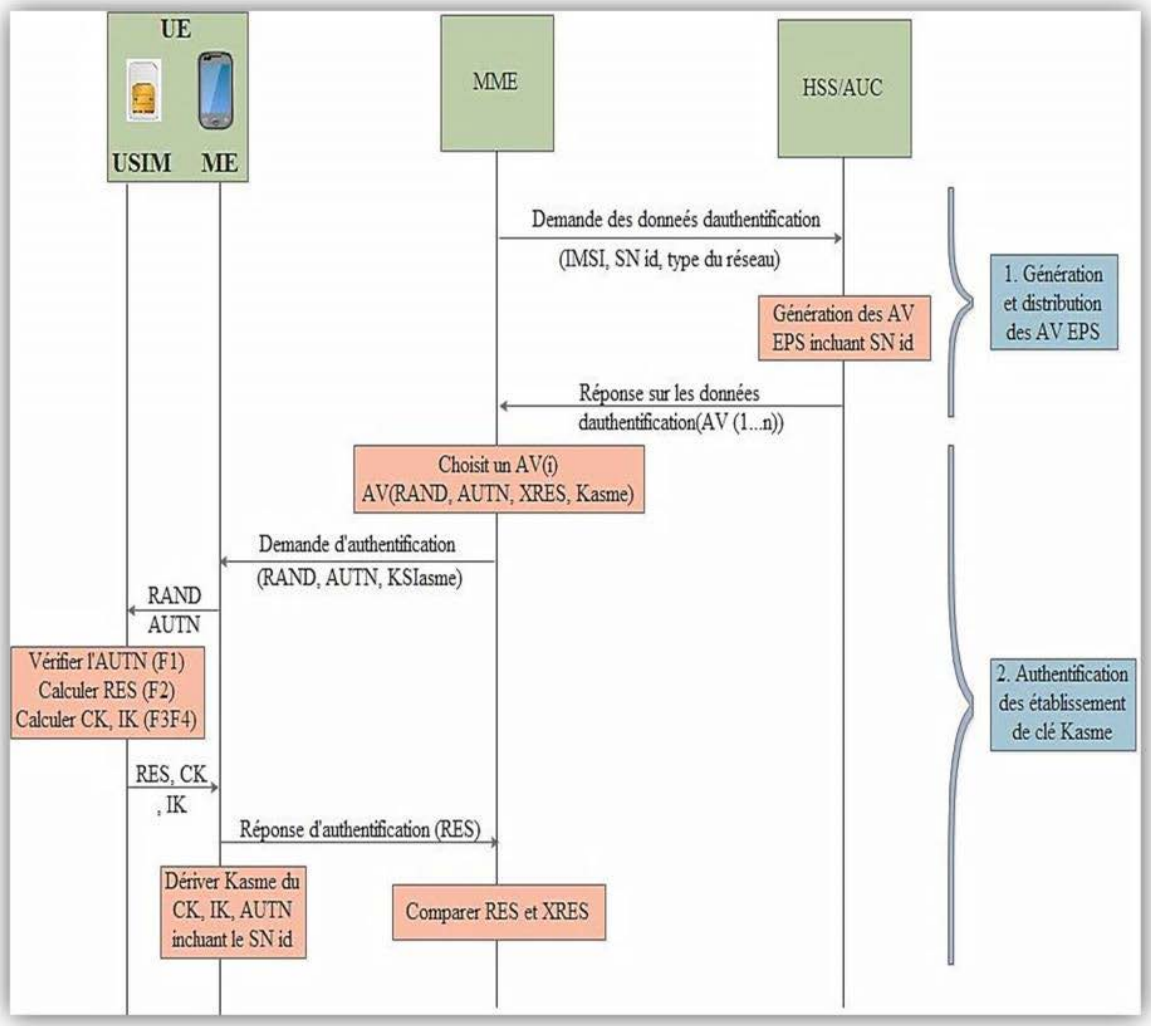

Figure 8 : Procédure EPS-AKA

A la réception de la demande du MME, le HSS calcule les vecteurs AVs (ou il les cherche dans sa base de données s'ils sont déjà pré-calculés) et il les envoie au MME dans sa réponse appelée Authentication Data Response. Cette dernière contient un ensemble ordonné de n vecteurs d'authentification AV EPS, AV (1 ... n).

Le vecteur d'authentification contient les paramètres suivants :

- ✓ Le paramètre d'entrée RAND pour générer les autres paramètres de l'AV.
- ✓ la Réponse attendue XRES = F2 (K, RAND) pour l'authentification.
- ✓ le jeton d'authentification AUTN = SQN⊕AK || AMF || MAC.
- ✓ la clé de sécurité Kasme = KDF (SQN, SN ID, CK, IK).

Puis, le MME choisit un de ces vecteurs, AV(i), et il l'utilise pour effectuer l'authentification. Un vecteur AV EPS peut être utilisé pour une seule authentification.

Le MME envoie après à l'équipement utilisateur UE, et plus précisément à l'équipement mobile ME qui le transmet à son tour à l'USIM, une demande d'authentification (appeléeUser AuthenticationRequest) contenant les paramètres RAND et AUTN extrait du vecteur AV(i) choisit. Le MME envoie également dans cette même demande d'authentification, un identificateur de la clé Kasme, KSIasme (ou appelé eKSI, evolved KSI).

Dès la réception des deux paramètres RAND et AUTN, l'USIM effectue le calcul des différents paramètres. Au début l'USIM détermine la clé AK = F5 (K, RAND) qui lui permet le déchiffrement du numéro deséquence SQN = (SQN $\oplus$AK) $\oplus$AK.

Ensuite, l'USIM utilise le SQN calculé, le champ AMF inclut dans l'AUTN reçu,et le RAND reçu pour calculer la valeur XMAC=F1 (K, SQN, RAND, AMF) dans le butde vérifier l'authenticité du jeton. Si XMAC est égale au MAC reçu inclut dans l'AUTN,l'USIM confirme la validité du SQN calculé et vérifie s'il est dans la gamme correcte ou non. Si oui, le réseau est alors authentifié. Si non, l'utilisateur envoie soit un message d'échec d'authentification en expliquant la raison de l'échec, soit un message d'échec de synchronisation (synchronizationfailure) à cause du SQN invalide.

A ce moment-là l'USIM calcule RES = F2 (K, RAND) ainsi que les clés CK, IK et il les envoie au ME. Ce dernier calcule la clé Kasme en utilisant la même fonction KDF et les mêmes paramètres d'entrée utilisés par le HSS. Après, le ME supprime tout de suite les clés CK et IK, puis il envoie le RES dans un message de réponse d'authentification (User AuthenticationResponse) au MME.

Le MME vérifie ainsi si le RES reçu correspond à la réponse attendue XRES inclut dans l'AV(i). Si c'est le cas, alors l'utilisateur est authentifié avec succès, et le MME sélectionne la clé Kasme contenue dans AV(i) pour l'utiliser dans les étapes suivantes. Sinon, si le MME trouve que XRES est différent de RES, alors il décide soit initier une nouvelle procédure EPS-AKA, soit d'abandonner la procédure d'authentification et envoyer un message de rejet d'authentification (AuthenticationReject message) à l'UE.

3.2.6Hiérarchiedesclés :

La figure suivante présente l'hiérarchie des clés :

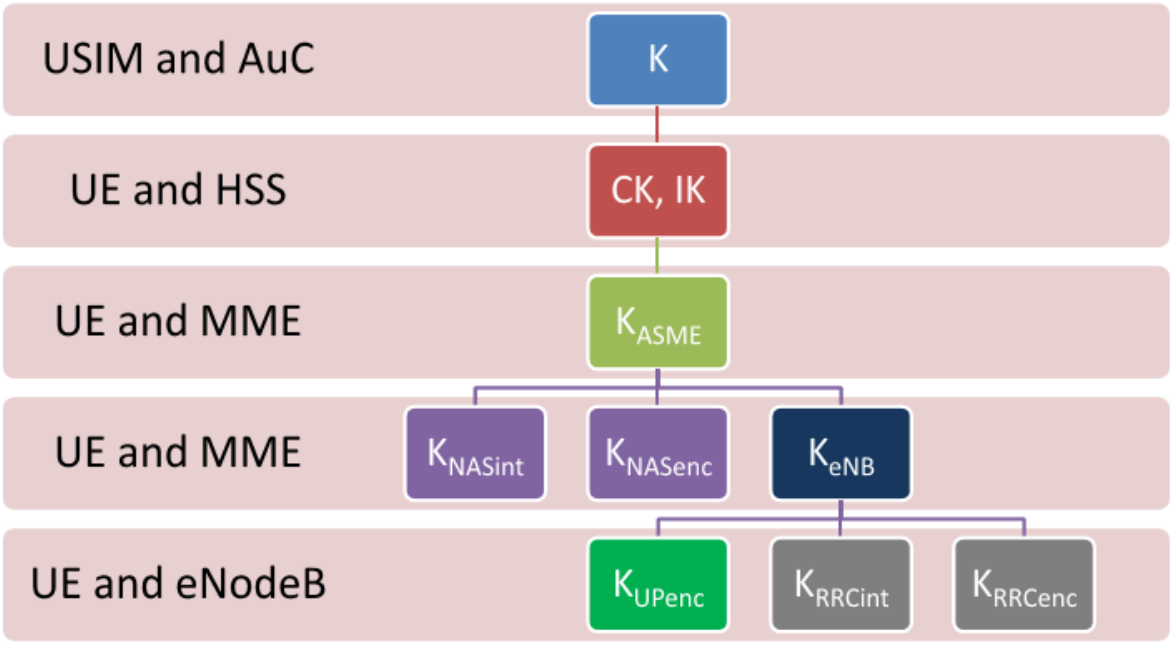

Figure 9 : Hiérarchie de clé de sécurité LTE

- **K_{ASME} (Access Security Management Entity)** est une clé maîtresse de session de
- 256 bits ou appelé aussi, clé de base MME, c'est une clé dérivée des clés de chiffrement et d'intégrité.
- **K_{eNB}** est une clé dérivée de KASME par l'UE et le MME ou par l'UE et l'eNB.
- **K_{NASint}** est une clé utilisée pour la protection du trafic NAS (non access Stratum) avec un algorithme d'intégrité particulier. Cette touche est dérivée de KASME par l'équipement utilisateur et le MME.
- **K_{NASenc}** est une clé de chiffrement de 128 bits pour les NAS confidentialité de signalisation entre UE et MME.
- **K_{UPenc}** est une clé de chiffrement de 128 bits pour le plan de la confidentialité des utilisateurs.
- **K_{RRCint}** est une clé utilisée pour la protection du trafic RRC (Radio Ressource Control) avec un algorithme d'intégrité particulier, cette clé est dérivée par l'équipement utilisateur et l'eNodeB à partir de KeNB.
- **K_{RRCe}nc** est une clé de chiffrement de 128 bits pour la confidentialité des données RRC de signalisation entre UE et eNB.

Lors des premiers échanges, le HSS génère une clé Kasme en prenant compte de l'identité du réseau défini par le couple (MCC, MNC) qui demande cette clé, cette dernière est ensuite envoyée au MME responsable de la communication avec le terminal mobile, c'est cette clé qui permettra au MME de générer le reste des clés nécessaires.

Suite aux échanges avec le terminal, le MME génère une autre clé KeNodeB à la base de la clé Kasme, c'est cette clé qui est transmise à l'eNodeB auquel s'attache le terminal ; par ailleurs la carte USIM génère la clé Kasme qu'elle envoi au terminal mobile qui a son tour déduit le KeNB.

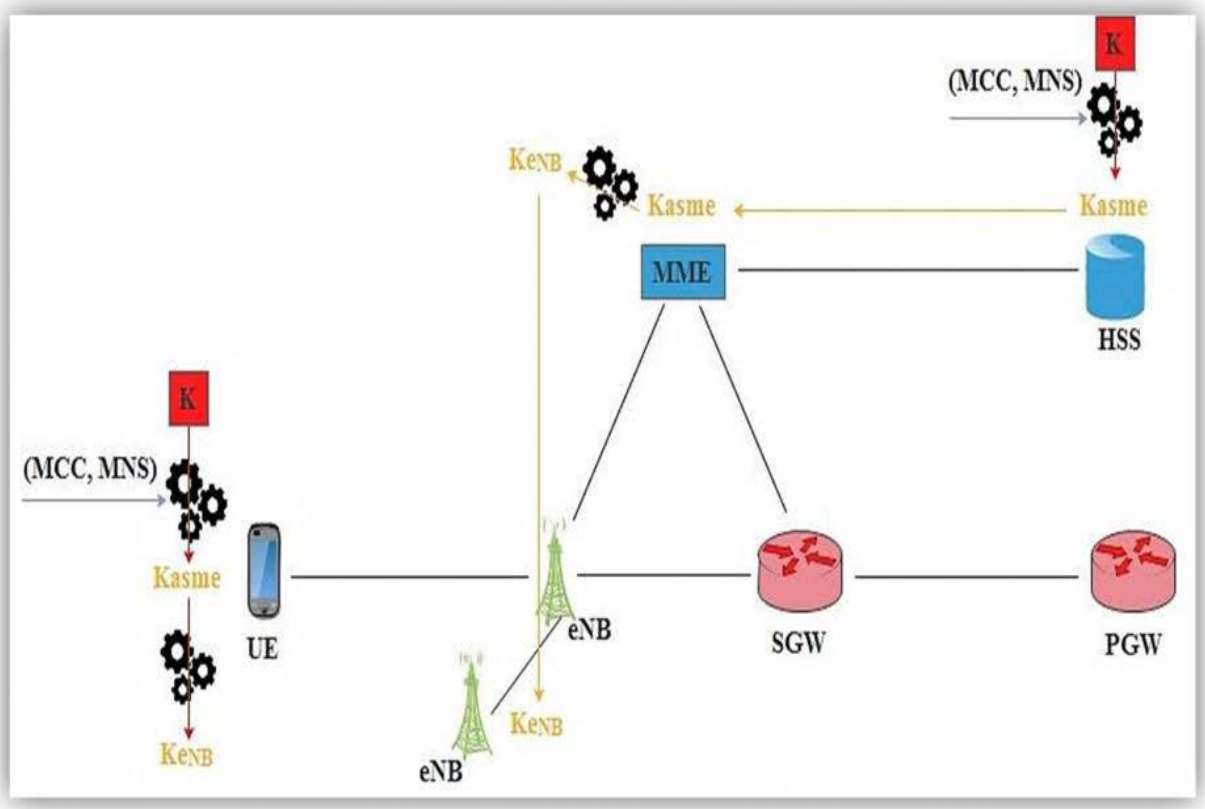

Figure 10 : Distribution des clés Kasme et KeNB

Les clés (Kasme, KeNB) ne sont pas utilisées directement pour protéger les échanges, elles servent comme bases afin de générer l'ensemble des clés nécessaire pour l'intégrité et le chiffrement des échanges.

En effet, cette hiérarchie de clés est construite à la base d'une utilisation ingénieuse des fonctions cryptographiques de hachage, une telle fonction prend commeparamètre une clé secrète et des données à hacher. Comme la sortie à une taille fixe et grâce aux propriétés des fonctions cryptographiques de hachage, la sortie peut être elle-même traitée comme une clé.

3.2.7 Protection de la signalisation NAS :

La figure 11 présente la procédure d'établissement de la sécurité NAS. Après la réception des capacités de sécurité de l'UE lors de la demande d'attachement, et après le déroulement de la procédure EPS-AKA, le MME choisit un algorithme de chiffrement et un algorithme d'intégrité pour la protection de la signalisation NAS. Les deux algorithmes sélectionnés doivent être disponibles et implémentés dans l'UE et dans le MME. Ensuite, le MME dérive les clés KNASEnc et KNASInt, et envoie le message 'Commande du mode de sécurité NAS' (appelé CMS NAS ou NAS Security Mode Command) à l'UE.

Ce message est protégé en intégrité via le champ NAS-MAC, mais il n'est pas chiffré. Puisque le MME connaît déjà les algorithmes et les clés qui ont été sélectionnés, Il peut donc commencer le déchiffrement de la signalisation NAS de la liaison montante juste après avoir envoyé le message 'CMS NAS'. S'il n'y a pas de problème dans le message CMS NAS reçu, l'UE envoie au MME le message 'mode de sécurité NAS établi' (NAS Security Mode Complete) chiffré et protégé en intégrité.

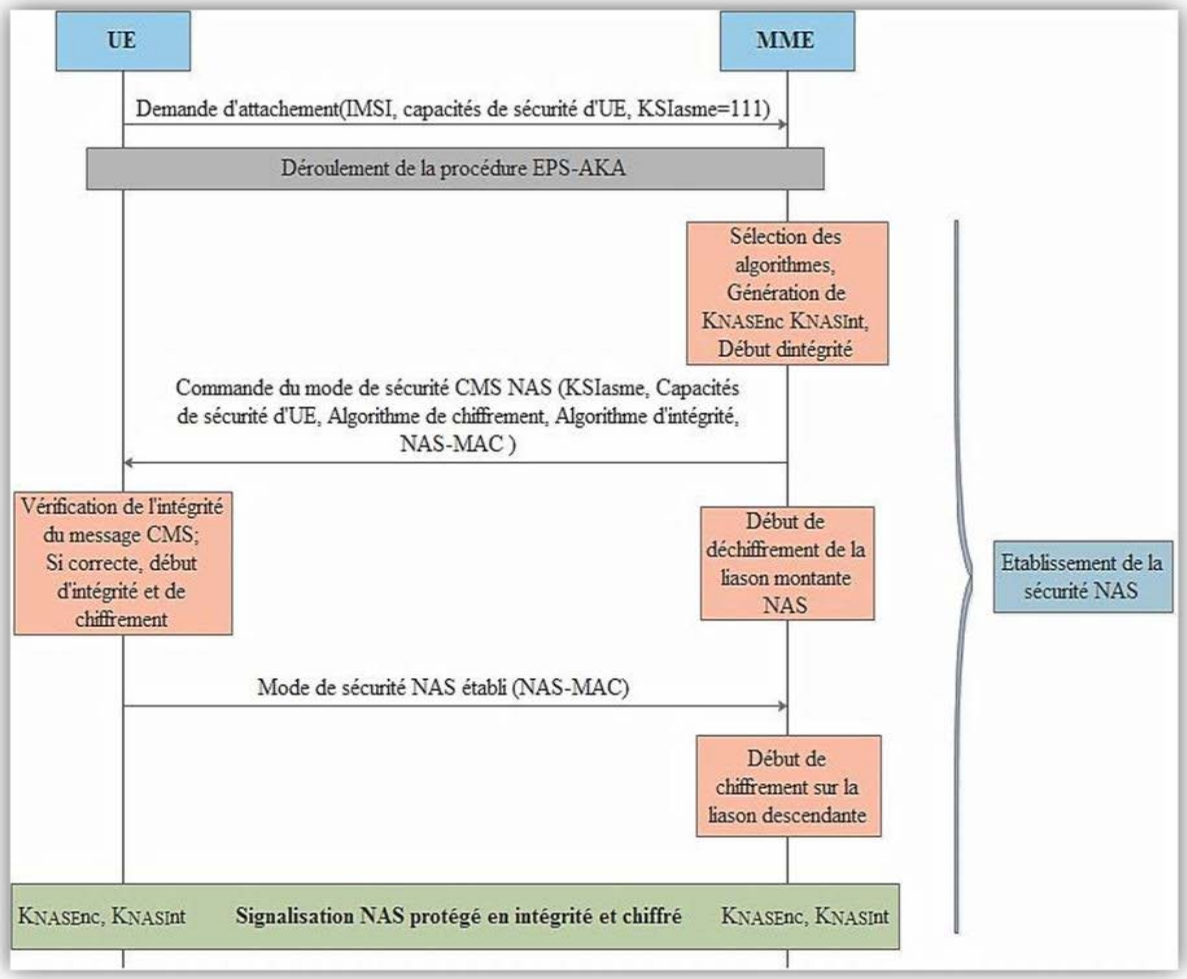

Figure 11: Procédure d'établissement de la sécurité NAS

Le MME peut commencer le chiffrement de la signalisation NAS émis sur la liaison descendante après réception et vérification du message ‘Mode de sécurité établi’.
Si le ME détecte que l'intégrité du message ‘CMS NAS’ n’est pas correcte, il envoie un message de rejet (NAS Security Mode Rejet) protégé avec les clésNAS établis (avant l’émission du message CMS NAS). Or, lors du premier attachement il n’y a aucun contexte de sécurité NAS qui est encore établit, et dans ce cas s’il y a un message de rejet à envoyer, il sera émis sans aucune protection.

3.2.8 Protection de la signalisation AS et des données usagers :

Après l’établissement de la sécurité NAS, le MME calcule la clé KeNodeB, etl’envoie à l’eNB avec les capacités de sécurité d’UE comme indiqué dans la figure.
L’eNB choisit un algorithme de chiffrement et un algorithme d’intégrité parmi les algorithmes disponibles dans l’UE. Les identifiants des algorithmes sélectionnés contribuent, en tant que paramètre d’entrée, à la dérivation des clés AS (KRRCEnc, KRRCInt et KUPEnc).
Ensuite l’eNB envoie le message ‘Commande du mode de sécurité AS’, CMS AS, pour indiquer à l’UE les algorithmes AS sélectionnés et pour annoncer le déclenchement de la sécurité. Ce message est protégé en intégrité via le champ MAC-I, généré à l’aide de KRRCInt. De son côté, l’UE dérive les 3 clés du niveau AS et, en utilisant l’algorithme d’intégrité indiqué dans le message CMS AS reçu, il vérifie avec léKRRCInt si le code MAC-I est correcte ou non.
Si oui, l’UE répond avec le message ‘Mode de sécurité AS établi’, protégé en intégrité et contre la répétition, et il se prépare à recevoir des messages RRC et des données usagers chiffrés sur la liaison descendante. Sinon, le MME répond avec un message d’échec.

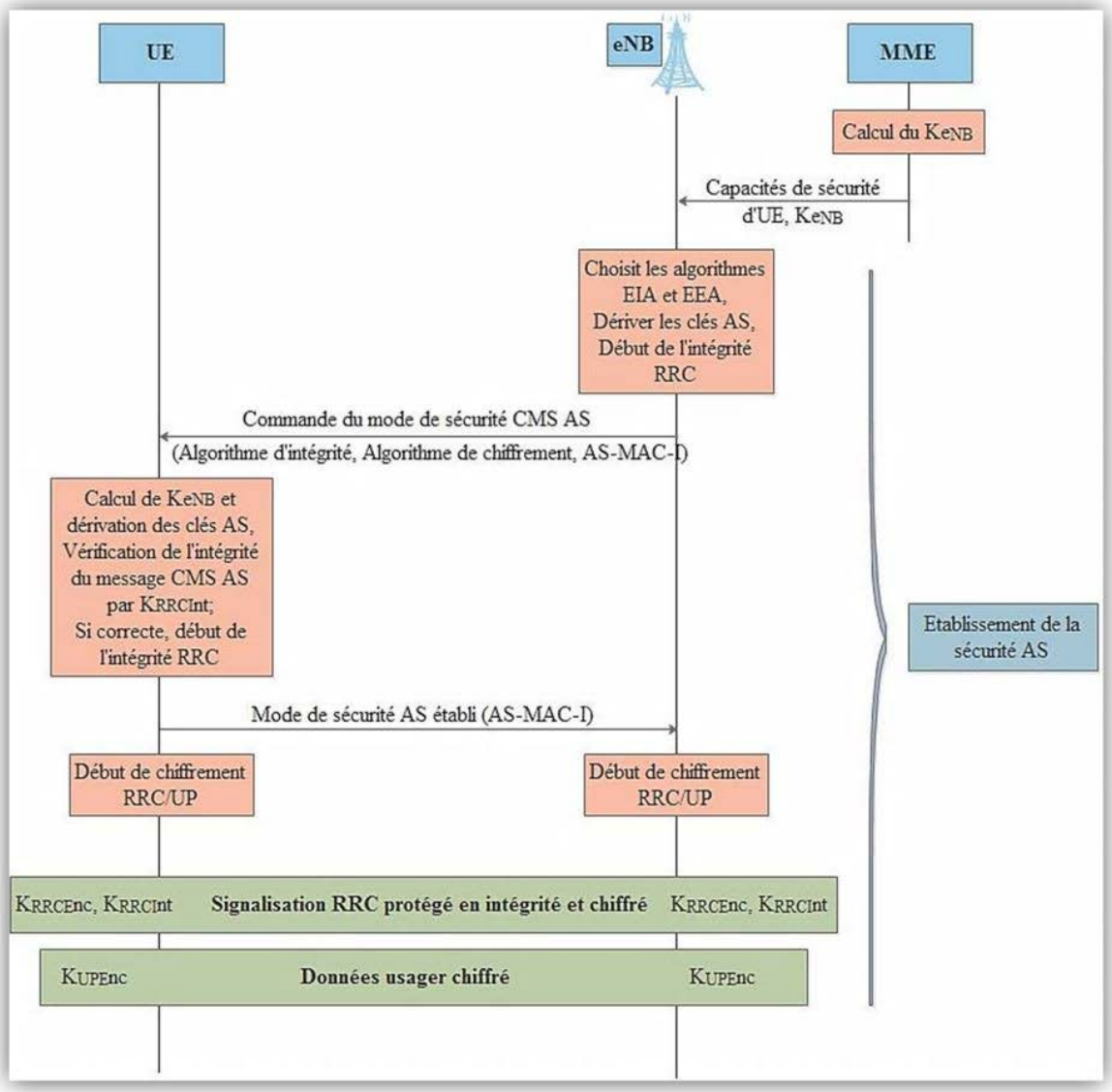

Figure12: Établissement de la sécurité AS

3.2.9 Protection de l'intégrité des messages RRC

La protection de l'intégrité de la signalisation a lieu à deux niveaux :

1. Entre le mobile et le MME pour la signalisation NAS : La protection de l'intégrité des messages NAS est effectuée entre l'UE et le MME, qui ajoute un code MAC à la fin des messages de signalisation NAS transmis. Ce code est calculé en utilisant l'algorithme d'intégrité EIA et la clé d'intégrité KNASInt. Plusieurs paramètres sont également appliqués à l'entrée l'algorithme afin d'assurer l'unicité du code MAC obtenu. La figure suivante montre la manière d'utilisation de cet algorithme :

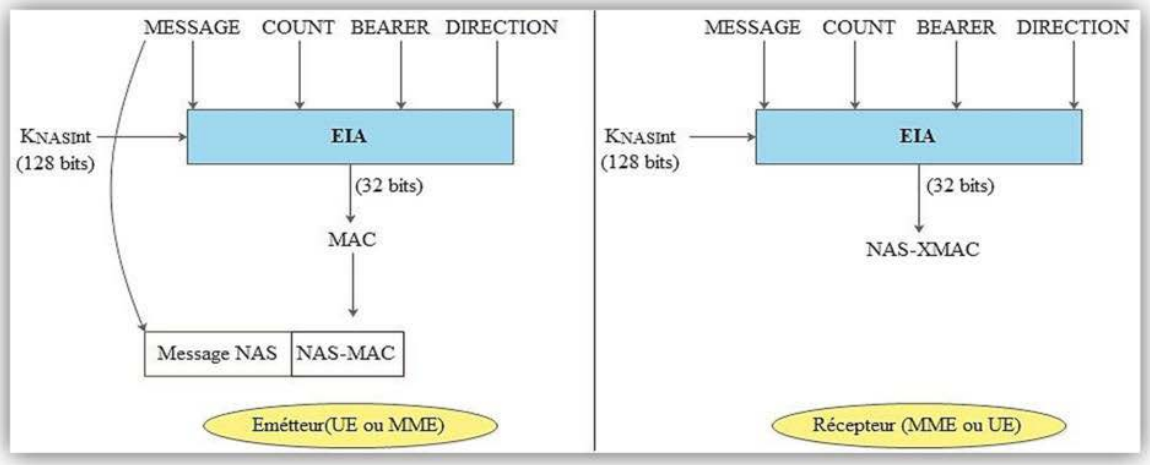

Figure 13: Mécanismes de protection et de vérification de l'intégrité des messages NAS

KNASInt : La clé d'intégrité NAS de 128 bits.

- ✓ **MESSAGE :** Le message NAS à protéger (comme par exemple le messageCMS-NAS ou autre).
- ✓ **COUNT :** Un compteur de séquence sur 32 bits.
- ✓ **BEARER :** L'identifiant, sur 5 bits, du bearer qui porte le message NAStransmis. Il prend une valeur constante égale à 0x00 puisque tous les messages
- ✓ NAS sont transportés sur un seul bearer.
- ✓ **DIRECTION :** Est un seul bit qui indique le sens du message et qui prend la valeur '0' pour la voie montante et '1' pour la voie descendante. Ce champ est utilisé pour éviter l'utilisation des mêmes paramètres d'entrée pour les deux voies.

Le côté qui envoie le message, calcule le code MAC, NAS-MAC de 32 bits et l'ajoute à la fin du message NAS. Le récepteur effectue la même opération de calcul du code d'authentification à partir du message NAS reçu, et le résultat NAS-XMAC est ensuite comparé avec le NAS-MAC reçu. S'ils sont égaux alors le message NAS est accepté et s'ils sont différents le message NAS sera rejeté.

2. Entre le mobile et l'eNodeB pour la signalisation RRC : Le même mécanisme de protection et de vérification d'intégrité utilisé pour les messages NAS est appliqué sur les messages RRC avec presque les mêmes paramètres d'entrée (voir figure 14) mais

avec un algorithme d'intégrité (EIA) qui n'est pas nécessairement le même. La petite différence par rapport à la protection d'intégrité NAS est que :

- ✓ La clé d'intégrité est la KRRCInt au lieu de KNASInt.

3.2.10 Chiffrement des RRC et des données usagers :

Le chiffrement a lieu à deux niveaux :

1. Entre le mobile et le MME (trafic de signalisation) : Le chiffrement des messages NAS, présenté dans la figure, est effectué entre l'UE et le MME avec l'algorithme EEA (EPS Encryption Algorithm). Ce dernier utilise les mêmes paramètres d'entrée (COUNT, BEARER, DIRECTION) que l'algorithme d'intégrité (EIA), à l'exception de la clé, qui est KNASEnc pour le chiffrement, et le paramètre supplémentaire 'LENGTH'. Ce dernier est un champ de 16 bits qui sert à indiquer la longueur du bloc de chiffrement.

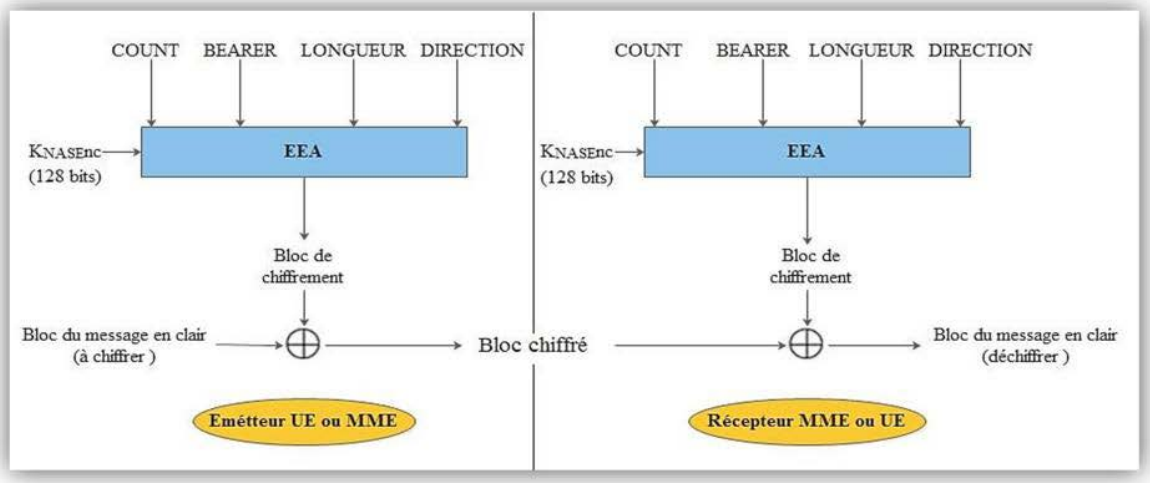

Figure 14: Mécanismes de chiffrement et déchiffrement des messages NAS

L'opération de chiffrement consiste à additionner bit par bit, par ou exclusive, un bloc du message NAS en clair, à un bloc de chiffrement (Keystream Block) généré par l'algorithme EEA et de même longueur (LENGTH).

De manière similaire, le déchiffrement est une opération symétrique. Il est effectué avec l'opération ou exclusive entre le bloc reçu et le même bloc de chiffrement (Keystream Block) généré à partir du même algorithme et le même ensemble de paramètres. En chiffrement, on utilise les mêmes algorithmes utilisés en intégrité.

2. Entre le mobile et l'eNodeB (trafic usager et trafic de signalisation) : Le même mécanisme de chiffrement utilisé pour les messages NAS est appliqué sur les messages AS (signalisation

et données) avec presque les mêmes paramètres d'entrée (voir figure ci-dessus) mais avec un algorithme de chiffrement (EEA) qui n'est pas nécessairement le même. Les petites différences par rapport au chiffrement NAS sont :

- La clé de chiffrement est la KRRCEnc au lieu de KNASEnc pour les messages de signalisation.
- L'utilisation de la clé KUPEnc pour le chiffrement des données usagers.

3.2.11 Identité temporaire :

IMSI est un identifiant permanant qui est unique pour chaque utilisateur dans le monde, comme nous avons vu précédemment avant chaque communication, le terminal s'authentifie auprès du réseau, pour rappel le chiffrement n'est pas activé lors des premiers échanges et si on utilise systématiquement IMSI pour s'identifier alors il serait très simple d'être localisé.

La solution consiste à mettre en place un mécanisme qui limite l'utilisation de l'IMSI au strict minimum. Ainsi lors de la première authentification, le terminal n'a d'autres choix que d'utiliser l'IMSI par contre une fois l'authentification réussie et le chiffrement du lien radio soit activé, le réseau lui attribue un identifiant temporaire appelé « TMSI ».

Comme ce dernier est alloué une fois que le chiffrement est activé, il est impossible à un pirate de faire le lien avec l'IMSI de l'abonné.

Le TMSI est alloué par le MME du terminal de façon autonome, il peut être changé plus ou moins fréquemment selon la politique de l'opérateur, par exemple :

- ✓ A chaque fois que le mobile établit une nouvelle session.
- ✓ A chaque changement de MME.
- ✓ Où lorsqu'il y a un changement important du côté du terminal mobile (la carteUSIM est retirée).

Le TMSI est un identifiant très court sur 4 octet avec une signification locale pour un MME, la même valeur peut être utilisée par deux MME pour deux mobiles différents. Il faut donc une structure plus grande d'identification qui a une signification globale, cette structure s'appelle le GUTI (Globally Unique Temporary UE Identity). Le GUTI contient le TMSI ainsi que l'identifiant unique du MME qui a alloué le TMSI. L'identifiant est constitué de :

- ✓ L'identité de l'opérateur (le couple MCC, MNC)
- ✓ Une identité de groupe MME (MME group ID)
- ✓ Un code MME propre au groupe.

A tout instant, un GUTI identifie de manière unique un utilisateur, tout en gardant lapossibilité de changer le GUTI pour un même abonné.

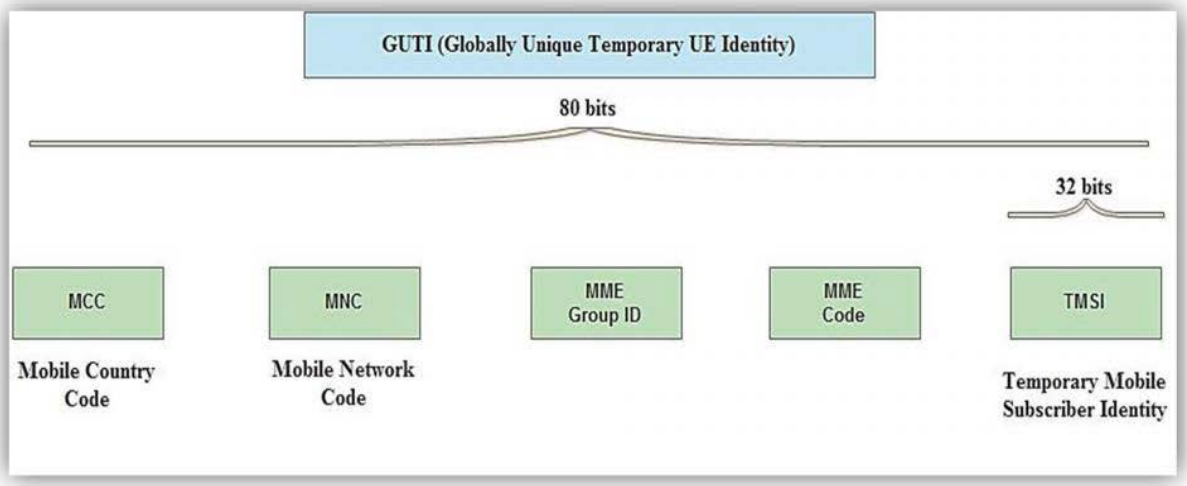

Figure 15: identité temporaire(GUTI)

3.3 La qualité de service (QOS)

3.3.1 Définition :

La qualité de service est la capacité de transmettre dans de bonnes conditions un certain nombre de paquets dans une connexion entre émetteur et récepteur, et cela peut être présenté sous plusieurs termes tels que la disponibilité, débit, délai de transmission…

3.3.2 Le but de la QOS :

Le but de la QOS est donc d'optimiser les ressources du réseau et de garantir de bonnes performances aux applications. La qualité de service sur les réseaux permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par application suivant les protocoles mis en œuvre au niveau de la touche réseau.

Selon les types d'un service envisagé, la qualité pourra résider :

-Le débit (téléchargement ou diffusion vidéo).

-Le délai (pour les applications ou la téléphonie).

-La disponibilité (accès à un service partagé).

-le taux de pertes de paquets

3.3.3 Paramètres de la QOS

3.3.3.1 Le débit :

Il définit le volume maximal en bits pour la transmission de l'information par unité de temps dans une communication entre un émetteur et un récepteur.

3.3.3.2 La perte de paquets :

Elle correspond aux octets perdus lors de la transmission des paquets. Elle s'exprime en taux de perte. Plutôt rare, elle correspond au nombre de paquet de données qui n'ont pas étaient reçu par la destination lors d'une communication.

3.3.3.3 Le délai de transit (latence) :

C'est le délai de traversé du réseau, d'un bout à l'autre, par un paquet. Les différentes applications présentes dans un réseau n'auront pas le même degré d'exigence en fonction de leur nature :

Faible : S'il s'agit d'une messagerie électronique ou de fichiers.

Fort : S'il s'agit de données « voix ».

3.3.3.4 La gigue :

Désigne les variations de latence des paquets. La présence de gigue dans le flux peut provenir des changements d'intensité de trafic sur les liens de sorties des commutateurs.
Elle dépend de volume et de trafic et du nombre d'équipements sur le réseau.

3.3.3.5 La bande passante :

Il existe deux modes de disponibilité de la bande passante, en fonction du type de besoin exprimé par l'application :

- Le mode « burst » est un mode immédiat, monopolise toute la bande passante disponible.
- Le mode « stream » est un mode constant, plus adapté aux fonctions audio/vidéo ou aux applications interactives.

3.3.4 Qualité de service dans le réseau 4G :

Le développement du réseau internet et le nombre d'utilisateurs pouvant se connectés à ce réseau impose le recours à des réseaux importants de QOS. Les nouveaux besoin en termes de mobilité des utilisateurs et la croissance des réseaux permettant le nomadisme des utilisateurs ont fait migrer le problème vers des réseaux sans fil.

3.3.4.1 Le bearer EPS :

Le bearer EPS est un équivalent du contexte PDP (Packet Data Protocol) en 2G/3G. Il représente un Concept logique qui est établi entre le terminal et la PDP GW et qui agrège plusieurs flux Data transportés entre les deux entités. Il permet d'identifier de manière unique des flux de trafic recevant la même qualité de service entre le terminal et la PDN GW. Tous les flux associés à un bearer EPS reçoivent les mêmes traitements en termes de forwarding (expédition des paquets).

IL existe deux types de bearers EPS :

- ✓ Le défaultbearer, le premier bearer établi lorsque le terminal se connecte à un PDN, il reste actif durant toute la connexion.
- ✓ Les dedicatedbearer, tous les bearers additionnels établis avec le même PDN.

3.4 Conclusion :

Nous avons étudié dans ce chapitre, l'ensemble des mécanismes de sécurité des réseaux de quatrième génération. D'une part, en passant par la migration progressive des protocoles de la troisième génération, l'authentification mutuelle et d'autre part, l'utilisation des algorithmes de chiffrement robustes apportent des améliorations significatives en matière des sécurité des échanges.

L'introduction de nouveaux mécanismes de protection et l'option du transport complet basé sur IP dans les réseaux 4G n'ont jamais été utilisé dans un réseau d'accès radio 2G ou 3G et font partie des améliorations nécessaires.

CHAPITRE 4 : Analyse et amélioration de la sécurité de la 4G/LTE

4.1 Introduction :

Dans ce chapitre, il est question d'analyser les faiblesses de la sécurité EPS et surtout les vulnérabilités du protocole EPS-AKA, sachant qu'il est la pierre angulaire de toute l'architecture de sécurité et permettant surtout l'accès des abonnés au réseau. Nous étudionsles faiblesses identifiées dans la littérature spécialisée, et nous identifions de nouvelles faiblesses de ce protocole qui peuvent conduire à des attaques malveillantes contre les abonnés et le réseau.

Nous étudions et analysons quatre protocoles permettant d'améliorer la sécurité en EPS. Les deux premiers protocoles (EMSUCU, et Enhanced EMSUCU) traitent le problème de la transmission de l'IMSI en claire. Ils protègent tous les deux, cette identité par le chiffrement symétrique afin d'éviter les risques d'identification des utilisateurs. Le troisième protocole étudié est le standard de 3GPP, l'EPS-AKA. Ses différentes faiblesses ont été identifiées ainsi que les différentes attaques que peuvent être montées sur ce protocole. L'analyse des deux meilleurs protocoles montre également des petites vulnérabilités. Notre objectif est de proposer un nouveau protocole AKA générique pour être utilisé comme une alternative de protocole 3GPP EPS-AKA.

Sur cette lancée, nous proposons un protocole, qui apporte des améliorations pour pallier tous les problèmes et toutes les faiblesses quant à l'EPS ainsi que les autres protocoles. Le protocole FP-AKA (Full Protection-AKA) a été évalué et a été comparé avec les autres protocoles considérés, selon quatre paramètres. Ces paramètres sont : le risque, le coût, le taux des données ajoutées sur les messages de signalisation. Nous allons montrer que FP-AKA a le meilleur résultat selon les deux premiers paramètres et un très bon résultat dans les deux paramètres restants.

4.2 Analyse des vulnérabilités du protocole EPS-AKA :

Dans cette partie nous effectuons une analyse et une synthèse des points faibles du protocole EPS-AKA et expliquons quels types d'attaques peuvent s'effectuer et quels dégâts cela peut causer. Selon nos recherches, nous admettons que trois (3) grands types d'attaques peuvent se faire contre des messages échangés ou des fonctions utilisées durant l'EPS-AKA.
Avant de voir les solutions existantes et notre propre protocole proposé qui assure la protection contre tous ces types d'attaques, nous proposons en premier lieu de présenter les 3 grands types d'attaques.

4.2.1 Attaque de déni de service contre l'UE :

Durant la procédure EPS-AKA, et comme l'UE et le MME ne peuvent pas authentifier les messages qu'ils échangent (ils ne possèdent pas encore des clés de sécurité communes), un attaquant peut modifier un message transmis ou renvoie un message déjà transmis. Ceci peut dans certains cas couper la connexion entre le mobile et le réseau et peut causer un déni de service.

4.2.2 Attaque contre la clé sécrète permanente K :

La meilleure attaque contre la clé K consiste dans la cryptanalyse des fonctions de sécurité f1 à f5, utilisées durant la procédure AKA.Pour mettre en évidence les failles de la sécurité EPS, nous montrons ci-dessous les types d'attaques contre les fonctions de sécurité.

4.2.2.1 Attaque sur la voie radio

Au cours du déroulement de la procédure AKA, les messages sont transmis en clair sans aucune protection. Dans ce cas, un attaquant qui écoute la voie radio peut facilement intercepter les messages échangés entre l'UE et le réseau. Ces messages peuvent être utilisés pour monter les attaques de cryptanalyse contre plusieurs fonctions de sécurité, dans le but de dévoiler la clé K.

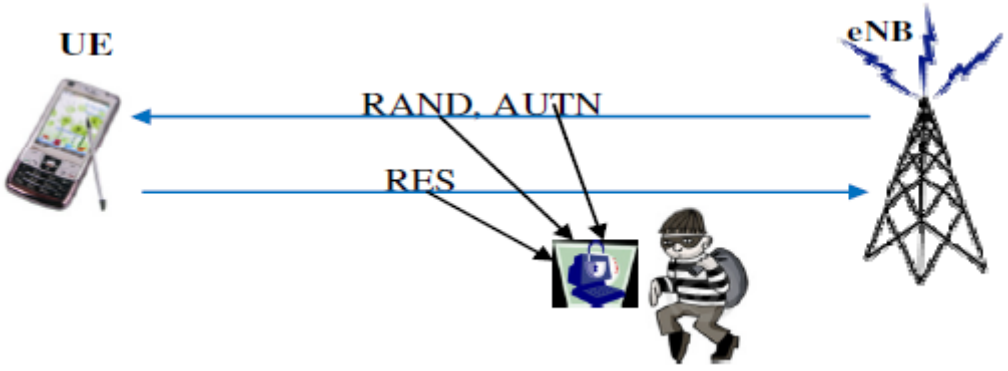

Figure 16 : Attaque sur la voie radio

Ces messages (interceptés par l'attaquant) sont normalement utilisés dans les fonctions de sécurité f1 à f5 comme montre la figure suivante.

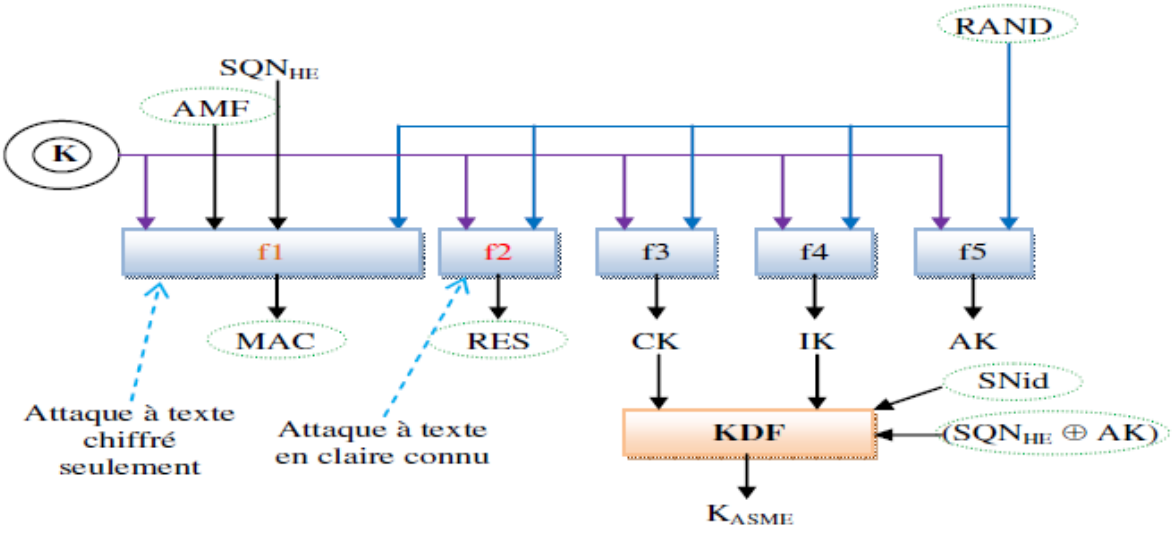

Figure 17 : Exposition des fonctions de sécurité f1, f2 aux attaques cryptographiques

Les valeurs des paramètres interceptés RAND, AMF, MAC et RES sont encadrés par des cercles pointillés. Dans ce cas l'attaquant peut monter une attaque de type à texte en clair connu contre la fonction f2, puisqu'il possède son entrée RAND et sa sortie RES. Aussi il peut monter une attaque à texte chiffré contre la fonction f1, puisqu'il possède seulement sa sortie (en absence du SQN qui est masqué par AK). Donc la fonction 'f2' présente la faiblesse la plus grave parmi toutes les fonctions de sécurité utilisées. Pour bien protéger les fonctions f1 et f2 nous pensons que la solution consiste à chiffrer les messages AKA envoyés sur la voie radio et ne rien envoyer en clair. Dans ce cas l'attaquant doit commencer son attaque sur l'algorithme de chiffrement avec lequel RAND, AUTN et RES sont chiffrés.

4.2.2.2 Attaque contre la carte à puce UICC

Elle consiste à utiliser un ME modifié qui lui permet de voir les messages reçus et envoyés par la carte UICC. Le pirate utilise ces informations pour monter une attaque de cryptanalyse contre la clé K lors de la procédure AKA.

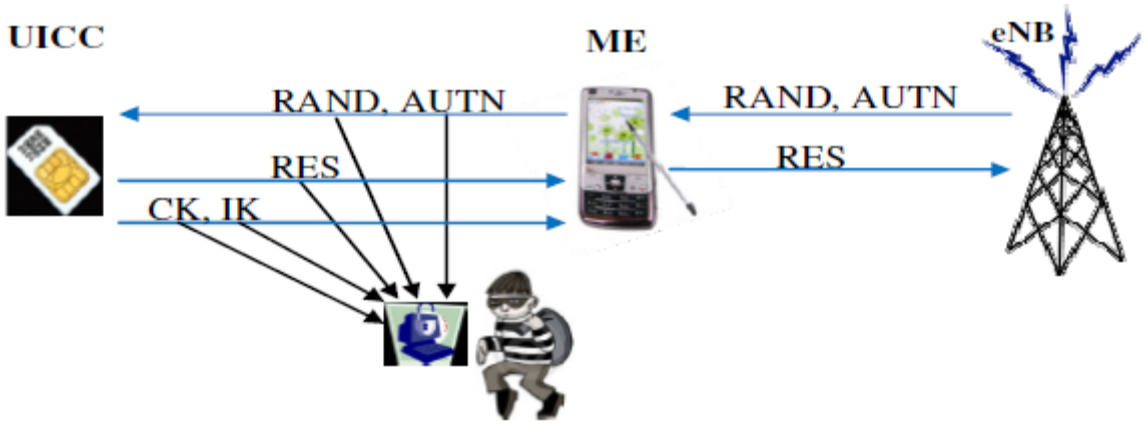

Figure 18: Attaque contre la carte à puce

Nous constatons que la différence entre l'attaque sur la voie radio et cette attaque, vient du fait que la carte à puce transmet les clés CK et IK au ME. Alors, dans ce cas, l'attaquant peut monter des attaques à texte en clair connu contre les fonctions de sécurité f3 et f4 (avec l'attaque contre f2) commemontre la figure 19. Les données qui sont à sa portée sont encadrées par des cercles en pointillés. La clé KASME peut être également dévoilée si on connaît la fonction KDF utilisée.

La fonction f2 est donc la plus fragile et la plus exposée aux attaques. Les fonctions f1, f3, f4 sont aussi disposées à des attaques et c'est seulement la fonction 'f5', qui semble la plus protégée. Il y a des méthodes de cryptanalyse qui permet de retrouver la clé secrète si on connaît la fonction utilisée comme la méthode qui a été développée pour retrouver la clé secrète de la fonction f8 cassée (KASUMI).

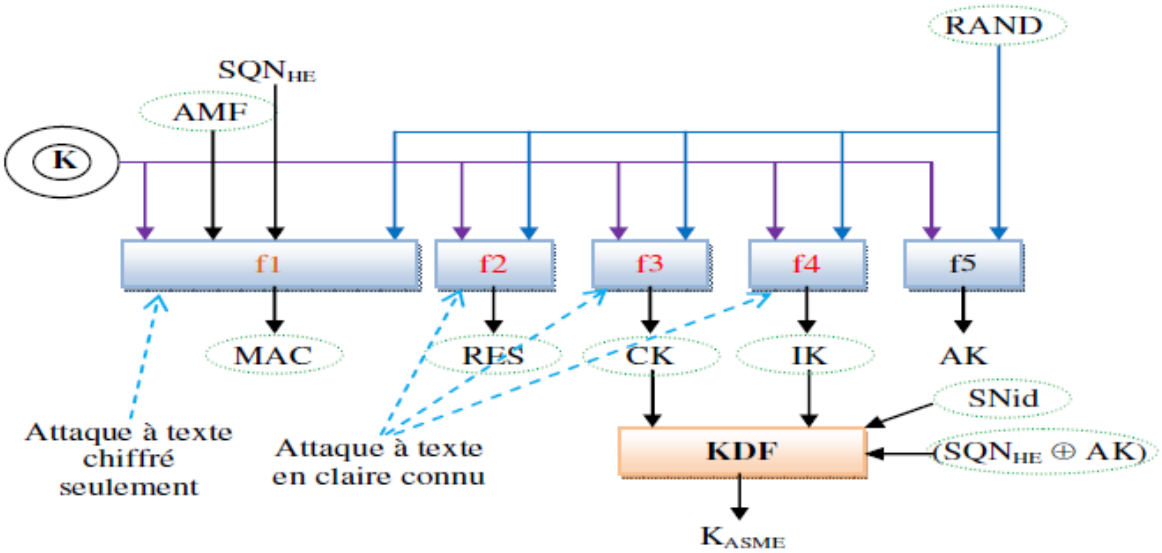

Figure 19 : Attaques contre les fonctions de sécurité, via l'attaque contre la carte à puce

Il est préférable d'augmenter la taille de la clé K à 256 bits et à utiliser une clé temporaire à la place de la clé K lors de la génération des AVs. Cela permettra de limiter l'exposition de la clé permanente K

4.2.3 Attaques sur les réponses des données d'authentification (AVs) :

Elle consiste à violer et permuter certains messages d'authentification échangés soit par un attaquant intérieur ou extérieur. Ces deux attaques, de l'extérieur ou de l'intérieur, s'appliquent même si les messages entre le MME et le HSS sont protégés en confidentialité et en intégrité.

Après l'analyse de la sécurité du protocole par l'outil CryptoVerif, il a été constaté que la vulnérabilité qui conduit à ces deux attaques vient de la permutation (swap) non détectée des réponses des données d'authentification. Elle peut êtrebloquéesi le MME peut déterminer pour quel IMSI la réponse du HSS est générée. Pour éviter les attaques actives de l'extérieur ou de l'intérieur, nous proposons que le MME génère et utilise un identificateur de la session, Session-id pour chaque demande des données d'authentification envoyée au HSS.Pour cela les réponses des données d'authentification, la protection en intégrité et en confidentialité de tous les messages échangés entre MME et HSS sera obligatoire.

4.3 Protocoles existants et proposés pour remplacer l'EPS-AKA :

Afin de renforcer la robustesse et la capacité du protocole EPS-AKA contre les différentes attaques, plusieurs protocoles ont été proposés.

Nous étudions dans ce paragraphe les deux protocoles les plus importants SE-AKA (Security Enhanced-AKA), et EC-AKA (EnsuredConfidentiality-AKA) qui ont été proposés pour remplacer le protocole EPS-AKA.Comme le 3GPP recommande d'utiliser la cryptographie à clé publique pour protéger l'IMSI, ces deux protocoles sont basés sur une infrastructure à clé publique afin de sécuriser les messages échangés.

4.3.1 Protocole SE-AKA :

Le protocole SE-AKA apporte des améliorations considérables sur l'EPS-AKA. Il a sécurisé la transmission entre les différents nœuds du réseau EPS par la protection, via le chiffrement à clés asymétriques, de presque tous les messages échangés entre les différentes entités du réseau.

L'UE commence l'exécution du protocole SE-AKA par le chiffrement de son IMSI avec l'appui de la clé publique du HSS (PKH). L'UE envoie la demande d'accès qui contient son IMSI chiffré, A=(IMSI) PKH, et l'identité du HSS IDHSS auquel l'utilisateur appartient et le MME. À la réception de cette demande par le MME, ce dernier utilise aussi le PKH afin de chiffrer son identité du réseau SN id pour générer le paramètre B= (SN id) PKH. Ensuite, la demande des données d'authentification formée par A et B, sera envoyée au HSS. À la réception de cette demande, le HSS déchiffre A et B par sa clé privée pour extraire l'IMSI de l'utilisateur et le SN id. Puis, il envoie par un message C, les n vecteurs d'authentification AV et l'IMSI de l'abonné, chiffrés tous par la clé publique PKM du réseau MME. Ce dernier envoie la demande d'authentification à l'UE, comme un message D chiffré par la clé publique de l'abonné. Le message D contient les paramètres : RAND, SN id, l'identité temporaire S-TMSI, et l'identité de clé KASME établie KSIASME. La suite du protocole se fait exactement comme dans l'EPS-AKA sauf le dernier message E transmis chiffré, de l'UE au MME, par la clé publique de ce dernier.

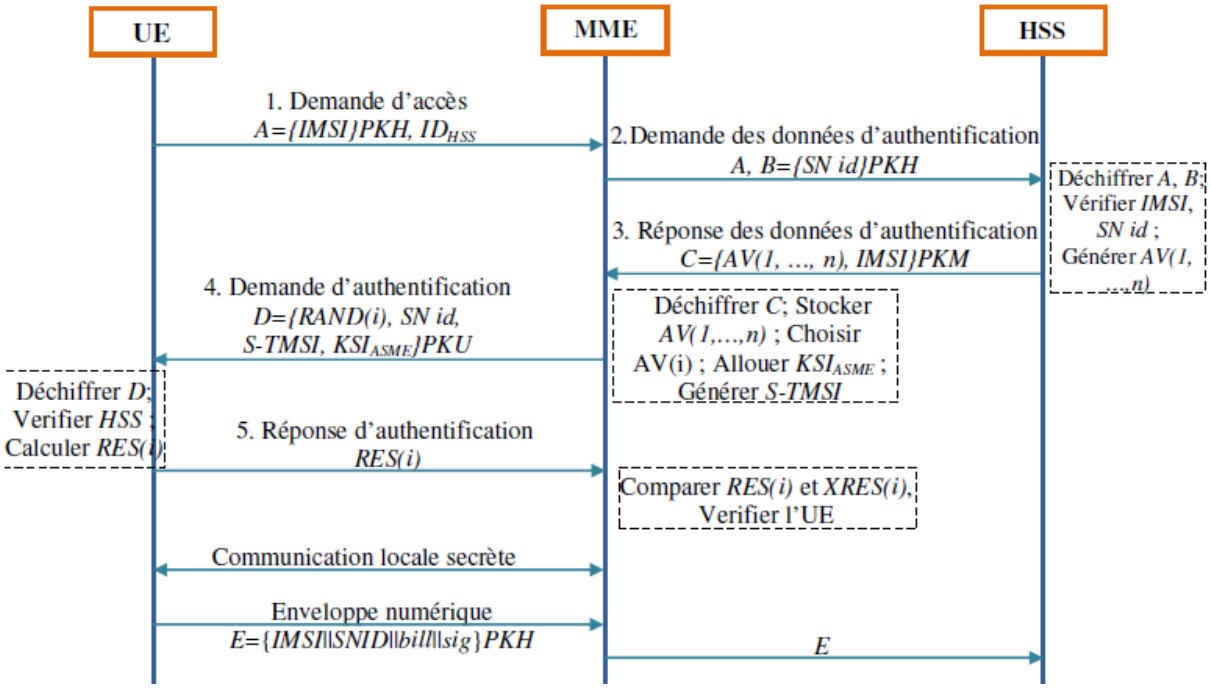

Figure 20 : Messages de signalisation SE-AKA

4.3.1.1 Cryptanalyse du protocole SE-AKA :

Vu que l'identité IMSI d'un abonné est toujours fixe,par suite son chiffrement par la même clé publique (du HSS), et en utilisant la méthode RSA ou ECC donnera toujours la même valeur. Ainsi un utilisateur'U' qui transmet son IMSI ou sa valeur chiffrée (constante) aura la

même confidentialité et le chiffrement n'améliore pas le niveau de sécurité. Un IMSI chiffré sera aussi vulnérable que l'IMSI lui-même.

Après, le protocole SE-AKA et nous avons trouvé qu'il est vulnérable à plusieurs attaques : attaque par dictionnaire, attaque par rejoue, et sur l'UE, et attaque MITM.

4.3.1.1.1Attaque par dictionnaire : La plupart du temps, le choix du mot de passe est laissé libre auxutilisateurs du système et ces derniers utilisent généralement des mots de passe qu'ils peuvent retenir facilement en rapport avec leur nom, année de naissance ou le nom des choses ou des personnes qu'ils aiment. Donc, une alternative du pirate consiste à constituer un dictionnaire de mot de passe possibles d'un utilisateur et ensuite procéder au teste de ces combinaisons.

4.3.1.1.2 Attaque par rejoue : Elle consiste à usurper l'identité, à travers l'écoute du réseau et intercepter des paquets afin de les exploiter

4.3.1.1.3 Attaques homme du milieu « man in the middle » :Cette attaque est aussi appelée attaque de l'intercepteur. C'est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour une des parties sans que ni l'une ni l'autre ne puisse se douter que le canal de communication a été compromis.

4.3.2 Protocole EC-AKA

Ce protocole a aussi introduit des améliorations importantes sur l'EPS-AKA. Il utilise le chiffrement asymétrique pour chiffrer les messages A, B, et C, avec l'aide des clés publiques de HSS (PKH), et de MME (PKM), et sur le chiffrement symétrique pour chiffrer les autres messages D, E et F en se basant sur la clé de chiffrement EK générée dans l'UE et dans le HSS, et envoyé par ce dernier au MME.

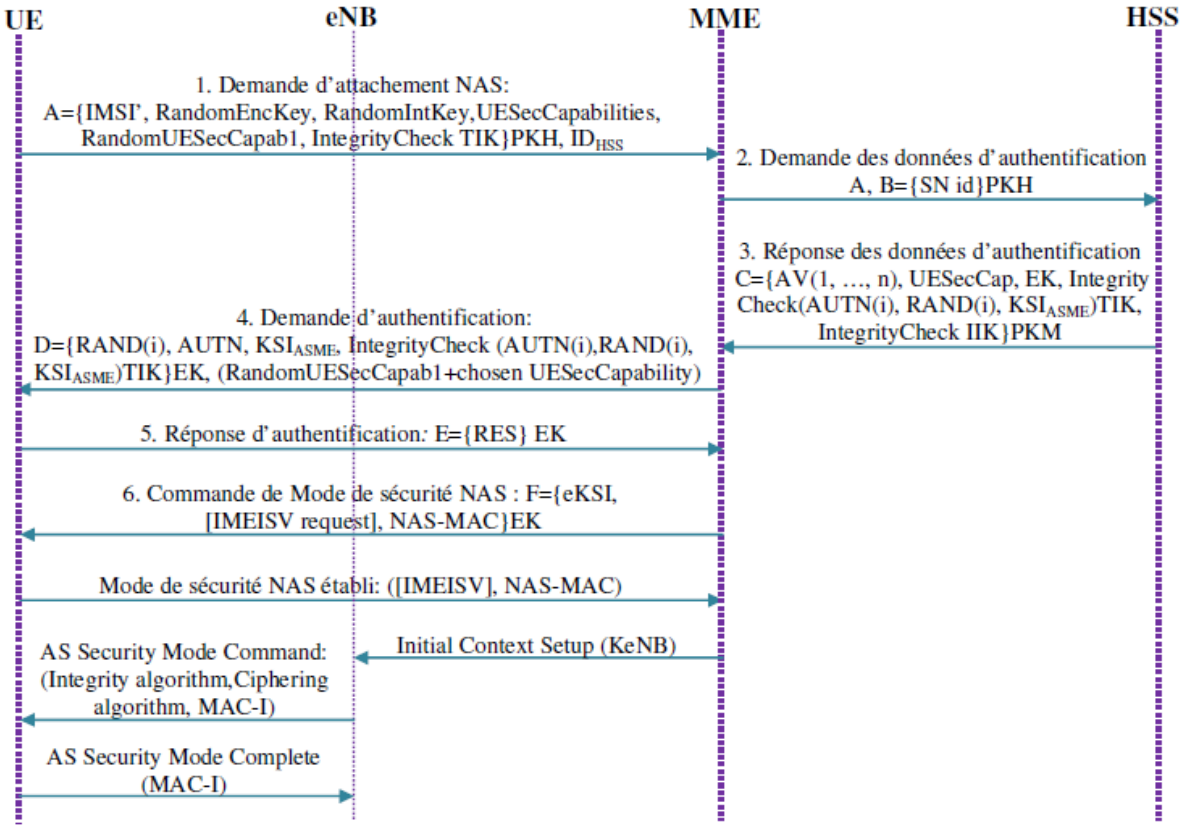

Figure 21 : Message de signalisation du protocole EC-AKA

En effet, l'UE envoie son IMSI et les capacités de sécurité (*UESecCapabilities*) dans la demande d'attachement et aussi des valeurs aléatoires comme le *RandomEncKey*, et le *RandomIntKey*qui servent à garantir l'obtention d'un IMSI chiffré dynamique. Ce qui permet de protéger l'IMSI contre l'attaque par dictionnaire. Ces valeurs aléatoires seront utilisées aussi pour d'autres fins de chiffrement et d'intégrité.

4.3.2.1 Cryptanalyse du protocole EC-AKA

Les améliorations de l'EC-AKA ont ajouté une sécurité importante au réseau, mais en analysant ce protocole nous avons trouvé qu'il est aussi vulnérable, tout comme le protocole SE-AKA aux trois attaques : attaque par dictionnaire, attaque par rejoue, et attaque MITM.

4.3.3 Nomenclature :

- **PSQN** (32 bits) : une valeur aléatoire de 32 bits spécifiée par l'UE lors de la première connexion. À partir de la deuxième connexion cette valeur sera égale au NSQN (New SQN) fourni par le HSS.

- **RandIK**(128 bits) : une valeur aléatoire (RandomIntegrity Key) générée par l'UE et utilisée pour dériver la clé d'intégrité TIK.
- **RandEK**(128 bits) : une valeur aléatoire (RandomEncryption Key) générée par l'UE et utilisée pour dériver la clé de chiffrement EK.
- **TIK** (128 bits) = KDF (K, RandIK).
- **EK** (128 bits) = KDF (K, RandEK).
- **RandUESecCapab**(6 bits) : Un nombre aléatoire généré par l'UE dans le but de permettre au MME et à l'utilisateur de se mettre d'accord et en toute sécurité sur les algorithmes de chiffrement et d'intégrité (ChosenUEsecCap).
- **UESecCapab**(12 bits) : la liste des algorithmes de chiffrement et d'intégrité supportés par l'UE.
- **(M), MACx**(32 bits): Le code Mac d'intégrité du message (M), généré en utilisant la clé d'intégrité x.
- **PKH**, **PKM** : Les clés publiques du réseau d'origine HSS, et du réseau de service MME respectivement.
- **KRM**, **KRH** : dénote la clé privée de MME et de HSS respectivement.
- **RandMH1** (128 bits) : valeur aléatoire générée par le MME et qui sert à la génération d'une clé de sécurité.
- **RandHM2** (128 bits) : valeur aléatoire générée par le HSS et qui sert à la génération d'une clé de sécurité.
- **MHK** (256 bits) : clé secrète partagée entre le MME et le HSS et donnée par MHK=KDF

(RandMH1||RandHM2, GUMMEI, IDHSS). Elle est divisée en deux clés MHIK et MHEK.

- **MHIK**, **MHEK** (128 bits) : sont les clés d'intégrité et de chiffrement respectivement, extraites du MHK telle que : MHIK est la première moitié de la clé MHK (les 128 bits de poids le plus fort) et MHEK est la deuxième moitié. Ces deux clés sont destinées à assurer l'intégrité et le chiffrement des messages échangés entre MME-HSS.

Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS

- **Session-id** (16 bits) : numéro utilisé à chaque demande des données d'authentification ou interaction entre le MME et le HSS. Il aide à indiquer à quel utilisateur ou à quelle session les messages échangés appartiennent.

- **NSQN** (32 bits) : Nombre généré par le HSS et envoyé chiffré à l'UE. Il servira à éviter les attaques par rejoue et DoS sur le HSS/AuC.
- **UMIK**, **UMEK** (128 bits) : ce sont deux clés partagées entre l'UE et le MME pour authentifier et chiffrer, respectivement les messages AKA échangés entre eux. On les utilise jusqu'à le début d'utilisation des clés NAS d'EPS-AKA, et elles sont données parKDF (EK, Distingueur d'Alogrithme, Alg.ID).
- **{*M*} K** : dénote le message *m* chiffré par la clé de chiffrement K.

4.3.4Protocole proposé FP-AKA

Nous proposons dans cette partie, notre protocole FP-AKA (Full Protection- Authentication and Key Agreement). Il est inspiré de l'EPS-AKA, EC-AKA, SE-AKA. Il resume leurs avantages et il apporte des améliorations pour palier contre les vulnérabilités.

- **Lancement du protocole FP-AKA :**

Le protocole FP-AKA consiste à assurer un canal sécurisé, et protégé en intégrité et en confidentialité. Ceci vise à identifier l'émetteur et échanger les données d'authentification en toute sécurité.

La figure suivante ci-dessousmontre la série des messages de signalisation échangés durant l'application du protocole FP-AKA.

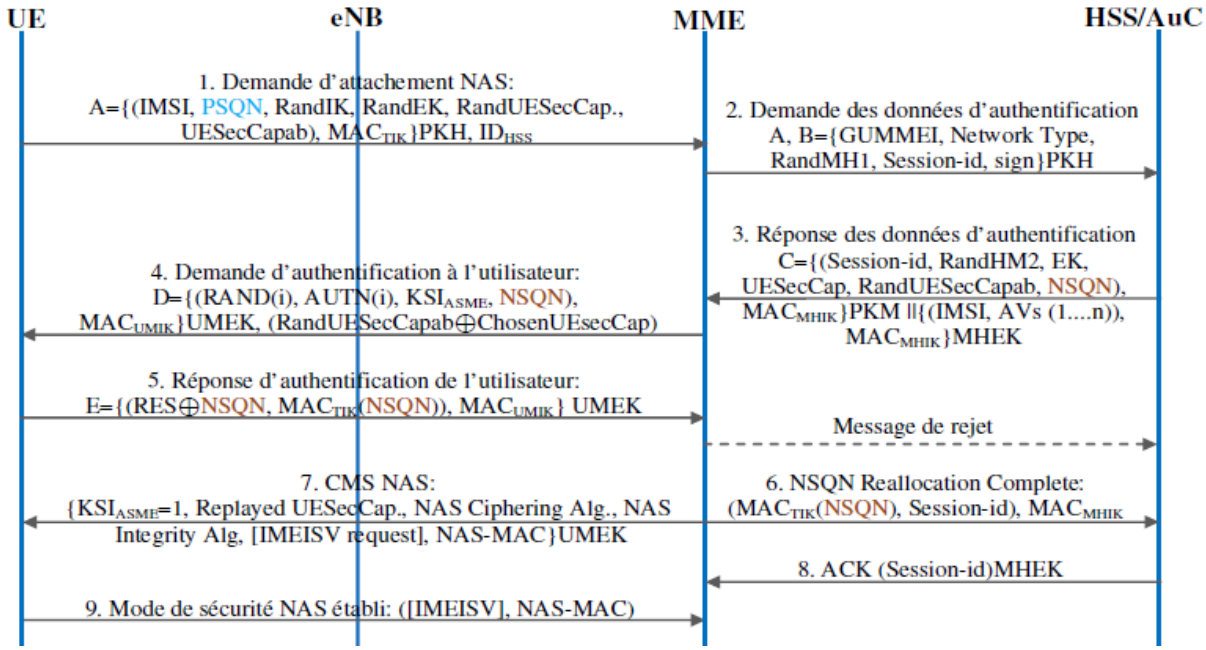

Figure 22 : Procédure de signalisation de FP-AKA

L'UE commence par générer les valeurs RandIK, RandEK, et RandUESec, et une valeur supplémentaire PSQN. Les 4 valeurs aléatoires générées seront transmises dans le message de demande d'attachement avec l'IMSI et les capacités de sécurité d'UE (UESecCapab). Le message est protégé en intégrité (en utilisant la clé d'intégrité TIK) et chiffré en utilisant la clé publique PKH. Après le chiffrement le message A obtenu est ajouté à l'identifiant du HSS, {A, ID_{HSS}}.

- Message émis de MME à HSS : Demande des données d'authentification : A, B={GUMMEI, Network Type, RandMH1, Session-id, Sign} PKH

Après la réception de la demande d'attachement de l'abonné, le MME extrait l'IDHSS afin de savoir vers quel réseau d'origine HSS il doit émettre sa requête et quelle clé publique PKH 160 Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS utilise-t-il pour la chiffrer. Le MME crée un message contenant : son identité GUMMEI, le type du réseau mobile (LTE ou UMTS), une valeur aléatoire RandMH1, et un identificateur de session Session-id. La RandMH1 sera utilisée dans le processus de génération d'une clé commune MHK entre MME et HSS. Le message est signé par la clé KRM afin de protéger son intégrité et authentifier le MME émetteur, et il est chiffré ensuite par la clé PKH pour former le message B. Ce dernier est transmis avec A au HSS convenable.

- Message émis de HSS à MME : Réponse des données d'authentification : C= {(Session-id, RandHM2, EK, UESecCap, RandUESecCapab, NSQN), MACMHIK} PKM || {(IMSI, AVs (1...n)), MACMHIK} MHEK
  C= {C1} PKM || {C2} MHEK

Le HSS doit déchiffrer le message reçu formé de deux parties A et B qui sont chiffrées toutes les deux par sa clé publique PKH. La première, A, est envoyée de l'UE et la deuxième du MME. Le HSS doit déchiffrer le message reçu formé de deux parties A et B qui sont chiffrées toutes les deux par sa clé publique PKH. La première, A, est envoyée de l'UE et la deuxième du MME. Ensuite, le HSS prépare sa réponse pour MME, formée aussi de deux parties C1 et C2. Les deux sont destinées au MME, mais la première C1 est chiffrée avec la clé publique PKM du MME, et la deuxième C2 est chiffrée avec la clé symétrique MHEK. Le HSS déchiffre tout d'abord A et ensuite, en déchiffrant B il génère la clé maîtresse MHK qui sera divisée en deux autres clés (MHEK pour le chiffrement des messages et MHIK pour leur intégrité) pour assurer la sécurité entre HSS et MME.

- Message émis de MME à l'UE : Demande d'authentification à l'utilisateur : {(Rand(i),AUTN(i), KSIASME, NSQN), MACUMIK} UMEK, (RandUESecCapab⊕ChosenUEsecCap)

En recevant le message numéro 3, le MME commence à déchiffrer C1 avec sa clé privée KRM. Il vérifie ensuite le session-id reçu afin d'authentifier le HSS. Après avoir générer la clé MHK par le MME, l'intégrité de C1 est vérifié à l'aide de MHIK. La deuxième partie C2 de C est déchiffrée en utilisant MHEK, et son intégrité est vérifiée à l'aide de MHIK.
Avec la clé MHEK, le MME déchiffre C2 et choisit un vecteur d'authentification AV (i) pour en extraire RAND(i), et AUTN(i). Ces paramètres seront ajoutés à KSIASME et à NSQN pour les protéger tous en intégrité avec la clé UMIK et en calculant le code MACUMIK ajouté aux paramètres. Les données chiffrées seront concaténées avec la combinaison, via l'opération XOR, des deux valeurs RandUESecCapab et ChosenUEsecCap.

- Message émis de l'UE à MME : Réponse d'authentification d'utilisateur : {(RES⊕NSQN, MACTIK(NSQN)), MACUMIK} UMEK

À la réception du message numéro 4, l'UE utilise sa valeur aléatoire RandUESecCap pour démasquer les algorithmes sélectionnés par le MME comme suivant : RandUESecCapab⊕ (RandUESecCapab⊕ChosenUEsecCap). Après avoir dériver les clés symétriques UMEK et UMIK l'UE peut déchiffrer le message 4 et vérifier son intégrité. À partir de ce message, l'UE extrait la valeur de NSQN et il la sauvegarde afin de l'utiliser lors de la prochaine AKA. À partir des paramètres RAND(i), AUTN(i), et KSIASME il vérifie l'authenticité du réseau de service.

- Message émis de MME à HSS : NSQN Réallocation Complete : (MACTIK(NSQN), Session-id), MAC_{MHIK}

Après le déchiffrement et la vérification d'intégrité du message numéro 5, le MME extrait RES en utilisant le NSQN comme suivant : NSQN⊕ (RES⊕NSQN). Si le RES extrait, est identique au RES attendu (XRES), le réseau authentifie l'UE et s'assure en même temps que le NSQN a été bien reçu par l'UE. Dans ce cas, et pour notifier le HSS que l'utilisateur est devenu en possession de NSQN, le MME envoie le message 6 contenant le code MACTIK(NSQN) accompagné du session-id correspondant, et protégés tous les deux par la clé MHIK. Le HSS sauvegarde dans ce cas la valeur NSQN qu'il a généré lui-même au début (après la réception du message 2) pour cet utilisateur.

- Message émis de MME à l'UE : Commande du mode de sécurité NAS, CMS NAS : {KSIASME=1, ReplayedUESecCap., NAS CipheringAlg., NAS IntegrityAlg, [IMEISV request], NAS-MAC} UMEK

En même temps et avec la transmission du message numéro 6, le MME envoie à l'UE le message qui annonce le début du mode de sécurité NAS Security Mode Command (CMS NAS). Selon le standard et d'habitude en EPS-AKA, on protège ce message seulement en intégrité avec la clé générée de l'AKA (KNASint). Nous proposons maintenant de chiffrer les informations se trouvant dans ce message ainsi que leur code d'intégrité NAS-MAC, par la clé UMEK. Les algorithmes de chiffrement et d'intégrité NAS choisis doivent appartenir à la liste des algorithmes de sécurité (UESecCapab) envoyé par l'UE.

- Message émis de HSS à MME : ACK : (Session-id) MHEK

À la réception du message NSQN Reallocation Complete, le HSS vérifie l'intégrité de ce message, et vérifie si le code MACTIK(NSQN) reçu est correct et égale au MAC attendu, XMACTIK(NSQN). Si les deux MAC sont égaux, le HSS obtient une double confirmation : premièrement il vérifie que c'est le bon utilisateur qui a été authentifié, et il s'assure qu'il possède le bon NSQN qui le servira dans la prochaine demande d'attachement (Attachrequest) avec le HSS ; deuxièmement le HSS s'assure que les clés secrètes partagées avec le MME sont correctes et que l'entité appropriée a bien déchiffré les données transmises.

- Mode de sécurité NAS établi : ([IMEISV], NAS-MAC)

Après la réception du message numéro 7, l'UE déchiffre ce message par UMEK, vérifie le NASMAC par la clé KNASint et répond au MME avec le message Mode de sécurité NAS établi. À partir de ce moment toute la signalisation NAS sera protégée en intégrité et chiffrée à l'aide les clés générées par la procédure EPS-AKA (KNASenc et KNASint). L'un des messages NAS transmis par le MME à l'UE contient le GUTI. Nous proposons d'ajouter à ce message un indicateur (flag) pour commander l'UE à stocker le NSQN maintenu. Le message GUTI Reallocation Complete confirme au MME que le NSQN est stocké dans l'équipement utilisateur et que le GUTI a été bien alloué.

4.3.4.1 Analyse de la robustesse du protocole FP-AKA

Comme les messages échangés durant le protocole FP-AKA sont tous protégés en confidentialité et en intégrité. Alors l'application du FP-AKA améliore nettement la sécurité

du réseau EPS en assurant une protection complète contre toutes les attaques déjà mentionnées :

- ✓ Le chiffrement de l'IMSI par la clé publique du HSS assure la confidentialité de l'IMSI (et par suite de l'utilisateur).
- ✓ La protection de l'intégrité du message A contenant les capacités de sécurité de l'UE par le code MACTIK, assure la protection contre le « bidding down attack » et par suite contre l'attaque DoS sur l'UE.
- ✓ Le champ NSQN est conçu pour éviter l'attaque par rejoue et l'attaque DoS sur le HSS/AuC.
- ✓ L'envoie de l'IMSI avec les vecteurs d'authentifications et la transmission de la session-id dans le même message C (réponse d'authentification), permettent d'éviter l'attaque sur les réponses des données d'authentificationet la violation des propriétés de l'authentification.
- ✓ Le changement permanent de la clé MHK (partagée entre MME et HSS), garantit une excellente sécurité entre les nœuds MME et HSS.
- ✓ Le compromis de la clé privée du MME ne permet pas de compromettre une clé MHK précédente et par suite on ne pourrait déchiffrer aucun message échangé avant, entreMME et HSS. De même, avec la possession de cette clé privée, on ne peut pas connaître ni les vecteurs d'authentification ni l'IMSI des utilisateurs.
- ✓ La protection, en intégrité et en confidentialité, de la liaison entre MME et HSS empêche les attaques de type MITM (compromis des AV et blocage des services).

Notre protocole assure donc une protection complète contre les différents types d'attaques. Il ne présente aucune vulnérabilité. Ça prouve qu'il est un vrai candidat pour remplacer le protocole standard de 3GPP EPS-AKA.

4.5Analyse de la qualité de Service des protocoles AKA étudiés

Dans cette partie, nous comparons les quatre protocoles EPS-AKA, SE-AKA, EC-AKA et FP-AKA à travers certains facteurs pour d'estimer la performance et la qualité de service QoS de chacun de ces protocoles.

La sécurité et la performance ne sont pas nécessairement opposées. En général, un niveau de sécurité élevé a un coût de traitement élevé et des grands taux de données ajoutées. Pour évaluer la performance de chaque protocole, nous allons considérer les paramètres suivants :

4.5.1 Sécurité/Risque :

La sécurité d'un protocole est définit comme sa capacité à résister aux attaques, et le risque est la probabilité qu'une attaque puisse réussir à violer le protocole.

Les deux termes sécurité et risque sont inversement proportionnel l'un à l'autre. Plus le protocole est sécurisé, plus le risque est faible.

Le paramètre risque est défini comme suivant :

Risque =Valeur d'actif * menace perçue * vulnérabilité

Valeur d'actif :l'importance que le protocole joue dans le réseau EPS.

Menace perçue :la valeur des menaces que le protocole peut subir.

Vulnérabilité :reflète les faiblesses du protocole.

Les deux premiers paramètres 'valeur d'actif' et 'menace perçue' sont les mêmes pour les quatre protocoles étudiés. Alors pour évaluer les protocoles vis-à-vis du paramètre 'risque' il suffit donc d'évaluer seulement le paramètre 'vulnérabilité' pour chaque protocole. Ce paramètre a la facilité d'exploiter une faiblesse du protocole ou le nombre d'attaques possibles.

Dans le tableau ci-dessous nous montrons la vulnérabilité de chaque protocole en dévoilant ses points forts et ses points faibles :

Vulnérabilité	EPS-AKA	SE-AKA	EC-AKA	FP-AKA
1-Assurer la Confidentialité de l'IMSI	Non	Oui (cassé)	Oui	Oui
2-Résistance contre l'attaque par rejoue	Non	Non	Non	Oui
3- Résistance contre l'attaque DoS de l'UE	Non	Non	Oui	Oui
4- Résistance contre le blocage des services par un MITM	Non	Non	Oui	Oui
5-Confidentialité de l'interface MME- HSS	Non	Oui	Oui	Oui
6- Résistance contre les attaques sur les réponses des données d'authentification	Non	Oui	Non	Oui
7- Résistance contre l'attaque DoS de HSS	Non	Non	Non	Oui
8-Résistance contre l'usurpation d'identité de MME	Non	Non	Non	Oui

Tableau 4: Comparaison de la sécurité des différents protocoles

Alors en comparant les quatre protocoles, FP-AKA est considéré comme étant le plus sécurisé oule moins visible aux attaques.

4.5.2 Cout :

Dans les protocoles proposés, on n'a pas besoin d'équipements supplémentaires et ce sont les certificats électroniques des entités qui peuvent coûter de l'argent. Comme le nombre des nœuds MME et HSS n'est pas et leurs certificats ne coûtent pas cher.

Les protocoles EC-AKA et FP-AKA n'exigent ni des équipements supplémentaires ni de payer pour des certificats aux utilisateurs. Ils utilisent le chiffrement symétrique pour envoyer leurs messages de signalisation à l'utilisateur. Le protocole SE-AKA est le seul qui compte sur des certificats électroniques des utilisateurs.

4.5.3 Taux de données ajoutées sur la signalisation :

Nous calculons, ici, le trafic généré en nombre de bits par tous les messages transmis durant l'application de chaque protocole,pour pouvoir estimer le taux des données ajoutées sur les messages de signalisation de l'EPS-AKA, par chacun des protocoles étudiés. Pour cela, nous allons faire ce calcul sur les interfaces suivantes :

- Liaison montante de l'interface radio, entre l'UE et l'eNB
- Liaison descendante de l'interface radio
- Liaison montante de l'interface appelé 'backhaul', entre l'eNB et le MME
- Liaison descendante de l'interface backhaul,
- Interface de transport dans le réseau coeur, entre le MME et le HSS (dans les deux sens).

Le calcul des tailles, en bits, de chaque message de signalisation transmis sur les différentes interfaces durant chacun des protocoles AKA considérés, a été effectué. Ce calcul dépend du nombre n de vecteurs d'authentification émis du HSS au MME, et qui peut prendre n'importe quelle valeur entière (fortement conseillé entre cinq et dix). Le résultat obtenu sur chaque interface est présenté dans le tableau :

Protocole	Liaison radio-voie montante	Liaison Backhaul - voie montante	Liaison radio- voie descendante	Liaison Backhaul-voie descendante	Trafic moyen sur l'interface Transport (réseau cœur)
EPS-AKA	204	204	260	260	82+(n*640)
SE-AKA	1180	1180	1024	1024	2048+ ceil((n*640+8252)/1024)*1024
EC-AKA	1180	1180	394	394	3072+ ceil ((n*640+399)/1024)*1024
FP-AKA	1244	1244	330	330	1er demande d'attachement : 4284+(n*640) Durant les *i* attachements suivants: 1476+(n*640). ========== Trafic moyen égale à : 1535+(n*640).

Tableau 5: Trafic de signalisation, en bits, généré par les protocoles étudiés

Puisque l'EPS-AKAprésente le plus de vulnérabilités, il transmet le trafic minimal par rapport aux autres protocoles. Les autres protocoles prennent des mesures pour se protéger contre ces faiblesses et cela augmente leur coûte du trafic supplémentaire. Les protocoles EC-AKA et FP-AKA transmettent presque le même nombre de bits sur les liaisons radio et backhaul, montante et descendante. Le SE-AKA envoie un trafic nettement supérieur aux

autres sur les voies descendantes de la liaison radio et backhaul, puisqu'il est le seul à utiliser le chiffrement asymétrique sur ces voies.

Le protocole FP-AKA montre des résultats intéressants en transmettant beaucoup moins de trafic sur l'interface de transport et sur la voie descendante des deux liaisons radio et backhaul que les deux autres concurrents SE-AKA et EC-AKA.

4.5.4 Résumé des résultats :

Ce tableau donne un classement des protocoles pour chaque paramètre (sécurité, coût, taux de données), où on donne la valeur « 4 » pour signifier le plus faible, et la valeur « 1 » signifie le meilleur.

Paramètres de QoS	FP-AKA	EC-AKA	SE-AKA	Standard EPS-AKA
Sécurité	1	2	3	4
Coût	1	1	3	1
Taux de données ajoutées (Overhead)	2	3	4	1

Tableau 6 : Fiche technique évaluant la QoS de FP-AKA, EC-AKA, SE-AKA, et EPS-AKA

Il est important d'admettre que notre protocole FP-AKA a le meilleur niveau de sécurité et de coût. La sécurité est un facteur très important et elle nécessite une augmentation acceptable des ressources. L'EC-AKA a une performance acceptable par rapport à SE-AKA qui a le plus mauvais performance sur l'ensemble des paramètres, il est donc considéré comme non adéquat pour les futures implémentations.

Puisque FP-AKA est le seul protocole satisfaisant les exigences de la sécurité du réseau EPS en atteignant d'excellentes performances de QoS, il est donc un excellent candidat pour remplacer le mécanisme d'authentification des clés standard de 3GPP EPS-AKA.

4.6 Conclusion:

Avons avoir identifié les vulnérabilités, ainsi que les scénarios qui permettent les attaques contre leprotocole standard 3GPP EPS-AKA. Nous admettonsque les risques résultant par l'exploitation de ces faiblesses peuvent empêcher les utilisateurs d'accéder au réseau, compromettre la clé permanente K, bloquer les services de l'opérateur mobile, provoquer l'usurpation des identités des utilisateurs ou de MME. Pour chacune des attaques identifiées, nous avons proposé des solutions convenables.

Pour résoudre les faiblesses des trois protocoles étudiés, nous avons proposéun nouveau protocole qui s'intitule 'Full Protection Authentication and Key Agreement' FP-AKA. Il assure une protection complète de la procédure AKA et de la sécurité EPS contre toutes les attaques possibles. Ce protocole a été présenté avec toutes ses composantes de sécurité.Et il a obtenu les meilleurs résultats dans les deux premiers paramètres et atteint de très bons résultats dans les paramètres restants. Il est un excellent protocole AKA, par ce qu'il satisfait les exigences de sécurité et les spécifications de l'EPS, tout en proposant une meilleure QOS avec un cout minimal.

Conclusion générale

Dans ce travail, nous avons pu montrer les failles de la sécurité dans les réseaux de téléphonie mobiles 4G/LTE. Ce qui nous a permet de proposer des solutions contre les différentes vulnérabilités.

L'objectif que nous nous étions fixé a été atteint, car nous avons pu comprendre le fonctionnement des divers mécanismesde sécurité (l'authentification, la confidentialité, l'intégrité et la disponibilité)permettant de protéger les réseaux 4G/ LTE à travers des études sur des protocoles EPS-AKA, SE-AKA, EC-AKA et FP-AKA. En effet, nous avons montré que le risque résultant des attaques contre ces protocoles peut : empêcher les utilisateurs d'accéder au réseau, provoquer l'usurpation desidentités des utilisateurs ou de MME, etc.

Afin de pouvoir d'assurer la sécurité des réseaux 4G/LTE, nous avons analysé les meilleurs protocoles AKA proposés. Cependant, des vulnérabilités existent toujours pour chacune des solutions à travers une attaque spécifique.

Par ailleurs nous avons proposé le protocole FP-AKA qui a permis de renforcer toutes les faiblesses relevées, et assure la protection de la procédure AKA, et de la sécurité EPS contre tous les attaques.

Enfin, l'étude comparative que nous avons effectué entre le protocole FP-AKA et les autres protocoles AKA (EC-AKA, SE-AKA, EPS-AKA) sur quatre paramètres de QOS a montré l'importance de notre protocole. L'excellente performance du FP-AKA, le place comme étant le meilleur protocole AKA proposé à ce jour. Il est toujours recommander de suivre de près le cours de l'évolution et s'informer à tout moment sur les nouveaux protocoles qui peuvent apporter plus de performances et mieux sécuriser les réseaux 4G/LTE.

Bibliographie

[1] H.BOUCHENTOUF et R.BOUDGHENE STAMBOULI, Etude des performances des réseaux 4G (LTE). Mémoire de master, Département de génie électrique et électronique, Option : réseaux mobiles et services (RMS), Faculté de technologie, université Abou Bekr Belkaid de Tlemcen, 2013.

[2] A.GHANEMI et A.OULED-AISSA, Evolution de 2G au 4G. Mémoire d'ingénieur, Spécialité : Systèmes de télécommunications, Institut national des télécommunications et des technologies de l'information et de la communication d'Oran, 2010.3GPP TS 23.002 V8.4.0 (2008-12) Network Architecture.

[3] Moray Rumney, "LTE and the Evolution to 4G Wireless", Design and Measurement Challenges, Agilent Technologies Publication, Reprinted July 2009.

[4] Kassem AHMAD, Protocoles, gestion et transmission sécurisée par chaos des clés secrètes, Applications aux standards : TCP/IP via DVB-S, UMTS, EPS. Thèse de Doctorat, Département Electronique, Spécialité : Traitement du signal et des images, École doctorale Sciences et Technologies, Liban, École doctorale Sciences et Technologies de l'Information et Mathématiques (STIM), Nantes, France, 2013.

[5] Praphul Chandra, Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security. Livre, 2005.

[6] Sécurité informatique risques, stratégies et solutions – Didier GODART – Editions des CCI - Edition 2005.

[7] AMAVI Ayi Roméo, BOUKONO Axel Clyde et DIOP SeydinaLimamoulaye, Sécurité des Réseaux 2G / 3G / 4G : Mécanisme de Sécurité, Vulnérabilité et Solutions. Supervisé par le Dr KORA Ahmed.

[8] Daniel CARAGATA, Protocoles de communications sécurisées par des séquences chaotiques, Applications aux standards de communications : IP via DVB-S et l'UMTS.

[9] I.DAOUDA et M.MOUSSA, Evolution des réseaux mobiles 2G vers la 3G. Mémoire d'ingénieur, Spécialité : Systèmes de télécommunications, Institut national des télécommunications et des technologies de l'information et de la communication d'Oran, 2005.

Webographie

A- Http://www.efort.com/r_tutoriels/SECURITE_MOBILE_EFORT.pdf

B- Http: //www.c7.com/ss7/whitepapers/cellular/umts security.pdf

C-Http: //www.umtsworld.com/technology/security.html

D-www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASHS.../PDF/CM_securite.pdf

E-http://www.securitybugware.org/works.html

F-https://fr.linkedin.com/pulse/sécurité-des-réseaux-4g-lte.pdf

G-www.mi.parisdescartes.fr/~mea/cours/Mi/Mi.1.pdf