الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de 8 Mai 1945 – Guelma -

Faculté des Mathématiques, d'Informatique et des Sciences de la matière

Département d'Informatique

Mémoire de Fin d'études Master

Filière : Informatique

Option : Ingénierie des Médias

Thème :

Attaque de l'homme du milieu dans les réseaux sociaux 4G

Encadré Par :

Dr. FERRAG Mohamed Amine

Présenté par :

BOUGHAZI Manal

LAKHAL Asma

Juin 2017

Remerciements

En premier lieu et avant tout nous tenons à remercier « **ALLAH**» le tout puissant qui nous a entouré de sa bienveuillance et nous a renforcé avec le courage et la force pour avoir enfin mené à bien ce travail.

Ensuite, nous exprimons notre profonde gratitude à notre encadreur **Dr. Mohamed Amine Ferrag** pour avoir accepté de nous suivre, ses conseils judicieux, ses remarques objectives et sa sympathie dont il nous a fait preuve tout au long de l'élaboration de ce travail.

Nous adressons également nos remerciements, à tous nos enseignants, qui nous ont donné les bases de la science, nous remercions très sincèrement, les membres de jury pour nous avoir acceptés l'honneur d'examiner notre travail.

Nous tenons remercier nos familles de nous avoir soutenu, nous ne serons jamais assez reconnaissants envers nos parents qui nous ont toujours entourés par la tendresse et l'amour dévoué depuis notre enfance. Merci de votre soutien de tous les jours et nous espérons que vous soyez aussi fiers de nous que nous le sommes de vous.

Et finalement à tous ceux qui nous ont aidés de près ou de loin à durant notre travail Merci.

Dédicace

Ce mémoire est dédié à

Nos parents,

Nos familles,

Nos ami(e)s,

Tous ceux qui nous aiment et qu'on aime.

Résumé

Les réseaux sans fil cellulaires de la quatrième génération (4G) ou Long Terme Evolution (LTE) ont continué à évoluer, apportant à l'architecture du réseau de nouvelles interfaces et protocoles, ainsi que des services unifiés, une grande capacité de transmission de données et une transmission par paquets. Cette évolution a également introduit de nouvelles vulnérabilités et menaces qui peuvent être utilisées pour lancer des attaques sur différents composants de réseau, tels que le réseau d'accès et le réseau de base. Ces inconvénients constituent une préoccupation majeure pour la sécurité et la performance des réseaux mobiles, car différents types d'attaques peuvent réduire tout le réseau et causer un déni de service ou effectuer des activités malveillantes. L'une de ces attaques est l'attaque de l'homme du milieu (MITM) qui touche la confidentialité et l'intégrité des informations, elle est désigné aussi écoute clandestine des transmissions sans fil pour objectif d'extraire et d'entraîner une perte des informations confidentielles, une facturation incorrecte et une falsification de données.

Nous proposons une implémentation de l'attaque de l'homme du milieu (MITM) à partir de créer une virtuelle station de base (fake base station (eNB)). Cette dernièrre est implémenté et évalué par la simulation en utilisant le logiciel spécialisé libre et open source « NS-3 ».

Mots clés : 4G, LTE, QoS, Sécurité, Attaque MITM, simulation, NS-3

Abstract

Fourth generation (4G) or Long Term Evolution (LTE) cellular wireless networks continued to evolve, providing new network interfaces and protocols, as well as unified services, a large data transmission capacity And a packet transmission. This evolution has also introduced new vulnerabilities and threats that can be used to launch attacks on various network components, such as the access network and the base network. These disadvantages are a major concern for the security and performance of mobile networks because different types of attacks can reduce the entire network and cause a denial of service or malicious activity. One of these attacks is the attack of the middle man (MITM), which affects the confidentiality and integrity of information, and is also referred to as clandestine listening to wireless transmissions in order to extract and train a Loss of confidential information, inaccurate billing and falsification of data.

We propose an implementation of the attack of the middle man (MITM) from the creation of a virtual base station (fake base station (eNB)). The latter is implemented and evaluated by the simulation using the free and open source software "NS-3".

Keywords: 4G, LTE, QoS, MITM attack, security, simulation, NS3.

Table des matières

Table des figures

Liste des Abréviations

1G	**Première génération**
2G	**Deuxième génération**
3G	**Troisième Génération**
3GPP	**3rd Generation Partnership Project**
4G	**Quatrième Génération**
A	
AS	**Access Stratum**
AKA	**Authentication and Key Agreement**
ARP	**Allocation Retention Priority**
AuC	**Centre d'Authentification**
B	
BTS	**Base Transceiver Station**
C	
CSCF	**Call Service Control Functions**
CAC	**Call Admission Control**
CQI	**Channel Quality Indicator**
D	
DoS	**Deny of Service**
E	
E-UTRAN	**Evolved UTRAN**
ECC	**Elliptic Curve Cryptography**
ENB	**Evolved Node B**
EPC	**Evolved Packet Core**
EPS	**Evolved Packet System**
F	

FBS **False Base Station**

FDD **Frequency Division Duplexing**

G

GBR **Guaranteed Bit-Rate**

GSM **Global System for Mobile communications**

H

HLR **Home Location Register**

HSS **Home Subscriber Server**

I

I-CSCF **Interrogating-CSCF**

IMS **IP Multimedia Subsystem**

IMSI **International Mobile Subscriber Identity**

IP **Internet Protocol**

L

LTE-A **LTE-Advanced**

LTE **Long Term Evolution**

M

M2M **Machine to Machine**

MAC **Medium Access Control**

MitM **Man in the Middle**

MME **Mobility Management Entity**

MMS **Multimedia Messaging Servic**

MS **Mobile Station**

N

NAS **Non Access Stratum**

NFC **Near Field Communication**

NS-3 **Network Simulator 3**

O

OFDMA **Orthogonal Frequency Division Multiple Access**

P

P-CSCF **Proxies- CSCF**

P-GW	**Packet-data Network Gateway**
PDCP	**Packet Data Convergence Protocol**
Q	
QCI	**QoS Class Identifier**
QoS	**Quality of Service**
R	
RAN	**Radio Access Network**
RRC	**Radio Resource Control**
RLC	**Radio Link Control**
S	
SAE	**System Architecture Evolution**
S-CSCF	**Serving-CSCF**
S-GW	**Serving Gateway**
SC-FDMA	**Single Carrier Frequency Division Multiple Access**
SINR	**Signal Interference Noise Ratio**
SIP	**Session Initiation Protocol**
SMS	**Short Message Service**
SQN	**Sequence Number**
SSL	**Secure Sockets Layer**
T	
TDD	**Time Division Duplexing**
U	
UE	**User Equipment**
UICC	**Universal Integrated Circuit Card**
USIM	**l'UMTS SIM**
UM	**Unacknowledged Mode**
UL	**Up Link**
UMTS	**Universel Mobile Télécommunications System**
UIT	**Union Internationale des Télécommunications**
V	
VoIP	**Voice over IP**

W

WAP **Wireless Application Protocol**

WIMAX **Worldwide Interoperability for Microwave Access**

Introduction générale

Aujourd'hui presque chaque aspect de notre vie peut être associé à l'utilisation de réseaux Internet ou cellulaires (1G, 2G, 3G et 4G). Par exemple, nous utilisons la banque à domicile en ligne, le divertissement en ligne et les achats, les réseaux sociaux, etc. Tous ces services en ligne stockent ou transfèrent les informations sensibles de l'utilisateur, ce qui représente une cible clé pour les pirates informatiques. Dans ce nouveau monde de personnes toujours connectées au moyen d'Internet, il est très courant de lire quotidiennement les attaques réussies à des activités connectées et des services en ligne. L'une des attaques les plus réussies est connue sous le nom de Man-In-The-Middle (MITM), ce qui entraîne un contrôle sur les données transférées entre les utilisateurs utilisant les réseaux 4G.

Notre mémoire est reparti sur quatre chapitres. Dans le premier chapitre nous avons introduit l'évolution des différentes générations de réseaux mobile jusqu'à la quatrième génération 4G (LTE), ainsi les composants de réseau LTE. Dans le deuxième chapitre nous avons parlé des menaces contre les réseaux 4G et les mécanismes de sécurité adoptés par le système LTE. La sécurisation de communication dans les réseaux sociaux 4G passe principalement par la mise en place des conditions ont différent degrés d'importances selon le contexte d'utilisation du réseau, donc une vulnérabilité de l'intégrité facilite une des attaques redoutées par les responsables de sécurité informatique est L'attaque de l'homme du milieu (Manin-the-middle (MITM)) ce qui est présenté dans le troisième chapitre, ensuite on a proposé un schéma qui montre cette attaque dans l'architecture des réseaux de la quatrième génération (4G) et l'utilisation comme mécanisme la cryptographie elliptique. Enfin dans le quatrième chapitre nous avons travaillé avec le simulateur NS3 (Network-Simulator-3) pour simuler l'attaque MITM dans les réseaux sociaux 4G.

Chapitre 1 : Introduction aux réseaux mobiles 4G

1.1 Introduction

Avec l'évolution et la progression technologiques qui ont connu une grande propagation dans le monde, les réseaux mobiles sont devenus sans aucun doute obligatoires dans notre vie.

Les téléphones mobiles sont en accroissement constante. Ils sont utilisés non seulement pour les communications vocales, mais aussi pour les communications visuelles grâce aux technologies avancées, comme dans les différentes générations des réseaux mobiles (2G, 3G ,4G).

1.2 Historique

La première génération des systèmes de communication mobiles sans fil 1G a été introduite dans les années 70 et la deuxième génération 2G dans les années 80. Ces systèmes ont cependant été abandonnés il y a quelques années laissant la place à la seconde génération, appelée 2G lancée en 1991. Elle est encore active de nos jours. Le principal standard utilisant la 2G est le GSM. A la différence de la 1G, la seconde génération de normes permet d'accéder à divers services, comme l'utilisation du WAP permettant d'accéder Internet, tant dit que pour la 3ème génération connue sous le nom de 3G permet un haut débit pour l'accès l'internet et le transfert de données**. [1]**

1.2.1 La première génération des téléphones mobiles (1G)

La première génération des téléphones mobiles est apparue dans le début des années 80 en offrant un service médiocre et très couteux de communication mobile. La 1G avait beaucoup de défauts, comme les normes incompatibles d'une région une autre, une transmission analogique non sécurisée (écouter les appels), pas de roaming vers l'international (roaming est la possibilité de conserver son numéro sur un réseau d'un autre opérateur). **[1]**

1.2.2 La deuxième génération des téléphones mobiles (2G)

La deuxième génération de réseaux mobiles (2G) a été introduite, à la fin des années 1980. Les deux systèmes 2G les plus connus sont l'IS-95 (Interim Standard 95) et le GSM (Global System for Mobile Communications) qui est le système le plus répandu, **[1]** Ces systèmes cellulaires utilisent une technologie numérique pour la liaison ainsi que pour le signal vocal. Le principe du GSM étant de passer des appels téléphoniques, celui-ci s'appuie sur une connexion orientée circuit et sur une grande capacité transmissions numériques à moindre coût pour l'utilisateur, permettant ainsi la sécurisation des données (chiffrement). Cette norme est mondiale et autorise le *roaming* entre pays. elle apporte la possibilité d'émettre de courts messages SMS (Short Message Service) et

le MMS (Multimedia Message Service) et aussi fournir des services de téléphonie avec l'ajout de fonctionnalistes d'accès radio et de mobilité mais généralement, ces systèmes permettaient des transferts de données à faible débit. [**1]**

1.2.3 La troisième génération des téléphones mobiles 3G

La conception de la troisième génération de réseaux mobiles (3G) définie par l'ITU (International Telecommunication Union) afin de permettre l'utilisation d'applications vidéos sur les téléphones mobiles (vidéos YouTube, visiophonie, . . .) et d'augmenter le débit pour pouvoir passer d'un service téléphonique (connexion orientée circuit) vers un service data (connexion orientée paquets).

En effet, les réseaux orientés circuits sont, à l'origine, utilisés pour les appels téléphoniques, alors que les réseaux orientés paquets s'occupent des données (sur Internet par exemple). Il est dès lors utile de pouvoir combiner les deux, afin de profiter non seulement des réseaux téléphoniques existants, mais aussi du réseau Internet. **[1]**

La norme « LTE-Advanced » apparait et impose des critères de base sur les débits, les bandes de fréquence, la latence et l'efficacité spectrale.

1.3 Long Term Evolution (4G)

LTE est la norme de communication mobile la plus récente qui est proposée par l'organisme 3GPP dans le contexte de la 4G.

La norme « LTE-Advanced », aussi dénommée 4G, est la norme téléphonique de quatrième génération. Elle permet d'améliorer les performances d'une communication radio mobile comparativement à la 3G. **[2]**

En théorie, elle permet d'atteindre des débits de l'ordre de 50 Mb/s en lien ascendant et de 100 Mb/s en lien descendant, de partager entre les utilisateurs mobiles à l'intérieure d'une même cellule. Pour les opérateurs (qui ont la partie la plus importante pour supporter cette technologie), LTE implique de modifier le cœur du réseau et les émetteurs radio. Il faut également développer des terminaux mobiles adaptés. **[2]**

En réalité, l'ensemble de ce réseau s'appelle EPS (Evolved Packet System), et il est composé d'UE (User Equipment), l'EPC (Evolved PacketCore) et l'E-UTRAN (Evolved UTRAN).

1.3.1 Définition de la quatrième génération 4G

La définition de la 4G a évolué comme une nouvelle vague d'efforts de données de commercialisation des mobiles qui se déplace le terme dans l'œil du public à différencier les marques. L'union internationale des télécommunications (UIT), qui supervise le développement de la plupart des normes de données cellulaires, a récemment publié une déclaration soulignant que la 4G terme n'est pas défini. En réponse, les opérateurs mobiles avec des architectures 3G avancés a commencé la commercialisation des services «4G». Avec le réseau 4G, un utilisateur pourra se connecter où qu'il se trouve : à l'intérieur des bâtiments avec les technologies Bluetooth, UWB ou WiFi…, à l'extérieur (dans la rue et les lieux publics) avec l'UMTS ou le WiMAX. **[3]**

1.3.2 Caractéristiques des systèmes sans fil 4G

Voici quelques fonctionnalités possibles des systèmes 4G:

1. Prise en charge multimédia interactives, voix, vidéo, Internet sans fil et autres services large bande.
2. Haute vitesse, haute capacité et à faible coût par bit.
3. La mobilité mondiale, la portabilité des services, réseaux mobiles évolutifs.
4. une optimisation automatique du réseau : les équipements 4G se configurent automatiquement afin d'améliorer la qualité de service (QoS). **[3]**
5. Une meilleure planification et des techniques de contrôle d'admission d'appel.
6. Les réseaux ad-hoc et réseaux multi-sauts.

1.3.3 Architecture LTE (4G)

La quatrième génération présente, pour l'amélioration des services, des plateformes multi-technologiques capables de supporter de nouvelles applications innovatrices. De même que ces précédentes, la 4G présente une architecture qui comporte un réseau d'accès : l'E-UTRAN et un réseau cœur véhiculant que des paquets de données Elle est dite pour cela tout-IP. **[3]**

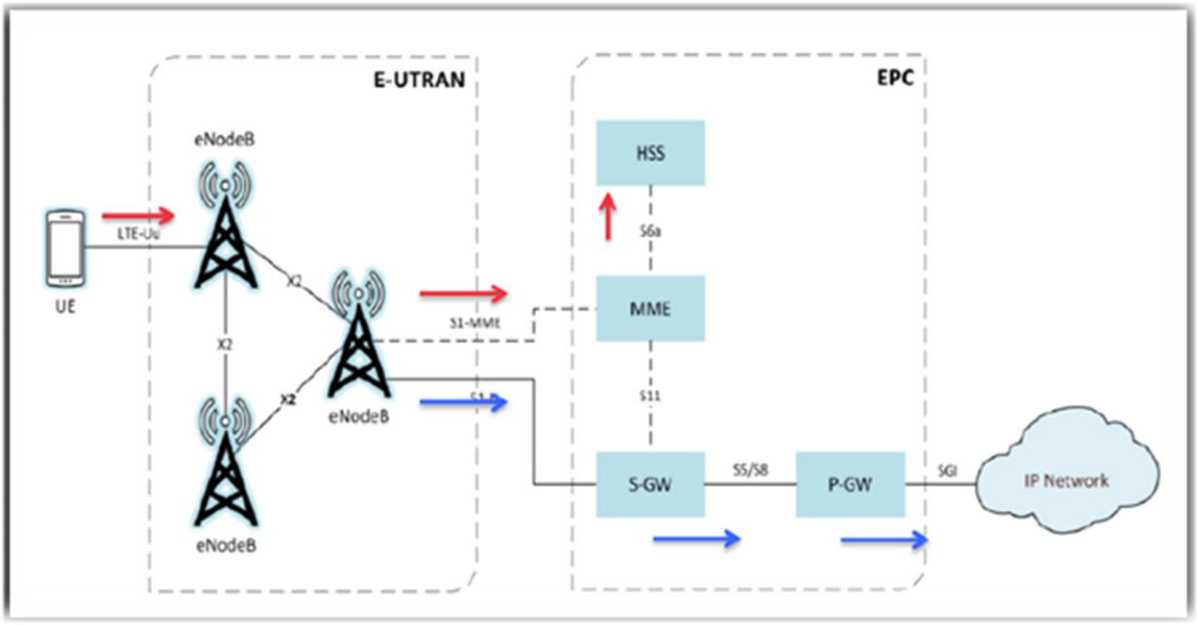


Figure 1.1: *Architecture LTE.* **[3]**

1.3.3.1 Équipement Utilisateur (UE) : Il est présenté sous deux plans :

• Le plan utilisateur: il contient les couches PHY (physique), MAC (Medium Access Control), RLC (Radio Link Control) et PDCP (Packet Data Convergence Protocol).

• Le plan de contrôle: il contient le NAS (Non Access Stratum) et le RRC (Radio, Resource Control), avec le plan utilisateur.

1.3.3.2 Réseau cœur 4G/LTE (EPC):

Connu aussi sous le nom de SAE (System Architecture Evolution), l'EPC représente le réseau cœur de LTE. Il se compose d'équipements devant supporter la connectivité toute-IP entre les domaines multi-technologiques dans l'architecture 4G. Il assure la gestion des utilisateurs, la gestion de la mobilité, la gestion de la qualité de service et la gestion de la sécurité**. [4]**

Il est composé de :

• **MME (Mobility Management Entity**) : MME est responsable de la gestion de la mobilité et l'authentification des utilisateurs. Elle est responsable aussi du Paging lorsque l'utilisateur est en état inactif. Il fait la mise à jour des paramètres de localisation de l'UE se retrouvant dans une zone qui n'est pas prise en charge par le MME

• **ServingGW (ServingGateway) ou UPE (User Plane Entity) :**est défini pour gérer les "données utilisateur "et il est impliqué dans le routage et la transmission de paquets de données entre les eUTRAN et le réseau cœur. L´échange des paquets est acheminé par le SGW au PDN-GW

par l'interface S5. Le SGW est connecté à l'eUTRAN via l'interface S1-U qui sert de relai entre l'utilisateur et l'EPC

- **P-GW (PacketData Network Gateway) ou IASA (Inter-Access System Anchor) :**
  Est l'entrée et le point de sortie pour le trafic de données dans l'EPC. Il exécute l'application de la politique et de filtrage de paquets pour chaque flux de données de chaque abonné.

- **HSS (Home Subscriber Server) :** base de données, évolution du HLR de la 3G. Elle contient les informations de souscriptions pour les réseaux GSM, GPRS, 3G et LTE...

- **PCRF (Policy &Charging Rules Function) :** fournit les règles de la taxation.

ePDG (Evolved Packet Data Gateway) : un élément réseau qui permet l'interopérabilité avec le réseau WLAN en fournissant des fonctions de routage des paquets, de Tunneling, d'authentification, d'autorisation et d'encapsulation / décapsulation des paquets.

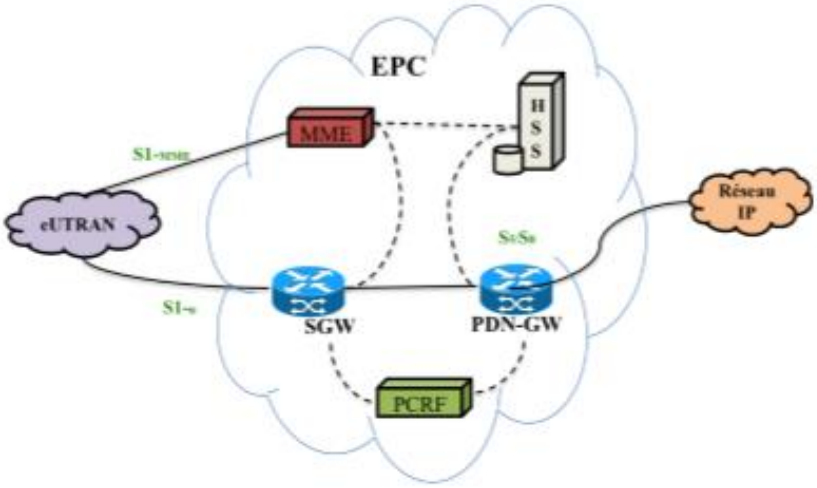


Figure 1.2 : *Architecture EPC.* **[4]**

1.3.3.3 :L'E-UTRAN:

La partie radio du réseau, appelé « eUTRAN » est la partie est responsable sur le management des ressources radio, la porteuse, la compression, la sécurité, et la connectivité vers le réseau cœur évolué.

Enode-B : La principale fonction de l'eNode B est d'acheminer les flux de données de l'UE vers l'EPC (Evolved Packet Core Network) au moyen des fonctions comme le RRM (Radio Ressource Management) et le CAC (Call Admission Control). Les eNodeB sont normalement interconnectés l'un avec l'autre au moyen d'une interface «X2» et à l'EPC au moyen de l'interface S1 plus précisément, au MME au moyen de l'interface S1-MME et du S-GW par l'interface S1-U. **[4]**

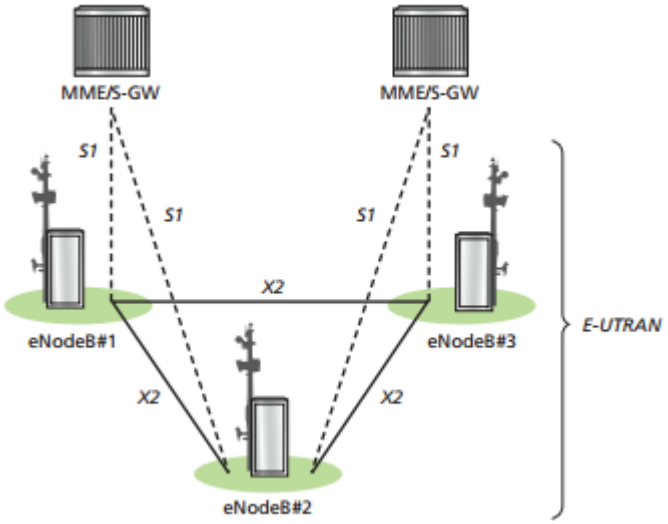


Figure 1.3: *Architecture E-UTRAN.* **[4]**

1.3.4 L'interface radio

L'interface radio assure le rôle clé de transférer par la voie des airs les données issues de la couche IP associées au service demandé par l'utilisateur. Ce transfert doit respecter des exigences de qualité de service (latence, débit) malgré un medium extrêmement variable, tout en optimisant l'accès à une ressource spectrale limitée. En outre, la disponibilité du spectre, variable selon les régions du globe, impose de pouvoir s'adapter à différents types de bandes disponibles. **[4]**

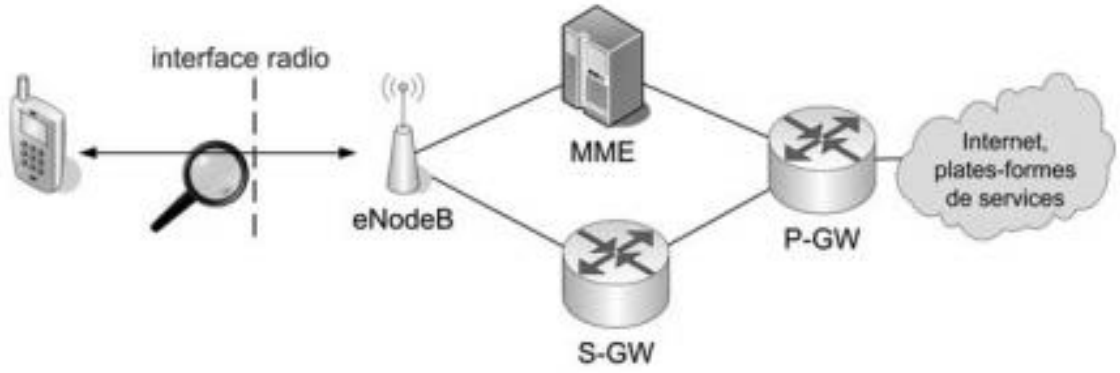


Figure 1.4 : *L'interface radio LTE.* **[4]**

1.3.5 Le Hand over dans LTE

Dans LTE la gestion de mobilité est distribuée, les eNodeBs prennent la décision de Hand over d'une façon autonome sans implication des éléments : MME et S-GW. Les informations nécessaires au Hand over sont échangées entre les eNodeBs via une interface appelée X2. Le MME et le S-GW recevront une notification avec un message complet de Hand over après que la nouvelle connexion aura été attribuée entre l'UE et la nouvelle eNodeB. Après réception du message, les Gateways effectuent le chemin de commutation. Durant le Hand over il y a un délai durant lequel l'UE n'est pas connecté au système. Pour résoudre cela, une solution temporaire de transmission des données perdues de l'ancien eNB vers le nouveau eNB est proposée. Dans ce cas il n y a pas de mémorisation des données au niveau des Gateways. L'intérêt de cette solution est de minimiser la charge de signalisation au niveau de l'interface entre l'eNB et l'MME/S-GW. **[5]**

1.4 Les couche du modèle LTE

Les couches les plus importantes de cette technologie :

1.4.1 Couche NAS (non Access Stratum) :

Cette couche est responsable de plusieurs tâches de contrôle comme:

• La gestion des entrées au réseau.

• L'authentification.

• La gestion de la mobilité.

• Elle est responsable de la mise en place du porteur de données (Data bearer).

1.4.2 Couche AS (Access Stratum):

Cette couche représente la connexion directe entre nous et eNodeBs et comprend tous les messages, c'est-à-dire les données utilisateur qui sont échangées sur la couche radio pour accéder physiquement à un réseau LTE.

1.4.3 Couche RRC (Radio Resource Control) :

La couche RRC est présenté au niveau d'eNodeB voici quelques opérations qu'elle assure:

- La diffusion des informations du système.
- La procédure de la pagination.
- L'allocation des identificateurs temporaires aux UE
- Elle assure le transfert de la situation de « handover » entre deux eNodeB à l'UE**. [5]**

1.4.4 Couche PDCP (Packet Data Convergence Protocol):

- La couche PDCP au plan utilisateur prend la charge d'assurée: la compression et la décompression des entêtes lP liées aux données utilisateurs.
- Les messages de la couche NAS sont chiffrés deux fois, au niveau de

MME et d'eNodeB, puisqu'ils passent par la couche RRC.

1.4.5 Couche RLC (Radio Link Control) :

Cette couche est située au-dessous de la couche PDCP, son travail est de formater et de transporter les données entre l'eNodeB et l'UE.

1.4.6 La couche MAC (Medium Access Control) de LTE :

Elle est parmi les couches les plus importantes du modèle. Elle assure le mappage des données entre les canaux logiques et les canaux de transport en utilisant une fonction de multiplexage de RLC.

1.4.7 La couche physique de LTE (PHY) :

La couche physique utilise la technique OFDMA (Orthogonal Frequency Division Multiple Access) pour le flux descendant (d'eNodeB vers UE) et la technique SC-FDMA (Single Carrier-Frequency Division Multiple Access) pour le flux ascendant. Elle offre aussi la possibilité d'utiliser trois modes de transmission: Full Duplex FDD (Frequency Division Duplex), HalfDuplex FDD et TDD (Time Division Duplex). **[5]**

1. 5 Qualité de service dans le réseau 4G

La qualité de service (QDS) ou Quality of service (QoS) est la capacité de transmission dans de bonnes conditions un certain nombre de paquet dans une connexion entre un émetteur et un récepteur.

Les nouveaux besoins en termes de mobilité des utilisateurs et la croissance des réseaux permettant le nomadisme des utilisateurs ont fait migrer le problème vers la des réseaux sans fil. **[6]**

• Le porteur EPS (the bearer) :

Le porteur EPS est un tuyau (tunnel) construit entre l'UE et le P-GW selon les caractéristiques contenues dans l'EPS session. Le premier bearer EPS construit, nommé default bearer EPS est mis en place lors de la procédure d'enregistrement.

Un bearer EPS est un tuyau caractérisé par des paramètres de QoS car les applications n'ont pas les mêmes besoins : Certaines applications comme le streaming, la vision et la phonie nécessitent un débit garanti (GBR) alors que le browsing et le téléchargement se suffisent de Best Effort (Débit Non Garanti). **[7]**

Il existe deux types de porteurs EPS :

- Le Default bearer, le premier porteur établi lorsque le terminal se connecte un PDN, il reste actif durant toute la connexion.
- Les Dedicated bearer, tous les porteurs additionnels établis avec le même PDN

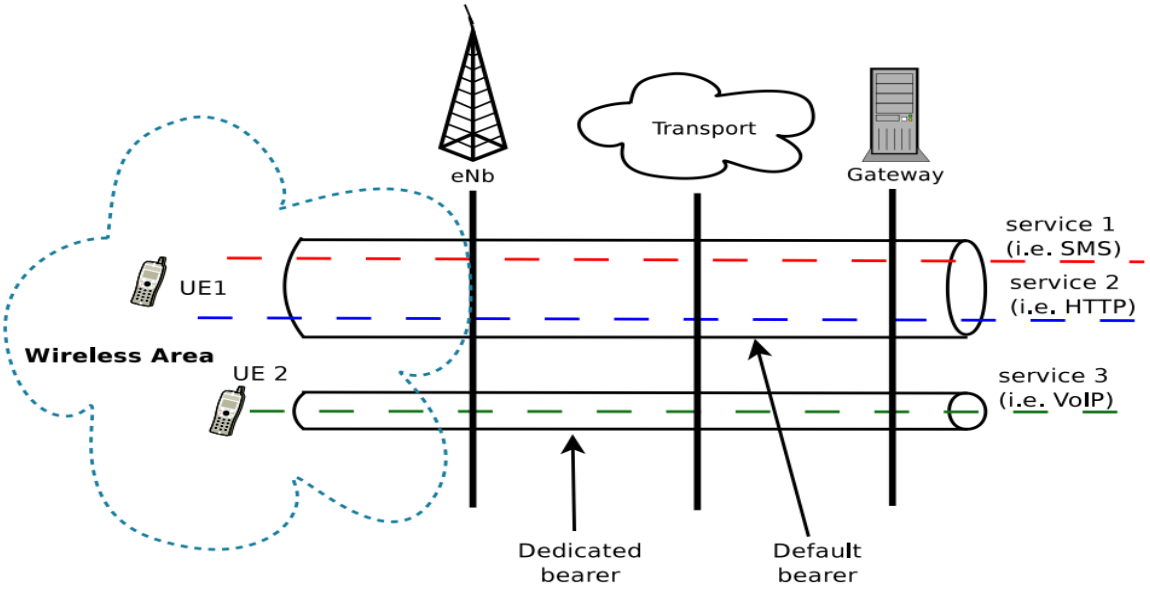


Figure 1.5 : *Les types de porteur.* **[7]**

1.6 Conclusion

Dans ce chapitre, nous avons présenté un aperçu sur les différentes générations des réseaux mobiles (1G, 2G, 3G) et leurs évolutions vers la quatrième génération (4G). Nous avons aussi définis la technologie LTE (la quatrième génération), et ses différentes caractéristiques et composantes.

Dans le chapitre suivant nous allons présenter les vulnérabilités dans LTE et les menaces connues contre les réseaux 4G ainsi les mécanismes de sécurité pour le LTE.

Chapitre 2 : Les menaces sur les réseaux 4G et les mécanismes de sécurité

2.1 Introduction

La technologie de la quatrième génération s'est décrite comme La grande innovation technologique des télécoms aujourd'hui, elle vise à améliorer la communication des réseaux mobiles en augmentant le débit et la vitesse de transmission des données. Le LTE (4G) a connu des vulnérabilités de sécurité, ce qui permet aux attaquants de cibler les appareils mobiles et les réseaux 4G.

2.2 Architecture de sécurité

L'architecture 4G LTE a été développée par le 3GPP en tenant compte des principes de sécurité dès sa création et la conception basée sur cinq groupes de fonctions de sécurité :

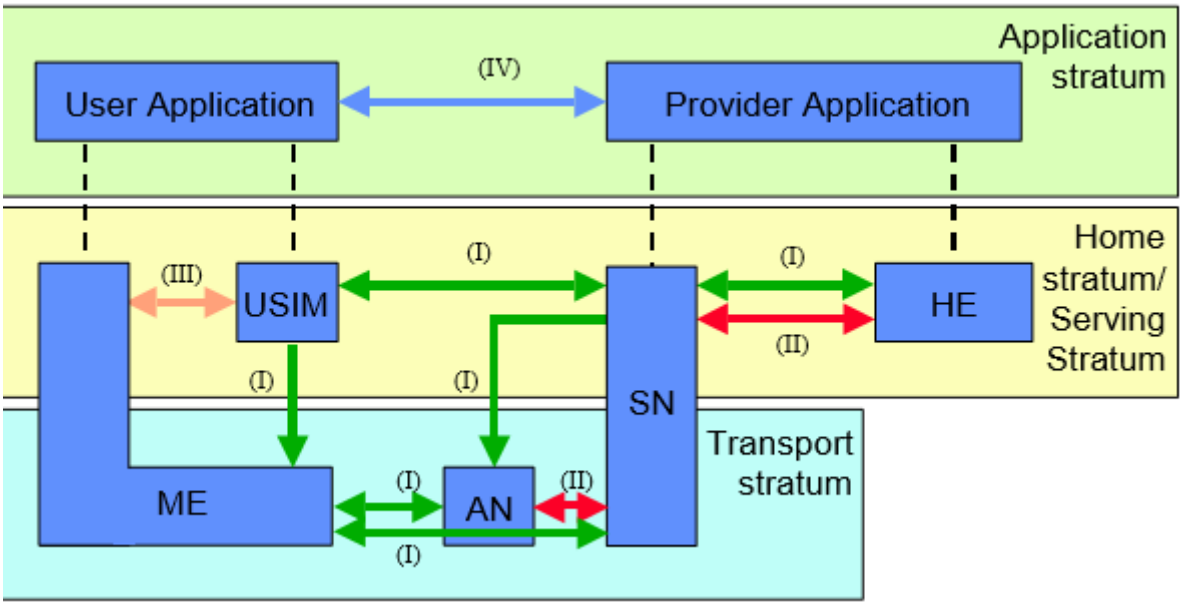


Figure 2.1 : *Architecture de sécurité du LTE.* **[8]**

- **La sécurité d'accès réseau (I):** fournit aux utilisateurs des fonctions de sécurité pour un accès sécurisé aux services et empêche les attaques sur le lien d'accès (radio).

- **La sécurité du domaine réseau (II):** fournit des fonctions de sécurité pour permettre un échange sécurisé des données de signalisation entre les nœuds et protège contre les attaques sur le réseau câblé fixe,
- **La sécurité du domaine utilisateur (III):** fournit un accès sécurisé à la MS,
- **La sécurité de domaine d'application(IV):** comprend l'ensemble de fonctionnalités de sécurité qui permettent l'application dans l'utilisateur et dans le domaine fournisseur pour un échange sécurisé de messages entre les entités,
- **La visibilité et la configuration de la sécurité (IV)**: comprend un ensemble de caractéristiques de sécurité fournissant à l'utilisateur la possibilité de s'informer si une caractéristique de sécurité est en cours d'utilisation et si l'utilisation et la fourniture de services doivent dépendre de la caractéristique de sécurité.

Les objectifs des dispositifs de sécurité présentés ci-dessus peuvent être résumés comme suit:

- Assurer la sécurité de l'utilisateur vers le réseau: en protégeant l'identité de l'utilisateur et la confidentialité du périphérique, ainsi que l'authentification de l'entité, ce qui peut être obtenu à l'aide d'une identification et d'un chiffrement temporaires. En tant que protocole d'authentification, la procédure EPS AKA est utilisée dans les réseaux LTE pour une authentification mutuelle entre utilisateurs et réseaux.
- Assurer la confidentialité des données utilisateur et des données de signalisation: en fournissant un algorithme de cryptage et un chiffrement à la signalisation RRC afin d'empêcher le suivi de l'UE.
- Assurer l'intégrité des données utilisateur et des données de signalisation: en protégeant l'intégrité de l'authentification d'origine des données de signalisation et en assurant l'authentification du réseau par l'UE. **[8]**

2.3 Vulnérabilités et menaces dans LTE (4G)

En raison de l'introduction de nouvelles technologies d'accès radio et de la migration vers une architecture basée sur IP, de nouvelles vulnérabilités ont été introduites dans l'architecture réseau, qui expose les réseaux mobiles à différentes menaces ciblant les piles de protocoles, les fonctionnalités de sécurité et les interfaces réseau. Une vulnérabilité dans le réseau mobile peut être comprise comme une faiblesse inhérente à l'architecture du réseau et des composants, qui peuvent être exploités par une menace pour effectuer une attaque.

Par conséquent, une menace est déterminée par la capacité de tenter délibérément d'accéder sans autorisation à l'information, de manipuler des informations et de rendre un système peu fiable ou inutilisable. Les menaces auxquelles sont confrontés les réseaux LTE, décrits dans les spécifications du système, peuvent être classées comme suit:

2.3.1 Menaces pour l'UE :

- **Transmission de l'IMSI en claire (IMSI capture):**

Un des premiers points faibles identifié de la sécurité de LTE, et hérité de l'UMTS, est l'envoie de l'identité permanente IMSI en claire

La transmission de l'IMSI se fait lors de la première connexion RRC établie lorsque le mobile est mis sous tension ou lors d'une demande par le réseau de service (MME). Le réseau de service demande l'identité de l'UE dans certains cas particuliers et sans l'obtention de l'IMSI, l'utilisateur serait définitivement exclu du système.

Il existe des cas où les requêtes IMSI (International Mobile SubscriberIdentity) en texte brut sont nécessaires. Cette vulnérabilité de sécurité a donc permis d'accroître l'aptitude à l'exploitation dans certaines zones, telles que les aéroports. De plus, les identificateurs de service sont envoyés en clair, une décision prise en fonction de la sécurité IMSI, augmentant ainsi l'impact potentiel des vulnérabilités IMSI **[9]**.

- **Suivi de l'UE :**

Le suivi de l'ID temporaire de l'abonné peut être utilisé sur la base des techniques d'enregistrement de données, afin de surveiller les actions prises par l'ID temporaire et de les corréler à un utilisateur lorsque suffisamment d'informations sont disponibles. En combinaison avec les techniques de capture IMSI, l'ID temporaire assigné peut être identifié et utilisé pour suivre les activités des utilisateurs.

Les menaces liées au transfert forcé nécessitent l'utilisation d'un eNB compromis, qui peut demander ou inciter l'UE à se connecter sur un eNB qui délibérément ou involontairement abandonne la connexion établie. **[9]**

2.3.2 Menaces pour l'eNB :

L'atteinte du compromis physique de l'eNB ou du détournement, l'injection / modification de paquets est possible. Cela donne à l'intrus la capacité d'injection en amont (vers l'environnement de réseau) et d'aval (vers l'unité d'accès à la qualité) et de dégradation du service. Les attaques physiques sur eNB peuvent également entraîner des extractions de données clés et non cryptées, combinées à des attaques DoS et à une violation d'intégrité. **[9]**

Les attaques DoS imposent une menace significative à la fois sur le réseau-eNB et les chemins eNB-UE. L'injection de paquets à partir d'un faux UE ou d'un élément de réseau peut être utilisée pour imposer un DoS, un brouillage radio ou un état de dégradation de service sur le eNB.

2.3.3 Menaces pour la passerelle MME / SAE :

De telles attaques peuvent inclure DoS contre le MME, basé sur des messages de signalisation provenant du RAN. Cela peut inclure l'utilisation de diverses procédures système, telles que l'authentification d'accès initial **[9].**

2.3.4 Les attaques dans les réseaux 4G :

Parmi ces attaques : les attaques de sécurité et de confidentialité, les attaques basées sur IP, les attaques de signalisation et les attaques de brouillage. Les attaques dans le réseau de 4G peuvent résulter d'une défaillance des exigences de sécurité, qui portent sur:

• **La sécurité de l'application:** est liée à l'intégrité du matériel, des logiciels, des données et du système d'exploitation (OS).

• **La sécurité d'accès réseau:** est liée à la Confidentialité, l'intégrité, l'authentification et l'autorisation (CIAA) des données.

• **La sécurité de l'utilisateur:** est liée à l'identité de l'utilisateur, à sa confidentialité et à son autorisation.

• **La sécurité de la zone réseau:** est liée à l'authentification et à la confidentialité de l'emplacement ME.

• **La maintenance QoS :** est liée à la sécurité contre les attaques par déni de service (DoS).

• La sécurité de la couche physique: est liée à la résistance contre la falsification.

2.4 Mécanismes de sécurité des réseaux de mobiles

Cette section propose un survol des nombreuses familles de crypto systèmes utilisés dans les réseaux de télécommunication mobiles pour satisfaire les exigences de confidentialité et d'intégrité des communications et pour authentifier les terminaux mobiles. L'emploi de tel ou tel crypto système dépend de la fonction de sécurité visée (authentification, négociation de clé, chiffrement, intégrité), de l'opérateur du réseau de télécommunication et de la génération de réseau considérée. **[10]**

2.4.1 La sécurité des réseaux mobiles GSM (2G)

La sécurité GSM est adressée sur deux plans : authentification et chiffrement. L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.

Après que l'usager se soit identifié au réseau à l'aide de son IMSI (International Mobile Subscriber Identity) ou de son TMSI (Temporary IMSI), il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification (A) sont utilisés. L'AuC (fonction du HLR physique) et la carte SIM contiennent la même clé Ki et l'algorithme (A).

La 2G ne fournit pas d'authentification mutuelle. Seule une authentification du client est réalisée. La carte SIM du mobile n'est pas en mesure de vérifier l'identité et la validité du réseau auquel le mobile est rattaché. Ceci laisse en théorie la porte ouverte à des attaques de l'homme du milieu (MITM). **[10]**

2.4.2 La sécurité des réseaux mobiles 3G

Le protocole AKA (Authentiquassions and Key Agreement) a été conçu afin de sécuriser l'accès aux réseaux mobiles, plus précisément les réseaux UMTS/3G et LTE/EPS. Il est aussi utilisé pour l'authentification du client IMS (cf. tutoriel EFORT sur l'authentification IMS).

La partie « authentiquassions » du protocole AKA (Authentication and Key Agreement) permet de vérifier l'identité de l'usager alors que la partie Key Agreement permet de générer des clés qui sont ensuite utilisées pour le chiffrement du trafic de l'usager dans le réseau d'accès et aussi pour la protection de l'intégrité des messages de signalisation. **[10]**

2.4.3 La sécurité dans LTE (4G)

Sur les couche AS et NAS, diverses procédures de sécurité sont mises en œuvre pour protéger contre les attaques malveillantes. Par exemple, la couche AS est responsable de la sécurité des données utilisateur et des données de gestion radio, alors que la couche NAS gère la sécurité des messages de gestion de la mobilité.

2.4.3.1 La sécurité de l'eNB :

L'importance de la sécurité de l'eNB vient du fait qu'il est un point de terminaison pour les mécanismes de sécurité principales de l'EPS, et qu'il est souvent installé dans des endroits exposés, en dehors du domaine de la sécurité de l'opérateur. En effet, l'eNB est en générale situé sur un site distant non protégé et dont l'accès ne peut pas être complètement contrôlé par l'opérateur (toits d'immeubles, édifices publics, emplacements extérieurs,..). Il peut en être de même pour les liens physiques qui relient l'eNB (fibre optique enterrée, faisceau hertzien) à l'EPC. **[11]**

2.4.3.2 La Sécurité dans 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, on cite : l'authentification du réseau de service introduit dans la procédure EPS-AKA, une nouvelle hiérarchie des clés ; et l'introduction de deux niveaux de sécurité. **[11]**

Authentification mutuelle entre le MME et l'utilisateur :

Le but de cette procédure est de réaliser une authentification mutuelle entre l'utilisateur (UE) et le réseau LTE.

Des vecteurs d'authentification (AV, AuthenticationVector) sont téléchargés par le MME à partir du HSS (Figure 2) à travers l'interface S6 (basée sur DIAMETER) lorsque le MME reçoit de l'UE les messages Attach Request ou Service Request. **[7]** Les paramètres présents dans le vecteur d'authentification (quadruplé) sont :

• RAND – le challenge (non aléatoire généré par le HSS) qui sert en tant qu'un des paramètres d'entrée pour générer les autres paramètres de l'AV.

• XRES – Le résultat attendu, utilisé par le réseau pour l'authentification de l 'USIM de l'UE.

• AUTN – Le jeton d'authentification utilisé par l 'USIM pour l'authentification réseau.

• KASME – La clé permettant de dériver les clés de chiffrement et d'intégrité.

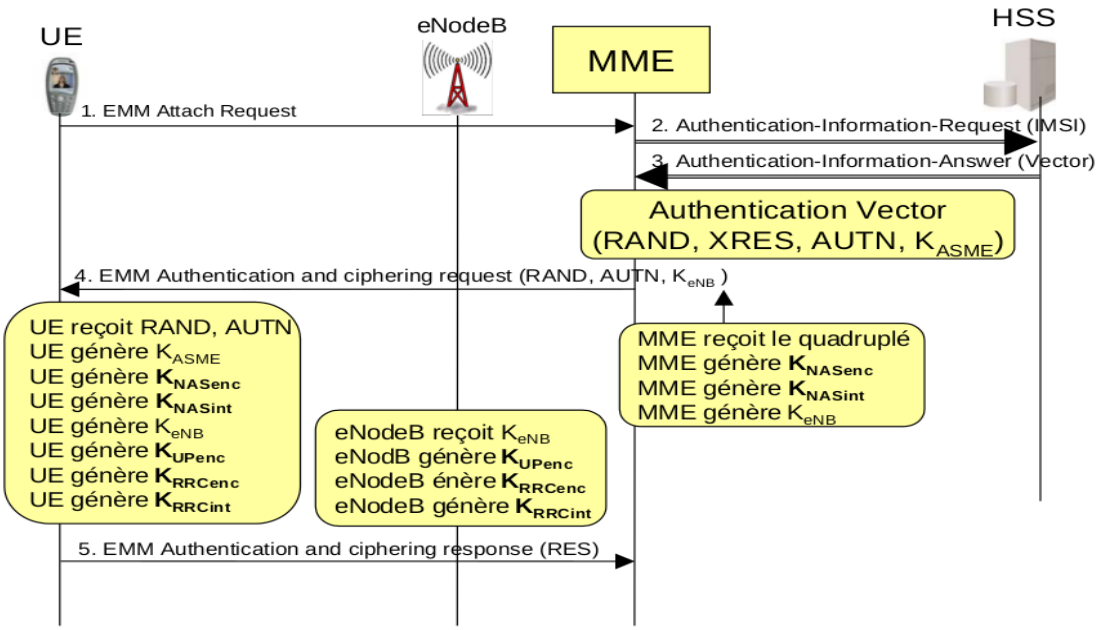


Figure 2.2: *Sécurité EPS.* **[7]**

• KNASenc est calculé par le terminal et le MME à partir de KASME. Il est utilisé pour la protection du trafic NAS avec un algorithme de chiffrement particulier.

• KNASint est calculé par le terminal et le MME à partir de KASME. Il est utilisé pour la protection du trafic NAS avec un algorithme d'intégrité particulier.

• KUPenc est calculé par le terminal et l'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic usager avec un algorithme de chiffrement particulier.

• KRRCenc est calculé par le terminal et l'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic de signalisation RRC avec un algorithme de chiffrement particulier.

• KRRCint est calculé par le terminal et l'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic de signalisation RRC avec un algorithme d'intégrité particulier.

L'authentification EPS est réalisée lorsque :

- ✓ Le mobile se rattache au réseau
- ✓ Le mobile établit un default bearer
- ✓ Le mobile établit un dedicatedbearer
- ✓ Le mobile met à jour sa localisation (Tracking Area)

L'authentification est réalisée entre le mobile et MME.

- ✓ Le chiffrement a lieu à deux niveaux :
- ✓ entre le mobile et l'eNodeB (trafic usager et trafic de signalisation)
- ✓ entre le mobile et le MME (trafic de signalisation)

La protection de l'intégrité de la signalisation a lieu :

- ✓ entre le mobile et l'eNode B pour la signalisation RRC
- ✓ entre le mobile et le MME pour la signalisation NAS (Non-Access Stratum)

2.4.3.3 La Sécurité dans l'IMS:

IMS (IP Multimedia Subsystem) est développé par le 3GPP, il offre une architecture permettant la convergence des données, de la voix et de la technologie, il se repose sur le standard de connectivité IP et représente une architecture pour le contrôle de service. **[11]**

Les utilisateurs (UE) qui veulent mettre en place une cession doivent communiquer avec le cœur du réseau IMS en utilisant des messages du protocole session Initiation Protocol" (SIP). Après avoir négocié les paramètres de la cession et le protocole de transport "Real-time Transport Protocol" (RTP), la cession de médias est établie. Un exemple typique d'une telle cession est la voix sur IP (VoIP). Les principaux éléments architecturaux de l'IMS sont les procurations SIP, connu comme CSCF (les fonctions de contrôle d'appels de service). Toute la signalisation de session SIP peut être manipulé par les CSCFs, qui peut être divisé en trois entités ; P-CSCF, I-CSCF and S-CSCF. Quand un utilisateur de messagerie instantanée veut communiquer avec l'IMS, la S-CSCF représente le HSS pour authentifier l'utilisateur de messagerie instantanée et assure le contrôle de session du multimédia service pour elle. Les services multimédias ne seront pas fournis jusqu'à ce que l'UE ait réussi à établir l'association de sécurité avec le réseau. **[11]**

2.4.3.4 La Sécurité NAS :

NAS est l'abréviation de « Non Access Stratum ». Le but principal de la sécurité NAS est de transmettre les messages de signalisation entre le MME et l'équipement usager en toute sécurité, donc chiffrés, au niveau du plan de commande. Les clés de sécurité NAS sont générées à partir de la 10 clé KASME. Après avoir établi la sécurité NAS, le MME et le UE partagent une clé de chiffrement (KNASenc) et une clé d'intégrité (KNASint) utilisées pour le chiffrement et la protection de l'intégrité de la signalisation entre l'UE et le MME. **[11]**

2.4.3.5 La Sécurité AS :

AS est l'abréviation de « Access Stratum ». Les clés de sécurité AS sont utilisées pour transmettre en toute sécurité des paquets IP et des messages Radio Resource Control (RRC) entre le point d'accès (ENodeB) et le UE. Elles sont générées à partir de la clé KeNB. Après avoir établi la sécurité AS, l'eNodeB et l'équipement usager partagent une clé d'intégrité RRC (KRRCint), une clé de cryptage RRC (KRRCenc) et la clé de cryptage du plan d'usager (KUP enc). Ces clés servent au chiffrement et à la protection de l'intégrité. **[10]**

2.5 Conclusion

Dans ce chapitre nous avons présenté les groupes de fonctions de sécurité définis par le comité 3GPP, ainsi que les vulnérabilités et les menaces connues dans le LTE et les réseaux 4G. Puis, nous avons présenté les mécanismes de sécurité pour les différentes composantes de LTE.

Dans le prochain chapitre, nous allons établir une étude détaillée sur l'attaque de l'homme de milieu et les solutions possibles pour éviter cette attaque.

Chapitre 3 : L'attaque du l'homme du milieu (MITM) dans les réseaux sociaux 4G et le protocole d'attaque proposé

3.1 Introduction

Les menaces contre les réseaux mobiles s'accentuent chaque jour, malgré que les connexions via les réseaux cellulaires sont bien sécurisées, mais elles ne sont pas infaillibles et peuvent éventuellement être interceptées par des experts en sécurité de réseaux mobiles équipés de matériels légers et de logiciels très sophistiqués qui permettent d'attaquer la gestion complexe de sécurité de la quatrième génération long Term génération (4G LTE), l'un des plus attaques connues qui menace la sécurité de ces réseaux est l'attaque de Man-In-The-Middle (MITM), ce qu'il fait un contrôle sur les données transférées aux utilisateurs.

3.2 Le principe de l'attaque MITM

L'attaque "Man-in-the-Middle" (l'homme du milieu) également connu sous : Monkey-in-the-middle attack, Session hijacking, TCP hijacking, TCP session hijacking, c'est une attaque informatique qui se réalise dans un réseau local. Son objectif est de forcer plusieurs machines d'un réseau à envoyer des données sur sa machine pour pouvoir communiquer avec leurs destinataires. On peut visualiser le schéma de l'attaque MITM comme indiqué sur la ***Figure 3.1***.

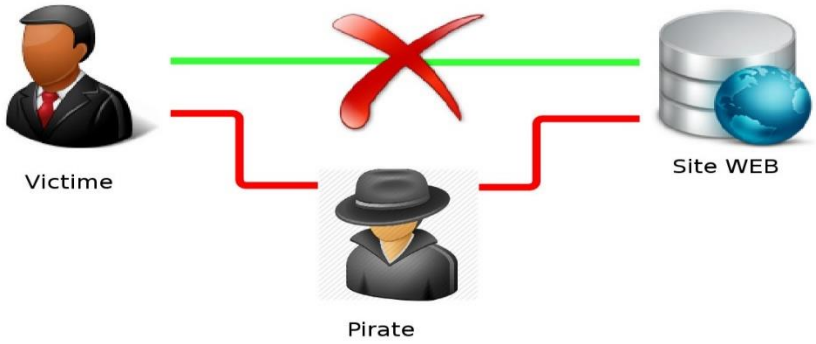


Figure 3.1 : *schéma illustre l'attaque MITM.* **[12]**

Donc le scénario de l'attaque MITM se base sur deux points finaux (victimes) et un tiers (pirate). L'attaquant a accès sur un canal de communication entre deux points d'extrémité : l'utilisateur cible et un réseau authentique, et donc d'écouter, de modifier, de supprimer, de réorganiser, de rejouer et de falsifier et de signaler les données des utilisateurs. **[12]** Il peut être utilisé pour recueillir des informations, accéder aux ressources du réseau privé en détournant les sessions en cours, dériver des information sur un réseau et ses utilisateurs grâce à l'analyse du trafic, altérer l'authenticité et l'intégrité des données transmises et l'injection de nouvelles informations confidentielles non

identifiées dans les sessions réseau.

3.3 MITM sur le réseau combiné GSM / UMTS

L'attaque MITM peut être exécutée dans différents canaux de communication tels que GSM, UMTS, Evolution à long terme (LTE), Bluetooth, Near Field Communication (NFC) et Wi-Fi. Les cibles d'attaque ne sont pas seulement les données réelles qui circulent entre les points d'extrémité, mais aussi la confidentialité et l'intégrité des données elles-mêmes .En particulier, l'attaque MITM vise à compromettre :

- Confidentialité, en écoutant la communication.
- Intégrité, en interceptant la communication et en modifiant les messages.
- Disponibilité, en interceptant et en détruisant des messages ou en modifiant des messages pour que l'une des parties mette fin à la communication.

Nous pouvons identifier au moins trois façons de caractériser les attaques MITM, conduisant à trois catégorisations différentes :

1) MITM basé sur les techniques d'emprunt d'identité.
2) MITM basé sur le canal de communication dans lequel l'attaque est exécutée.
3) MITM basé sur l'emplacement de l'attaquant et la cible dans le réseau. **[12]**

La plupart du temps, l'attaquant utilise les techniques de détournement de flux décrites dans les suivantes sections pour rediriger les flux du client et du serveur vers lui.

Dans cette perspective, les attaques MITM peuvent être divisées en :

- Le MITM basé sur la falsification est une attaque dans laquelle l'attaquant intercepte une communication légitime entre deux hôtes au moyen d'une attaque de falsification et contrôle les données transférées, alors que les hôtes ne connaissent pas l'existence d'un homme intermédiaire. Dans certains cas (p. Ex., Spoofing DNS), les dispositifs d'inoccupation d'attaquants entre les victimes, dans d'autres cas (p. Ex., Spoofing ARP), l'attaquant falsifie directement les dispositifs de la victime.

- SSL / TLS MITM est une forme d'interception de réseau active, où l'attaquant s'installe dans le canal de communication entre deux victimes (habituellement le navigateur de la victime et le serveur Web). Ensuite, l'attaquant établit deux connexions SSL séparées avec chaque victime et relève les messages entre eux, d'une manière telle que les deux ignorent l'intermédiaire. **[12]** Cette configuration permet à l'attaquant d'enregistrer tous les messages sur le fil, et même de modifier sélectivement les données transmises.

- BGP MITM est une attaque, basée sur le détournement d'IP, mais où l'attaquant fait livrer le trafic volé à la destination. Ainsi, le trafic passe par la station autonome (AS) de l'attaquant, où elle peut être manipulée. **[13]**

- Le MITM basé sur la station de base False (basée sur FBS) est une attaque, lorsque le tiers force la victime à créer une connexion avec une fausse station de réception de base (BTS), puis, en l'utilisant, l'attaquant manipule le trafic des victimes **[13]** comme il est mentionné dans la **figure 3.2** .

Figure 3.2 : la création d'une station de base malveillante dans les réseaux cellulaires. **[14]**

Considérons l'exemple suivant : un réseau se compose des BTS légitimes 3G, des MS légitimes, des fausses 3G BTS, Fausse 2G BTS et Fausse MS. Le réseau de l'attaquant est une combinaison des False 3G BTS, False 2G BTS et False MS. De même que dans l'attaque MITM sur GSM (voir la section VI-B), la MS légitime ne doit pas être connectée à la station réelle locale. L'algorithme d'attaque MITM sur GSM / UMTS combiné est le suivant (voir ***Figure 3.3***) :

1) L'attaquant lance 3G False BTS et attrape l'identité internationale d'abonné mobile (IMSI) du SM de la victime.

2) L'attaquant utilise l'IMSI de la victime pour se faire passer pour le MS de la victime contre les faux MS. Ensuite, il récupère AUTN du réseau réel (de HLR en utilisant la connexion avec Légitime 3G BTS), et après avoir reçu des données, il brise la connexion. À ce stade, l'attaquant a une valeur AUTN, ce qui prouvera pour le MS légitime que False 2G BTS est un réseau valide.

3) L'attaquant commence 2G False BTS et force la victime à se connecter. Après que la MS de la victime vérifie avec succès le jeton d'authentification, l'attaquant envoie un message de cryptage préféré ou aucun chiffrement (puisque GSM ne fournit pas l'intégrité des données **[14]**). En fin de compte, finir, l'attaquant MITM devrait fournir un accès au réseau réel en utilisant la connexion entre

False MS et le réseau légitime.

La dernière étape de la méthode présente un inconvénient évident : elle laisse des traces. L'utilisation de False MS pour la redirection du trafic intercepté révélera le module universel d'identité d'abonné (USIM). En outre, l'attaquant devrait prendre en considération que AUTN contient SQN, et il est essentiel que la victime n'ait pas fait l'authentification entre l'obtention de l'emprunt d'identité AUTN et GSM. Sinon, le jeton pourrait être hors de portée et sera rejeté par une instance légitime.

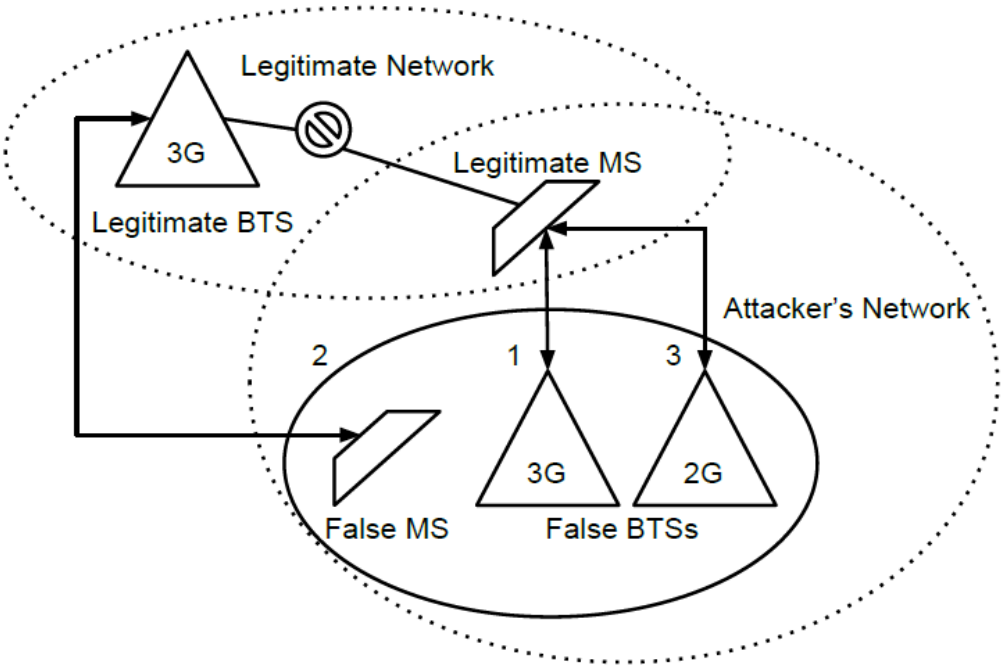


Figure 3.3 : *l'Attaque MITM sur les réseaux combinés GSM / UMTS.* **[13]**

3.4 L'attaque du l'homme du milieu (MITM) dans les réseaux sociaux 4G

L'échec des exigences de sécurité peut être exploité par un attaquant afin d'effectuer différents types d'attaques telles que les attaques de disponibilité, la confidentialité et l'intégrité, cette dernière qui peut être obtenue grâce aux modifications de trafic et de données sur les éléments du réseau -et on parle alors de l'attaque du l'homme du milieu MITM.

3.4.1 Architecture général de l'attaque MITM dans les réseaux sociaux 4G

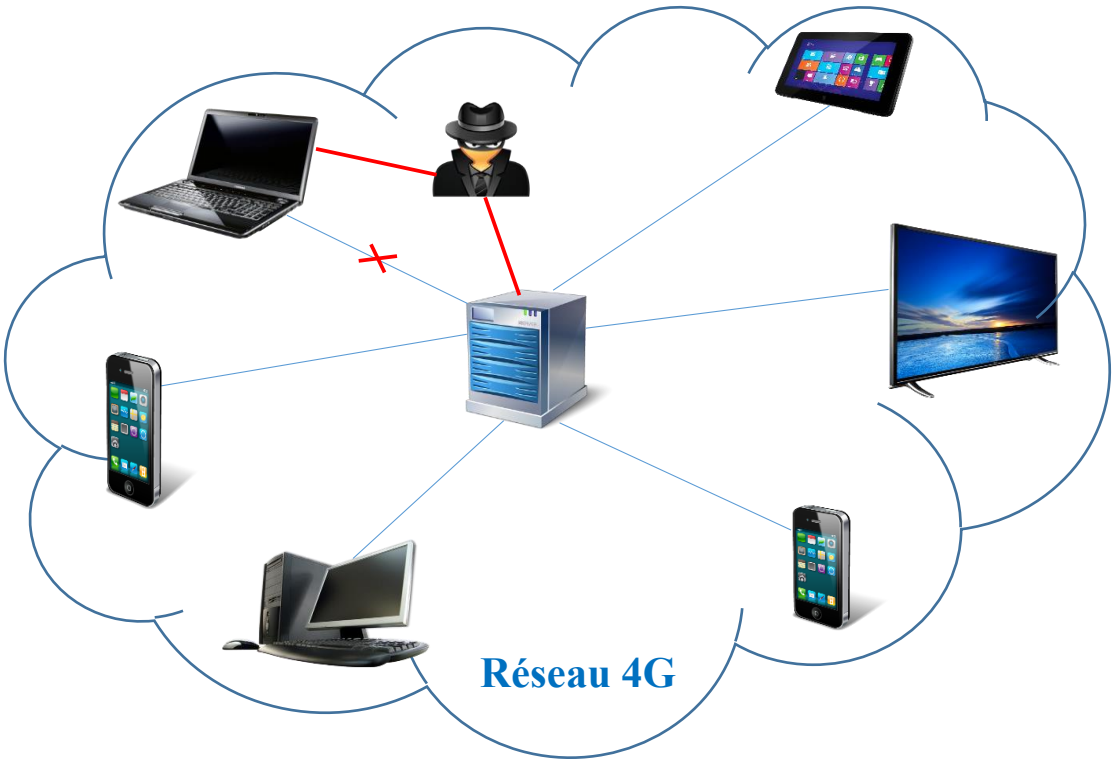


Figure 3.4 : *schéma général de l'attaque MITM dans les réseaux*

3.4.2 L'attaque MITM sur l'interface radio dans les réseaux 4G

L'attaque **MITM** dans les réseaux 4G est une attaque sur l'interface radio qui est plus vulnérable aux attaques. Le support de transmission étant partagé. Quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise. De plus, si une personne malveillante est assez bien équipée, cette dernière n'a pas besoin d'être située dans la zone de couverture. Il lui suffit d'utiliser une antenne avec ou même sans l'aide d'un amplificateur pour accéder au réseau. **[12]**

- **Le déroulement d'attaque de l'homme du milieu (MITM) dans le LTE:**

Les attaquants peuvent tirer parti d'une faiblesse connue dans LTE dans laquelle le transfert d'identité d'utilisateur se produit non chiffré, en texte clair entre l'UE et l'eNodeB, lors de la procédure de connexion initiale. Cela permet à un auditeur d'écoute de suivre l'emplacement de la cellule de l'utilisateur ou de lancer un homme dans l'attaque du milieu par l'identifiant international d'abonné mobile de l'utilisateur (IMSI) et le relais des messages utilisateur

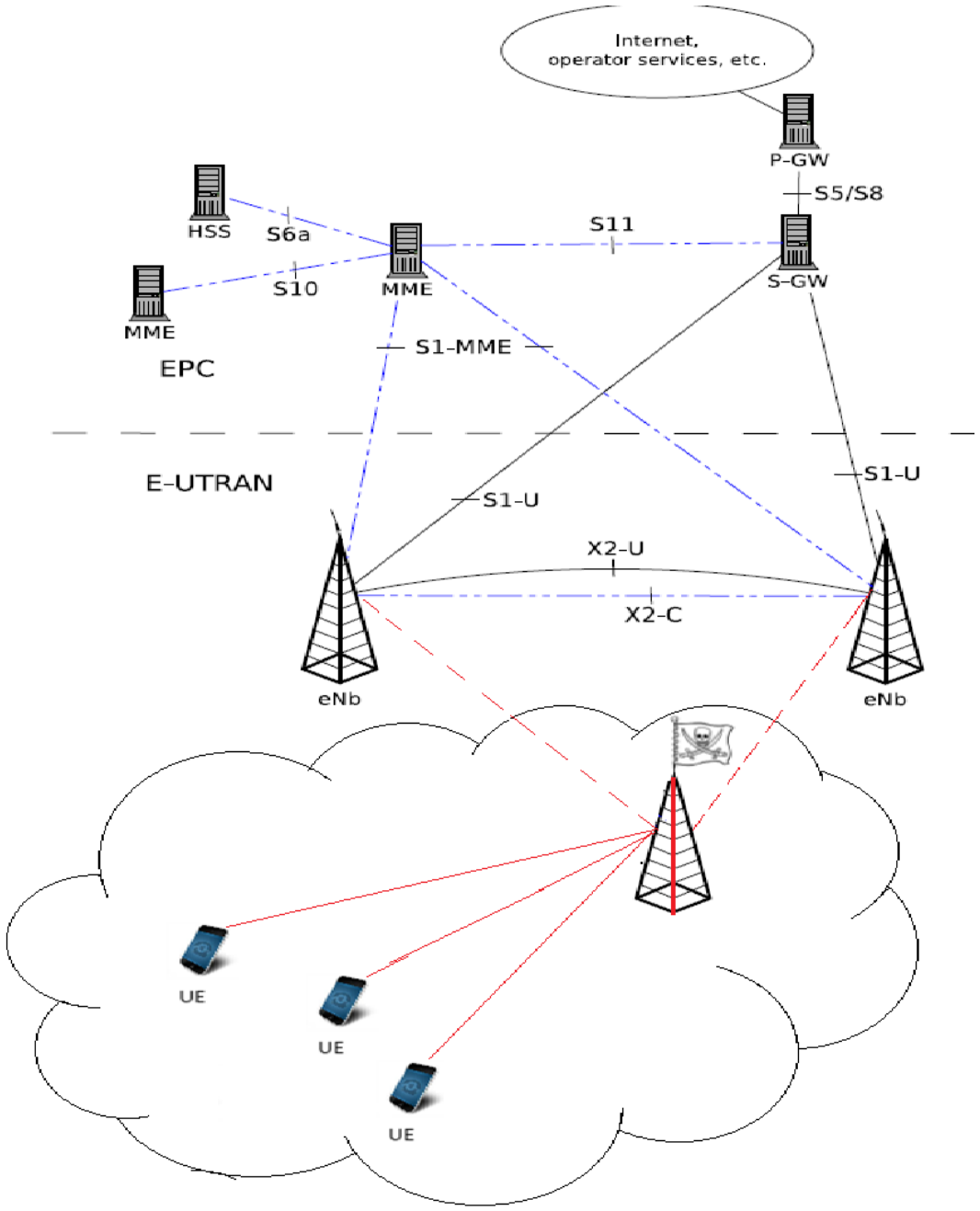


Figure 3.5 : *schéma proposé illustre l'attaque* ***MITM*** *dans l'architecture des réseaux 4G.*

L'attaquant utilise un appareil portatif de haute technologie appelé 'IMSI catcher' (capteur d'IMSI),

qui joue le rôle d'une fausse station de base eNB et prétend d'être un réseau de service légitime. Dans ce cas l'attaquant prend la position de l'homme du milieu (MITM), lorsque l'utilisateur allume son téléphone mobile ou même dans certains cas lorsqu'il est en mode de veille, il se connecte à cette station de base qui lui demande (en lui transmettant le message Identity Request message) de s'authentifier avec son identité permanente IMSI. Ensuite l'UE doit obligatoirement, et pour ne pas se faire exclure du réseau, répondre en envoyant son identité IMSI.

Algorithme d'attaque en langage naturel :

- Création d'un réseau (LTE).
- Des utilisateurs se connectent à un réseau 4G utilisant des appareils mobile, tablette, tv… (User Equipment (***UE***)).
- Un pirate s'installe entre l'***EU*** et le serveur ***EPC*** pour se mettre en écoute par la création d'une virtuelle station de base ***" fakeeNB"*** .
- Les appareils communiquent avec le faux réseau LTE 4G (fake base station).
- Dès que tel appareil envoie une requête, l'attaquant la reçoit, il ouvre son contenue peut être le changé , et il lui renvoie au ***EPC***.

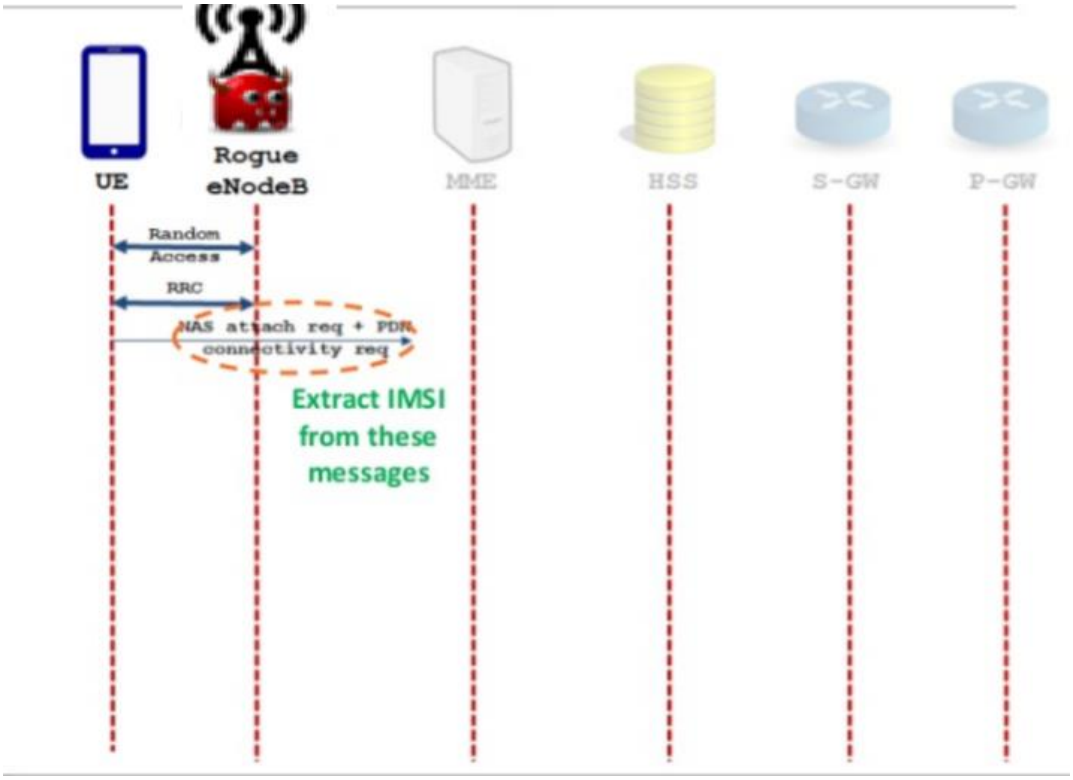


Figure 3.6 : *schéma illustre le déroulement de l'attaque MITM dans les réseaux 4G.*

Algorithme de détection de l'attaque :

- Le serveur (**EPC**) et les appareils se mettent d'accord sur le temps de repense durant l'envoi du message.
- A chaque réception d'une requête envoyée (de l'EPC aux ***UE*** ou bien l'inverse) le destinataire vérifie et compare le temps d'envoi avec le temps attendu :
  - ✓ Si le temps d'envoi égale le temps attendu, donc le réseau et clean et il n'existe aucun intrus.
  - ✓ Si le temps d'envoi est supérieur au temps attendu dans ce cas-là, il y'a un intrus dans le réseau, car la requête est passée par un autre chemin avant qu'elle soit reçue par l'***EPC***.
  - ✓ Le serveur envoie un message d'alerte à l'appareil (UE) concerné disant qu'il existe un attaquant en écoute dans le réseau.

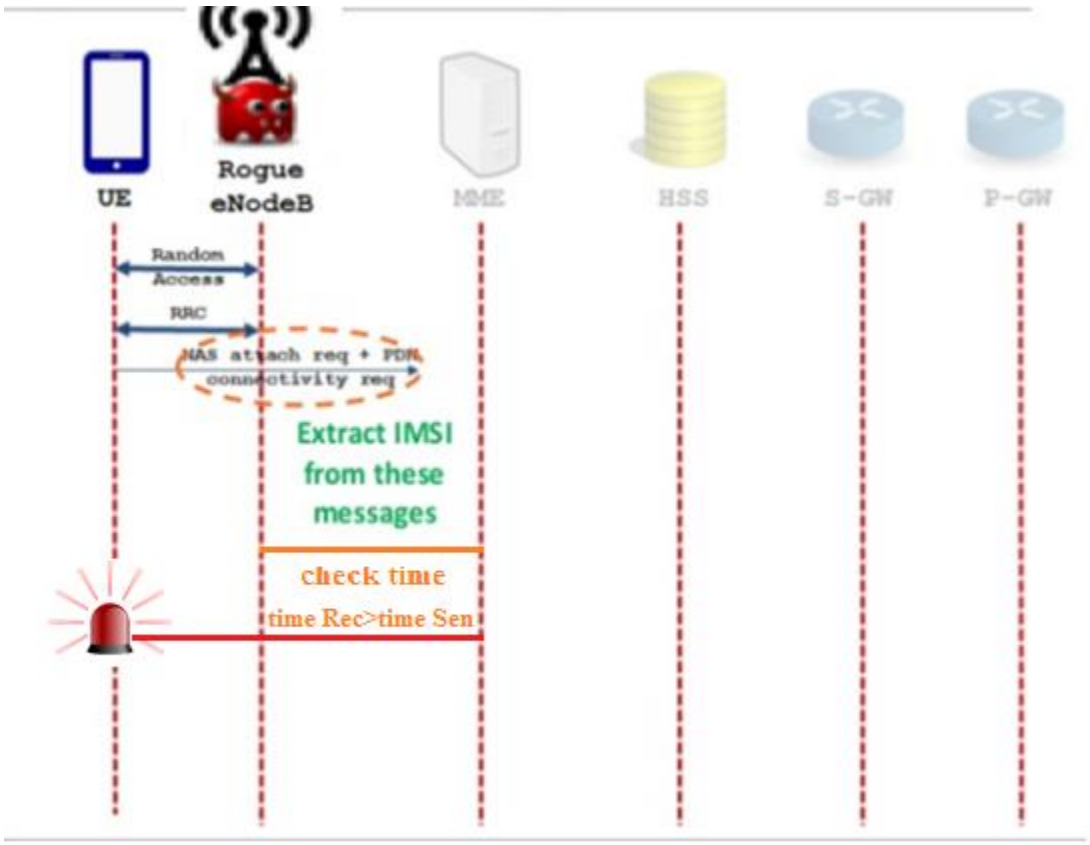


Figure 3.7 : *Schéma illustre les détections de l'attaque MITM dans les réseaux 4G*

Algorithme de l'attaque MITM en pseudo Langage :

```
/** initialisation du système
 *enregistrement des parties  * détection de l'attaque*/
varchar  user, attacker, password ;
int Port=9 ;
Begin {
Server_on(9 );
// attack and user connect in the same network
user.connect(9 );
attacker.connect(9);
// user identify to access to his session
if (connection = true)
{ user.Identify();
     //attacker listen in the network
          attacker.Get.UserName();
          attacker.Get.Password();
          user.Disconnected();
} else{
          System.out.print(" Server not found ") ;
        }
// attacker  can connect, disconnect and modify user data
}
```

Algorithme de détection de l'attaque MITM en pseudo Langage :

```
input : Serv1, Mobile, Tab, PC, TV,
int Port=9, Time= 5;
String: msg1, msg2
Begin {
Server_on(Port=9 );
// attack and user connect in the same network
user.connect(9);
attacker.Connect(9);
server_on(9);
server_send_msg (msg1)   ;
attacker_get_msg(msg1)  ;
```

```
Attacker_send_msg_to_user(msg1);
Message_processing_ by_user(msg1)  ;
User_send_reply (msg2) ;
attacker_get_ reply (msg1);
attacker_send_ reply_to_server (msg1)  ;
Check(Time){
while (Time=5){
        server_send_msg ()   ;
} else{
        server_send_alert();
        }
}
```

Algorithme de sécurité contre l'attaque MITM en pseudo Langage :

```
public static void main (String [] args){
Server_on(Port=9 );
// attack and user connect in the same network
user.connect(9);
attacker.Connect(9);
server_on(9);
server_share_public_key (K1)   ;
server_send_msg (msg1)   ;// msg crypté avec son clé privé
attacker_get_msg(msg1)  ;// msgcrypté
Attacker_send_msg_to_user1(msg1);
User_get_msg(msg1)  ; // user décrypté avec leur clé pub
User_send_reply (msg2) ; ;// msg crypté avec son clé privé
attacker_get_ reply (msg1);//msgcrypté
attacker_send_ reply_to_server (msg1);//msgcrypté
server_get_ reply (msg2)// user décrypté avec le clé pub}
```

3.5 Mécanismes de sécurité

3. 5.1. La cryptographie

La cryptographie (ou **chiffrement**) est la science de l'utilisation des mathématiques pour chiffrer et décrypter les données. Elle était essentiellement utilisée pour obtenir la confidentialité des messages. Il s'agit de transformer les lettres qui composent le message à l'aide d'une clé de chiffrement. [**15]**. Donc elle permet de stocker des informations sensibles ou de la transmettre à travers des réseaux non sécurisés afin de ne pouvoir être lue par personne que par le destinataire prévu.

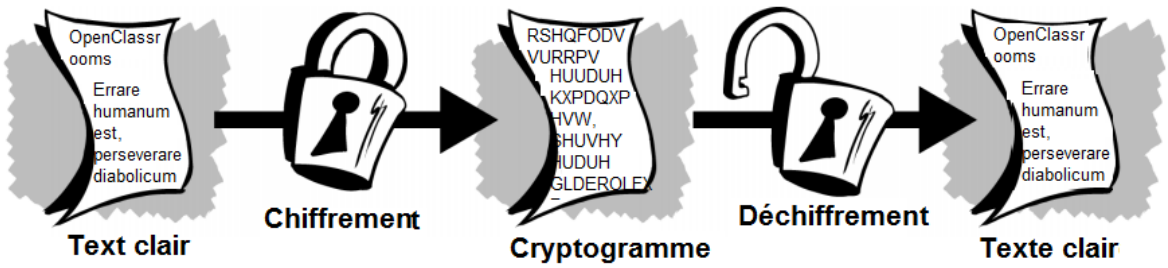


Figure 3.8 : *Le processus de cryptographie.* **[16]**

Il existe des techniques de cryptographie :

- ***La cryptographie à clé symétrique***

Il fondée sur l'utilisation d'une clé unique, qui permet à la fois de chiffrer et de déchiffrer les données.

Cette clé est appelée la clé symétrique (par fois secrète). Dans le cadre d'échanges sur un réseau, une entité émettrice chiffre les données avec une clé et l'entité destinatrice déchiffre les données avec la même clé. Si les algorithmes symétriques sont performants et permettent d'atteindre des débits importants dans le chiffrement et déchiffrement, ils posent cependant le problème de la mise en place d'une même clé entre émetteur et récepteur. Partager une clé avec chaque entité communicante potentielle, même dans un groupe fermé d'entités est extrêmement contraignant et conduit rapidement à un très grand nombre de clés à gérer. Il est donc préférable d'automatiser la mise en place de ces clés.

Les algorithmes symétriques les plus connus sont dans l'ordre chronologique de définition, le DES (*Data Encryption Standard*), le 3DES (prononcé « Triple DES »), et l'AES *(Advanced Encryption Standard*). **[15]**

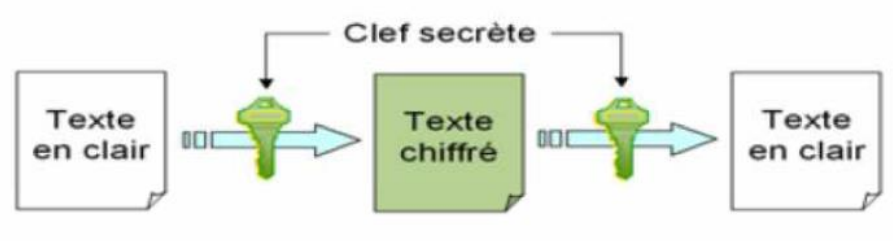


Figure 3.9 : *Cryptographie à clé symétrique.* **[15]**

- ***La cryptographie asymétrique (à clé publique)*** *:*

La technique de cryptographie à clé publique résout le principal problème des clés symétriques, qui réside dans la transmission de la clé. **[15]** C'est un schéma asymétrique qui utilise une paire de clés pour le cryptage ou clés de chiffrement, dites "clés asymétriques": une clé publique, qui crypte des données et une clé privée correspondante (clé secrète) pour le décryptage. **[17]** Ces deux clés sont générées simultanément et sont complémentaires car le chiffrement avec l'une de ces clés nécessite le déchiffrement avec l'autre clé. Chaque clé a un rôle bien défini. La clé privée est une clé qui ne doit être connue que d'une seule entité, c'est elle qui permettra à cette entité de s'authentifier.

Il est nécessaire de chiffrer le message émis avec la clé publique du destinataire pour garantir la confidentialité d'un message. Cette clé publique est connue de tout le monde et peut donc servir à n'importe quelle entité pour chiffrer un message. Par contre, la clé privée complémentaire n'est connue que du destinataire du message, le destinataire sera donc le seul à pouvoir déchiffrer le message. **[15]**

RSA et Diffie-Hellman sont des algorithmes utilisés dans la cryptographie à clé publique.

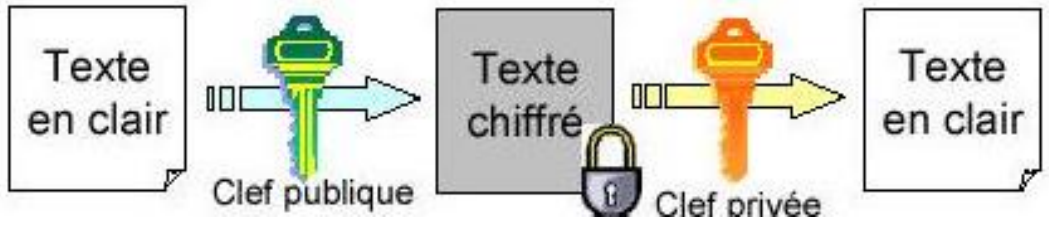


Figure 3.10 **:** *Cryptographie asymétrique.* **[15]**

3. 5.2. Les fonctions de hachage

Le hachage consiste à déterminer une information de taille fixe et réduite à partir d'une donnée de taille indifférente**.** C'est en particulier cette propriété que l'on utilise pour valider l'intégrité d'un

transfert des données. Une fonction hash est une fonction mathématique qui convertit une valeur d'entrée numérique en une autre valeur numérique compressée. L'entrée de la fonction hash est de longueur arbitraire, mais la sortie est toujours de longueur fixe. Les valeurs retournées par la fonction sont appelées digest de message ou simplement valeurs de hash. Un résultat sur un nombre limité d'octets. **[17]**

Les propriétés attendues de ces fonctions de hachage sont les suivantes :

- Un résultat sur un nombre limité d'octets.
- L'impossibilité de retrouver le message original à partir du résultat de la fonction.
- Deux messages différant de 1 bit seulement produisent deux résultats qui diffèrent d'au moins la moitié des bits **[15]**.

3.5.3. Cryptage avec ECC (EllipticCurvesCryptography)

La cryptographie elliptique *ECC (Elliptic curve scryptography)* a été proposée par *Victor Mill*er et *Neal Koblitz*au milieu des années 1980s. Actuellement *ECC* est un crypto système mur, il est une alternative attractive au crypto système *RSA* particulièrement pour les dispositifs contraints en ressources. Il a été récemment adopté par le gouvernement U.S. **[18]**

Les systèmes cryptographiques basés sur les courbes elliptiques permettent d'obtenir un gain en efficacité dans la gestion de clés**.** En effet, de tels cryptosystèmes nécessitent des clés de taille beaucoup plus modeste ce qui représente un avantage pour les systèmes utilisant les cartes à puces dont l'espace mémoire est très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de générations et d'échanges de clé beaucoup plus important**.** **[18**]

3.6 Conclusion

Dans ce chapitre, nous avons défini l'attaque man-in-the-middle MITM. Plus précisément, nous avons présenté le principe de l'attaque MITM dans les différentes générations des réseaux mobiles combinés GSM / UMTS (2G et 3G), et aussi dans les réseaux LTE (4G). Puis, nous avons proposé un schéma qui illustre l'attaque MITM dans l'architecture des réseaux 4G. Nous avons expliqué comment l'attaquant peut créer une station de base (eNB) fausse. En fin, nous avons proposé des mécanismes de sécurité à savoir la cryptographie asymétrique (ECC) et la fonction de hachage qui sont la base de notre proposition.

Dans le prochain chapitre, nous allons évaluer l'impact de l'attaque MITM à travers le simulateur réseau NS-3.

Chapitre 4 : L'implémentation du système proposé

4.1 Introduction

Les réseaux informatiques ont connus un développement énorme au cours du temps, mais pour tester leurs performances il est couteux. C'est pour cela on utilise les simulateurs réseaux qui offrent beaucoup d'économie de temps et d'argent pour l'accomplissement des tâches de simulation et qui sont également utilisés dans le but de pouvoir tester les nouveaux protocoles existant dans les concepteurs des réseaux

Dans ce chapitre nous présentons la simulation de l'attaque de l'homme du milieu (MITM) dans les réseaux sociaux 4G, ainsi que l'ensemble des données nécessaires pour un bon fonctionnement.

4.2 Les apports de la simulation

- Simuler le réseau
- Simuler l'activité du réseau
- Outils de visualisation et d'analyse
- Possibilité d'être proche de la réalité
- Ne nécessite pas d'investissements particuliers

4.3 Présentation des outils de développement

Vu le nombre de programmes, le choix d'un langage de programmation est donc une décision importante. Dans ce qui suit, nous présentons brièvement les environnements que nous avons choisis pour l'implémentation :

- Network simulator NS-3.
- Un langage de programmation C++.
- Une plate-f
- orme Linux (Ubuntu).

4.4 Le simulateur NS-3

Ns-3 (Network simulator) est un logiciel gratuit, open source, et il est publiquement disponible pour la recherche, le développement et l'utilisation pédagogique. Il a été développé pour fournir une plate-forme de simulation de réseau ouverte et extensible, pour la recherche en réseau et l'éducation ns-3 fournit des modèles de fonctionnement des réseaux des données par paquets.

4.4.1 Présentation générale

- Simulation à évènements discrets
- 3eme génération (annoncé le 2/7/2006)
- Composé de modules
- Ecrit en C++
- Scripts de programmation et d'utilisation en C++ ou Python

4.4.2 Outils de visualisation du scénario de simulation

- PyViz (visualisation en temps réel)
- NetAnim (visualisation basée sur un fichier traçant le scénario)

4.4.3 Téléchargement et installation du simulateur NS-3 :

Ns-3 est un simulateur de réseau pour les systèmes Internet. Nous devons installer ns3 sur n'importe quelle plate-forme linux comme Ubuntu/Debian, dans notre projet nous avons installé la version Ubuntu 15.10.

- **Les paquets d'installation :** Afin de terminer l'installation de Linux, la première chose à faire c'est ouvrir le terminal et coller (ctrl+alt+T) le code suivant:

Figure 4.1 : Les paquets d'installation.

Voici les conditions préalables pour l'installation **: [19]**

- Package pour C++, c'est le package minimal pour le besoin de l'installation de ns-3.

Sudo apt-get install gcc g++ python

- Package pour Python:

Sudo apt-get install gcc g++ python python-dev

- Package pour Mercurial:

Sudoap t-get install mercurial

- Package pour Bazaar utilisé pour l'exécution des scripts Python sur ns-3:

Sudoapt-getinstallbzrssssss

- Débogage:

Sudo apt-get install gdbvalgrind

- GSL pour éviter les erreurs dans les modèles du réseau WiFI:

Sudo apt-get install gsl-bin libgsl0-dev libgsl0ldbl

- NSC requires the flex lexical analyzer and bison parser generator:

Sudo apt-get install flex bison libfl-dev

- Installation des paquets gcc et g++ de la leur dernière version:

Sudo apt-get install g++-4.6 gcc-4.6

- Pour lire pcap paquet traces:

Sudoapt-getinstalltcpdump

- Support de base de données pour les statistiques cadre:

Sudo apt-get install sqlite sqlite3 libsqlite3-dev

- Xml-based version of the config store (requires libxml2 >= version 2.7):

Sudo apt-getinstall libxml2 libxml2-dev

- A GTK-based configuration system:

Sudo apt-get install libgtk2.0-0 libgtk2.0-dev

- Pour expérimenter avec des machines virtuelles et ns-3:

Sudoapt-getinstallvtunlxc

- Support for utils/check-style.py code style check program:

Sudoapt-getinstalluncrustify

- Doxygen and relatedinline documentation:

Sudo apt-get install doxygengraphvizimagemagick

Sudo apt-get install texlivetexlive-extra-utilstexlive-latex-extra

- Le manuel et le tutoriel ns-3 sont écrits en reStructuredText pour Sphinx (doc / tutorial, doc / manuel, doc / modèles), et les chiffres généralement en dia:

Sudo apt-get install python-sphinx dia

- Prise en charge Gustavo Carneiro ns-3-pyviz visualiseur :

Sudoapt-getinstall python-pygraphviz python-kiwi python-pygoocanvaslibgoocanvas-dev

- Prise en charge du module d'OpenFlow (nécessite certaines bibliothèques boost) :

Sudo apt-get install lib boost-signals-devlibboost-filesystem-dev

- Soutien à la simulation distribuée basée sur MPI :

Sudoapt-getinstallopenmpi

Afin de passer à l'étape suivante on assure nous n'avons pas exécuté sudo pour être un super-utilisateur.

Installation du NS-3 :

- cd: pour retourner ver le dossier initial.
- mkdir ns3 : pour créer un dossier sous le nom ns3.
- cd ns3: pour entrer dans le dossier ns3.
- wget: http://www.nsnam.org/release/ns-allinone-3.26 (le lien pour télécharger NS3).
- tar xjf ns-allinone-3.26 tar.bz2: pour exporter NS3.
- cd ns-allinone-3.26/: pour entrer au dossier ns-allinone-3.26.
- ls: pour afficher tous ce qui existe dans le dossier ns-allinone-3.26.
- ./build.py : pour la construction
- Maintenant, exécutez la commande suivante pour configurer avec waf (outil de construction):
- . /waf -d debug --enable-examples --enable-tests configure.

Pour tester si tout va bien:

- ./test.py

Enfin voici le dossier de l'NS-3

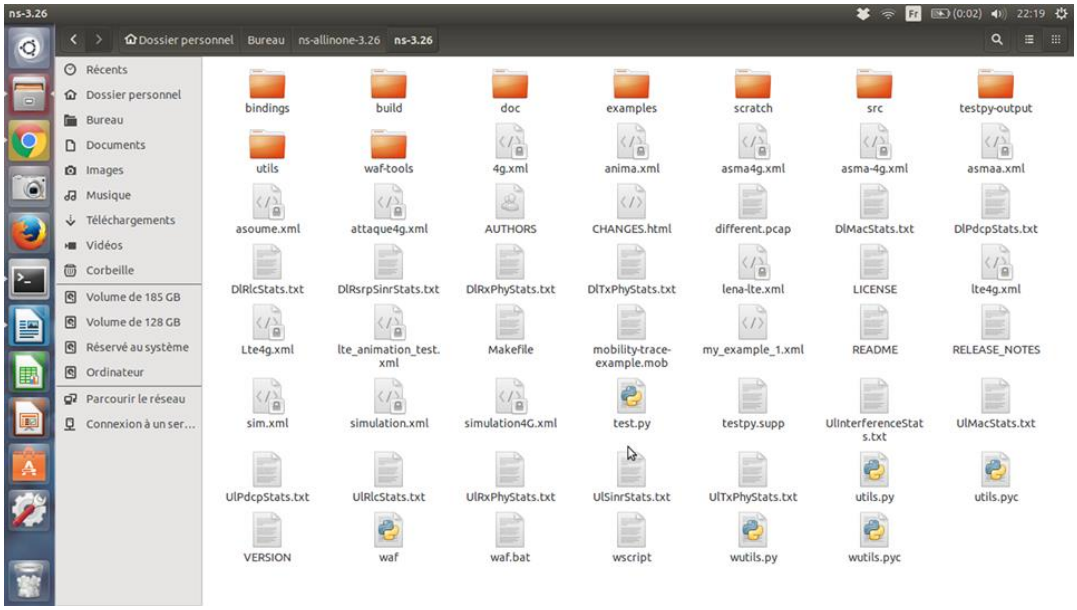


Figure 4.2 : Le dossier de l'NS-3.

4.5 Les démarches de la simulation :

Avant de commencer à faire la simulation, il faut définir le problème, la figure suivant illustre les démarches d'une simulation :

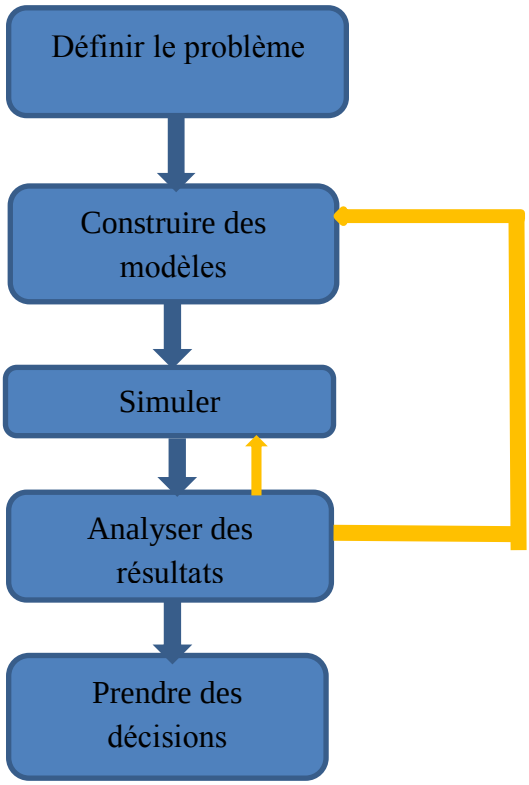


Figure 4.3 : *Les étapes de la simulation*

Tout d'abord pour installer le NS-3 et réaliser la simulation il faut avoir une interface Linux, pour cela nous avons installé le système Ubuntu/debian (Linux) version 15.10 directement sur ordinateur.

4.6 Installation de NetAnim

NetAnim est un animateur hors connexion basé sur la boîte à outils Qt. Il anime actuellement la simulation en utilisant un fichier de trace XML collecté lors de la simulation. La première version a été développée par George F Riley **[20]**. Le NetAnim Permet de :

- visualiser le scénario de simulation
- Utiliser un fichier trace
- Fichier trace =>xml
- Ajouter de codes supplémentaires
- Afficher les métadonnées des paquets

4.6.1 Téléchargement de NetAnim

NetAnim utilise un outil de configuration QT appelé qmake, pour construire netanim il faut d'abord installer Qt4 en collant cette commande dans le terminal de Linux :

$apt-getinstall qt4-dev-tools

Pour télécharger la dernière version du NetAnim on fait coller (Cntrl+Alt+T) le code suivant :

$hg clone http://code.nsnam.org/netanim**[20]**

4.6.2 Construction et utilisation de NetAnim

On utilise les commandes suivantes pour construire le NetAnim :

cd netanim

make clean

qmake NetAnim.pro

make

Cela devrait créer un exécutable nommé "NetAnim" dans le même répertoire, l'utilisation de NetAnim se faite en deux étapes :

Etape 1: Générer le fichier de trace XML de l'animation pendant la simulation en utilisant "ns3 ::AnimationInterface" dans la base de code ns-3

Etape 2 : Chargez le fichier de trace XML généré à l'étape 1 avec l'animateur hors ligne (NetAnim).

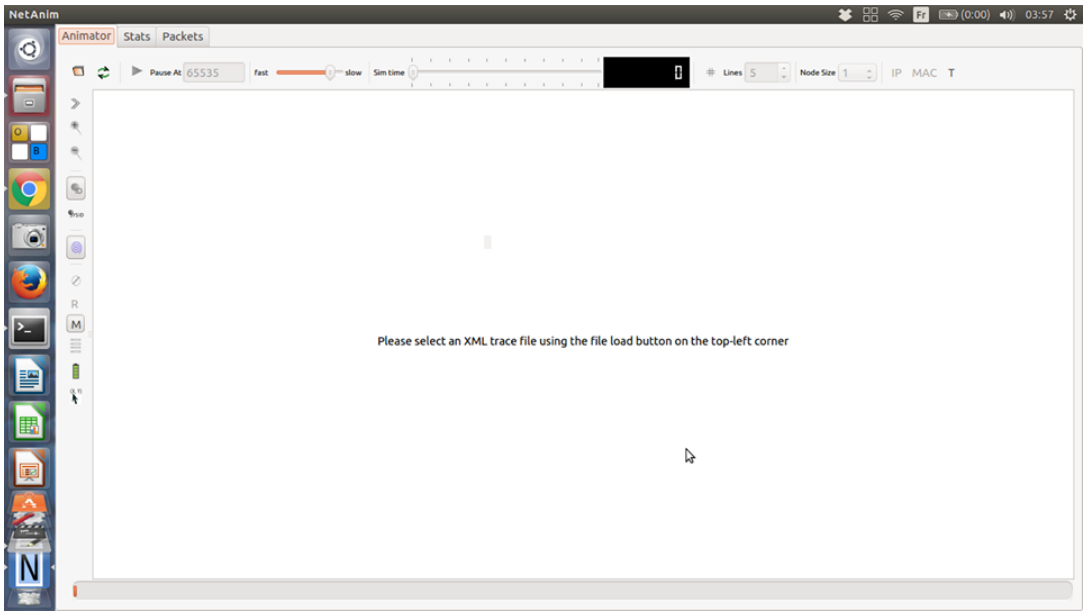


Figure 4.4 : *Accueil NetAnim*

4.7 La simulation de réseau LTE

Le NS-3 possède un module qui permet de simuler le réseau LTE avec une variété de mécanismes de qualité de services.

LENA :

LENA est un logiciel open source LTE / EPC Network Simulator qui permet aux fournisseurs de petites et petites cellules de LTE de concevoir et tester des algorithmes et des solutions de réseau auto-organisé (SON). LENA est basé sur le simulateur de réseau ns-3 populaire pour les systèmes Internet.

La topologie de réseau prise en charge par le modèle de simulation proposé par la communauté LENA est illustrée à la ***Figure 4.5.***

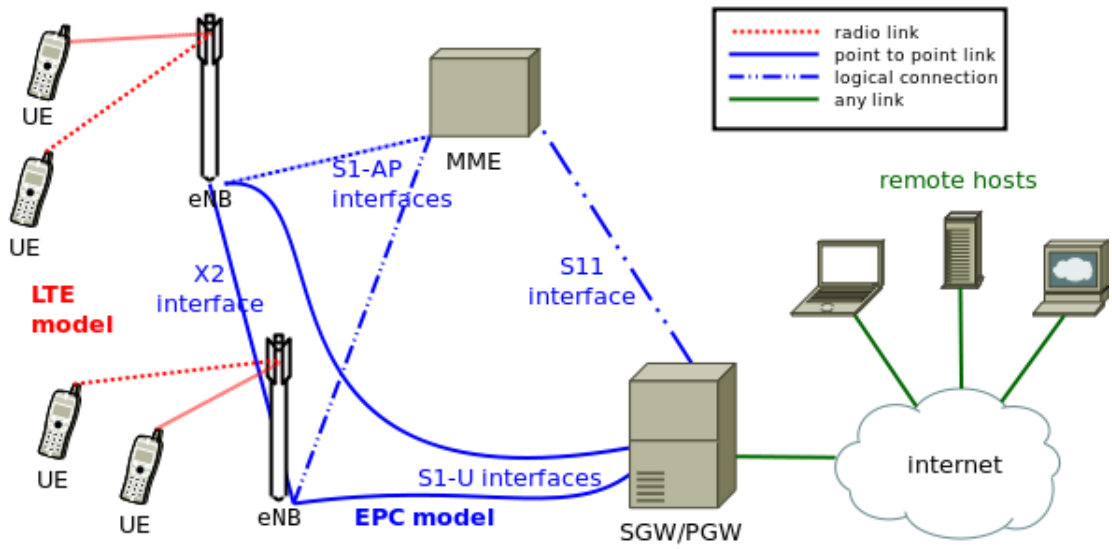


Figure 4.5 : *Topologie de réseau soutenue par le modèle proposé par Lena* **[12].**

Il existe deux composantes principales:

- Le modèle LTE: il comprend la pile protocole radio LTE (RRC, PPPC, RLC, MAC, PHY). Ces entités se trouvent entièrement dans l'UE et aux nœuds eNB.
- Le modèle de l'EPC: il comprend des interfaces de réseau de base, les protocoles et les entités. Ces entités et protocoles résider dans les nœuds SGW, PGW et MME, et partiellement dans les nœuds eNB.

Nous présentons le programme de base de notre simulation (pour la partie ETURAN):

La première étape à faire c'est :

1. Initialiser les bibliothèques (LTE) :

```
#include <ns3/core-module.h>

#include <ns3/network-module.h>

#include <n #include <ns3/core-module.h>

#include <ns3/network-module.h>

#include <ns3/mobility-module.h>

#include <ns3/lte-module.h>
```

2. Création de l'objet LteHelper :

```
Ptr<LteHelper>lteHelper = CreateObject<LteHelper> ();
```

Cela fournira les méthodes pour ajouter des eNB et des UE et les configurer

3. Création des nœuds pour les UEs et les eNBs :

On a créé quatre nœuds pour les eNBs (les points d'accès) et seize nœuds pour les UEs (User Equipement)

```
uint16_tnumberOfNodesENB = 4

uint16_tnumberOfNodesEU = 16;

NodeContainerenbNodes;

enbNodes.Create (numberOfNodesENB);

NodeContainerueNodes;

ueNodes.Create (numberOfNodesEU
```

4. Configuration le modèle de mobilité pour les nœuds d'utilisateurs(UE):

```
mobility.SetPositionAllocatorn("ns3::GridPositionAllocator","MinX",
DoubleValue (-900.0),
                    "MinY", DoubleValue (-850.0),
                    "DeltaX", DoubleValue (420.0),
                    "DeltaY", DoubleValue (150.0),
                    "GridWidth", UintegerValue (4),
                    "LayoutType", StringValue ("RowFirst"));
mobility.SetMobilityModel ("ns3::RandomWalk2dMobilityModel",
                    "Mode", StringValue ("Time"),
                    "Time", StringValue ("0.5s"),
"Speed",StringValue ("ns3::ConstantRandomVariable[Constant=50.0]"),
                    "Bounds", RectangleValue (Rectangle (-12000.0,
12000.0, -12000.0,   12000.0)));
```

5. Installation de la pile de protocole LTE sur les eNB :

```
NetDeviceContainerenbDevs;
enbDevs = lteHelper->InstallEnbDevice (enbNodes);
```

6. Installation de la pile de protocole LTE sur les UEs :

```
NetDeviceContainerueDevice
ueDevs = lteHelper->InstallUeDevice (ueNodes);
```

7. Attacher l'UE à l'eNB:

```
lteHelper->AttachToClosestEnb (ueDevs, enbDevs);
```

8. Activer un support radio de données entre chaque UE et eNB:

```
enumEpsBearer::Qci q = EpsBearer::GBR_CONV_VOICE;

EpsBearerbearer (q);

lteHelper->ActivateDataRadioBearer (ueDevs, bearer);
```

Pour compléter notre simulation, il est nécessaire d'ajouter des paramètres de configuration du modèle LTE

4.8 La configuration des paramètres du modèle LTE :

Tous les paramètres du modèle LTE pertinentes sont configurés et gérées par defaults par le système d'attribut NS-3.

Premièrement on met le code suivant dans la main () de programme de la simulation :

```
CommandLinecmd;

cmd.Parse (argc, argv);

ConfigStoreinputConfig;

inputConfig.ConfigureDefaults ();
```

Pour ajouter les paramètres, premièrement il faut créer un fichier .txt et le renommer par exemple les-paramètres.txt mettant les valeurs par defaults :

```
default ns3::LteHelper::Scheduler "ns3::PfFfMacScheduler"

default ns3::LteHelper::PathlossModel
"ns3::FriisSpectrumPropagationLossModel"

default ns3::LteEnbNetDevice::UlBandwidth "25"

default ns3::LteEnbNetDevice::DlBandwidth "25"

default ns3::LteEnbNetDevice::DlEarfcn "100"

default ns3::LteEnbNetDevice::UlEarfcn "18100"

default ns3::LteUePhy::TxPower "10"

default ns3::LteUePhy::NoiseFigure "9"

default ns3::LteEnbPhy::TxPower "30"

default ns3::LteEnbPhy::NoiseFigure "5"
```

4.9 L'exécution de la simulation

Pour exécuter le programme de la simulation on ouvre le terminal et on écrit la commande qui permettra d'exécuter notre simulation (voir ***Figure 4.6***)

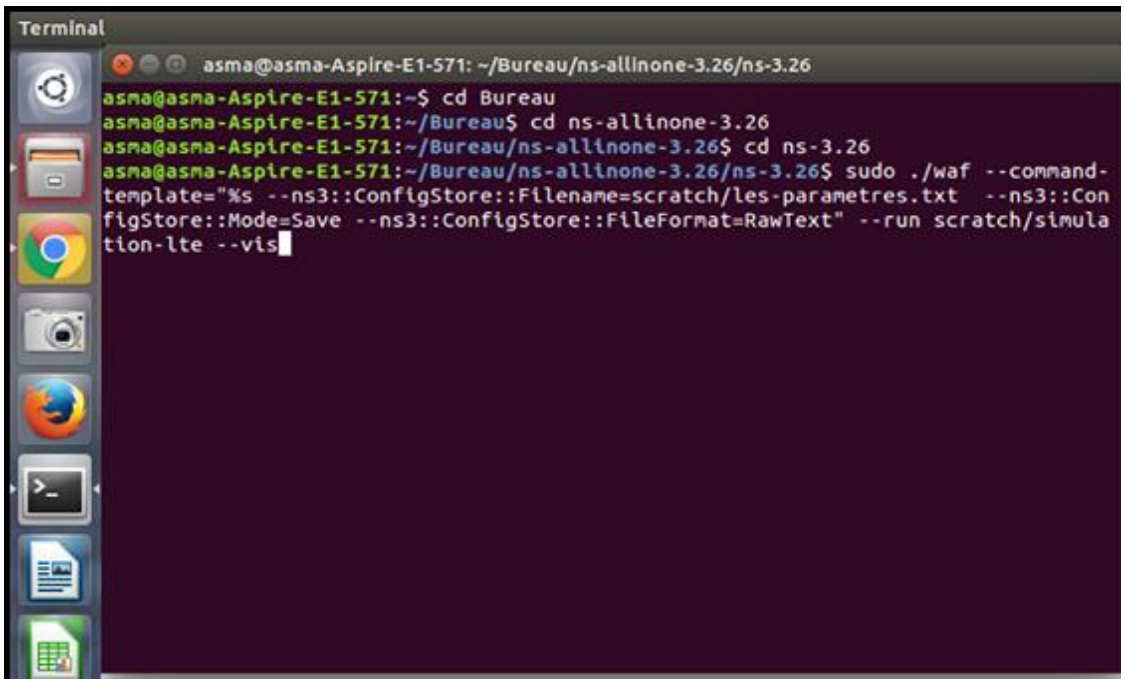


Figure 4.6 : *processus d'exécution de programme de la simulation*

Le résultat de ce processus est un affichage sur python qui montre la simulation du réseau LTE.

NS-3 PyViz (python visualiser) est un visualiseur de simulation en direct, Il contient une liste de nœuds et de canaux, une liste de flèches utilisées pour représenter les transmissions des paquets.

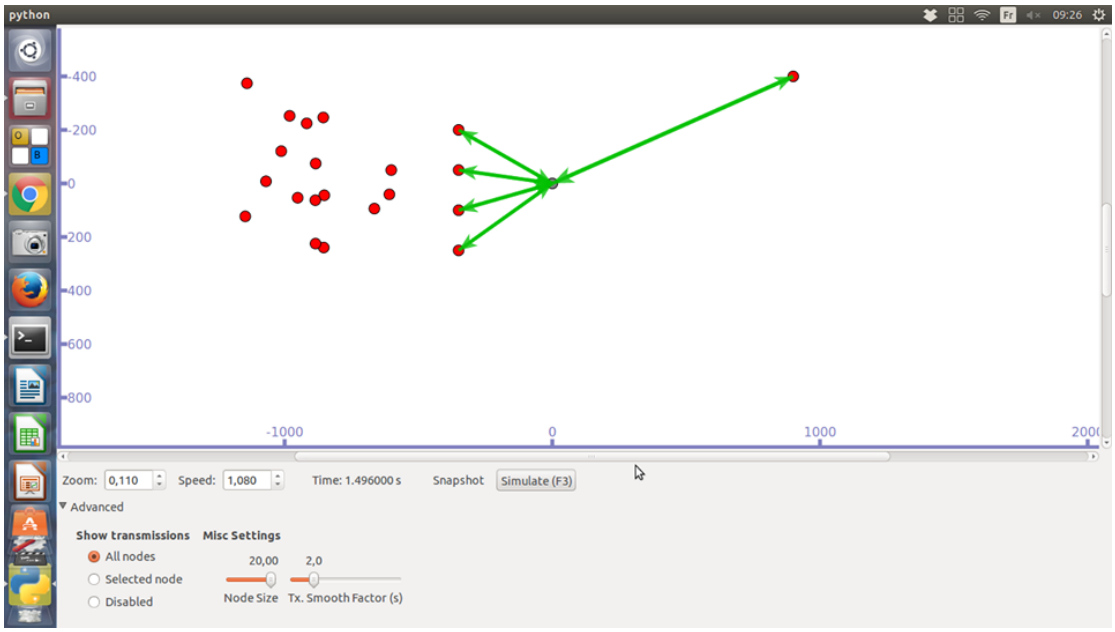


Figure 4.7 : *La simulation du LTE en python*

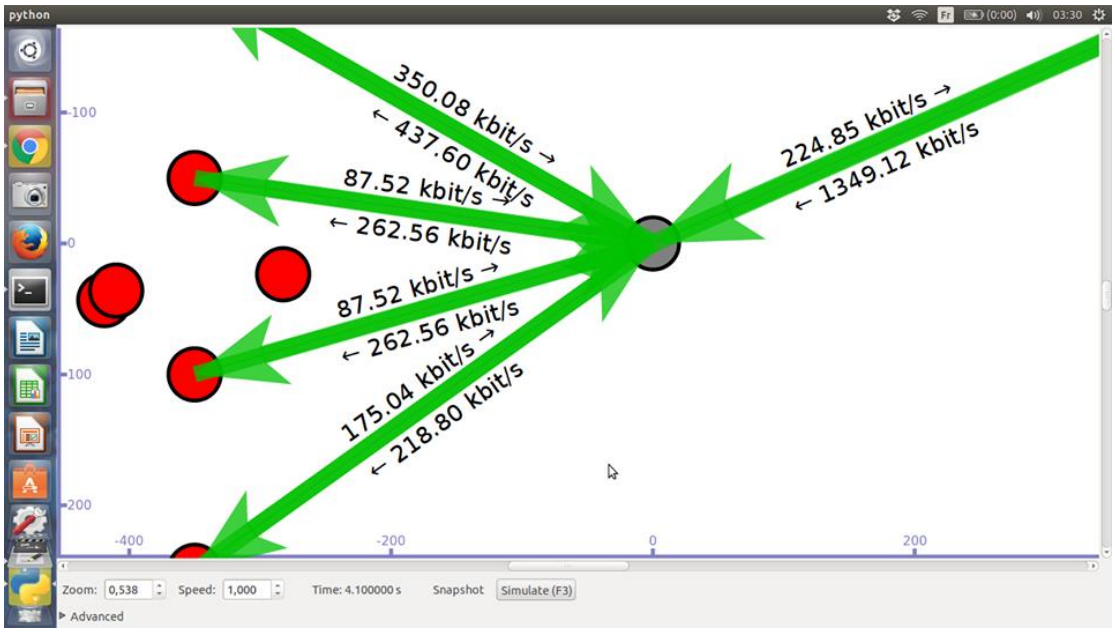


Figure 4.8 : *Les transmissions des paquets*

Après l'affichage de la simulation avec python, NS-3 crée automatiquement un fichier XML que l'on va ouvrir avec NetAnim pour voir notre simulation avec l'animateur :

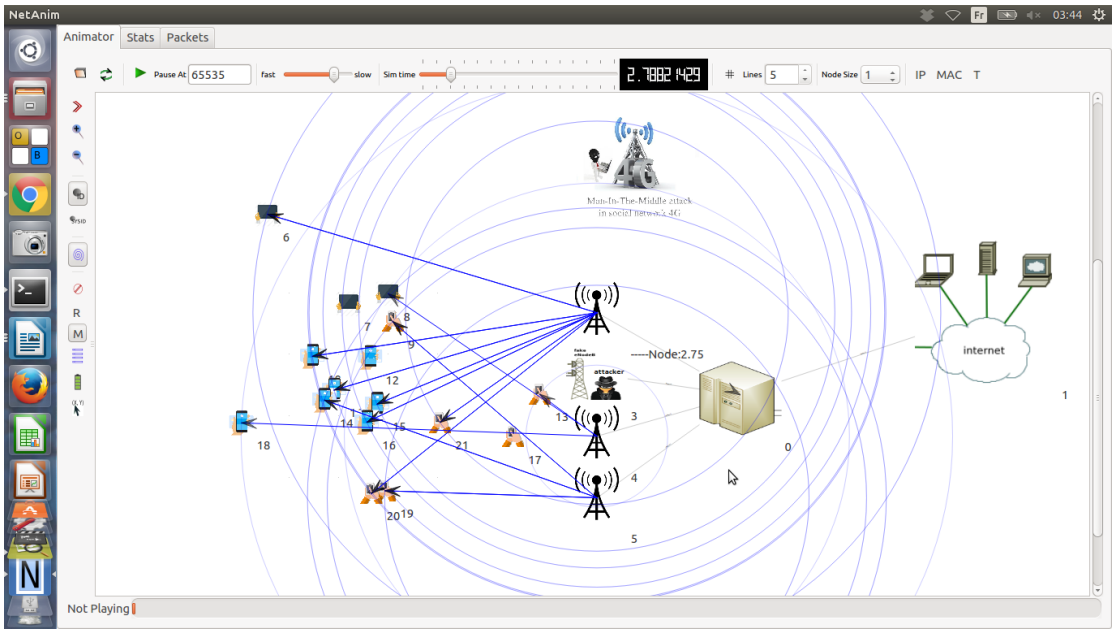


Figure 4.9 : *La simulation de réseaux LTE (4G)*

4.10 Simulation de l'attaque de l'homme du milieu dans les réseaux sociaux 4G

Dans le réseau LTE un attaquant crée une station de base malveillante (faux eNB),le virtuel eNB s'installe comme un vrais eNB et s'authentifie normalement par le cœur réseau (EPC), enfin il va jouer un rôle d' un vrais eNB, et l'attaquant obtient une position homme-dans-le-milieu(MITM) d'où il peut écouter des appels ou lire des SMS, ou forcer les téléphones vers des réseaux GSM 2G où seuls les services de données vocales et de base sont disponibles.

Les attaques fonctionnent à travers une série de messages envoyés entre les stations de base malveillantes générées par les attaquants et les téléphones ciblés.

Une fois qu'un téléphone cellulaire parcourt la zone de couverture de fausse station de base, son IMSI sera signalé à la fausse, et sera capté par l'attaquant (MITM).

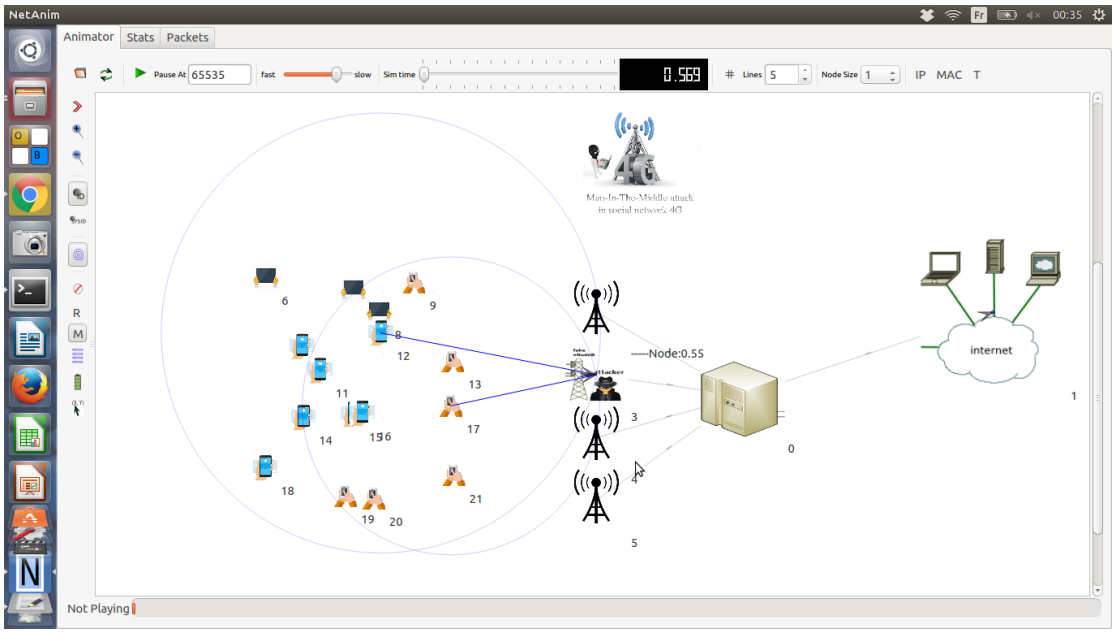


Figure 4.10 : *Redirection des UEs vers le faux eNB*

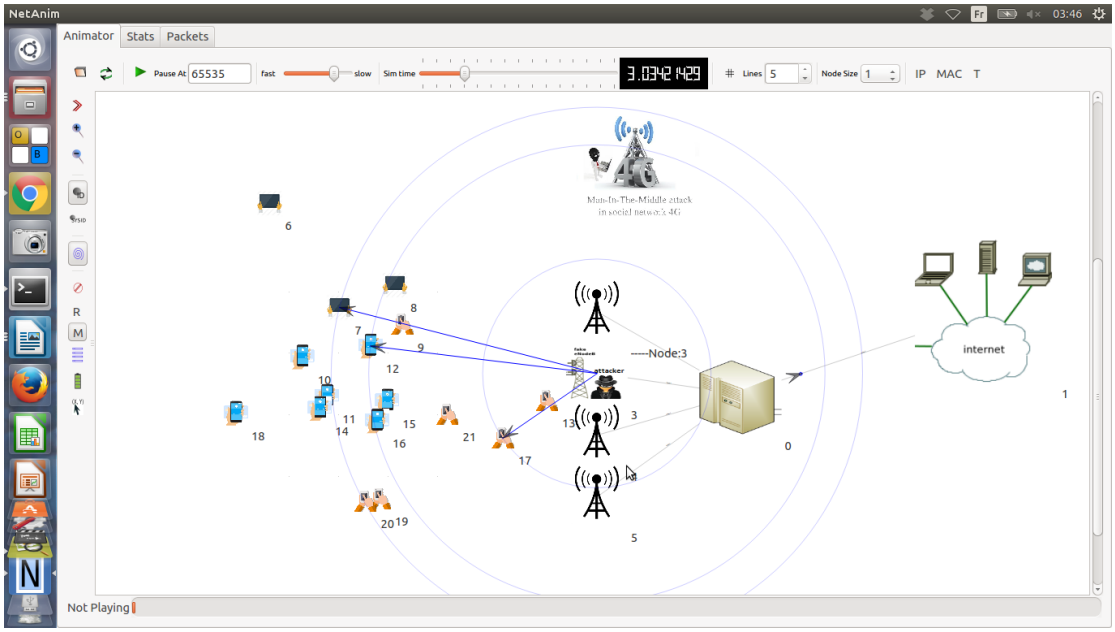


Figure 4.11 : *L'identification des victimes dans la fausse station de base crée par MITM*

Le NetAnim n'affiche pas seulement la simulation mais on peut aussi dessiner la trajectoire de chaque nœud pendant la simulation (voir Figure 12)

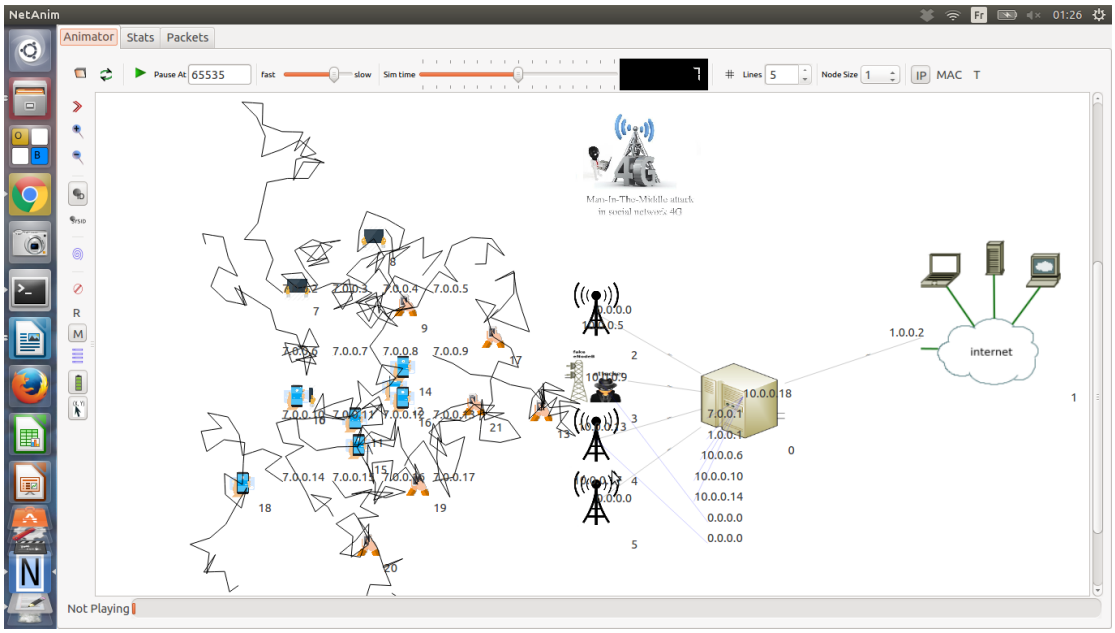


Figure 4.12 : *La trajectoire des nœuds (UEs)*

Aussi le NetAnim permet d'afficher les tables de routage de chaque nœud, comme le montre la Figure 13.

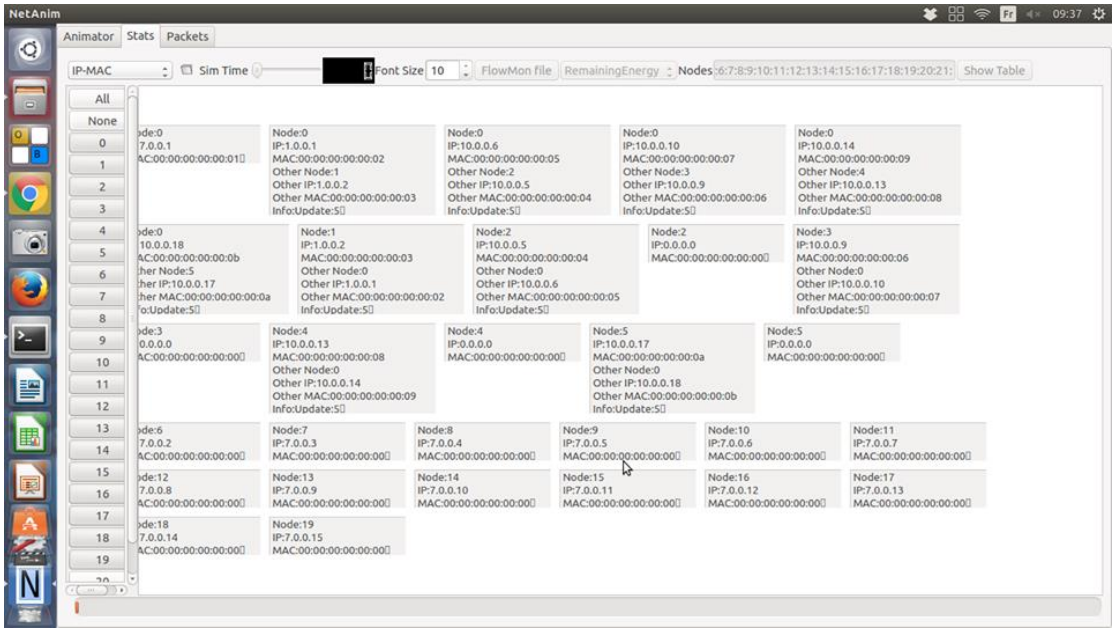


Figure 4.13 : *Table de routage des nœuds*

4.11 Paramètres de QoS (qualité de service)

Le simulateur NS-3 permet de tester quelques paramètres de qualité de service (SINR, CQI), ce sont des paramètres définis par la norme LTE pour mesurer la qualité de transmission en liaison montante (uplink) et descendante (downlink).

4.11.1 SINR (le rapport signal sur bruit)

Le SINR (Signal-to-noise ratio) est une mesure de la qualité du signal, utilisé beaucoup par les opérateurs, et l'industrie LTE en général, les UE utilisent généralement SINR pour calculer le CQI (Channel Quality Indicator) qu'ils signalent au réseau.

4.11.2 CQI (**Indicateur de qualité des canaux)**

Comme son nom l'indique, il s'agit d'un indicateur portant l'information sur la qualité de la chaîne de communication, il est reçu par l'UE, alors que ce dernier le renvoi à l'eNodeB pour savoir s.il doit l'augmenter pour avoir en final une bonne communication.

4.12 Résultats de simulation

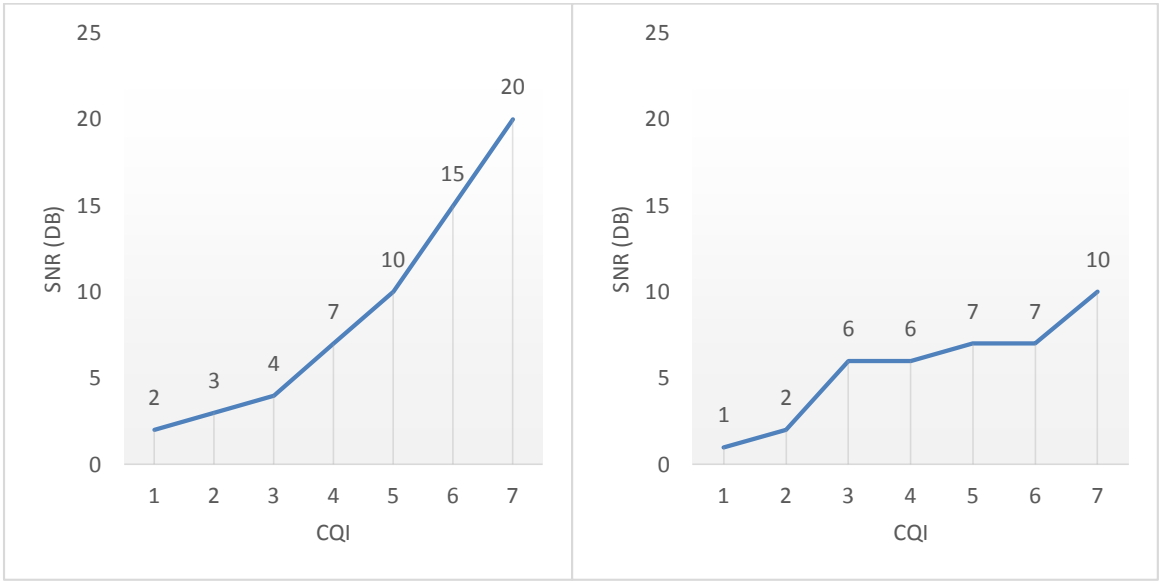
Nous avons testé les paramètres SINR et QCI pour mesurer les performances de réseau 4G avant et après l'attaque ***MITM*** grâce au simulateur NS-3

Figure Cartographie mesurée du SNR-CQI rapportées à l'eNodeB,

A) *Avant l'attaque MITM*

B) *Après l'attaque MITM*

$$SNR\ (décibel\ (dB)) = \frac{Puissance\ d'un\ signal}{Puissance\ du\ bruit\ de\ fond}$$



A) Avant l'attaque MITM *B) Après l'attaque MITM*

La figure présente une cartographie mesurée du SNR-CQI (Signal-to-noise ratio - Channel Quality-Indicator) avant et après l'attaque HDM. A travers cette figure, on remarque clairement qu'avant l'attaque HDM, plus l'un indicateur de la qualité de la transmission d'une information (SNR) est augmenté, plus qu'on aura une meilleure qualité de l'onde radio des téléphones mobiles dans le réseau LTE.

Après l'attaque MITM, nous remarquons l'effet des attaquants par la diminution de la qualité de l'onde radio.

4.13 Conclusion

Dans ce chapitre, nous avons présenté le simulateur Ns-3 avec les étapes d'installation proposé par la communauté Lena. Ensuite, nous avons simulé le réseau LTE et l'attaque de l'homme du milieu dans les réseaux sociaux 4G faite par la création d'une fausse station de base eNB où l'attaquant peut intercepter, écouter et modifier la communication entre les utilisateurs sur le réseau.

En fin, nous avons testé les paramètres SINR et QCI pour mesurer les performances de réseau LTE avant et après l'attaque MITM.

Chapitre 5 : Rapport de stage fait au sein de l'entreprise Algérie Telecom

5.1 Présentation du groupe Algérie Telecom

5.1Présentation de l'entreprise

Algérie Telecom est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques. Sa naissance a été consacrée par la loi 2000/03 du 5 août 2000, relative à la restructuration du secteur des Postes et Télécommunications, qui sépare notamment les activités Postales de celles des Télécommunications donc c'est le leader sur le marché Algérien des télécommunications qui connait une forte croissance. Offrant une gamme complète de services de voix et de données aux clients résidentiels et professionnels. Cette position s'est construite par une politique d'innovation forte adaptée aux attentes des clients et orientée vers les nouveaux usages. **[21]**

5.2 Les objectifs

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs :

- Rentabilité
- Efficacité
- Qualité de service.

Son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel.

Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie. **[21]**

5.1.3 Les activités

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles…
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications ;
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

ALGERIE TELECOM est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales ;
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications ;
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.**[22]**

5.3 Le fonctionnement des réseaux 4G LTE

Les étapes de fonctionnement :

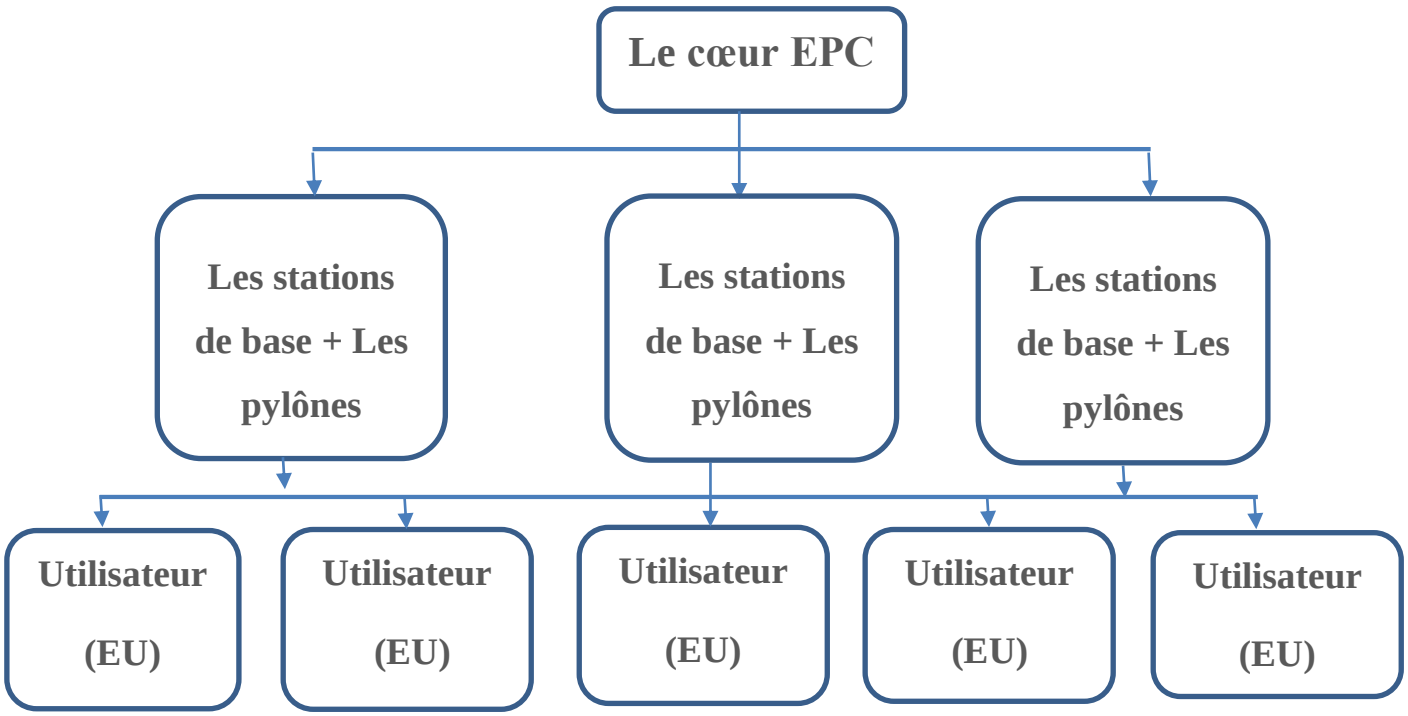


Figure 5.1 : *Architecture du fonctionnement des réseaux LTE*

- **Utilisateur (Equipment User) :** c'est toute equipment permet à acéder au réseau.
- **Le cœur EPC (Evolved PacketCore) :** Se compose de certains nœuds de contrôle-avion, appelé Entité de gestion de mobilité (Mobility Management Entity (***MME***)), contrôle du serveur d'abonné domestique (Home Subscriber Server ***(HSS)***) et deux nœuds de plan utilisateur, appelés Gateway de service (S-GW) et Gateway de réseau de paquets-données (Packet-data Network Gateway (P-GW)). Le cœur EPC Principal qui distribue vers tout l'Algérie se situe à Alger,
- **Les pylônes (Antennes) :** On voit l'antenne n'est pas tout, mais aussi contient une **station de base**. On savait que l'architecture des réseaux 4G est pyramide ; alors, le pylône principale de Guelma (***Figure 5.1***) reçoit le signale arrivé du cœur secondaire qui se trouve à Constantine (qui le reçoit lui-même d'Alger ***(le cœur principale)***) à partir les ***RRU***[1] (Remote Radio Unit) et le partage vers les **pylônnets**[2] ***(Figure 5.3)*** comme illustre l'architecture dans ***Figure 5.2***.

Figure 5.2 : *Le pylône principale de Guelma "Maouna".*

[1] *Convertir* un *signal* analogique en *signal numérique*
[2] Des petits pylône

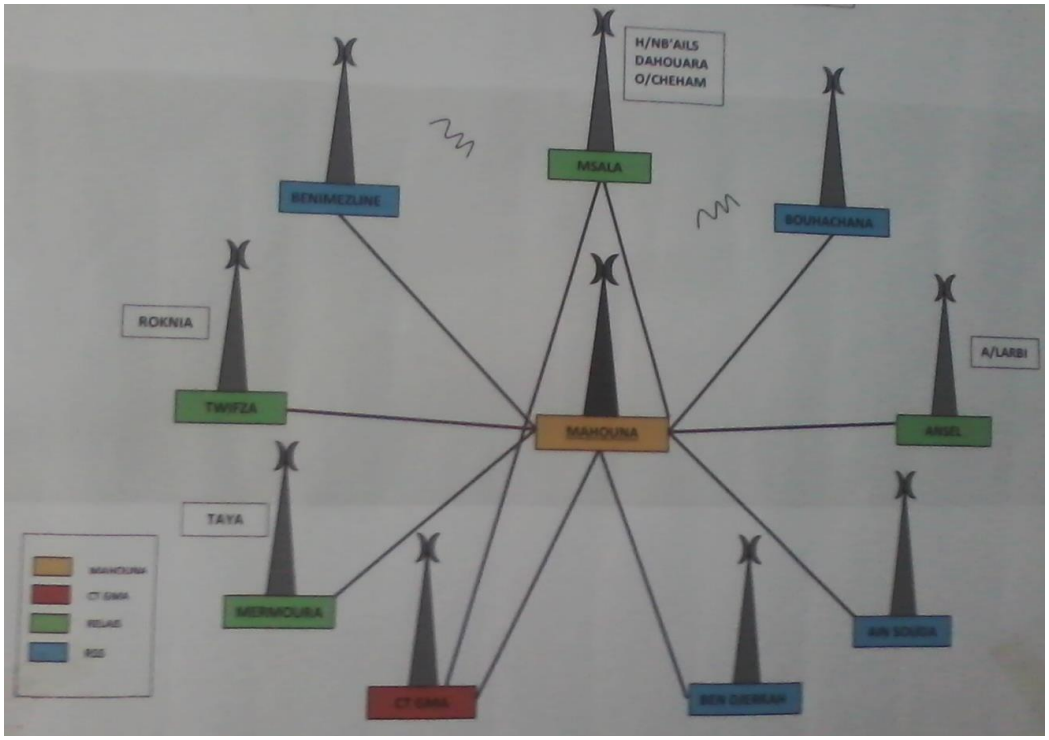


Figure 5.3: *Schéma des laisons FHN MAOUNA.*

Figure 5.4 : *Pylône de Boumahra.*

Donc, les stations de base travaillent dans un equipement appele eNodeB:

1) couvre un territoire restreint (i.e. une cellule), de quelques centaines de mètres à quelques dizaines de kilomètres (à l'avenir, quelques dizaines de mètres)

2) gère la transmission et la réception du signal suivant des formats et un protocole spécifique à chaque génération (2G, 3G, 4G).

3) contient les algorithmes d'allocation de la ressource radio et gère les messages associés (exemple, allocation d'une fréquence et d'un intervalle de temps)**.**

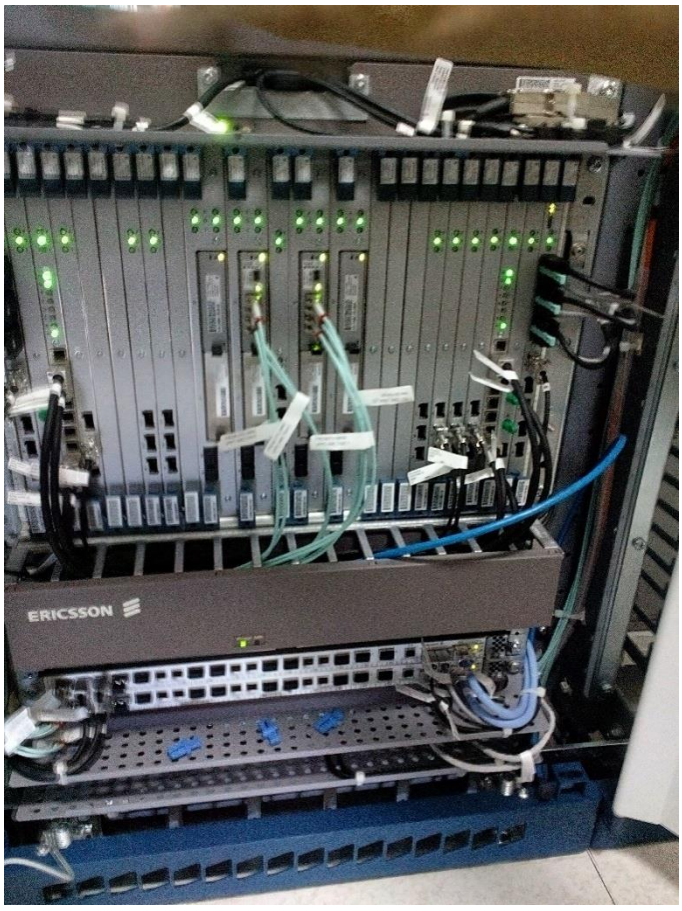


Figure 5.5 : *Relation des cités par un câble avec un grand-switcher.*

Figure 5.6 : *Pylône Guelma centre-ville.*

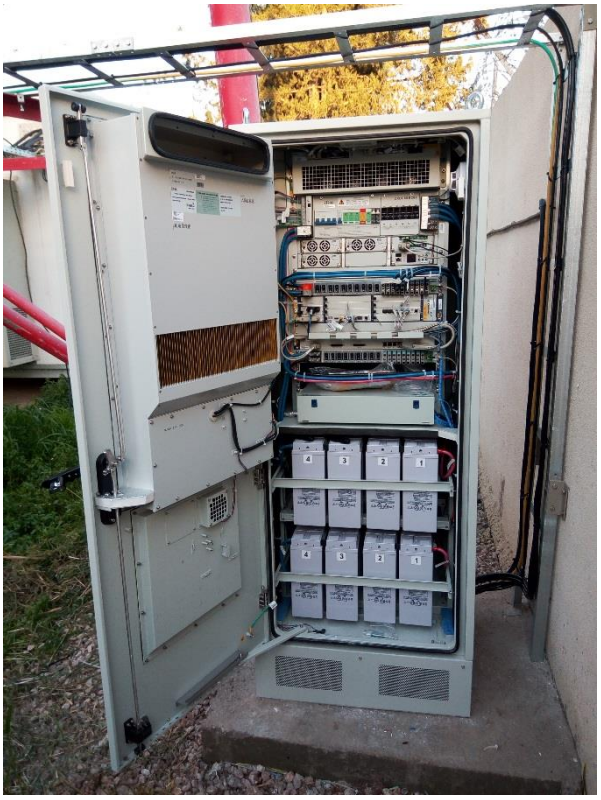


Figure 5.7 : *Configuration du pylône Guelma centre-ville pour être compatible avec la 4G.*

5.3 Les attaques qui peuvent menacer les systèmes d'entreprise :

Un employé non satisfait de l'entreprise sait vraiment comment le système travaille donc connait leur failles ce qu'il lui permet des faire des attaques peut être causées des problèmes techniques et peut être pas selon le but de pirate, donc ce dernier peut :

- ✓ Injecte une fibre et fait des boucles infinis de saturation.
- ✓ Débrancher un câble quelconque tous simplement.

Dans ce cas-là on parle sur une attaque d'un vrai homme du milieu (MITM).

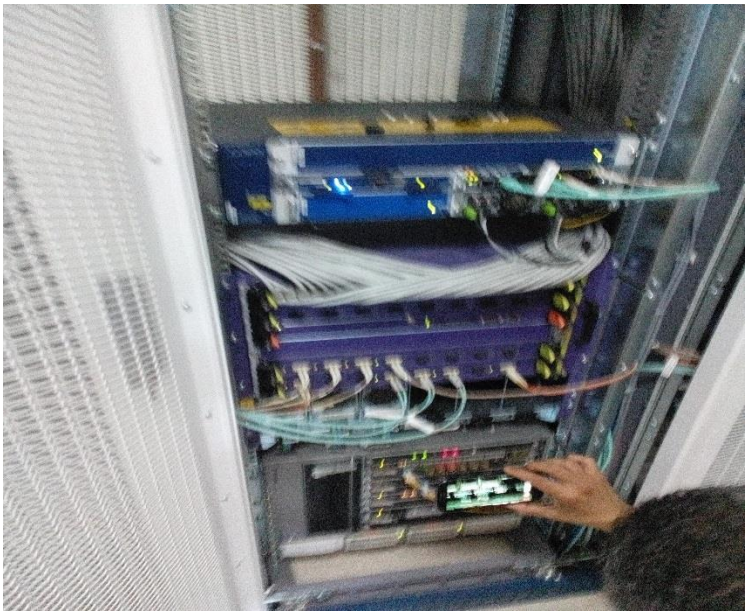


Figure 5.8 : *Un vrai homme de milieu fait une coupure.*

- ✓ Créer une fausse station de base et mis en réseau et faire ; 'écouter, saisir des donnés ou les modifier …….etc.

5.4 Conclusion

Dans ce rapport, nous avons présenté le groupe d'Algérie télécom : l'entreprise, ses activités et ses objectifs, puis on a illustré un schéma indique le fonctionnement des réseaux 4G depuis le EPC jusqu'au utilisateur passant par la station de base, ainsi qu'on l'a accompagné avec des photos prises au seine de notre stage en Algérie télécom interne (au sein de l'entreprise) ou externe s'il y'a des missions dehors.

Conclusion générale

Durant ce travail, après les analyses de recherche, on trouvé que les réseaux sans fil cellulaires de la quatrième génération (4G) ou Long Terme Evolution (LTE) sont déployés actuellement à travers le monde pour garantir une meilleure performance en particulier les Qualités de Services afin d'apporter de nouvelles applications, de nouveaux services, ainsi qu'une meilleure gestion.

Ces réseaux 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 peut permettre des attaques sur les réseaux de cette nouvelle génération 4G qui touche la confidentialité, l'authentification, l'intégrité, à travers les attaques réseaux, comme l'attaque MITM.

On a proposé un schéma de détection de l'attaque MITM dans les réseaux sociaux de la quatrième génération. Notre schéma se base sur la technique de cryptographie à courbe elliptique.

Finalement, on a conclu notre travaille par l'implémentation du protocole proposé utilisant le simulateur réseau NS-3.

[1] Hwang, Y. et Park, A. (2008). "Vertical handover platform over applying the open API for WLAN and 3G LTE systems". VehicularTechnologyConference, 2008. VTC 2008-Fall. IEEE 68th. IEEE/Date de consultation décembre 2016.

[2] https://www.cs.ucsb.edu/~mturk/Courses/CS290I-2012/misc/4GEngrMarketing.pdf Date de consultation Décembre 2016

[3] 3GPP TR 23.882 V8.0.0, 3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 8), Décembre 2008.pdf

[4] http://www.efort.com/r_tutoriels/LTE_SAE_EFORT.pdf

[5] Bechini.T , « Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération », Thèse de doctorat, Université e Toulouse,10/06/2010.

[6] Couzinet.H, Nanfack.J et Njoudji.R, « Analyse et suivi de la QoS dans le système LTE », Rapport de Stage, Université Telecom Bretagne, 2009.

[7] http://4glte.over-blog.com/page/2 / Date de consultation janvier 2017

[8] http://www.etsi.org/deliver/etsi_ts/133400_99/133401/10.03.00_60/ts_133401v100300p.pdf

[9] Mavoungou.S , Kaddoum.G, Member, IEEE, MostafaTaha, Member, IEEE, and Georges Matar , Survey on Threats and Attacks on Mobile Networks , DOI 10.1109/ACCESS.2016

[10] Kasmi.C et Benjamin.M, État des lieux de la sécurité des communications cellulaires,ANSSI 51 bd.de la Tour Maubourg 75700 Paris Cedex 07 France

[11] Jin Cao, Maode Ma, Senior Member, IEEE Hui Li, Member, IEEE, Yueyu Zhang, and ZhenxingLuo, A Survey on Security Aspects for LTE and LTE-A Networks,IEEE Com- munications Surveys Tutorials, Vol. 16, No. 1, First Quarter 2014

[12] https://www.malekal.com/man-in-the-middle/ , cours Attaque Man in the Middle (MITM), dernière consultation Mars 2017.

[13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, « A Survey of Man In The Middle Attacks », IEEE communication surveys & tutorials, Citation information: DOI 10.1109/COMST.

[14] Z. Chen, S. Guo, K. Zheng, and Y. Yang, "Modeling of man-in-themiddle attack in the wireless networks," in Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2255–2258.

[15] M.Bensari, 'Sécurité des échanges dans un réseau de nœuds mobiles', Mémoire de magitere , Université El Hadj LAKHDER – BATNA ; 2012 .

[16] Cour openclassrooms & quot; Protégez l'ensemble de vos données sur votre ordinateur & quot;, dernière consultation 29/05/2017, https://openclassrooms.com.

[17] TutorialPoint, « cryptography course », https://www.tutorialspoint.com, dernière consultation 29/05/2017.

[18] J.Pagé, Mécanismes de sécurité dans la signalisation des réseaux IMS 4G (2012–2013), Mémoire de Master en Sciences Informatiques, Université libre de Bruxelles

[19] https://www.nsnam.org/wiki/Installation, Date de la dernière consultation février 2017.

[20] https://www.nsnam.org/wiki/NetAnim, Date de de la dernière consultation février 2017.

[21] le site officiel d'Algérie Télécom, https://www.algerietelecom.dz . , la dernière consultation le 29/5/2017