Déploiement et configuration d'une architecture matérielle de capture et d'analyse de la signalisation des réseaux cellulaires pour la détection des fraudes à la SIMBox

Cliton Stephane Nyobe

Université de Yaoundé 1
****
Ecole Nationale Supérieure Polytechnique de Yaoundé
****
Département des Génies Électrique et des Télécommunications
****

University of Yaoundé 1
****
National Advanced School of Engineering of Yaoundé
****
Department of Electrical and Telecommunications Engineering
****

DÉPLOIEMENT ET CONFIGURATION D'UNE ARCHITECTURE MATÉRIELLE DE CAPTURE ET D'ANALYSE DE LA SIGNALISATION DES RESEAUX CELLULAIRES POUR LA DETECTION DES FRAUDES A LA SIMBOX.

MÉMOIRE DE FIN D'ETUDES

PRÉSENTÉ ET SOUTENU PAR :
NYOBE CLITON STEPHANE

EN VUE DE L'OBTENTION DU :
DIPLOME D'INGENIEUR DE CONCEPTION EN TELECOMMUNICATIONS

SOUS LA DIRECTION DE :
LELE CHRISLIN MARTIAL, Chargé de cours, ENSPY

DEVANT LE JURY COMPOSÉ DE :

PRÉSIDENT : **NGOHE-EKAM PAUL SALOMON, MAÎTRE DE CONFÉRENCES, UY1**

RAPPORTEUR : **LELE CHRISLIN MARTIAL, CHARGÉ DE COURS, UY1**

EXAMINATEUR : **BINELE ALPHONSE, CHARGÉ DE COURS, UY1**

INVITÉ : **TCHANA ALAIN, PROFESSEUR, ENS LYON**

INVITÉ: **ALINE CARNEIRO VIANA, HDR, INRIA**

INVITÉ : **KOUAM ANNE JOSIANE, DOCTORANTE, INRIA**

ANNEE ACADÉMIQUE : 2020-2021

Date de soutenance : 29/09/2021

DÉDICACE

A LA FAMILLE NYOBE

REMERCIEMENTS

- A **JESUS-CHRIST** le Dieu Tout Puissant sans qui rien n'est possible ;
- Au **Professeur NGOHE EKAM Paul Salomon**, pour l'immense honneur qu'il nous fait de présider ce jury ;
- Au **Docteur LELE Chrislin Martial**, mon encadreur académique et enseignant pour sa disponibilité, sa rigueur et son engagement dans notre formation ;
- Au **Docteur BINELE Alphonse** pour le temps précieux à moi accordé pour avoir examiné ce travail ;
- A la **Direction de l'INRIA Saclay** pour m'avoir accordé ce stage ;
- A mon encadreur professionnel, le **Professeur TCHANA Alain,** pour ses consignes, ses conseils et la confiance qu'il m'a accordée ;
- A **Aline CARNEIRO VIANA** pour son encadrement, sa disponibilité inconditionnelle et ses conseils inestimables ;
- A **l'Ingénieur KOUAM Josiane**, de la promotion 2019 de l'ENSPY auprès de qui j'ai travaillé et énormément appris ;
- A tout le personnel du centre INRIA Saclay pour nous avoir accueilli spécialement M**esdames Laurence FONTANA, Valérie BERTHOU et Monsieur GOMIS ;**
- A tous les **membres de l'équipe TRIBE** qui ont rendu mon apprentissage plus riche ;
- Au **corps professoral de l'Ecole Nationale Supérieure Polytechnique**, pour toutes les connaissances transmises durant toutes ces années et en particulier au **Professeur TONYE Emmanuel** et au **Professeur NDZANA Benoit** ;
- A **mes parents NYOBE Charles Ernest et NYOBE Victorine** pour leur immense soutien dans tous les aspects de ma vie ;
- A **mes frères et sœurs LIPOT Andrienne, BATOCK Charles, MBOCK NYOBE Nicolas et NYOBE Thérèse Esther** pour leur amour et soutien inconditionnels ;
- A **MVONGO ESSENGUE Philibert Lionel** qui m'a accompagné, conseillé et aidé pendant tout mon séjour en France ;

- A **mes camarades du Génie Electrique et Télécommunications ayant** contribué de près ou de loin à ma réussite en particulier NKUH **Rholy, KAMGAING Steve, ADAMOU MASSAMA, ABESSO Kevy, NGWASIRI Carlson, KETCHEMEN Armel, EKASSI Anicet, EMINE II, TAMWA Daniel, TSANGA Emmanuel, ASSOUALA Gérard, TATAH Noel, NLEMBA Cécile, NGANE Noelle, MARYLYNE ENONCHONG, TCHUISSEU Leslie, BISI FLORA, NDONGO Sonia, DIKWELE, KOUWOS, MOUGNOL BOL Alima, SAGOU Djunis, TCHAPO Jean Roger, MANGA Yvan, NKANA Yvan, NGUEGUIM Auriol, TEJIONA, KAMGNO, M.MBANGA, EYOMANE Audrey, ABOUBAKAR** et tous ceux que je ne peux mentionner**;**
- A mes **amis de tous horizons** toujours présents **NSATA Ange, MACHE Kevin, MBOKE Kevin, EPIE Kingsley, NFORMI Kingsley, KUETE Berry, DJOMO Eddy, WAFO Jerry, Menehould LAVAL-JEANTET ;**
- A mes ainés les ingénieurs **SEPPE Lionel**, **OTTOU Abed**, N**GNADOU Leticia, ABOUBAKAR ISSIAKOU, CHUISSEU Francelle, BANG Florent, LYEB Harry** ;
- A mes camarades de promotion **ONANA MOUTASSI Christian, TEGUIA Brice, FANDIO Esdras, MAMOUDOU, MUKAM Augusta, TITA DOH, NGUIFFO Samuel** et tous les autres**.**

LISTE DES ACRONYMES

3GPP: Third Generation Partnership Project

A

ACD: Average Call Duration

AM: Acknowledged Mode

ANN: Artificial Neural Network

APN: Access Point Name

ART : Agence de Régulation des Télécommunications

AS: Access Stratum

ASN.1: Abstract Syntax Notation One

ASR: Answer Seizure Ratio

AuC: Authentication Center

B

BSS: Base Station Subsystem

C

CDMA : Code Division Multiple Access

CFCA: Communications Fraud Control Association

CDR: Call Detail Records

CN: Core Network

CS: Circuit Switched

D

DC-HSPA: Dual Carrier- High Speed Packet Access

DN: Data Network

E

EIR: Equipment Identity Register

EPC: Evolved Packet Core

ETSI: European Telecommunications Standards Institute

E-UTRAN: Enhanced Universal Terrestrial Radio Access Network

F

FDMA: Frequency Division Multiplexing Access

FDD: Frequency Division Duplexing

FEC: Forward Error Correction

FMS: Fraud Management System

G

GoIP: GSM over IP

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

GTP: GPRS Tunneling Protocol

GUTI: Globally Unique Temporary Identifier

H

HARQ: Hybrid Automatic Repeat reQuest

HBS: Human Behaviour Simulation

HSS: Home Subscriber Server

HTTP: Hyper Text Transfer Protocol

I

IEEE: Institute of Electrical and Electronics Engineers

IMEI: International Mobile Equipment Identity

IMSI: International Subscriber Identity

IMT: International Mobile Telecommunications

IP: Internet Protocol

ISDN: Integrated Services Digital Network

ITR: International Termination Rate

J

JSON : JavaScript Object Notation

L

LAN: Local Access Network

LLC: Logical Link Control

LTE: Long Term Evolution

LTE-A: Long Term Evolution- Advanced

LTR: Local Termination Rate

M

MAP: Mobile Application Part

ME: Mobile Equipment

MIMO: Multiple Input Multiple Output

MME: Mobility Management Equipment

MMTC: Massive Machine Type Communications

MNO: Mobile Network Operator

MT : Mobile Termination

N

NAS : Non-Access Stratum

NAT : Network Address Translation

NSS: Network and Switching Subsystem

O

OFDMA: Orthogonal Frequency Division Multiplexing

OSI: Open Systems Interconnection

OTT: Over The Top

P

PBX: Private Branch Exchange

PCF: Policy Control Function

PCRF: Policy Charging and Rules Functions

PDCP: Packet Data Convergence Protocol

PDN: Packet Data Network

PDU: Protocol Data Unit

PGW: PDN Gateway

PLCP: Physical Layer Convergence Procedure

PS: Packet Switched

Q

QoS: Quality of Service

R

RAN: Radio Access Network

RB: Resource Block

RLC: Radio Link Control

RNIS: Réseau Numérique à Intégration de Services

RRC: Radio Resource Control

RTP: Real Time Protocol

RoHC: Robust Header Compression

RSSI: Received Signal Strength Indicator

S

SC-FDMA: Single Carrier-Frequency Division Multiplexing

SDR: Software Defined Radio

SDU: Service Data Unit

SIM: Subscriber Identity Module

SIP: Session Initiation Protocol

SINR: Signal Noise to Ratio

SGW: Serving Gateway

SVM : Support Vector Machine

T

TA: Tracking Area

TAC: Type Allocation Code

TCG: Test Call Generators

TCP: Transmission Control Protocol

TDMA: Time Division Multiplexing Access

TE: Terminal Equipment

TM: Transparent Mode

U

UDP: User Datagram Protocol

UE: User Equipment

UICC : Universal Integrated Circuit Card

UIT : Union Internationale des Télécommunications

UM: Unacknowledged Mode

UMTS: Universal Mobile Telecommunications System

URI: Uniform Resource Identifier

USD: US Dollar

USSD: Unstructured Supplementary Service Data

UTRAN: Universal Terrestrial Radio Access Network

V

VoIP: Voice Over IP

W

WCDMA : Wideband Code Division Multiple Access

RÉSUMÉ

Le recours à la technologie pour commettre de la fraude n'est pas une nouveauté et les réseaux cellulaires, constituent depuis des décennies une des principales cibles de plusieurs méthodes de fraude. Méthodes qui grâce à l'évolution d'internet et des techniques d'automatisation, ont gagné en éfficacité, réduisant de la même manière la détectabilité des fraudeurs et par ricochet augmentant le nombre de fraudeurs. Ces attaques constituent un véritable problème pour les opérateurs de télécommunications et leur coûtent environ 28,3 milliards USD par an, comme l'indique la Communications Fraud Control Association en 2019. La fraude à la SIMBox consiste à détourner des appels internationaux sur le réseau VoIP et à les faire aboutir en tant qu'appels locaux à l'aide d'un dispositif, communiquant avec le réseau mobile. Les méthodes de détection de la SIMBox sont assez peu nombreuses. La plupart sont basées sur les comportoments anormaux d'utilisateurs dans le réseau mobile. Ces méthodes deviennent de moins en moins éfficaces, avec l'évolution de la SIMBox qui permet de simuler le comportement humain de façon automatique. D'où l'intérêt du developpement d'une méthode de détection inaltérable par les fraudeurs. Dans cette optique, nous avons ainsi d'une part déployé et configuré des architectures de SIMBox dans un écosystème de réseau 4G, et d'autre part nous avons analysé la signalisation correspondante au niveau de la station de base afin de faire ressortir un critère de classification, permettant d'identifier les cas de SIMBox parmi terminaux réguliers. Les expérimentations que nous avons menées nous ont permi d'observer que la latence engrendrée par la signalisation pendant la procédure d'attachement au réseau 4G était beaucoup plus élévée dans le cas de la SIMBox. Cela constituant ainsi un moyen éfficace de détecter la SIMBox avant que toute fraude ne puisse être éffectuée.

Mots clés : Fraude à la SIMBox, Signalisation, Réseaux mobiles, LTE

ABSTRACT

The use of technology to commit fraud is not new and cellular networks have been one of the main targets of various fraud methods for decades. These methods, due to the evolution of the Internet and automation techniques, have become more efficient, decreasing the detectability of fraudsters and in the same way increasing their number. These attacks are a real problem for telecom operators, costing them approximately 28.3 billion USD per year, as indicated by the Communications Fraud Control Association in 2019. SIMBox fraud involves diverting international calls over the VoIP network and terminating them as local calls using a device or a set of devices, communicating with the mobile network. The SIMBox detection methods are quite few. Most of them are based on the abnormal behavior of users in the mobile network. These methods are becoming less and less efficient, with the evolution of the SIMBox which allows to simulate human behavior automatically. This is why it is important to develop a detection method that is unalterable by fraudsters. In this perspective, we have deployed and configured SIMBox architectures in a 4G network ecosystem, and we have analyzed the corresponding signaling at the base station level in order to bring out a classification criterion, allowing to identify SIMBox cases among regular terminals. The experiments we have conducted have allowed us to observe that the latency generated by the signaling during the attachment procedure to the 4G network was much higher in the case of the SIMBox. This is an efficient way to detect the SIMBox before any fraud can be performed.

Key Words: SIMBox fraud, Signaling, Cellular networks, LTE

TABLE DES FIGURES

LISTE DES TABLEAUX

TABLE DES MATIÈRES

INTRODUCTION GÉNÉRALE

La téléphonie mobile est un secteur d'activité qui représente aujourd'hui une très grande source de revenus aussi bien pour les opérateurs de télécommunications que pour les équipementiers. En 2018 les technologies et services mobiles ont généré plus de 144 milliards de Dollars USD en Afrique subsaharienne soit 8.6% du PIB (Produit Intérieur Brut) de cette région [1]. Dans bien des pays africains en général et au Cameroun en particulier, il devient de plus en plus utilisé pour des applications et services divers. Ce secteur florissant est sujet à de nombreuses fraudes, engendrant d'énormes pertes pour les opérateurs en Afrique et dans le monde. Selon le CFCA (Communications Fraud Control Association), la perte totale due à la fraude dans les réseaux cellulaires est estimée à 28.3 milliards de dollars USD en 2019 [2]. Dans ce contexte, la terminaison illégale d'appels, également connue sous le nom de fraude à la SIMBox, est de loin l'une des fraudes les plus répandues affectant le marché des télécommunications [3]. Dans de nombreux pays, le tarif de terminaison d'appel international ou International Termination Rate (ITR) est considérablement plus élevé que le tarif de terminaison d'appel local, Local Termination (LTR) à l'intérieur d'un pays (par exemple, jusqu'à 2,8 fois de différence au Cameroun [4]). Il est donc rentable pour les fraudeurs de contourner l'opérateur d'interconnexion régulier lorsqu'ils terminent des appels dans le pays cible, car ils peuvent payer le tarif local plus faible plutôt que l'ITR. La fraude à la SIMBox est un problème majeur dans les pays en voie de développement et dans le cas d'espèce du Cameroun en 2015, des pertes s'élevant à 39,9 millions de dollars USD [5]. De nombreux facteurs favorisent cette fraude, autant dans la règlementation, sur le plan humain, que sur le plan technique. Tout ceci fait que la fraude SIMBox se situe dans le top trois des types de fraudes de système téléphonique qui causent une perte importante pour les opérateurs de réseaux mobiles [6]. Les techniques de détection sont assez peu nombreuses, classifiées en méthodes actives et passives selon le degré d'implication humaine dans le processus. Parmi ces méthodes, nous nous sommes intéressés à une méthode récente pas encore explorée [7] qui suggère une analyse de la signalisation du réseau cellulaire afin de reconnaitre la SIMBox. C'est dans cette optique que nous avons observé la latence de communication de la SIMBox, dans un réseau LTE pour

la comparer avec celle de terminaux ordinaires, dans le but d'établir un critère de détection, partant du principe que chaque communication IP entre équipements de la SIMBox s'ajouterait à la latence observée du point de vue LTE. Ainsi dans ce mémoire de fin d'études il s'agira pour nous de traiter du sujet suivant : « **Déploiement et configuration d'une architecture matérielle de capture et d'analyse de la signalisation des réseaux cellulaires pour la détection des fraudes a la SIMBox**. ». Afin d'y parvenir, notre travail s'est articulé autour des trois chapitres suivants :

- Chapitre 1 : Contexte et Problématique : qui nous permettra d'appréhender le cadre dans lequel notre travail est effectué, de présenter les notions qui seront utilisées et par la suite poser le problème auquel répond notre projet de fin d'études ;
- Chapitre 2 : Méthodologie : nous présenterons les solutions existantes permettant de résoudre ce problème et nous expliquerons par la suite la démarche méthodologique que nous avons adoptée afin de mener notre expérience ;
- Chapitre 3 : Résultats et discussions : Il présentera les résultats obtenus après expérience assortis de quelques commentaires liés à ces derniers.

A la fin de notre travail seront évoquées la conclusion et les perspectives liées à notre projet de fin d'études, pour la continuité de la recherche dans le domaine.

CHAPITRE I : CONTEXTE ET PROBLÉMATIQUE

Partie 1 : CONTEXTE

DESCRIPTION

Cette partie nous permettra de présenter le contexte dans lequel notre travail s'effectue, c'est-à-dire l'ensemble des éléments qui sont à l'origine du problème que nous cherchons à résoudre. Nous allons donc étudier à tour les notions de réseaux cellulaire et de fraude à SIMBox.

PLAN :

1. LE CENTRE DE RECHERCHE D'ACCEUIL

L'Institut national de recherche en informatique et en automatique (Inria) est un institut de recherche français public, à caractère scientifique et technologique spécialisé en mathématiques et informatique, créé le 3 janvier 1967. Il est constitué de plusieurs centres disséminés dans les quatre coins de la France, et de plusieurs équipes travaillant sur des thèmes spécifiques autour des mathématiques et de l'informatique. Nous avons travaillé dans l'équipe TriBE (inTeRnet BEyond the usual) basée à Palaiseau, dans le bâtiment Alan Turing. Cette équipe travaille sur des problématiques liées au réseaux et à leurs multiples usages. Dans le cadre de ce projet de fin d'études, nous avons travaillé dans le cadre d'un projet de recherche, qui à terme proposera des solutions pour la détection de la fraude à la SIMBox.

2. GENERALITES SUR LES RESEAUX MOBILES

2.1. Définition et présentation générale d'un réseau mobile

2.1.1. Définition

Un réseau de téléphonie mobile est un réseau téléphonique qui permet l'utilisation simultanée de millions de téléphones sans fil, immobiles ou en mouvement, y compris lors de déplacements à grande vitesse et sur une grande distance. Pour ce faire, un ensemble d'équipements doivent être déployés notamment pour la couverture réseau sans-fil et pour la gestion et les calculs importants. En somme une architecture particulière doit être déployée pour pouvoir atteindre ce but de desserte de services à des terminaux mobiles. Les réseaux mobiles ont donc une architecture de base commune indépendamment de la technologie utilisée.

2.1.2. Architecture générique d'un réseau mobile [8]

Un réseau mobile comprend trois grandes parties (Figure 1) essentielles à savoir :

- **Access Network** : qui est le réseau d'accès radio responsable de la couverture réseau sans-fil des utilisateurs.

- **Core Network** : le réseau cœur responsable de l'ensemble des processus internes du réseau.
- **UE (User Equipment)** : qui représente le terminal de l'utilisateur.

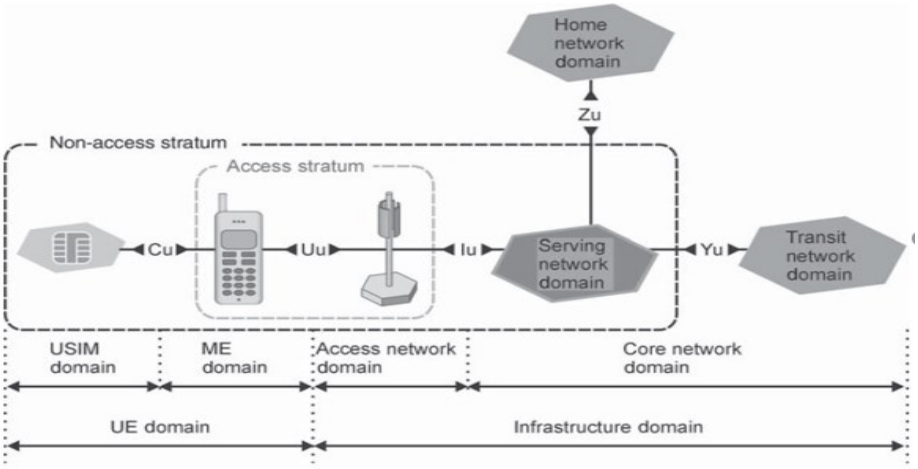


Figure 1 : Architecture générique d'un réseau mobile [8]

Dans la suite nous présentons chacune de ces parties.

1.1.1.1. Le terminal de l'utilisateur

C'est tout équipement qui permet à l'utilisateur d'accéder aux services de téléphonie mobile cellulaire. Cela inclut les téléphones, les tablettes, les routeurs 3G/4G et même un ordinateur s'il est connecté à une clé 3G/4G. Il se connecte au réseau par le réseau d'accès. Le terminal mobile a de diverses appellations selon le standard de téléphonie utilisé. Le terminal est constitué de deux parties :

- **Mobile Equipment (ME)** : le téléphone en lui-même, identifié par son IMEI
- **Carte SIM (USIM)** : la carte à insérer dans le ME pour qu'il puisse se connecter et bénéficier des services du réseau mobile. A partir de la 3G il prend la dénomination de USIM.

1.1.1.2. Le réseau d'accès

Le réseau d'accès est constitué d'un ensemble de stations de base, qui communiquent par ondes électromagnétiques avec les terminaux afin de leur fournir les services. Pour atteindre cet objectif, toutes les technologies d'accès radio doivent résoudre un même problème

: répartir aussi efficacement que possible une bande de fréquences hertzienne unique entre de très nombreux utilisateurs. Pour cela, diverses techniques de multiplexage sont utilisées pour la cohabitation et la séparation des utilisateurs et des cellules radio : le multiplexage temporel (TDMA), le multiplexage en fréquence (FDMA) et le multiplexage par codes (CDMA), ou le plus souvent une combinaison de ces techniques.

1.1.1.3. Le réseau coeur [9]

C'est l'organe central du réseau, c'est lui qui fournit les services aux utilisateurs en fonction de leur souscription. Les services fournis par le cœur de réseau peuvent être classés en deux domaines :

- Le **domaine de commutation de circuit** dont les services sont la téléphonie, le SMS, la messagerie vocale, le customized ring back tone, le push to talk, les services prépayés.
- Le **domaine de commutation de paquets** dont les services sont l 'accès à Internet/Intranet, la télévision mobile, MMS (Multimedia Messaging Service), le streaming vidéo, le mail (e.g., Blackberry Mail), le WEB/WAP, la messagerie instantanée (e.g., Blackberry Messenger), les communications machine to machine (M2M), etc.

Ces services sont acheminés jusqu'à l'utilisateur final via un ensemble d'équipements interconnectés et communicant les uns avec les autres par des protocoles.

1.1.1.4. Les interfaces entre équipements

Les interfaces sont en fait les moyens d'interconnexion existants entre différents équipements du réseau cellulaire. Elles sont différentes pour chaque type d'équipement à interconnecter.

2.1.3. Le concept cellulaire

Un réseau de téléphonie mobile a une structure « cellulaire » qui permet de réutiliser de nombreuses fois les mêmes fréquences ; il permet aussi à ses utilisateurs en mouvement de changer de cellule (handover) sans coupure des communications en cours. Dans un même pays, aux heures d'affluence, plusieurs centaines de milliers, voire plusieurs millions d'appareils sont en service répartis (dans le cas du GSM) sur seulement 500 canaux disponibles.

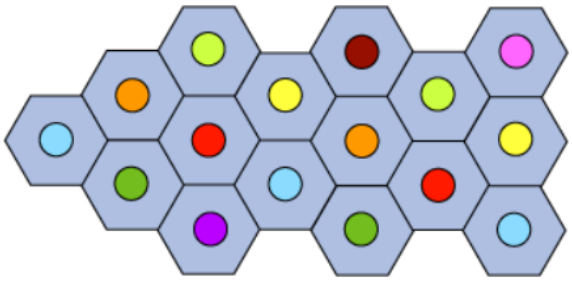


Figure 2 : Le Concept cellulaire (une couleur, une fréquence)

2.2. Evolution des réseaux mobiles

Apparue dans les années 70, la 1G, qui est la première génération de réseaux mobiles est uniquement dédiée aux appels vocaux. Elle reposait sur une technologie dite « analogique ». Ceci à la différence des générations suivantes (2G, 3G, 4G, 5G) qui, elles, exploitent la technologie « numérique ». La 2G a marqué l'arrivée des réseaux numériques intégrant des services à valeur ajoutée dont les SMS, les appels et de meilleure qualité et le début de l'internet mobile, mais a des débits très faibles. La 3G quant à elle a apporté la notion d'internet mobile haut débit, démocratisant ainsi les applications du web, telles que l'envoi d'images, les appels video de basse qualité, le streaming, et d'autres. La 4G quant a elle a permi un révolution totale de l'internet mobile, permettant de nouveaux usages, comme le streaming haute definition, la télépresence, les jeux en ligne. Et enfin la 5G qui aujourd'hui va encore plus loin avec la multiplication des objets connectés, l'industrie 4.0, l'ultra haut debit la realité augmentée et bien d'autres applications [10]. Dans la suite nous nous appesantirons sur le réseau 4G, sur lequel nous avons majoritairement travaillé.

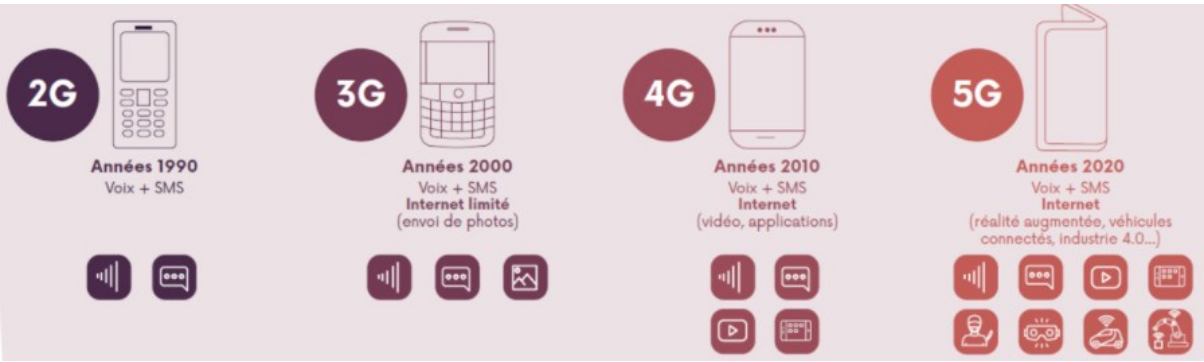


Figure 3 : Evolution des réseaux et des services mobiles [10]

2.3. Le réseau 4G

2.3.1. Le standard LTE

La norme LTE, définie par le consortium 3GPP, a d'abord été considérée comme une norme de troisième génération « 3.9G » (car proche de la 4G), spécifiée dans le cadre des technologies IMT-2000, car dans les « versions 8 et 9 » de la norme, elle ne satisfaisait pas toutes les spécifications techniques imposées pour les normes 4G par l'Union internationale des télécommunications (UIT). C'est en octobre 2010, que l'UIT a reconnu la technologie LTE-Advanced (évolution de LTE définie par le 3GPP à partir de sa release 10) comme une technologie 4G à part entière [11]. Nous présentons ensuite ses caractéristiques.

2.3.2. Caractéristiques de la 4G [12]

Les spécifications générales de la 4G sont :

- **Bandes de fréquences** : largeur pouvant varier de 1,4 MHz à 20 MHz,
- **Fréquences** : allant de 450 MHz à 3,8 GHz selon les pays,
- **Débit binaire théorique** (pour une largeur de bande de 20 MHz) : 300 Mbit/s en liaison descendante.
- Utilisation d'algorithmes d'ordonnancement et de configurations **multi-antennes** avancées prises en charge qui améliorent les débits de données avec DL – 4x 2, 2x2, 2x1, 1x1 et avec UL – 1x2 et 1x1.
- **Efficacité du spectre** : DL 3 à 4 fois celle du HSDPA Release 6 et UL 2 à 3 fois celle du HSUPA Release 6.

- **Latence** : Pour le plan de contrôle (C-plane), moins de 50 à 100 ms pour établir le plan utilisateur (U-plane) et pour le U-plane, moins de 10 ms entre l'UE et le serveur.
- **Mobilité :** optimisé pour les faibles vitesses (< 15 km/h), haute performance pour des vitesses allant jusqu'à 120 km/h ; et liaison maintenue pour des vitesses allant jusqu'à 350 km/h (et des vitesses ciblées jusqu'à 500 km/h avec prise en compte de la bande de fréquence).
- **Rayon de couverture de pleine performance** jusqu'à 5 km ; légère dégradation de 5 à 30 km.

La « vraie 4G », appelée LTE Advanced offre un débit descendant pouvant atteindre ou dépasser **1 Gbit/s** ; ce débit nécessite l'utilisation de bandes de fréquences agrégées de 2×100 MHz de largeur qui sont définies dans les versions 10 à 15 (3GPP releases 10, 11, 12, 13, 14 et 15) des normes LTE Advanced.

2.3.3. Architecture et composants d'un réseau 4G

2.3.3.1. Architecture du réseau LTE

Le LTE est une évolution de l'accès radio et de l'accès non radio. L'accès radio évolue grâce à l'UTRAN amélioré (E-UTRAN). L'accès radio correspond essentiellement à l'évolution de la couche physique du LTE, tandis que l'accès non radio est regroupé dans l'évolution de l'architecture du système sous le nom de System Architecture Evolution (SAE), est l'évolution de l'architecture de réseau du LTE. Les principaux composants de l'architecture du système LTE (Figure 4) sont les suivants [13] :

- User Equipment (UE), tel que UE = Terminal + USIM
- Réseau d'accès radio, Evolved UTRAN(E-UTRAN)
- Le cœur de réseau, Evolved Packet Core (EPC)

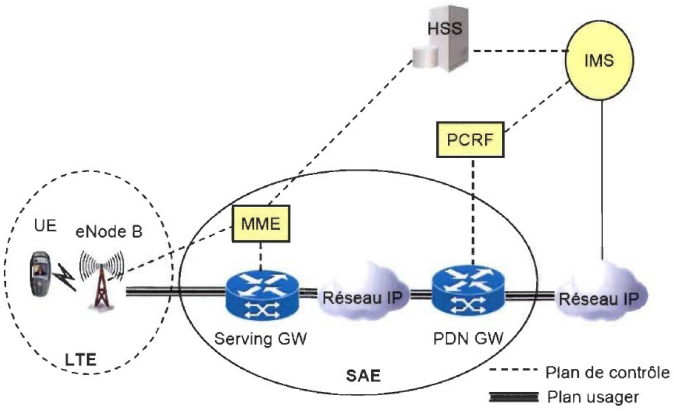


Figure 4: Architecture du réseau LTE [13]

Présentons leurs différentes fonctions et rôles de chacune de ces entités.

2.3.3.2. Le réseau cœur : EPC

Le réseau cœur assure le contrôle global de l'UE et établit les *bearers*. Le CN comporte un certain nombre de nœuds différents, dont les suivants :

- Mobility Management Entity (MME) ;
- Passerelle (P-GW) du réseau de données par paquets (PDN) ;
- Passerelle de service (S-GW) ;
- Evolved Serving Mobile Location Centre (E-SMLC);
- Policy and Charging Rules Function (PCRF);
- Home Subscriber Service (HSS);

MME [14]: Le MME est le principal nœud de contrôle de l'EPC. Les informations du plan de contrôle provenant de l'eNodeB sont principalement acheminées vers le MME. Les protocoles responsables de la communication entre l'UE et le CN sont les protocoles Non-Access Stratum (NAS). Les rôles principaux du MME sont :

- **La signalisation EMM et ESM avec l'UE** : Les terminaux LTE disposent des protocoles comme EMM (EPS Mobility Management) et ESM (EPS Session Management) qui leur permettent de gérer leurs mobilités (attachement, détachement, mise à jour de localisation) et de gérer leurs sessions

(établissement/libération de session de données). Ces protocoles sont utilisés pour les échanges entre l'UE et le MME ;

- **L'authentification** : L'entité MME est responsable de l'identification des équipements utilisateurs grâce aux informations recueillies par l'entité HSS ;
- **La joignabilité de l'UE dans l'état ECM-IDLE (incluent le « paging »)** : L'entité MME prend la responsabilité du « paging », lorsque l'UE est dans l'état IDLE, les paquets à destination de l'équipement utilisateur sont reçus et sauvegardés en mémoire par le Serving Gateway ;
- **La gestion de la liste de zone de localisation (Tracking Area)** : Ce mécanisme consiste à informer l'équipement utilisateur d'être sur les zones de localisation prises en charge par le MME, appelée « Tracking Area ». L'équipement utilisateur met à jour sa localisation lorsqu'il se retrouve dans une « Tracking Area » qui n'est pas encore prise en charge par son MME ;
- **La sélection du « Serving Gateway » et du « PDN-GW »** : C'est le travail du MME de sélectionner le « Serving GW » et le « PDN GW » qui serviront à mettre en œuvre le « Default Bearer » au moment où l'équipement utilisateur se joindra au réseau.
- **La sélection de MME lors d'un « handover » avec changement de MME** : Lorsque l'usager est dans l'état ACTIF et qu'il se déplace d'une zone prise en charge et sous le contrôle d'un autre MME, il est nécessaire que l'ancien et le nouveau MME s'engagent pour le « handover » ;
- **La sélection du SGSN (Serving GPRS Support Node) lors d'un « handover » avec les réseaux d'accès 2G et 3G** : Au moment où l'usager se déplace d'une zone LTE à une zone 2G/3G, c'est l'entité MME qui sélectionnera le SGSN qui sera impliqué dans la mise en place du « default bearer » ;
- **Le « roaming » avec interaction avec le HSS (Home Subscriber Server) nominal** : Lorsque l'usager se rattache au réseau, l'entité MME s'interface au HSS nominal. Le but est de mettre à jour la localisation du mobile et d'obtenir le profil de l'usager ;

- **Le Fonctionnement de la gestion du « bearer » incluant l'établissement de « dedicated bearer »** : Parmi les fonctions de MME l'une d'elles est d'établir pour le compte de l'usager les « defaults » et « dedicated bearers » nécessaires pour la prise en charge des communications ;
- **L'interception légale du trafic de signalisation** : L'entité MME reçoit toute la signalisation qui a été envoyé par l'équipement utilisateur et peut la sauvegarder à des fins de traçabilité.

P-GW : Le P-GW sert de routeur intermédiaire de point d'extrémité entre l'EPS et les réseaux réseaux externes. Il fournit principalement une connexion IP et effectue également l'adressage IP des UE, le traçage et le filtrage lorsque cela est nécessaire.

S-GW : Le S-GW est responsable de la gestion des tunnels du plan utilisateur et de la commutation. Il fait office d'ancre mobile entre l'EPC et le RAN LTE. Tous les paquets des utilisateurs sont acheminés par le S-GW.

PCRF : Le PCRF assure les fonctions de contrôle des politiques et de tarification.

HSS : C'est une base de données qui contient les détails de l'abonnement de tous les utilisateurs. Il contient les informations sur le PDN auquel chaque utilisateur est connecté ou peut se connecter. En fait, il contient toutes les données des abonnés permanents. Le HSS peut également intégrer le centre d'authentification (AuC).

2.3.3.3. Le réseau d'accès : E-UTRAN

Le réseau d'accès LTE (appelé E-UTRAN) est une composition de réseaux d'eNodeBs. Il est responsable des fonctions liées à la radio au sein du réseau :

- Gestion des ressources radio,
- La compression des en-têtes,
- La sécurité,
- Le positionnement et la connectivité EPC.

L'eNodeB se distingue des autres stations de base des précédentes générations du fait qu'il n'a pas de contrôleur central. C'est un équipement intelligent. Les eNodeBs sont interconnectés

par des interfaces appelées "interface X2" et sont connectés à l'EPC par des interfaces S1 (cette connexion est faite vers le S-GW par des interfaces S1-U et vers le MME par l'interface S1-MME).

2.3.3.4. Les interfaces entre équipements du réseau 4G

La Figure 5 présente les différentes interfaces du réseau 4G, et le Tableau 1 les plus importantes.

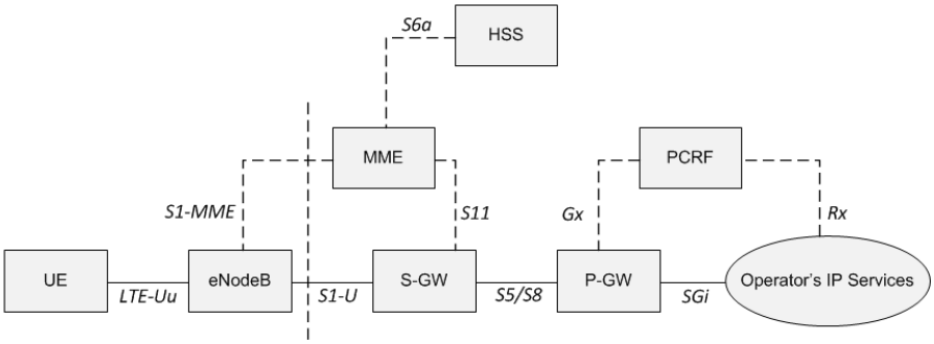


Figure 5: Interfaces entre équipements dans le réseau 4G [12]

Type d'interface	Rôle
Interface X2	Utilisée pour la mobilité entre deux eNodeBs et pour la préparation de procédures de handover.
Interface S1-MME	Permet la communication entre EPC et E-UTRAN
Interface S1-U	Connecte l'E-UTRAN et le S-GW correspondant

Nous présenterons par la suite le type de données qui transitent dans le réseau 4G.

2.4. La signalisation dans les réseaux mobiles

2.4.1. Définition de la signalisation : plan de contrôle et plan utilisateur

En télécommunications, la signalisation peut désigner trois choses [15] :

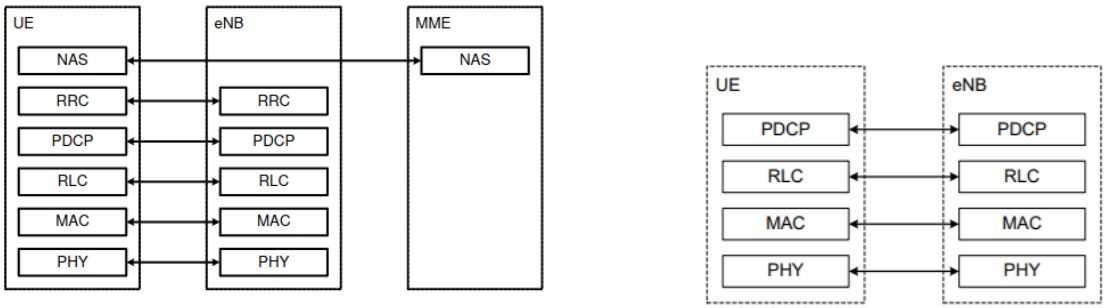
1. L'utilisation de signaux pour contrôler des communications
2. L'échange d'information permettant l'établissement et le contrôle d'un circuit de télécommunication et la gestion du réseau, en opposition avec le transfert de données utilisateurs.
3. L'envoi d'un signal par une terminaison en émission d'un circuit de télécommunication pour informer un utilisateur situé sur la terminaison en réception qu'un message doit être envoyé.

Dans notre cas c'est la deuxième définition qui nous intéresse. On peut donc en dégager deux différents plans. Le plan de contrôle représentant les échanges d'information avant tout transfert d'informations utilisateur, et le plan utilisateur étant lesdites informations. Dans la suite nous nous intéresserons au plan de contrôle réseau LTE.

2.4.2. La signalisation dans le réseau 4G

2.4.2.1. Pile protocolaire LTE

En effet, LTE possède deux piles protocolaires : la première est pour la signalisation ou le contrôle, et la seconde pour les données utilisateur [14]. L'architecture et les couches du réseau LTE peuvent être résumées par les figures suivantes :



(a) Plan de contrôle *(b) Plan utilisateur*

Figure 6: Pile protocolaire LTE, plan de contrôle et plan utilisateur [16]

Ces figures nous montrent un parallèle avec le modele OSI. Nous présentons dans la suite, chacune des couches et son role dans la pile.

2.4.2.2. La couche NAS [16]

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).

La sécurité de la transmission des données de signalisation est assurée par le système de chiffrement et la protection de l'intégrité. Le transfert des messages de NAS depuis et vers les UE est réalisé par la couche RRC (Radio Resource Control).

2.4.2.3. La couche RRC (Radio Resource Control) [16]

La couche RRC au niveau de l'eNodeB est responsable des opérations suivantes :

- La diffusion des informations du système ;
- La procédure de paging ;
- Elle prend les décisions de « handover » en se basant sur les informations d'UE sur les cellules voisines ;
- L'allocation des identifiants temporaires aux UE ;
- Elle assure le transfert du contexte de « handover » entre deux eNodeB à l'UE ;
- La configuration de la signalisation des bearers radio pour la connexion RRC ;
- Elle facilite les services MBMS (Multimedia Broadcast Multicast Service).

2.4.2.4. La couche PDCP (Packet Data Convergence Protocol)

La couche PDCP au plan utilisateur prend la charge d'assurer : la compression et la décompression des entêtes lP liées aux données utilisateurs. Elle utilise ROHC (Robust Header Compression) pour augmenter l'efficacité de la bande passante. Elle est aussi responsable du chiffrement des données sur les deux plans (données et signalisation). Les messages de la

couche NAS sont chiffrés deux fois, au niveau du MME et de l'eNodeB, puisqu'ils passent par la couche RRC. Enfin, elle assure le transfert du SDU reçu du NAS vers la couche RLC et vice versa. [17]

2.4.2.4.1. La 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. Elle offre trois modes de fiabilité [14] :

- **AM (Acknowledged Mode)**, qui nécessite un acquittement. Ce mode est intéressant pour les applications tolérantes aux délais tels que le téléchargement de fichiers ;
- **UM (Unacknowledged Mode)** ne nécessite pas d'acquittement. Il convient aux applications à temps réel, comme le streaming vidéo ;
- **TM (Transparent Mode)** qui n'ajoute aucune des entêtes des couches supérieures, le paquet garde sa taille d'origine (PDU = SDU + entête PDCP). [18]

2.4.2.4.2. La couche MAC (Media Access Control)

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. Au niveau de cette couche, les mesures de l'état du trafic et de la correction des erreurs sont assurées par la méthode de retransmission HARQ (Hybrid Automatic Repeat reQuest). De plus, la couche MAC offre le service d'ordonnancement. [19]

2.4.2.4.3. La couche PHY [14]

Cette couche a comme tâche de :

- Assurer la détection des erreurs de transmission et la notification vers la couche supérieure ;
- Utiliser FEC (Forward Error Correction) du canal de transmission pour les fonctions de codage et de décodage ;
- Permettre le mappage des symboles codés avec les canaux physiques ;
- Assurer la modulation/démodulation ;
- Fournir la synchronisation des fréquences et de l'horloge ;
- Mesurer les caractéristiques radios et envoyer les indications aux couches supérieures ;

- Être le support du MIMO (Multiple Input Multiple Output).

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

3. LA TELEPHONIE SUR IP

3.1. Définition

La voix sur IP, ou « VoIP » pour « Voice over IP », est une technologie informatique qui permet de transmettre la voix sur des réseaux compatibles IP, via Internet ou des réseaux privés (intranets) ou publics, qu'ils soient filaires (câble/ADSL/fibre optique) ou non (satellite, Wi-Fi et réseaux mobiles) [20], qui autrefois était transmise par le RTC.

3.2. Fonctionnement

La VoIP fonctionne par numérisation de la voix, décomposition puis envoi sous forme de paquets IP, puis par reconversion des paquets en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Il est bien plus tolérant au bruit que l'analogique. La pile protocolaire TCP/IP est ainsi la pierre angulaire de ce moyen de communication. La notion de protocole de communication au niveau de la couche application de ladite pile devient fondamentale. La Figure 7 illustre les éléments constituant un réseau téléphonique basé sur la VoIP.

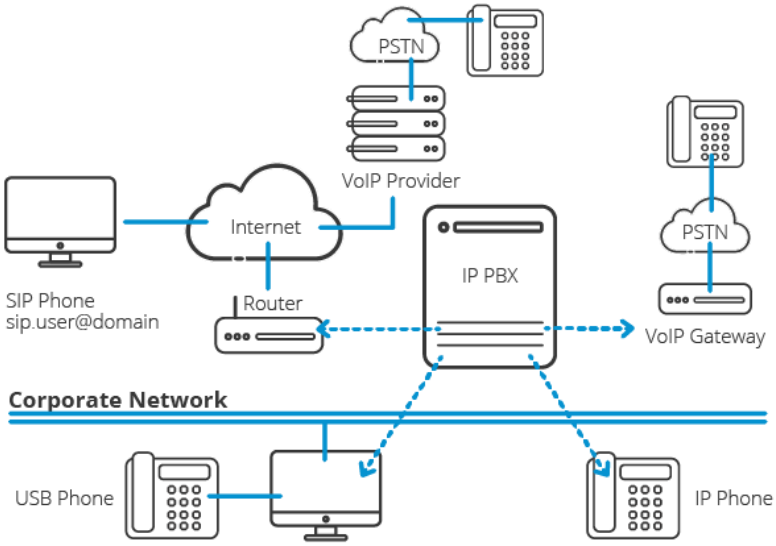


Figure 7: Système VoIP standard [21]

Nous pouvons observer plusieurs éléments que nous présentons plus en détail.

3.2.1. Le PBX (Private Branch Exchange) [21]

Un système IPBX (PBX sur IP) est la composante centrale de la plupart des standards VoIP. Le serveur IPBX est similaire à un serveur proxy. Les softphones ou téléphones matériels, s'enregistrent sur le serveur et quand ils souhaitent passer des appels téléphoniques, ils demandent au PBX d'établir la connexion.

3.2.2. Le réseau de l'entreprise [21]

Il s'agit du réseau local de l'entreprise, via lequel les ordinateurs sur lesquels sont installés des clients SIP tels que des softphones, et les téléphones IP, se connectent directement à l'IPBX.

3.2.3. Le routeur/pare-feu de l'entreprise [21]

Il se connecte à Internet et de là, il peut se connecter aux extensions distantes. Les extensions distantes incluent les ordinateurs personnels qui utilisent des softphones du PBX, des téléphone IP distants, des appareils portables avec les applications Android ou iOS, ou d'autres PBX connectés via ponts. Le routeur peut aussi se connecter au réseau RTC si un opérateur de VoIP est utilisé.

3.2.4. Passerelle VoIP

Une passerelle VoIP connecte le PBX directement au réseau RTC pour que vous puissiez continuer à passer des appels et à répondre à des appels entrants depuis des lignes analogiques. Une fois l'aspect matériel des systèmes de VoIP présenté, montrons à présent son aspect protocolaire.

3.3. Protocoles utilisés dans la VoIP

On en compte plusieurs, mais deux principaux dont SIP et H.323.

3.3.1. H.323

H.323 regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. C'est un protocole développé par l'UIT-T qui le définit comme : « systèmes de communication multimédia en mode paquet ». La première version est publiée en novembre 1996 et l'actuelle date de 2009. Il est dérivé du protocole H.320, utilisé sur RNIS, (Réseau Numérique à Intégration de Services ISDN en anglais) [22].

3.3.1.1. Architecture et composants d'un système H.323 [23]

La Figure 8 présente l'architecture d'un système H.323 complet et ses composants.

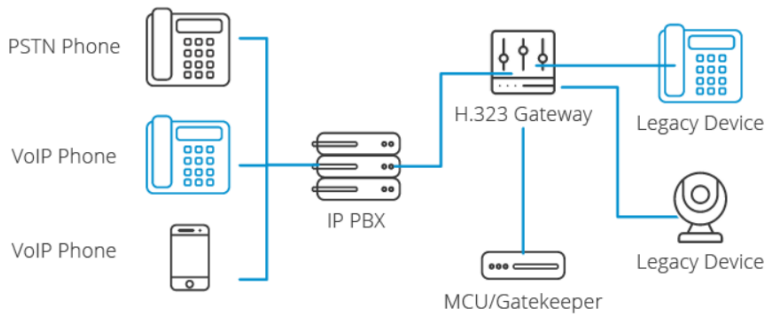


Figure 8: Architecture d'un système H.323 [23]

On peut citer :

- **Les terminaux H.323** : Ce sont des téléphones IP, des smartphones, ou même un combiné téléphonique à condition d'implémenter au minimum la norme de compression de la voix G.711.

- **La gateway H.323** : elle assure l'interconnexion du réseau IP/H.323 avec d'autres réseaux comme le RTC ou RNIS, par la translation de formats de transmission.
- **MCU (Multipoint Control Unit)** : ils offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées et plusieurs MP distribués sur le réseau et faisant partie d'autres MCU. [24]
- **Gatekeeper** : c'est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323, regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement [24].

3.3.1.2. Signalisation H.323 [25]

La Figure 9 présente, le flow complet de communications, pour un appel H.323. Il se fait en 4 étapes :

- **SETUP** : le terminal appelant s'enregistre auprès du gatekeeper et fait une demande de connexion avec la destination. Une fois que la destination reçoit le message, le terminal s'enregistre de la même manière que la source, et renvoie la sonnerie à l'appelant. Enfin, il envoie le message CONNECT pour indiquer que le lien est établi.
- **CONTROL SIGNALLING** : cette phase consiste à un échange de messages pour définir le contexte de la communication.
- **AUDIO** : Les terminaux communiquent en s'envoyant des données voix via le protocole RTP.
- **RELEASE** : L'une des deux parties interrompt l'appel, et les deux terminaux se désenregistrent.

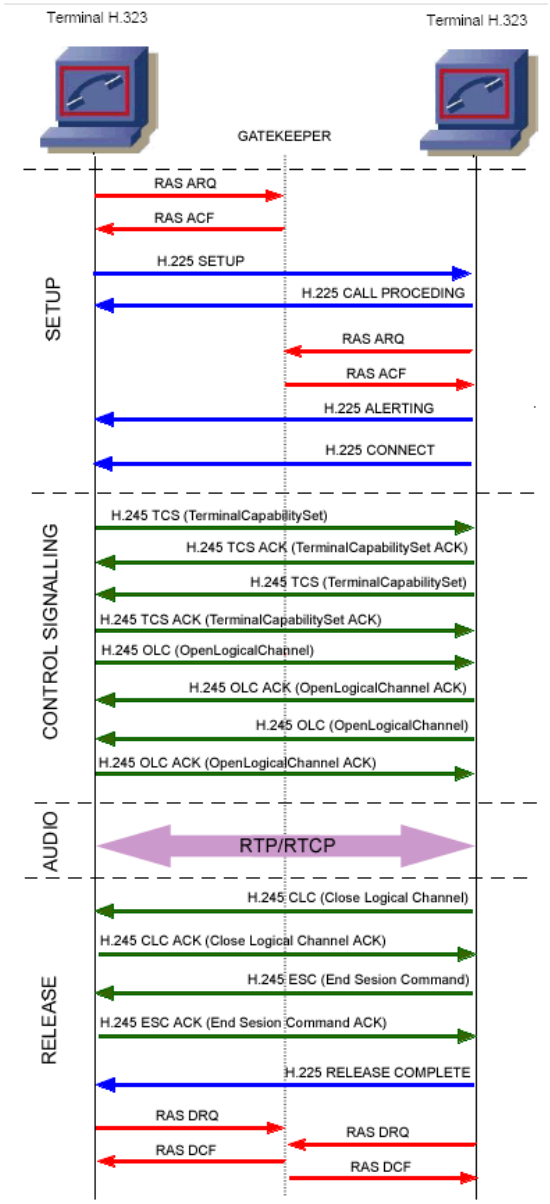


Figure 9: Processus d'un appel H.323 [25]

Dans la suite nous présentons le protocole SIP.

3.3.2. SIP (Session Initiation Protocol)

Le protocole SIP (Session Initiation Protocol) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) en 1999 et est désormais repris et maintenu par l'IETF en tant que RFC 3261. SIP est un protocole de signalisation appartenant à la couche

application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP essentiellement.

3.3.2.1. Fonctionnement global de SIP [26]

SIP fonctionne aussi bien avec IPv4 qu'avec IPv6. SIP est supporté par TCP ou UDP sur le port 5060 par défaut. La version sécurisée SIP-TLS utilise par défaut le port TCP 5061.

SIP prend en charge cinq facettes de l'établissement et de la terminaison de communications multimédia :

- **Localisation de l'utilisateur** : détermination du système terminal à utiliser pour la communication ;
- **Disponibilité de l'utilisateur** : détermination de la volonté de l'appelé à s'engager dans une communication ;
- **Capacités de l'utilisateur** : détermination du support et des paramètres de support à utiliser ;
- **Etablissement de session** : "sonnerie", établissement des paramètres de session à la fois chez l'appelant et l'appelé ;
- **Gestion de session** : y compris le transfert et la terminaison des sessions, la modification des paramètres de session, et l'invocation des services.

La notion de numéro de téléphone est présente dans SIP. Elle porte le nom de URI (Uniform Resource Identifier) et est formatté comme suit :

SIP URI = sip:x@y:Port ***x=nom d'utilisateur et y=hôte (domaine ou IP)***

3.3.2.2. Architecture et composants d'un système SIP

On distingue plusieurs rôles logiques dans un système SIP. Dont :

- **Les Users Agents (UA)** : ce sont les extrémités du système, on a le client SIP ou User Agent Client (UAC) qui fait des requêtes d'enregistrement au serveur SIP ou User Agent Server (UAS) qui rejettent acceptent, rejettent ou redirigent celles-ci.

- **Les proxy ou serveurs mandataires** : ce sont des intermédiaires qui agissent à la fois comme des clients et des serveurs.
- **Les serveurs de redirection :** qui redirige le client par des réponses.
- **B2BUA - Back-to-Back User Agent** : est une entité logique entre des UA qui reçoit une requête et la traite comme UAS. Afin de déterminer comment il devrait répondre à la requête, il agit comme un UAC vers l'UAS final et génère lui-même des requêtes.
- **REGISTRAR Server :** gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant.
- **SBC - Session Border Controller** : est placé comme élément intermédiaire pour rendre des services entre les UA et les serveurs SIP en matière de sécurité, de camouflage de topologie, de filtrage ou encore de chiffrement du trafic.
- **Les Gateways (passerelles)** : sont des entités logiques qui sont capables d'établir des liaisons vers des destinations non-IP notamment les réseaux PSTN.

3.3.2.3. Requêtes SIP [26]

Le client envoie des requêtes au serveur ; serveur qui, en retour, lui renvoie une réponse. Les méthodes de base (RFC 3261) comprises dans ces requêtes sont :

- **INVITE** : permet à un client de demander une nouvelle session,
- **ACK** : confirme l'établissement de la session,
- **CANCEL** : annule un INVITE en suspens,
- **BYE** : termine une session en cours,
- **OPTIONS** : permet de récupérer les capacités de gestion des usagers, sans ouvrir de session,
- **REGISTER** : permet de s'enregistrer auprès d'un serveur d'enregistrement.

D'autres méthodes existent et sont spécifiées dans les autres RFC relatives à SIP. A chacune des requêtes effectuées par un client SIP, correspondra une réponse conformément à la situation.

3.3.2.4. Réponses SIP ou status code [26]

Selon les contextes une réponse est attendue après chaque requête SIP. Les réponses possibles sont similaires aux réponses HTTP. Dans le meilleur des cas on obtient un 200 OK.

On distingue six catégories de status code :

- **Provisional (1xx)** : La requête est reçue et est en cours de traitement.
- **Success (2xx)** : L'action a été reçue, comprise et acceptée avec succès.
- **Redirection (3xx)** : Une action supplémentaire doit être prise (par l'appelant) pour compléter la requête.
- **Client Error (4xx)** : La requête comporte une mauvaise syntaxe et ne peut être prise en charge par le serveur.
- **Server Error (5xx)** : Le serveur a échoué remplir une requête apparemment valide.
- **Global Failure (6xx)** : La requête ne peut être prise en charge par aucun serveur.

3.3.2.5. Processus d'un appel SIP

La Figure 10 présente la signalisation et le trafic (RTP) d'un appel SIP complet avec l'ensemble des requêtes et réponses.

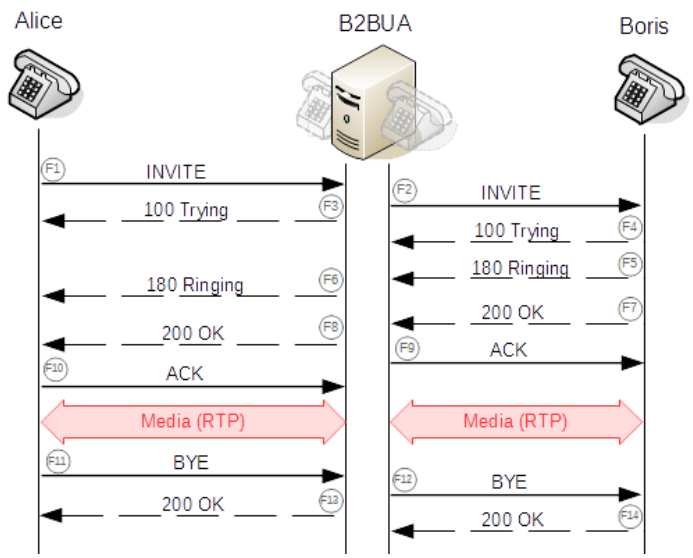


Figure 10: Processus d'un appel SIP [26]

1. Une requête **INVITE** est envoyée à un serveur proxy pour initier une session.

2. Le serveur proxy envoie immédiatement une réponse **100 Trying** à l'appelant (Alice) pour arrêter les retransmissions de la demande **INVITE**.
3. Le serveur proxy recherche l'adresse de Boris dans le serveur de localisation. Après avoir obtenu l'adresse, il transmet la demande **INVITE**.
4. Ensuite, **180 Ringing** (réponses provisoires) est générée par Boris est renvoyée à Alice.
5. Une réponse **200 OK** est générée peu après que Boris ait décroché le téléphone.
6. Boris reçoit un **ACK** de la part d'Alice, une fois qu'il a reçu **200 OK**.
7. En même temps, la session est établie et les paquets RTP (conversations) commencent à circuler des deux côtés.

3.3.3. Comparaison SIP et H.323

Bien que le protocole H.323 et le protocole SIP proposent deux ensembles de structures de systèmes téléphoniques IP, ils poursuivent les mêmes objectifs. Ils sont indépendants l'un de l'autre. Un seul à la fois peut être sélectionné dans une implémentation. Le Tableau 2 synthétise la comparaison entre les deux protocoles.

Tableau 2: Comparaison entre SIP et H.323 [27]

	SIP	H323
Nombre échanges pour établir la connexion	1,5 aller-retour	6 à 7 aller-retour
Maintenance du code protocolaire	Simple par sa nature textuelle à l'exemple de HTTP	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert à de nouvelles fonctions	Ajout d'extensions propriétaires sans concertation entre vendeurs
Méyhode de codage	Plus complexe utilise le codage ASN1	Utilise n'importe quel type de protocole de codec
Fonction de conférence	Distribuée	Centralisée par l'unité MC
Fiabilité	Moins élevée	Très élévée
Capacité de traitement	Très accrue	Réduite
Signalisation multicast	Oui, par défaut	Non

Ainsi présentés nous avons tous les éléments nécessaires au sujet des réseaux mobiles utiles pour notre étude de la fraude à la SIMBox que nous présenterons ensuite.

4. LA FRAUDE A LA SIM BOX

Notre travail sur la SIMBox est basé sur une étude menée par Anne Josiane Kouam dans [28], qui a investigué sur les méthodes et stratégies de fraude à la SIMBox, les méthodes de détection et fait une projection dans les prochaines années de l'évolution du marché de la fraude à la SIMBox. Nous allons nous focaliser sur le principe de la fraude, les architectures de SIMBox et les stratégies associées.

4.1. Généralités sur l'écosystème des réseaux mobiles.

Le secteur des télécommunications étant devenu très florissant ces dernières années, le nombre de méthodes de fraude a également augmenté. Il existe un écosystème complet autour duquel évolue le secteur de la téléphonie. On distingue :

- **Les réseaux cellulaires** : qui proposent les services de téléphonie et d'internet
- **Les opérateurs de VoIP** : qui acheminent le trafic voix sous forme de paquets
- **Les utilisateurs finaux** : qui profitent des services fournis
- **Les organes de régulation** : qui définissent la règlementation de la fourniture de services à l'échelle nationale.
- **International carriers** : ce sont des entités qui peuvent être étatiques ou bien privées dont la fonction est de router du trafic international émanant d'une source vers une destination, moyennant une commission.

La Figure 11 nous montre comment se déroule la facturation (cash-flow) dans le cas d'un appel international réussi sans influence d'une quelconque fraude.

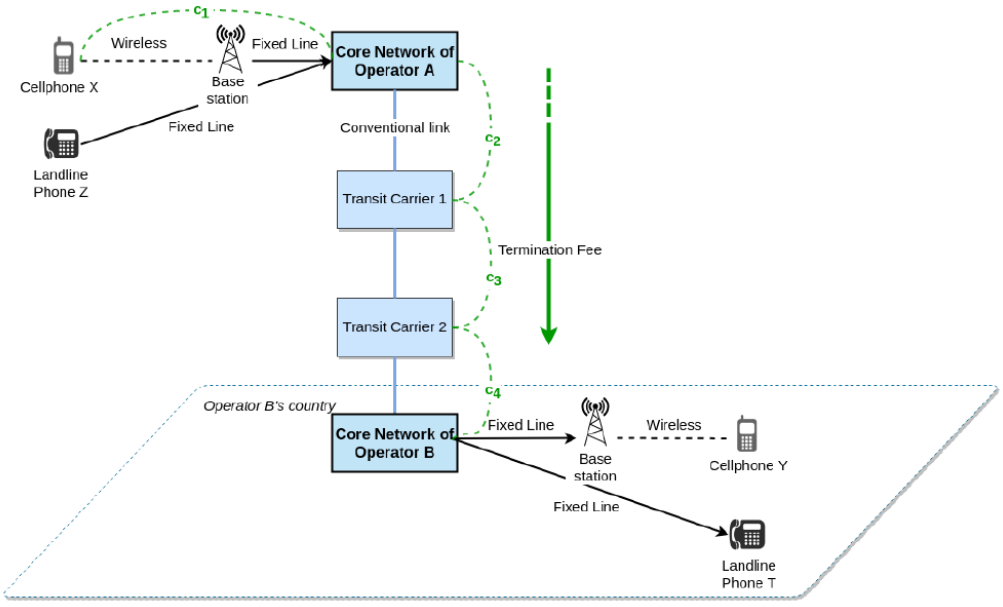


Figure 11 : Cash-flow dans le cas d'un appel international entre opérateurs [28]

4.2. Principe de la fraude à la SIM box

4.2.1. Techniques de fraude à la SIM box [28]

La fraude à la SIMBox consiste à détourner le trafic d'appel des routes conventionnelles vers le réseau VoIP en utilisant des passerelles appropriées. Son schéma peut être décomposé en quatre étapes, résumées dans la Figure 12.

1) Un appel (mobile ou fixe) est émis d'un pays à l'autre et transite par des routes réglementées jusqu'à un *carrier* frauduleux.
2) L'opérateur frauduleux utilise une passerelle VoIP pour acheminer le trafic à travers le réseau VoIP vers un pays où les partenaires des fraudeurs ont une SIMBox, et le trafic est reçu au niveau de la SIMBox (manipulation du routage des appels).
3) La SIMBox reconvertit le trafic VoIP en un appel mobile en utilisant une carte SIM comme origine de l'appel.

4) L'appel émis par la SIMBox est acheminé jusqu'au destinataire de l'appel. L'appel transite par l'opérateur local fournissant le réseau de la carte SIM utilisée par la SIMBox.

Pour que la quatrième étape puisse être réalisée, les fraudeurs ont besoin d'un grand nombre de cartes SIM appartenant à l'opérateur cible. Les fraudeurs disposent de divers moyens :

- Obtenues illégalement par vol ou clonage (*superimposed fraud* [29] ; [30])
- Par usurpation de comptes existants (*subscription fraud* [31]).

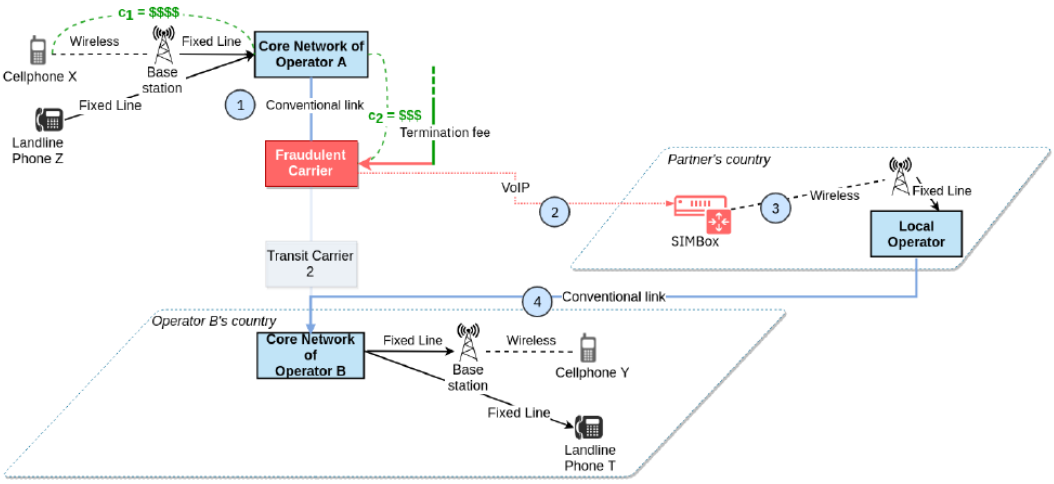


Figure 12 : Call flow dans un scénario de fraude à la SIMBox [28]

4.2.2. Source de revenu des fraudeurs

La principale motivation de la fraude au SIMBox est d'ordre financier. Les fraudeurs visent à obtenir une part de la facturation des appels internationaux : les frais de terminaison. Plus ils sont coûteux, plus c'est intéressant pour les fraudeurs. Pour gagner de l'argent de cette activité, les fraudeurs s'insèrent dans l'itinéraire de terminaison du trafic vocal

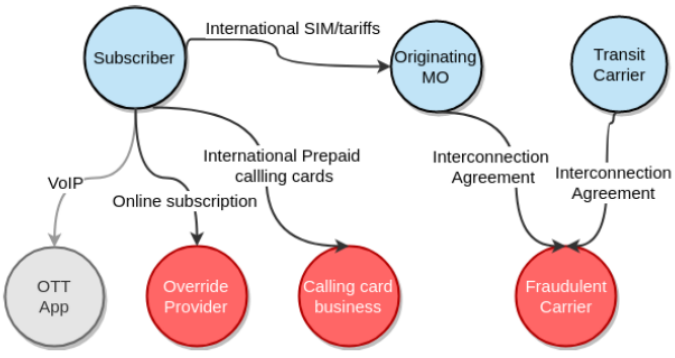


Figure 13: Diagramme d'intrusions possibles dans le routage d'un appel international. [28]

afin de détourner l'itinéraire conventionnel et de percevoir les frais correspondants. Cela peut se faire soit à l'origine de l'appel, en incitant les abonnés à ne pas envoyer le trafic à leur opérateur mais à leur envoyer directement le trafic, ou quelque part sur l'itinéraire de l'appel en tant que carrier frauduleux. Dans les deux cas, le comportement typique des fraudeurs est de prétendre pouvoir acheminer des appels à des coûts suffisamment bas pour intéresser leur public.

Dans la Figure 13 , Les cercles rouges représentent les acteurs frauduleux. Les cercles bleus représentent les acteurs qui pourraient être usurpés.

Les fraudeurs utilisent une technique appelée *number range hijacking* qui consiste pour des carriers frauduleux de proposer des couts très faibles pour une plage de numéros de téléphone de destination. Cela pousse les opérateurs à utiliser ceux-ci. Cela est facilité car :

- Il n'existe pas de mécanisme d'authentification directe d'un possesseur d'une plage de numéros.
- Les accords de partenariats entre carriers ne sont pas toujours optimisés.

4.3. Architecture de la SIM box

Il existe plusieurs manières de déployer la SIMBox dans un réseau cellulaire. Ces différentes architectures peuvent être résumées en un seul équipement ou alors distribuées, selon le matériel à disposition du fraudeur. La SIMBox peut être composée de trois équipements principaux : la GSM gateway, la SIMBank, le SIM Server.

4.3.1. La GSM Gateway [28] [32]

Cet équipement permet la terminaison d'appels depuis le réseau VoIP vers le réseau cellulaire (2G, 3G,4G) et inversement. Il reçoit le trafic depuis un softswitch et assure son routage dans le réseau cellulaire. Il est constitué de :

- **GSM modules** : qui est constitué de canaux responsables de l'établissement de la connexion avec le réseau cellulaire. Ces modules peuvent être compatibles pour d'autres standards (3G et 4G). Chaque canal possède son firmware et de ce fait un IMEI, l'identifiant comme équipement mobile.

- **SIM client** : qui est responsable de l'association entre carte SIM et canal. Il fait des requêtes au SIM Server pour lier un canal a une carte SIM dans le cas où ledit canal n'est pas encore lie. Une fois qu'ils sont lies ils constituent un *voice channel* et peuvent de ce fait faire des appels, SMS ou requêtes USSD

Un canal GSM est caractériséé par :

- **IMEI** qui identifie le canal comme un terminal mobile.
- **IMSI** de la carte SIM, s'il y en a.
- **Remaining call duration time** le temps de communication restant du canal.
- **Carrier,** l'opérateur de la carte SIM, s'il y en a.
- **Current base station ID (BST ID)** si le status est *mobile registered*.
- **Received Signal Strength Indicator (RSSI)** de la cellule actuelle.
- **Bit Error Rate**, le taux d'erreur binaire entre le module GSM et la station de base.
- **Answer-Seizure Ratio (ASR)**, le pourcentage d'appels décrochés.
- **Average Call Duration (ACD)**, la Moyenne des durées d'appels.
- **Post Dial Delay**, la durée entre l'initiation de l'appel et la sonnerie.
- **Status,** l'état du canal comme : *Idle*, quand le canal est inactif ; *Processing*, quand un appel est en train d'être établi ; *Alerting*, quand le téléphone destinataire sonne ; *Active*, quand l'appel est en cours ; and *Calling Waiting*, quand la gateway reçoit un appel pendant qu'elle est active dans un autre appel.
- **Idle time** indiquant le temps écoulé après le dernier appel.

La Figure 14, présente, un extrait de l'interface graphique d'une GSM gateway.

Summary

CH	Line	M	SIM	GSM	VOIP	Status	SMS	ACD(S)	ASR(%)	Duration(S)	Count	CDR Start	RSSI	Carrier	BST ID	Idle	Remain	SMS Remain	Reset
☐	1	Y	N	N	N	IDLE	N	0	0	0	0	2016-06-07 14:00:59	99			676	NO LIMIT	NO LIMIT	Remain SMS ACD&ASR
☐	2	Y	N	N	N	IDLE	N	0	0	0	0	2016-06-07 14:00:59	99			676	NO LIMIT	NO LIMIT	Remain SMS ACD&ASR
☐	3	Y	N	N	N	IDLE	N	0	0	0	0	2016-06-07 14:00:59	99			676	NO LIMIT	NO LIMIT	Remain SMS ACD&ASR
☐	4	Y	N	N	N	IDLE		0	0	0	0	2016-06-07 14:00:59	99			676	NO LIMIT	NO LIMIT	Remain SMS ACD&ASR
☐ All																			Remain SMS ACD&ASR

Figure 14: Sommaire des caractéristiques d'une GSM gateway à quatre canaux, du constructeur HyberTone [32]

Sur le plan physique la GSM gateway est un équipement possédant une ou plusieurs antennes pour communiquer sur la voie radio, un ou deux ports Ethernet pour la connexion à internet/intranet et sa configuration via une interface graphique. Il peut parfois posséder un port USB, et nécessairement une alimentation. La Figure 15 nous montre l'aspect physique d'une gateway.

Figure 15: Apparence physique d'une GSM gateway à huit canaux, du constructeur HyberTone [32]

4.3.2. La SIM Bank [28]

Le rôle de la SIMBank est de contenir un ensemble de cartes SIM utilisées par le système pour l'acheminement des appels. La SIMBank n'est pas indispensable à l'architecture de la SIMBox car certains modèles de GSM gateway intègrent des emplacements de SIM. Cependant, contrairement aux GSM gateways, la SIMBank a l'avantage d'offrir une capacité d'opération à distance, ce qui facilite les tâches de gestion, minimise les dépenses de maintenance, et résout le problème de blocage de cartes SIM. On peut y mettre des cartes de SIM d'opérateurs différents et les connecter a des canaux de gateways situées à des lieux différents. Elle peut accueillir entre 32 [33] et 256 cartes SIM.

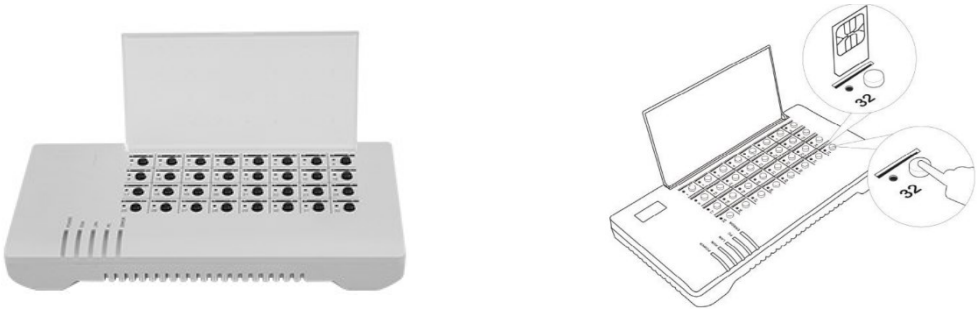


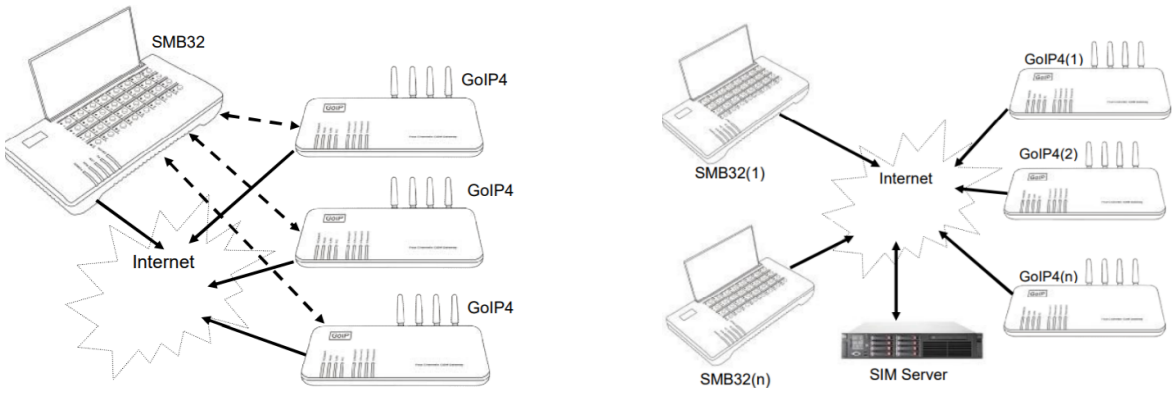
Figure 16: Apparence physique d'une SIMBank 32 slots, HyberTone [33]

La SIMBank a deux parties essentielles :

- **SIM Manager** : qui gère les SIM slots (emplacements de carte SIM)
- **Control Server** : qui permet d'interconnecter la SIM Bank avec des gateways et faire des mappages entre SIM slot et canaux de GSM gateway.

Elle a deux modes de fonctionnement principaux :

- **En serveur** : dans ce cas elle joue le point de connexion de toutes les gateways, et peut leur distribuer ses cartes SIM. L'inconvénient majeur de ce mode est la limitation du nombre de cartes SIM. En effet on ne peut pas avoir plus de canaux connectés que le nombre de SIM slots. (Figure 17.a)
- **En client** : dans ce cas la SIMBank est passive, et se connecte au SIM serveur qui gère les cartes SIM. Dans cette configuration on peut avoir plusieurs SIMBank pour plusieurs gateways. (Figure 17.b)



(a) En Serveur *(b) En client*

Figure 17: Les deux modes de fonctionnement de la SIMBank [33]

4.3.3. Le SIM Server [28]

Le SIM Server est l'équipement central de l'architecture comme le montre la Figure 17.b. Il est basé sur un système linux ainsi et d'un système de base de données. Il peut être installé localement ou alors dans un serveur dans le cloud. Il a 3 principaux rôles :

- **Rôle 1** : Il permet de visualiser et de configurer l'ensemble des équipements principaux de l'architecture. Il conserve les données (configurations, statistiques, journal, etc.) dans une base de données. Il communique avec une interface graphique accessible à distance via un navigateur.
- **Rôle 2** : Il met en place les voice channels pour le routage des appels en faisant des associations entre cartes SIM et les modules GSM des gateways distantes. Ces liens sont établis de façon continue qu'il y ait appel ou non. Il existe deux manières de créer de tels groupes :
    - Les canaux GSM en *GSM groups* et les cartes SIM en *SIM groups* créés par l'administrateur : Un *GSM group* est un ensemble de canaux GSM appartenant à différents voice servers mais partageant la même configuration. Le nom de groupe doit être unique. Il en va de même pour les SIM groups respectivement. Ainsi l'administrateur fait des liens entre GSM groups et SIM groups de manière à ce que les cartes SIM dans un groupe ne peuvent s'associer qu'a des canaux GSM dans le GSM group associée.
    - Les liens sont faits sur la base d'un *scheduling group* : qui inclue plusieurs cartes SIM et canaux GSM. Un scheduling group implique que les SIM slots et canaux GSM channels en son sein peuvent être dynamiquement lies selon les règles d'ordonnancement du groupe.
- **Rôle 3** : il réalise le routage du trafic VoIP aux gateways GSM via un softswitch. Le softswitch connecte le système avec le réseau VoIP externe et reçoit du trafic d'appel SIP ou H.323. Dans ce but, pendant la configuration des gateway GSM, des comptes SIP sont créés et enregistrés au niveau du softswitch (fonctionnant comme un serveur SIP) qui envoie du trafic a chaque compte. Ainsi il y a plusieurs possibilités :
    - (i) **Config by Line** : Un seul compte pour chaque canal GSM du système, et le trafic est directement envoyé à chaque gateway sans ambiguïté ;
    - (ii) **Single server mode** : Un seul compte pour tous les canaux GSM du système ou plusieurs comptes pour des groupes de canaux GSM ;
    - (iii) **Trunk gateway mode** : Aucun compte créé et de ce fait la gateway utilise des trunks SIP pour recevoir des appels VoIP.

La deuxième option est la plus utilisée car elle est moins coûteuse que la première. Mais il faut définir des algorithmes pour le choix du canal qui terminera l'appel. On distingue :

- **In-Turn** : Le trafic est envoyé au premier canal disponible.
- **Balance** : Le trafic est envoyé au canal qui a le moins communiqué.
- **Sequence** : le trafic est acheminé par canal vocal ascendant.
- **Random** : le voice channel est choisi au hasard parmi les canaux disponibles.

On peut également faire du routage intelligent en associant des préfixes dans la configuration des canaux GSM. Par exemple en ajoutant le préfixe +237, ce canal terminera les appels à destination du Cameroun. Dans la suite nous présentons les méthodes de déploiement de la SIMBox.

4.3.4. Interactions et déploiement d'une architecture complète

4.3.4.1. Interactions entre équipements de la SIMBox [28]

Dans cette partie nous présentons un scénario complet des communications de la SIMBox, consigné dans la Figure 18 .

(1) Un appel vient du réseau VoIP externe vers le softswitch.

(2) Le commutateur logiciel envoie la demande de routage de l'appel au serveur de contrôle.

(3) Après le traitement de la demande (qui comprend des règles anti-spam), le serveur de contrôle répond avec la route appropriée (voice channel), le cas échéant. Dans le cas contraire, l'appel est abandonné. Le canal vocal est choisi en fonction de la politique définie dans le rôle 3 du serveur de contrôle (Page 32).

(4) Le softswitch achemine l'appel vers le voice server du voice channel sélectionné.

(5) Le voice channel termine l'appel vers le réseau cellulaire.

(6) Enfin, la connexion de l'appel est terminée.

(0) En tant qu'étape préalable, les canaux vocaux sont continuellement créés dans le système par les requêtes des SIM clients au serveur :

a. Lorsqu'un SIM client demande une carte SIM pour un canal GSM libéré, le serveur de contrôle recherche parmi les cartes SIM (par exemple, les SIM groups liés à son GSM group).

b. Ces cartes SIM sont ordonnées selon un critère permettant d'assurer la rotation des cartes SIM. Selon ce critère, la première carte SIM est choisie pour le canal GSM et des vérifications sont effectuées. Le serveur de contrôle vérifie la disponibilité de la carte SIM en fonction de ses paramètres de limitation d'activité (limitation de temps ou de crédit de communication). Si la carte SIM est indisponible, la carte SIM suivante est sélectionnée, et la même vérification est effectuée jusqu'à ce qu'une carte SIM appropriée soit trouvée.

c. Le serveur de contrôle vérifie ensuite si la carte SIM sélectionnée peut être connectée au canal GSM selon les configurations de sélection du canal GSM de la carte SIM pour la migration (page 38). Le serveur de contrôle choisit la première carte SIM qui valide les deux contrôles. Si aucune carte SIM ne valide, la procédure de création de voice channel est annulée et peut être reprise ultérieurement.

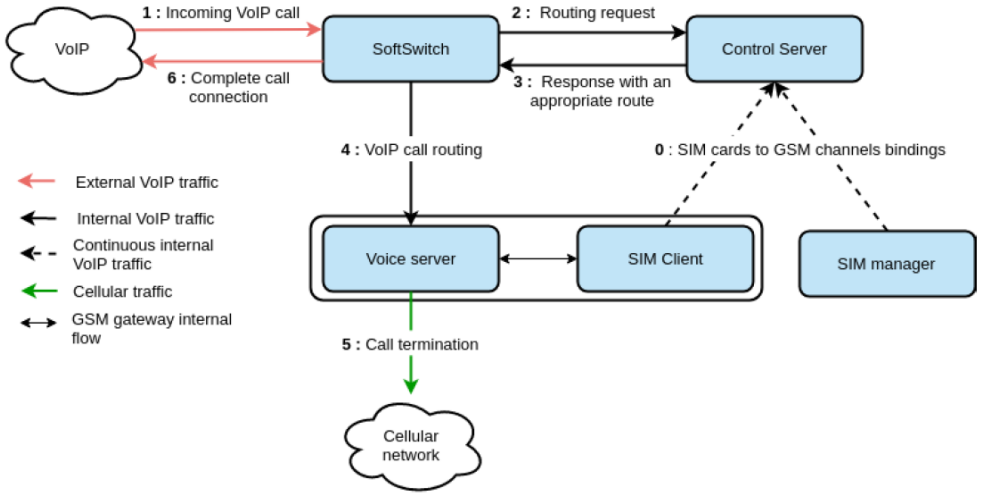


Figure 18: Diagramme de communication de la SIMBox : call-flow d'un appel [28]

4.3.4.2. Disposition géoraphique necessaire

En pratique, l'installation de ces différents composants dans le contexte d'une activité de terminaison d'appels dans un pays commence par le choix des différents emplacements des GSM gateways. Ces emplacements doivent être des lieux très fréquentés tels que les centres-villes, les immeubles de grande hauteur au centre du marché, les quartiers des gares, les zones de marché, les quartiers résidentiels denses ou les *call-centers*. Les endroits très fréquentés

permettent de camoufler les appels SIMBox par les flux massifs d'appels effectués dans ces zones.

Une fois la première condition remplie, les GSM gateways doivent être installées dans des lieux avec une alimentation stable et un accès à Internet à bon débit. Ces gateways sont ensuite connectées au système par des adresses publiques obtenues par NAT. D'autre part, la ou les SIMBank du système peuvent être situées n'importe où dans le pays cible ou même à l'étranger.

Dans l'architecture Hybertone, par exemple, l'environnement réseau entre le SIM Server, les SIMBank et les GSM gateways doit respecter :

- Un taux de retard de paquets de moins de **300ms**
- Perte de paquets inférieure à **1%**.
- La largeur de bande du réseau requise dépend du nombre de cartes SIM utilisées simultanément. Elle est à son maximum de **11Kbps** lors d'un enregistrement d'une GSM gateway.

Ainsi il est préférable d'avoir des SIMBank situées à l'endroit où réside l'administrateur du système afin qu'il puisse facilement ajouter ou retirer une carte SIM du système, si nécessaire. Le SIM Server, comme mentionné ci-dessus, est généralement hébergé sur un serveur privé, et son interface de visualisation et de configuration est accessible via un navigateur internet. Enfin, les softswitches qui émettent le trafic VoIP vers le système sont gérés par des partenaires frauduleux qui détournent le trafic et l'envoient conformément à un contrat prédéfini.

4.4. Stratégies de fraude à la SIM Box [28]

. Les opérateurs sont suffisamment outillés pour inférer un comportement très proche de celui d'une SIMBox (appels à des heures improbables, trafic trop élevé, sédentarité etc…) et de bloquer lesdites SIM. Les nouveaux modèles de SIMBox permettent donc de déjouer la vigilance des opérateurs en simulant le comportement humain. Cet ensemble méthodes est appelé *Human Behaviour Simulation* (HBS). Dans cette partie nous présentons ses différentes déclinaisons.

4.4.1. Rotation de cartes SIM

La rotation de cartes SIM permet d'utiliser plusieurs cartes SIM dans un canal GSM. Cela garantit la distribution du trafic de terminaison entre les cartes SIM du système, empêchant ainsi qu'une carte SIM ou un petit groupe de cartes ne soient utilisées de manière excessive pendant les heures de travail ou au-delà d'un certain seuil. Ainsi, les cartes SIM fonctionneront pendant un nombre limité d'heures par jour, simulant ainsi le comportement de clients réguliers. Le choix de la prochaine carte SIM à lier au canal GSM, peut déterminé par les algorithmes suivants :

- La méthode *round-robin* ou *constant method* place toutes les cartes SIM disponibles dans une boucle et choisit les prochaines à utiliser, étape par étape.
- La méthode *random* choisit aléatoirement une carte SIM parmi celles disponibles (la carte SIM active exclue).
- La méthode *statistic based factor* choisit la prochaine SIM selon les valeurs croissantes ou décroissantes d'un facteur particulier (temps de parole restant des cartes SIM, durée cumulée d'appel, nombre total d'appels ou le nombre total de SMS)
- La méthode *statistic based factor per time period* suit le même principe que la précédente, à l'exception du fait que les facteurs sont agrégés par période de temps.

4.4.2. Limitation de l'activité des cartes SIM

Un autre moyen de simuler le comportement humain c'est de fixer des limites d'activité des cartes SIM. Les limitations configurées permettent de verrouiller les cartes SIM du système automatiquement de telle sorte que le déverrouillage ne se fasse que manuellement ou automatiquement après une période définie. Les limitations sont classées comme suit :

Classe 1 – *Parameters limitations* : De nombreux facteurs liés au comportement des cartes SIM en matière d'appels et de SMS. Ils sont déduits en termes de nombre d'occurrences, de nombre total ou de durée totale.

Classe 2 - *Parameters limitations per time unit* : Certains paramètres sont agrégés et mesurés par unité de temps (jour, semaine et mois).

Classe 3 - *Time limitation* : Le système permet de fixer pour chaque carte SIM ou pour un groupe de cartes SIM, des périodes de travail, des temps de pause par jour ou des délais entre chaque utilisation. Pour certains systèmes, l'utilisateur peut sélectionner les jours de la semaine pendant lesquels une carte SIM ou un groupe de cartes SIM pourront fonctionner. Un groupe d'horaires par exemple, est caractérisé par deux propriétés nommées *reallocation interval* se rapportant au temps de travail et *sleep time* se rapportant à un temps de pause après chaque session de travail. Lorsque le temps de travail se termine, les cartes SIM et les canaux GSM annulent la liaison et se mettent dans un état d'hibernation. La durée de l'état d'hibernation est le sleep time.

4.4.3. Migration de cartes SIM

L'objectif de la migration de cartes SIM est de simuler la mobilité. En effet, l'équipement SIMBox est immobile (comme indiqué précédemment, son installation nécessite la mise en place d'un environnement favorable), ce qui ne correspond pas du tout au comportement d'un client ordinaire car les humains se déplacent et peuvent passer des appels à de nombreux endroits différents. Pour éviter d'être détectés, les SIMBox permettent de simuler des déplacements de cartes SIM en migrant leurs liens avec les canaux GSM d'une GSM gateway à l'autre (les GSM gateways étant situées à différents endroits de la ville).

Pour une carte SIM, le choix de la passerelle GSM à laquelle elle sera connectée s'effectue selon les méthodes suivantes :

- *Manually fixed method* : l'administrateur peut spécifier manuellement une liaison entre une carte SIM spécifique et un canal GSM spécifique. Par conséquent, la liaison sera arrêtée soit lors de la désactivation de l'un des deux éléments (canal GSM ou emplacement de SIM), soit manuellement par l'administrateur.
- *Any except previous :* une carte SIM peut s'enregistrer sur n'importe quel canal GSM, à l'exception d'une quantité déterminée des canaux précédents auxquels elle était liée. Le nombre de canaux GSM précédents est appelé profondeur de passerelle précédente (*previous gateway depth*).
- *Any except previous zone ID* : Une carte SIM ne doit pas sélectionner un canal GSM ayant le même ID de zone que le canal GSM précédent. De cette façon, les

cartes SIM changent automatiquement de canal GSM et d'emplacement à chaque réallocation.

- *Any gateway* : les cartes SIM s'enregistrent sur n'importe quelle gateway.
- *Specified order* : les cartes SIM s'enregistrent en fonction d'une liste de canaux GSM dont la séquence est définie. La liste comprend des canaux GSM sélectionnés parmi ceux disponibles et ordonnés selon une progression donnée définie par l'administrateur.

4.4.4. Changement/ verrouillage de station de base

Cette méthode permet de reproduire les micro mouvements des humains dans les cellules. En sélectionnant une station de base selon un critère, du point de vue de l'opérateur le terminal portant ladite carte SIM, soit la SIMBox, se déplace. Les différents critères de choix sont :

- Mode 1 – *Manually* : l'administrateur choisit la station de base à laquelle le canal GSM de la gateway se connectera ;
- Mode 2 – *Default* : le choix de la station de base se fait par défaut ;
- Mode 3 – *Fixed* : il verrouille le canal GSM a une station de base spécifique ou le limite à un choix entre jusqu'à trois stations de base
- Mode 4 – *Random* : la station de base est choisie aléatoirement mais selon les conditions, dont la puissance minimale du signal, la fréquence de changement de station de base, et selon si le système peut changer de station de base pendant un appel.
- Mode 5 – *Poll* : Ce mode permet à l'appareil de passer à la station de base suivante d'une liste ordonnée à une fréquence spécifiée. Cette liste est appelée *polling list* des stations de base. Elle rassemble toutes les stations de base environnantes dans l'ordre décroissant de l'intensité de leur signal, tel qu'enregistré par le module GSM. Le *maximum polling channel* définit le nombre maximum de stations de base dans la polling list. L'intervalle de changement de canal établit la fréquence d'occurrence du changement de station de base. La valeur de la fréquence peut être choisie de manière aléatoire à chaque commutation, entre une fourchette définie par l'administrateur. Une liste blanche et une liste noire de stations de base peuvent être

éditées pour définir les stations de base qui vont être utilisées dans le polling et les stations de base qui ne feront pas partie de la polling list respectivement ;

- Mode 6 – *Advanced* : Ce mode configure la commutation de station de base lors que le canal GSM, atteint une valeur limite, selon certains paramètres.

4.4.5. Changement d'IMEI

Une GSM gateway compte un IMEI par canal GSM. De ce fait, toutes les cartes SIM utilisées par un canal GSM correspondent à l'IMEI de ce canal GSM dans les CDR des opérateurs mobiles. C'est un moyen évident de détecter les SIMBox, car l'utilisation d'un grand nombre de cartes SIM dans un seul appareil mobile est assez inhabituel. La SIMBox offre la possibilité de définir un IMEI à n'importe quelle carte SIM utilisée pour surmonter cette faiblesse et simuler le comportement d'un client normal. Selon le fabricant de la SIMBox, les changements d'IMEI peuvent être effectués soit sur les canaux GSM ou pour chaque carte SIM.

Les changements liés au canal GSM peuvent être faits manuellement par l'administrateur ou automatiquement. Dans ce dernier cas, l'IMEI est modifié selon :

- Une fréquence spécifiée (par défaut par heure et pas plus que toutes 10 minutes),
- Un seuil sur le nombre d'appels effectués par le canal (pas moins de 10) et chaque fois qu'une carte SIM change.

Les changements au niveau de la carte SIM sont soit manuels, soit automatiques. Appliqués à un groupe préformé de cartes SIM selon l'un des schémas suivants : aléatoirement ou basé sur un préfixe (similaire à l'aléatoire, mais avec un préfixe), basé sur le Type Allocation Code (TAC qui est la partie initiale à huit chiffres de l'IMEI à 15 chiffres et de l'IMEISV à 16 chiffres utilisés pour identifier de manière unique les appareils sans fil), ou basé sur un registre (le code IMEI complet provient d'une liste d'IMEI).

4.4.6. Utilisation d'autres services du réseau

L'utilisation principale des cartes SIM de SIMBox est de terminer le trafic voix par le biais d'appels téléphoniques. C'est une faiblesse car les utilisateurs réguliers utilisent d'autres services tels que les SMS, les commandes USSD et internet. Certaines SIMBox permettent d'utiliser les services SMS/MMS ou l'Internet, et d'envoyer des commandes USSD, afin de simuler ce comportement humain.

4.4.7. List of family

Cette stratégie consiste à construire une famille virtuelle de contacts dans le réseau pour chaque carte SIM utilisée dans la SIMBox. En effet, les cartes SIM utilisées par le SIMBox effectuent plusieurs appels sortants vers un grand nombre de consommateurs de réseau non apparentés, dans le cadre de la terminaison du trafic vocal. Il s'agit d'un comportement anormal car la plupart des consommateurs réguliers n'appellent et reçoivent des appels d'un groupe restreint de consommateurs du réseau, appelé *list of family*, ou famille de contact qui, dans certains cas, passent également des appels entre eux. Par conséquent, certaines SIMBox offrent la possibilité d'échanger des SMS et du trafic vocal entre les différentes cartes SIM du système de sorte que ces cartes SIM constituent une list of family pour chacune d'entre elles. Les fonctions associées sont :

- SMS inter-sending : envoi automatique de messages entre membres
- Inter-calling : appels automatiques entre membres

4.4.8. Redirection d'appels

La fonction de transfert d'appel permet de transférer un appel destiné à une carte SIM utilisée dans la SIMBox vers un numéro spécifique afin qu'un complice humain puisse répondre à l'appel.

4.4.9. Autres fonctionnalités de la SIM Box

4.4.9.1. Anti-spam

C'est une méthode qui consiste à établir des listes afin de filtrer les appels. On peut en configurer trois types :

- White list : les numéros autorisés à faire des appels sortants
- Grey list : les numéros autorisés à appeler mais moyennant certaines conditions
- Black list : les numéros qui ne peuvent faire d'appels sortants

4.4.9.2. Configuration des codecs pour la voix

Les configurations de la voix et des codecs utilisés par le système, peuvent améliorer la qualité de l'appel. Ceci est utile pour les fraudeurs car certaines méthodes de détection sont

basées sur l'identification des chutes de qualité des appels audio (pertes de paquets et gigue). La SIMBox dispose d'une variété de codecs. L'utilisateur peut les activer et les ordonner en fonction de ses préférences. Certains codecs sont : G.711 a-law, G.711 -law, G.723, G.723.1, G.729, G.729-16, G.729-24, G.729-32, G.729-40, G.729A et G.729AB.

4.4.9.3. Gestion des CDR

La SIMBox fournit des CDR générés par son activité pour la gestion du trafic et de la comptabilité. Les CDR sont sauvegardés soit sur un disque externe, soit sur un serveur auquel il est possible de faire des requêtes. Les requêtes visent à obtenir des enregistrements CDR qui répondent à certaines conditions sur la durée de l'appel, les identifiants de l'appelant et de l'appelé, le début de l'appel, l'heure de fin d'appel et le type d'appel etc. Elles permettent aux fraudeurs d'identifier les cartes SIM/canaux GSM qui peuvent avoir un comportement suspect et ainsi affiner leur activité.

SYNTHÈSE

Dans cette partie, il a été question pour nous de vous présenter les réseaux mobiles dans leur fonctionnement global, d'une part et d'autre part de présenter la fraude à la SIMBox de façon sommaire. Nous constatons ainsi que la SIMBox est une méthode de fraude qui s'incorpore pratiquement parfaitement au réseau mobile et permet aux fraudeurs de tromper la vigilance des opérateurs dans la terminaison des appels.

Partie 2: PROBLÉMATIQUE

DESCRIPTION

Dans cette partie il sera question pour nous de présenter les différents challenges à relever par les opérateurs de réseau mobile par rapport à la fraude à la SIMBox et d'énoncer le problème que nous voulons résoudre dans notre travail.

PLAN :

1. CHALLENGES POUR LES OPERATEURS DE RESEAUX MOBILES

Les opérateurs de téléphonie mobile font face à plusieurs challenges. On peut citer :

- L'explosion du marché des télécommunications ;
- La prolifération de la fraude à la SIMBox ;
- L'évolution de la fraude.

1.1. L'explosion du marché des télécommunications

Dans le monde, le nombre d'abonnés au réseau de télécommunications mobiles a subi une importante croissance passant de 2 Milliards d'abonnées en 2006 à environ 7.95 milliards d'abonnés en 2019 selon [34]. Une Augmentation qui témoigne le succès de ce secteur dans l'économie mondiale.

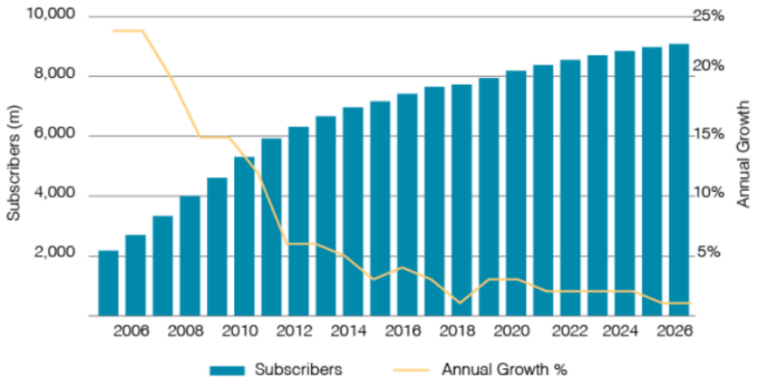


Figure 19: Evolution du nombre d'abonnés mobile dans le monde sur la période 2006-2026 [34]

Au Cameroun depuis 2007, nous constatons une augmentation vertigineuse du nombre d'abonnés au réseaux mobiles. Selon l'ART le Cameroun est passé de 4 Millions d'abonnés en 2007 à 14 Millions d'abonnés en 2013, pour atteindre 19,7 Millions d'abonnés en 2017. Cette croissance exponentielle du nombre d'abonnés contribue à la dissolution du trafic frauduleux parmi les utilisateurs réguliers.

1.2. Les facteurs de prolifération de la fraude

La fraude à la SIMBox cause des pertes importantes pour les opérateurs de télécommunications, et sa proportion est encore considérable au point où en 2019, plus de **80%** des opérateurs de téléphonie mobile africains en ont été victimes [35]. La Communications

Fraud Control Association (CFCA) réalise une enquête tous les deux ans, pour faire l'état de la fraude chez les opérateurs. Dans cette étude pour le compte de la session de 2019, elle a montré que les pertes mondiales dues à la fraude étaient estimées à **28,3 milliards de dollars (USD)**. Cela correspondait à **1,74 %** des revenus mondiaux estimés pour 2019 dans le secteur des télécommunications dans le monde qui s'élevaient à **1,625 trillions de dollars USD** [2]. Il s'agit d'une augmentation par rapport aux chiffres de 2017 de **1,27%**. La fraude par contournement (bypass fraud) dont fait partie la SIMBox, est classée 3^{e} parmi les types de fraudes et est responsable d'une perte de **2.71 milliards de dollars (USD)** [2]. Cela dû à des facteurs à de nombreux facteurs dont, l'immense différence entre ITR et LTR, l'accès facile aux cartes SIM prépayées, la corruption, la différence dans la réglementation des télécommunications, que nous présenterons tour à tour.

1.2.1. L'immense différence entre International Termination Rates (ITRs) and Local Termination Rates (LTRs)

C'est le carburant de la fraude à la SIMBox. La terminaison d'un appel peut être segmentée en trois parties, chacune impliquant un coût :

(1) La transmission nationale de l'appel depuis le terminal d'origine jusqu'à la passerelle internationale du pays d'origine,

(2) L'acheminement de l'appel depuis la passerelle internationale du pays d'origine vers le pays de destination,

(3) L'accès à l'infrastructure de l'opérateur mobile de destination pour la terminaison de l'appel, constituant par ailleurs le coût le plus important. Le Tableau 3 montre les destinations les plus intéressantes pour la terminaison d'appels.

Country	Population	Mobile penetration	Local call rate
1- Nigeria	203 million	75%	$0.042- $0.048
2- Côte d'Ivoire	25.9 million	128%	$0.1
3- Tanzania	58.9 million	90%	$0.12
4- Mali	19.9 million	91%	$0.17
5- Algeria	43.5 million	117%	$0.02-$0.22

Tableau 3: Top 5 des destinations pour la terminaison d'appels en Afrique [34]

1.2.2. Un accès facile aux cartes SIM prépayées

La fraude à la SIMBox nécessitant un grand nombre de cartes SIM, et surtout les fraudeurs n'ayant pas envie que leurs informations personnelles soient découvertes, la carte

SIM prépayée constitue le graal pour cette fraude. Cela car elle ne nécessite pas d'information précise sur son possesseur avant utilisation. En effet, en moyenne, **94%** des abonnements mobiles en Afrique sont prépayés, on en compte environ **80 %** au Moyen-Orient et **75%** dans le monde [36].

1.2.3. La corruption dans l'industrie des télécommunications

L'écosystème de la fraude à la SIMBox ne se limite pas à l'aspect technique. En effet les fraudeurs utilisent d'autres moyens frauduleux pour rendre leur business plus efficace. En effet les fraudeurs les plus avertis gagnent suffisamment d'argent pour soudoyer autant le revendeur de cartes SIM en kiosque, que les responsables d'équipe au sein des opérateurs.

1.2.4. Les différences dans la règlementation des télécommunications

Les pays n'étant pas soumis à la même législation en termes de télécommunications, les fraudeurs peuvent jouer sur ces failles pour se faire de l'argent. Notamment via les grey routes. Ce sont des routes qui sont légales à l'un des deux bouts de la communication, et illégales à l'autre. Leur utilisation massive permet aux fraudeurs d'éviter de payer des frais supplémentaires.

1.3. Evolution de la SIMBox

D'après l'enquête de 2019 du CFCA, **73 %** des opérateurs ont déclaré que les pertes dues à la fraude avaient augmenté ou étaient restées les mêmes [37]. Cela témoigne de l'évolution des méthodes de fraude. Au fil du temps, la SIMBox étend ses limites matérielles pour fournir une plus grande capacité de terminaison et de nouvelles architectures. Les fonctionnalités existantes sont affinées pour ressembler de plus en plus au comportement humain, posant ainsi de réels problèmes dans la détection.

2. ENONCE DU PROBLEME

Actuellement dans le monde et plus spécifiquement en Afrique et au Moyen-Orient, la fraude à la SIMBox engendre de lourds manques à gagner chez les opérateurs de téléphonie mobile. Notre travail se résume donc à la problématique suivante :

« Comment détecter la fraude à la SIMBox au sein d'un opérateur de télécommunications ?» de manière à :

- **Réduire le manque à gagner pour les opérateurs ;**
- **Réduire au maximum le nombre de faux positifs/ faux négatifs ;**
- **Réduire le cout de déploiement des techniques de détection de la fraude à la SIMBox ;**
- **Ouvrir une brèche dans la recherche pour la détection en temps réel de la fraude à la SIMBox.**

SYNTHÈSE

Dans de cette partie il a été question pour nous présenter la problématique de notre sujet de mémoire. Il en ressort que du fait de l'explosion du marché des télécommunications, de l'existence de facteurs de la prolifération de la fraude et de son évolution vertigineuse, il en ressort que développement d'une méthode efficace pour la détection de la fraude devient une évidence. D'où le thème de notre mémoire **« Déploiement et configuration d'une architecture matérielle de capture et d'analyse de la signalisation des réseaux cellulaires pour la détection des fraudes a la SIMbox. »**

CHAPITRE II : MÉTHODOLOGIE

Partie 1 : ETAT DE L'ART

DESCRIPTION

Malgré la dangerosité de la fraude à la SIMBox, il n'y a que très peu de recherche faite pour favoriser le déploiement de solutions efficaces. Cette partie nous permettra de présenter les méthodes existantes de détection de la fraude à la SIMBox, notamment les méthodes passives et actives, de les comparer et d'expliquer les raisons du choix de la méthode que nous avons exploré. Tout cela sur la base des informations proposées dans [28].

PLAN :

1. LES METHODES PASSIVES

Ce sont des méthodes qui ne nécessitent pas une action humaine permanente. Elles sont basées sur l'analyse de données de type différents.

Il en existe plusieurs parmi lesquelles :

- L'analyse basée sur les CDR ;
- L'analyse basée sur la qualité audio ;
- L'analyse basée sur la signalisation ;

1.1. Analyse basée sur les CDR

C'est une méthode passive qui consiste à analyser à la fois le contenu et les occurrences des CDR (Call Detail Records) qui sont des données qui répertorie l'activité dans le réseau, en termes d'appel, de SMS et d'internet. Cette méthode se base sur le Machine Learning pour faire sortir des anomalies dans ce grand jeu de données. C'est un problème de classification. Elle se fait en plusieurs étapes :

- **Préparation des données** : c'est une étape qui consiste à identifier les caractéristiques basées sur les données dans les CDR. On a :
  - La fréquence d'appels
  - La mobilité
  - L'utilisation des services mobiles
  - Propriétés des entités (les informations sur le terminal mobile)
- **Création et évaluation du modèle** : des méthodes de classification sont utilisées dont, Artificial Neural Network (ANN), Support Vector Machine (SVM), Fuzzy Logic, Random Forest. Ces modèles offrent des résultats pertinents mais leur efficacité peut être réduite par le HBS.

1.2. Analyse basée sur la qualité audio

Cette méthode consiste à analyser des enregistrements audios, qui révèlent un certain nombre d'informations sur le trafic. Notamment la source et le type de réseau téléphonique

utilisé, à partir d'une analyse des pertes de paquets et du bruit. Cette analyse approfondie peut permettre de dire, à partir de la dégradation de la qualité, si ce trafic vient d'un routage par la SIMBox.

1.3. Analyse basée sur la signalisation

C'est une méthode récente et pas suffisamment exploitée. Elle a été suggérée en 2015 par LATRO Services dans [7] et semble très prometteuse. L'idée est d'analyser la signalisation d'un utilisateur pour chacune de ses activités dans le réseau. A partir des protocoles connus de la pile protocolaire LTE, on peut extraire des informations sur l'utilisateur, et rechercher une caractéristique particulière, propre à la SIMBox. On peut, dans ce but, s'intéresser à des évènements particuliers tels que l'attachement au réseau et ainsi bloquer une carte SIM de la SIMBox dès sa première connexion au réseau.

2. LES METHODES ACTIVES

Ce sont des méthodes qui nécessitent une activité humaine permanente dans leur déploiement. Ce sont les méthodes les plus classiques qu'utilisent les opérateurs et demandent de grandes ressources matérielles. On peut citer :

- Test Call Generators ;
- Rule-based method in Fraud Management System (FMS)

2.1 Test call generators (TCG)

Les opérateurs télécoms utilisent les TCG pour consolider leurs stratégies d'assurance des revenus. Ils fournissent des tests automatisés en exécutant des appels en direct sur le réseau de l'opérateur pour identifier les problèmes potentiels de performance du réseau et les fuites de revenus. Les TCG produisent des CDR indépendants qui sont comparés aux CDR des opérateurs afin de valider l'intégrité des CDR et, en fin de compte, de découvrir les pertes de revenus. Voici quelques services offerts par TCG :

- Test en temps réel de plusieurs services d'appel et de données, par exemple voix, SMS, MMS, HTTP, télévision mobile, appels vidéo, téléchargement de contenu (jeux, sonneries, etc.).
- Réconciliation de bout en bout de la fiche d'appel (du commutateur à la facturation)
- Tests de vérification des nouveaux tarifs
- Réconciliation de la correspondance des CDR
- Validation de la tarification des appels pour la facturation d'interconnexion
- Tests de conformité réglementaire
- Tests de performance du réseau pour valider les nouveaux composants du réseau

Pour la détection de la SIMBox on réalise ses tests pour des appels internationaux et on, analyse la conformité des routes. C'est une méthode qui a peu de faux négatifs mais elle est très coûteuse à mettre en place.

2.1 Méthode basée sur des règles (rule-based method in Fraud Management System)

Les méthodes basées sur des règles [38] consistent à établir des règles de base pour le profilage des abonnés afin d'identifier les cartes SIM frauduleuses. Cela implique l'analyse et la surveillance des modèles d'appels (nombre d'appels sortants, ratio de destinations distinctes, sites cellulaires utilisés, rapport entre appels entrants et sortants, SMS, etc.) d'un ensemble d'abonnés par des experts à la recherche d'un comportement anormal provenant de la carte SIM d'un opérateur ou aboutissant sur celle-ci. Tout cas identifié et validé (par un appel ou une action similaire) peut alors être utilisé pour profiler et découvrir d'autres cartes SIM similaires.

Cette méthode est peu coûteuse et était très efficace pour les modèles de SIMBox n'implémentant pas la simulation du comportement humain. Par contre pour les nouveaux modèles implémentant HBS, le nombre de faux positifs devient plus élevé.

3. CHOIX DE LA METHODE UTILISEE

Au regard de toutes ces méthodes nous allons faire une étude comparative afin de mettre en évidence la pertinence de la méthode basée sur la signalisation.

Tableau 4: Comparaison des méthodes de détection de la fraude à la SIMBox

Méthode	Avantages	Inconvénients	Contre-mesures
TCG	Pas de faux positifs	Coûteuse	• Anti-spam • Sacrifice de cartes SIM
Rule-based	• Moins coûteuse • Grande couverture	• Monitoring constant • Grand nombre de faux positifs • Explosion du nombre de règles	HBS
Signaling-based	• Très précise • Détection en temps réel • Peu coûteuse	• Accessibilité des données • Complexité de l'analyse	
CDR-based	• Très efficace avec une bonne base de données	• Dépend des données de terrain (biais)	HBS

	• Evolution des techniques de ML	• Durée de détection énorme	
Audio quality	• Détection en temps réel	• Augmentation des faux positifs avec la qualité de la voix sur IP (5G, 6G)	Amélioration de la qualité du réseau IP entre équipements de la SIMBox

Ce tableau révèle que la méthode basée sur la signalisation est très efficace, peu coûteuse et à ce jour il n'existe pas encore de contre mesure du côté des fraudeurs.

SYNTHESE

Dans cette partie il a été question pour nous de présenter d'un point de vue scientifique et technique les travaux qui ont déjà été effectués sur la détection de la fraude à la SIMBox. Sur cette base nous avons pu sélectionner une méthode que nous allons implémenter.

Partie 2 : ANALYSE ET CONCEPTION

DESCRIPTION

Dans cette partie nous ferons une analyse approfondie de la méthode basée sur la signalisation, en présentant chacun des aspects et caractéristiques sur lesquelles nous nous baserons pour mener notre expérience.

PLAN :

1. HYPOTHESE DE BASE

Pour analyser la signalisation à notre niveau, nous avons recherché des variables caractéristiques qui nous permettront de distinguer la SIMBox des terminaux réguliers. Pour retrouver de telles variables nous avons étudié la signalisation dans le cas de l'attachement au réseau. Cette signalisation est précieuse car non seulement elle ne peut être modifiée par les fraudeurs, mais aussi elle permet de détecter les fraudeurs dès leur entrée dans le réseau.

Pour ce faire nous nous sommes intéressés à la latence de communications. Comme présenté à la page 31, la SIMBank est le lieu où l'on insère physiquement les cartes SIM, mais ne communique pas avec la station de base. Elle communique les informations à la gateway via IP, qui ensuite communiquera avec la station de base. Ainsi avant toute interaction avec la station de base, il y a une communication IP entre équipements de la SIMBox et de ce fait une latence supplémentaire indépendante du réseau LTE.

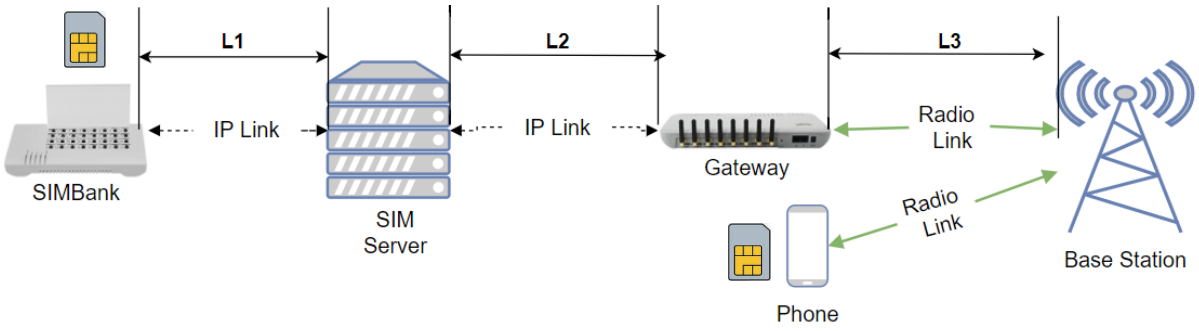


Figure 20: Latences supplémentaires dans la communication de la SIMBox

La Figure 20 nous montre que dans le cas de la SIMBox, il y a deux latences supplémentaires **L1** et **L2** qui s'ajoutent à **L3** qui elle, est la latence normale du réseau LTE. Ainsi nous nous attendons à ce que la latence de communication entre la station de base et la SIMBox soit plus élevée que celles des terminaux réguliers. Nous avons ainsi obtenu un critère de classification.

« **Notre hypothèse fondamentale réside donc dans le fait que la latence des communications IP entre équipements de la SIMBox est suffisamment grande par**

rapport à celle des terminaux réguliers pour faire la distinction. Ainsi il est possible détecter un utilisateur frauduleux localement en analysant la signalisation d'une station de base, et plus encore le faire dès son entrée dans le réseau via la signalisation de la procédure d'attachement. ».

2. SYNTHESE DES PROBLEMES ET SOLUTIONS

2.1. Difficultés liées à cette solution

Comme précédemment mentionné l'analyse de la signalisation pour la détection de la SIMBox est une solution peu explorée. Nous utilisons une méthode jamais encore utilisée et de ce fait des obstacles notables se sont présentés. On distingue notamment :

- La rareté d'articles scientifiques traitant du sujet ;
- L'accès difficile aux données de signalisation auprès d'opérateurs en production, sans lesquelles aucune analyse n'est possible ;
- La nécessité de reproduire l'écosystème de la fraude pour des tests. Et donc de ce fait des autorisations auprès d'opérateurs ;
- Les coûts de déploiement de station de base ;
- Les coûts très élevés d'acquisition de fréquences, même pour es raisons expérimentales par SDR.

2.2. Propositions de solution

La plupart des inconvénients de la méthode que nous souhaitons implémenter sont d'ordre matériel. Le Tableau 5 suivant présente les solutions que nous avons mis en place à chaque difficulté précédemment mentionnée.

Tableau 5: Tableau problème – solution de la méthode de détection à développer

Problème	Solution

Rareté d'articles sur le sujet de la détection basée sur la signalisation	Etude des normes de réseaux cellulaires
Accès difficile aux données de signalisation	Déploiement d'un opérateur privé, de manière à ne pas perturber de réseau en production, et de gagner du temps dans les procédures administratives.
Nécessité de reproduire l'écosystème de la fraude	Déploiement de la SIMBox (d'un fabriquant quelconque, HyberTone dans notre cas) dans un opérateur privé.
Coûts de déploiement de station de base	Utilisation de la technologie SDR, qui permet de déployer une station de base via une carte électronique à moindre coût.
Règlementation sur les fréquences	Expérimentation dans une cage de Faraday, pour empêcher les interférences sur les bandes de fréquences d'autres opérateurs.

SYNTHÈSE

Dans cette partie, il a été question pour nous de présenter les méthodes de détection précédentes, d'en ressortir les points forts et les points faibles, de manière illustrer les raisons de notre choix d'explorer la méthode de détection basée sur la signalisation. Il en ressort que la méthode de signalisation est plus intéressante du fait de sa grande précision, de son coût de déploiement peu élevé et du fait qu'il n'existe encore aucune contre-mesure du côté des fraudeurs. Ensuite nous avons présenté notre démarche dans l'expérimentation de notre solution.

Partie 3 : MODÉLISATION

DESCRIPTION

Dans cette partie nous parlerons des différentes architectures déployées pour la réalisation de notre expérience. Nous présentons, ensuite l'analyse des résultats de cette dernière.

PLAN :

1. ARCHITECTURES DE RESEAU

Dans le cadre de notre projet de fin d'études nous devons déployer et configurer une architecture matérielle qui va nous permettre de détecter la SIMBox parmi les utilisateurs normaux. Dans cette phase du travail, nous allons monter une architecture qui nous permettra d'obtenir de la signalisation autant de SIMBox que d'utilisateurs réguliers. Nous avons trois architectures principales à tester pour comparer les latences dans chacun des cas.

- Architecture avec une gateway seule ;
- Architecture complète de SIMBox, connectée en réseau local ;
- Architecture complète de SIMBox, connectée via internet ;

1.1. Architecture avec gateway seule

C'est le cas élémentaire de fraude à la SIMBox, dans ce cas-là il n'y a pas de communication IP entre équipements. La carte SIM est directement connectée à la gateway et communique directement avec la station de base. Ainsi à priori elle est similaire à un téléphone normal.

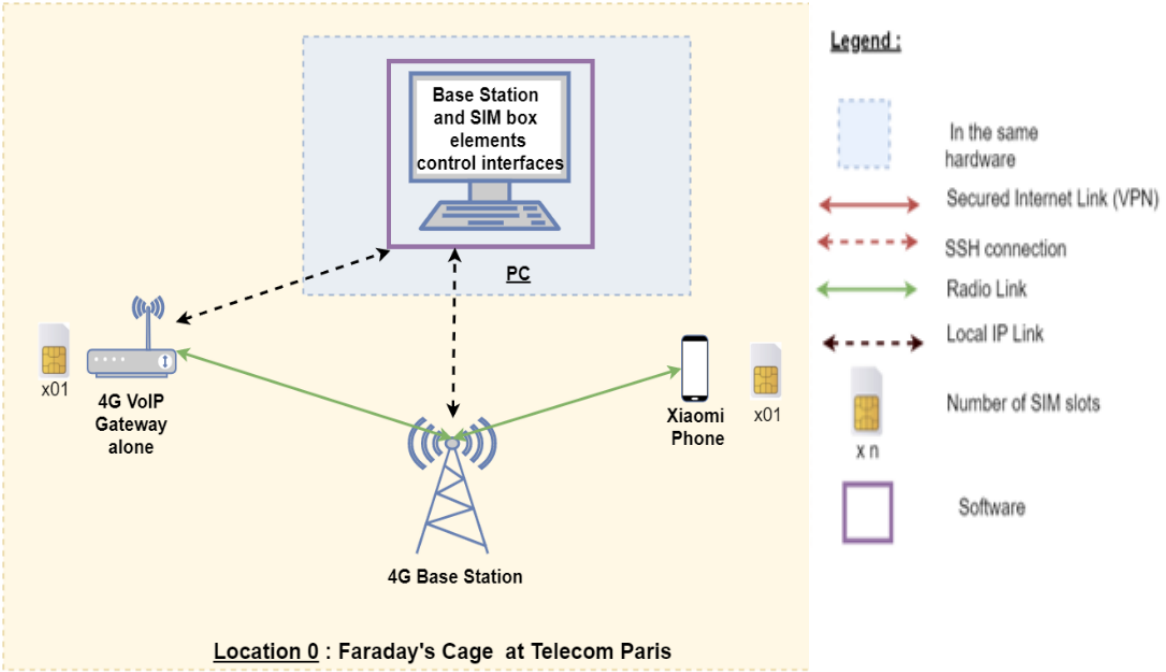


Figure 21: Architecture de SIMBox avec une gateway seule

1.2. Architecture complète de SIMBox connectée en réseau local.

Dans ce cas, nous déployons la SIMBox avec tous ses composants, mais connectés en local de manière à réduire au maximum la latence au niveau IP. Nous avons inséré une carte SIM dans la SIMBank, elle-même placée dans la même salle que la Gateway. Ainsi nous nous sommes assurés de créer une seule liaison « carte SIM - canal GSM » (voice channel) que nous avons configuré.

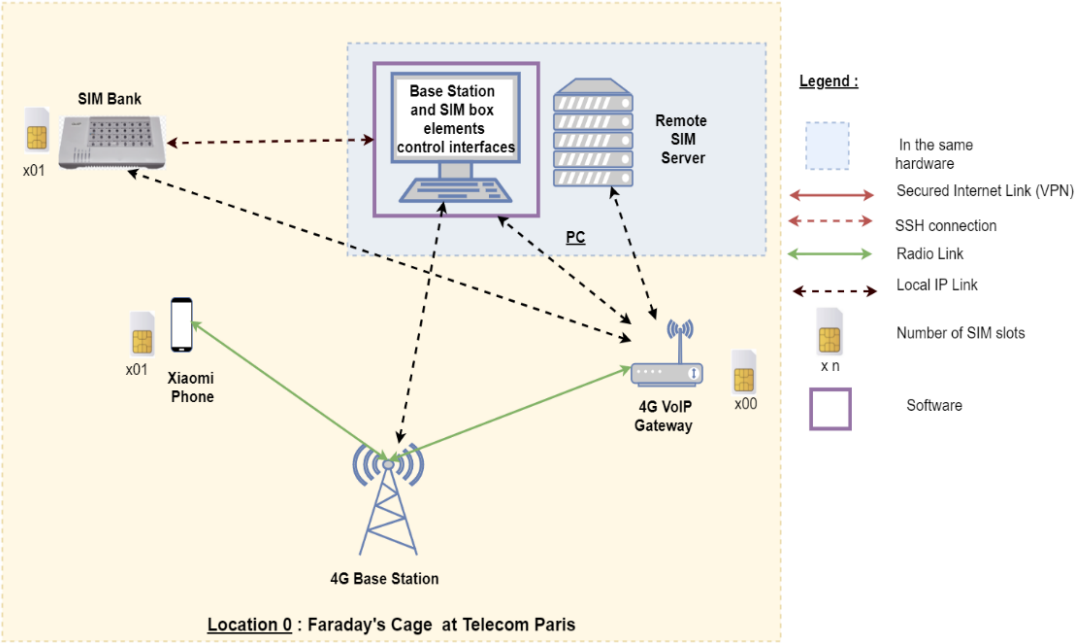


Figure 22: Architecture de SIMBox complète connectée en réseau local

1.3. Architecture complète de SIMBox connectée via internet.

Dans ce cas-ci nous voulons simuler le comportement de la SIMBox de manière plus réaliste en connectant les équipements sur deux sites différents en utilisant internet. Nous avons déployé la topologie dans le but de se mettre dans des conditions réalistes, pour se rapprocher au maximum. Pour que cette topologie puisse fonctionner, il est nécessaire d'activer le *port forwarding* sur le routeur derrière lequel se trouve le SIM Server, afin de rediriger vers lui tout flux en direction des ports concernés (TCP 56012 et UDP 56011 par défaut).

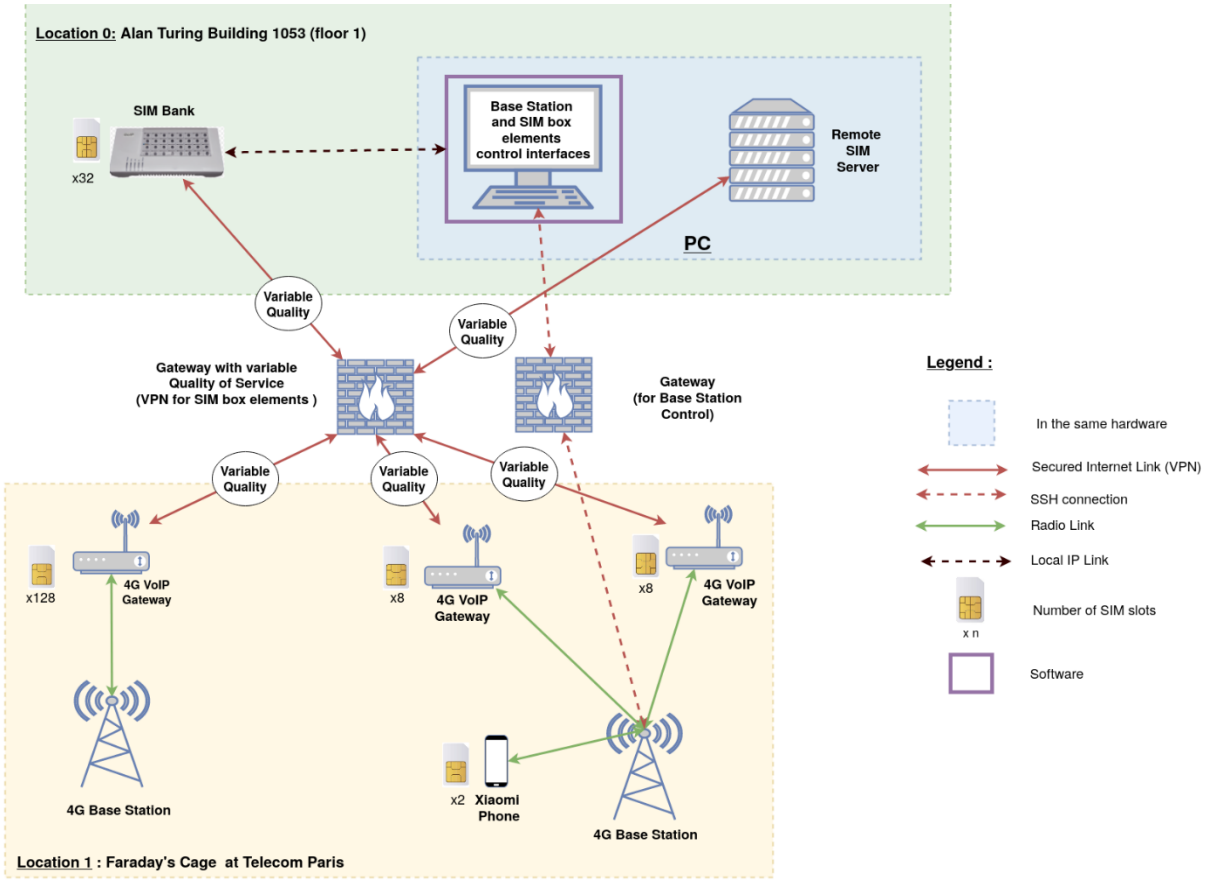


Figure 23: Architecture de SIMBox complète connectée via internet

2. CONDITIONS EXPERIMENTALES

Pour réaliser notre simulation et collecter des traces d'interactions entre station de base et les terminaux, nous nous sommes placés dans les conditions suivantes :

- Toute expérience doit être faite dans la cage de faraday (Figure 24)
- Par rapport à la station de base, tous les équipements communiquant sur la voie radio étaient à la même position.
- La station de base et les terminaux sont en visibilité directe
- Atténuation négligeable
- Paramètres de la station de base :

- **Fréquence: 2680 MHz (UL) and 2560 MHz (DL)**
- **Mode: FDD**

- Variations du débit de l'interface Ethernet du SIM server (10 Mbps, 100 Mbps, 1000 Mbps) à l'aide du package linux **ethtool ;**
- Mesure du débit à l'aide du package linux **speedtest ;**
- Capture de paquets IP à l'aide de **Wireshark** activé sur l'interface Ethernet du SIM server.

Figure 24: Images de cage de faraday en extérieur et à l'intérieur [40]

3. CALCUL DE LA LATENCE DE LA PROCEDURE D'ATTACHEMENT

3.1. La procédure d'attachement au réseau LTE

Dans cette partie nous nous intéressons à la procédure d'attachement qui peut nous permettre, conformément a l'hypothèse de départ de détecter la SIMBox dès son entrée dans le réseau et avant la fraude. Afin de pouvoir calculer la latence, nous avons observé le flux des messages de signalisation échangés entre équipements pendant ladite procédure. La procédure est résumée dans la Figure 25.

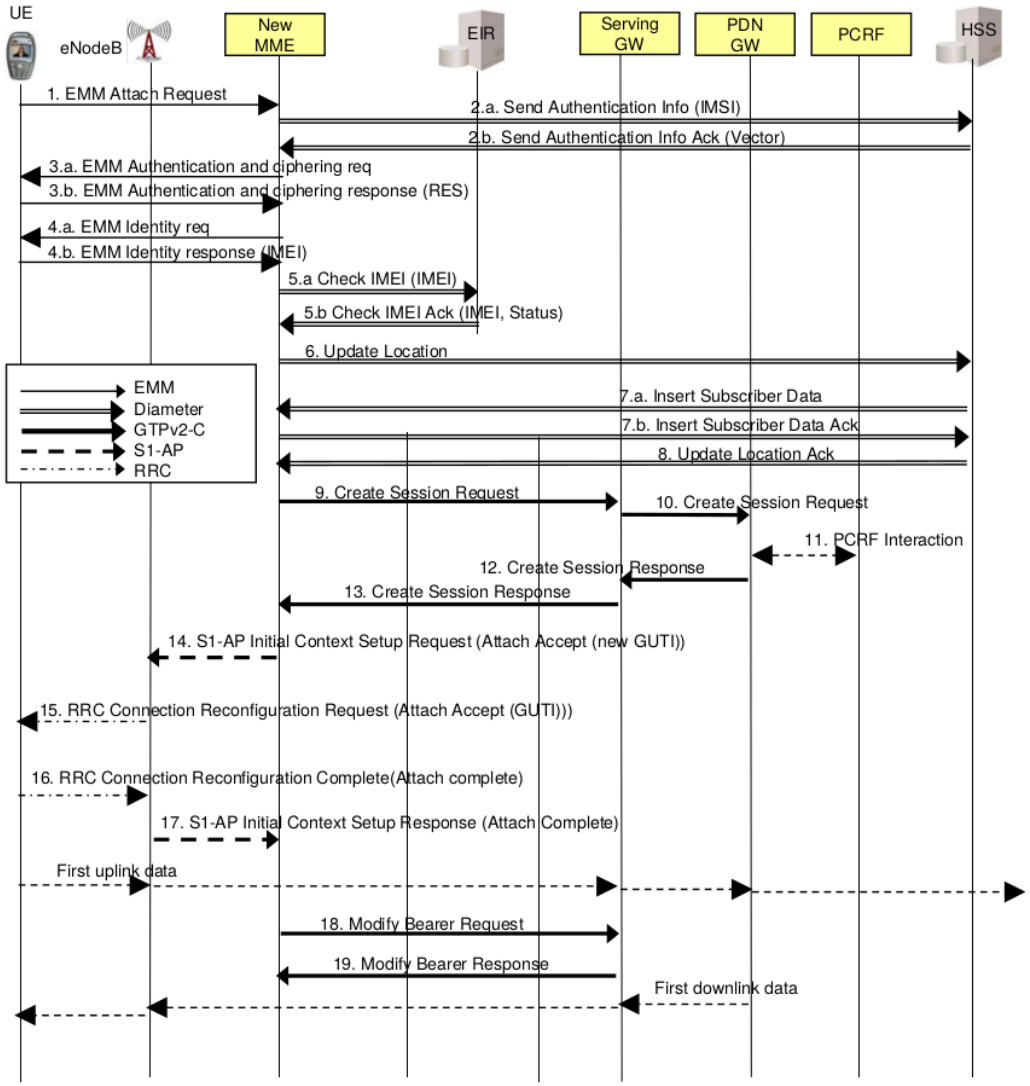


Figure 25 : Attachement au réseau EPS [13]

Cette procédure correspond à un attachement au réseau EPS qui conduira à la création d'un default bearer permanent correspondant à une connectivité IP permanente à un réseau IPv4 ou IPv6 [13] .

1. L'UE initie la procédure d'attachement en émettant une requête ***Attach Request*** à l'eNodeB. Cette requête contient son GUTI et l'identité de l'opérateur auquel l'UE souhaite se rattacher.
2. Le MME obtient auprès du HSS disposant du profil de l'UE, des quintuplets d'authentification à l'aide de la requête ***Send Authentication Info***.

3. Le MME soumet une valeur aléatoire à l'UE et escompte une réponse de l'UE contenant un résultat d'authentification égal à celui fourni par le HSS. L'UE retourne la réponse au MME.
4. Le MME demande à l'UE de lui fournir son IMEI.
5. L 'EIR, interrogé par le MME indique dans le message de retour si le terminal fait ou ne fait pas partie de la liste des équipements interdits (black list).
6. Le MME délivre un message ***Update Location*** (adresse MME sous forme de hostname, IMSI) au HSS.
7. Le HSS émet un message ***Insert Subscriber Data*** (IMSI, données de souscription EPS) au nouveau MME. Le nouveau MME retourne une ***réponse Insert Subscriber Data Ack*** (IMSI) au HSS.
8. Le HSS acquitte la mise à jour de localisation par une réponse ***Update Location Ack*** au MME. En cas de rejet de la procédure de mise à jour de localisation, le MME rejette la demande d'attachement de l'UE.
9. Le MME sélectionne un S-GW et assigne une valeur au paramètre EPS Bearer Identity (BI) pour le bearer par défaut associé à cet UE. Puis, il émet une requête ***Create Session Request*** (pour la création du default bearer) au S-GW sélectionné.
10. Le S-GW crée une nouvelle entrée dans sa table d'EPS bearer et émet à son tour une requête ***Create Session Request*** au P-GW.
11. Le P-GW interagit avec le PCRF afin d'obtenir les règles de taxation permettant de différencier les flux de service qui transiteront par le default bearer et ainsi différencier la taxation de ces flux.
12. Le P-GW retourne une réponse ***Create Session Response*** au S-GW contenant l'adresse IP allouée à l'UE.
13. Le S-GW retourne une réponse ***Create Session Response*** au MME.
14. Le MME émet un message ***Initial Context Setup Request***, afin de demander à l'eNodeB de créer un bearer d'accès entre l'UE et le S-GW.
15. L'eNodeB émet un message ***RRC Connection Reconfiguration request*** incluant l'identité du bearer d'accès et le message ***Attach Accept*** contenant le GUTI assigné à l'UE par le MME.

16. L'UE retourne une réponse ***RRC Connection Reconfiguration Complete*** à l'eNodeB incluant le message ***EMM Attach Complete***.
17. L'eNodeB retourne le message ***Initial Context Response*** au MME. L'UE peut à partir de ce moment émettre des paquets IP dans le sens montant vers l'eNodeB qui les routera sur le tunnel GTP-U au S-GW qui à son tour les relayera aussi sur un tunnel GTP-U au P-GW.
18. A la réception du message ***Initial Context Response*** et de l'***Attach Complete***, le MME émet une requête ***Modify Bearer Request*** au S-GW.
19. Le S-GW l'acquitte en retournant une réponse ***Modify Bearer Response*** (Identité du bearer EPS) au MME. Le S-GW est dès à présent prêt à relayer les paquets IP, qu'il a pu mettre temporairement en mémoire tampon, dans le sens descendant à l'UE à travers l'eNodeB.

3.2. Méthode de calcul de la latence

Dans cette partie nous présentons la méthode utilisée pour calculer la latence de la procédure d'attachement au réseau 4G. Nous partons du principe que nous nous intéressons uniquement aux évènements qui font intervenir la station de base. La Figure 26 nous montre la procédure d'attachement simplifiée, avec uniquement les messages envoyés et reçus par la station de base. Ainsi la latence pour une étape i est donnée par :

$$L_i = T_i - T_{i-1} \qquad (1)$$

- L_i : la latence pour l'étape i (en ms), avec **i>0** et T_0 **= 0 ms**
- T_i : le temps d'arrivée ou d'envoi du message i (en ms)
- T_{i-1} : le temps d'arrivée ou d'envoi du message précédent le message i (en ms)

La latence totale de l'attachement pour un utilisateur est donc ainsi donnée par :

$$L = \sum_{i=1}^{i=14} L_i = \sum_{i=1}^{i=14} T_i - T_{i-1} \qquad (2)$$

Il revient donc d'appliquer cette méthode de calcul à nos traces issues de la station de base, chose que nous avons implémenté dans nos scripts.

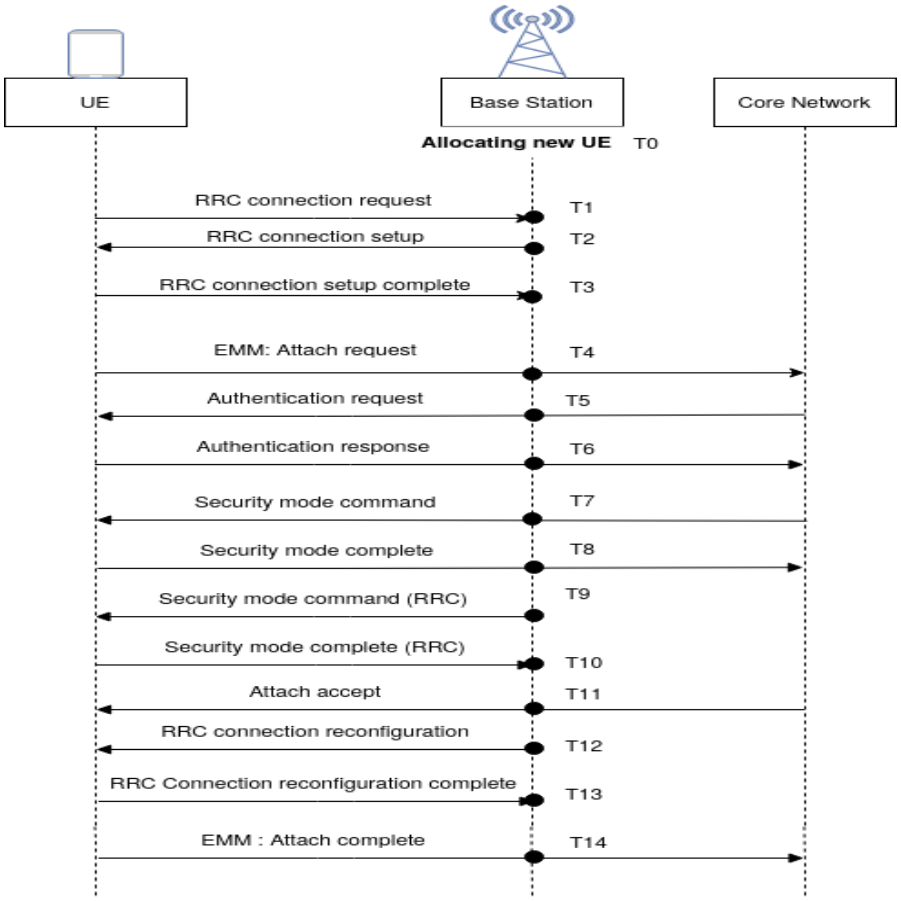


Figure 26: Procédure d'attachement de l'UE au réseau 4G (du point de vue de la station de base)

4. PROCESSUS DE COLLECTE DES DONNEES

Pour vérifier notre hypothèse, nous devons analyser la journalisation au niveau de la station de base pour pouvoir mesurer la latence de communications sur la base de la méthode montrée dans la partie précédente. Les fichiers de journalisation de la station de base

comprennent énormément d'informations. Il faut avoir une bonne visibilité et compréhension de la signalisation pour pouvoir extraire la latence. Pour ce faire nous avons choisi d'étudier l'attachement au réseau pour plusieurs situations de la SIMBox et pour des terminaux ordinaires.

Les tests que nous avons réalisés sont les suivants :

1. Connexion de téléphones (deux différents) à une station de base 4G ;
2. Connexion d'une Gateway seule à une station de base 4G ;
3. Connexion de la gateway, SIMBank et SIM server dans les situations suivantes :
    a. En local pour des débits différents (10 Mbps, 100 Mbps, 1000 Mbps)
    b. En local en utilisant UDP (débit à 100 Mbps)
    c. En local en utilisant le format de données de cartes SIM « short command » (débit à 100 Mbps, TCP et UDP)
    d. Connexion à internet en utilisant TCP à un débit de 100 Mbps pour des sites distants de 19 km.

Au bout de ces expériences nous avons obtenu un fichier de journalisation de l'activité de l'eNode B. A partir duquel nous allons extraire les latences à l'aide de scripts codés sur python.

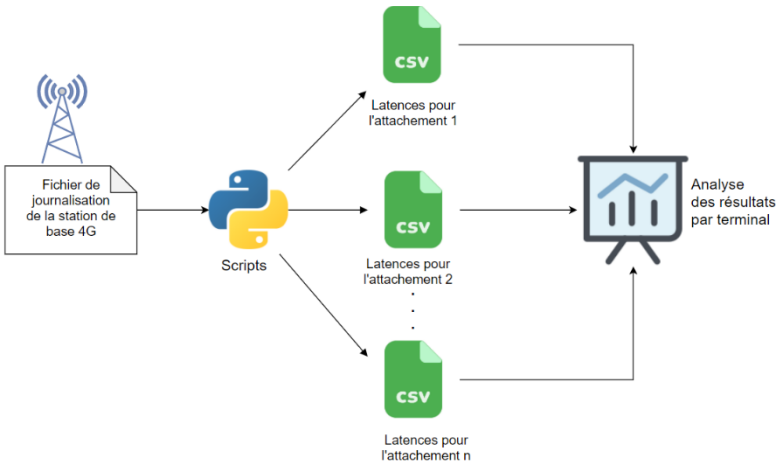


Figure 27: Processus de collecte et d'analyse des données.

Une fois que l'on a des fichiers csv contenant les valeurs de la latence pour chaque message envoyé pour chaque cas (les $\boldsymbol{L_i}$) on peut aisément, mettre le tout ensemble pour faire des comparaisons.

5. MATERIEL ET LOGICIELS UTILISES

5.1. Matériel

Le matériel nécessaire pour reproduire l'expérience est donné dans le Tableau 6. La plupart de ces appareils sont

Tableau 6: Matériel requis pour réaliser l'expérience

Fonction	Modèle utilisé
SIMBank	• HyberTone SMB32 Remote SIMBank
Gateway	• HyberTone GoIPx8
SIM Server	• Ubuntu Server 16.04 virtual machine
PC hôte	• DELL G7588 • Intel(R) Core (TM) i7-8750H CPU @ 2.20GHz (12 CPUs), ~2.2GHz • 16 GB RAM
Station de base	• Amarisoft callbox series
Cœur de réseau	• Cœur de réseau d'opérateur mobile avec tous les équipements associés
Téléphones	• Xiaomi Redmi Note 9 • Huawei Mate 8
Cartes SIM programmables	• SysmoSIM-SJS1 de Sysmocom

5.2. Logiciel

5.2.1. Ubuntu

Ubuntu est un système d'exploitation GNU/LINUX basé sur la distribution Linux Debian. Il est développé, maintenu et commercialisé pour les ordinateurs individuels par la société Canonical.

Nous avons utilisé la version d'Ubuntu Server 16.04 pour notre SIM Server et 18.04 pour le PC hôte.

Figure 28: Logo Ubuntu.

5.2.2. AMARI Callbox

AMARI Callbox est la solution idéale pour tester les appareils 5G NSA et SA, LTE, LTE-M et NB-IoT. Elle agit comme un eNB et un EPC conformes à la norme 3GPP, ce qui permet de réaliser des tests fonctionnels et de performance. La Callbox est alimentée par une suite logicielle de qualité pour le déploiement.

Figure 29: Logo Amarisoft.

5.2.3. Wireshark

Wireshark est l'analyseur de protocole réseau le plus utilisé et le plus utilisé au monde. Il vous permet de voir ce qui se passe sur votre réseau à un niveau microscopique et constitue la norme de facto (et souvent de jure) dans de nombreuses entreprises.

Figure 30: Logo Wireshark.

5.2.4. Python

Le langage de programmation utilisé pour effectuer la simulation est le Python. Python a été utilisé du fait de ses nombreux modules utiles pour la manipulation de fichiers et de chaines de caractères, utiles pour analyser les fichiers de journalisation.

Figure 31: Logo Python.

5.2.5. HyberTone SIMBank scheduler

C'est un service compatible avec des systèmes Linux, proposé par HyberTone qui permet de contrôler et d'organiser les équipements de la SIMBox. Une fois installé dans un ordinateur celui-ci devient un SIM Server capable d'orchestrer la fraude à la SIMBox.

SYNTHÈSE

Dans cette dernière partie dédiée à la modélisation de notre solution, il a été question pour nous de présenter l'architecture du réseau qui nous devions réaliser ; pour chacune des situations de fraude que nous avons présentées. Nous avons également présenté les conditions expérimentales ainsi que les prérequis matériels et logiciels pour réaliser cette expérience.

CHAPITRE III : RÉSULTATS ET DISCUSSIONS

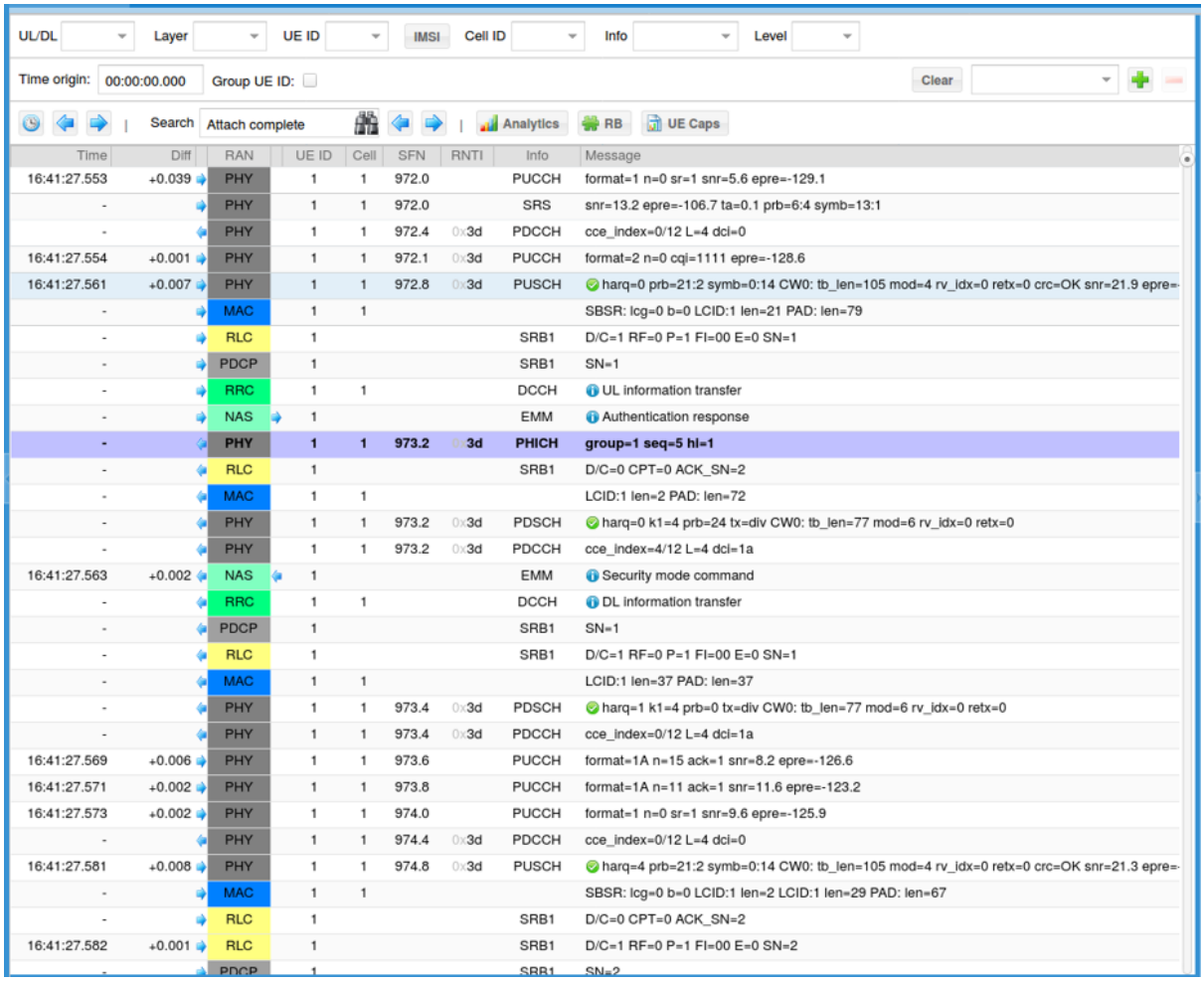
DESCRIPTION

Dans ce chapitre nous présenterons les résultats de l'expérience que nous avons menée pour différents cas de fraude à la SIMBox et nous comparons les résultats obtenus afin de conclure au sujet de l'efficacité de la méthode de détection utilisée.

PLAN :

1. RESULTATS DE LA STATION DE BASE

La station de base AMARI callbox, nous permet de visualiser l'activité en temps réel du réseau autant au niveau de la station de base qu'au niveau des équipements du cœur de réseau. Mais ici nous nous focalisons sur la station de base.



Time	Diff	RAN	UE ID	Cell	SFN	RNTI	Info	Message
16:41:27.553	+0.039	PHY	1	1	972.0		PUCCH	format=1 n=0 sr=1 snr=5.6 epre=-129.1
-		PHY	1	1	972.0		SRS	snr=13.2 epre=-106.7 ta=0.1 prb=6:4 symb=13:1
-		PHY	1	1	972.4	0x3d	PDCCH	cce_index=0/12 L=4 dci=0
16:41:27.554	+0.001	PHY	1	1	972.1	0x3d	PUCCH	format=2 n=0 cqi=1111 epre=-128.6
16:41:27.561	+0.007	PHY	1	1	972.8	0x3d	PUSCH	harq=0 prb=21:2 symb=0:14 CW0: tb_len=105 mod=4 rv_idx=0 retx=0 crc=OK snr=21.9 epre=
-		MAC	1	1				SBSR: lcg=0 b=0 LCID:1 len=21 PAD: len=79
-		RLC	1				SRB1	D/C=1 RF=0 P=1 FI=00 E=0 SN=1
-		PDCP	1				SRB1	SN=1
-		RRC	1	1			DCCH	UL information transfer
-		NAS	1				EMM	Authentication response
-		PHY	1	1	973.2	0x3d	PHICH	group=1 seq=5 hi=1
-		RLC	1				SRB1	D/C=0 CPT=0 ACK_SN=2
-		MAC	1	1				LCID:1 len=2 PAD: len=72
-		PHY	1	1	973.2	0x3d	PDSCH	harq=0 k1=4 prb=24 tx=div CW0: tb_len=77 mod=6 rv_idx=0 retx=0
-		PHY	1	1	973.2	0x3d	PDCCH	cce_index=4/12 L=4 dci=1a
16:41:27.563	+0.002	NAS	1				EMM	Security mode command
-		RRC	1	1			DCCH	DL information transfer
-		PDCP	1				SRB1	SN=1
-		RLC	1				SRB1	D/C=1 RF=0 P=1 FI=00 E=0 SN=1
-		MAC	1	1				LCID:1 len=37 PAD: len=37
-		PHY	1	1	973.4	0x3d	PDSCH	harq=1 k1=4 prb=0 tx=div CW0: tb_len=77 mod=6 rv_idx=0 retx=0
-		PHY	1	1	973.4	0x3d	PDCCH	cce_index=0/12 L=4 dci=1a
16:41:27.569	+0.006	PHY	1	1	973.6		PUCCH	format=1A n=15 ack=1 snr=8.2 epre=-126.6
16:41:27.571	+0.002	PHY	1	1	973.8		PUCCH	format=1A n=11 ack=1 snr=11.6 epre=-123.2
16:41:27.573	+0.002	PHY	1	1	974.0		PUCCH	format=1 n=0 sr=1 snr=9.6 epre=-125.9
-		PHY	1	1	974.4	0x3d	PDCCH	cce_index=0/12 L=4 dci=0
16:41:27.581	+0.008	PHY	1	1	974.8	0x3d	PUSCH	harq=4 prb=21:2 symb=0:14 CW0: tb_len=105 mod=4 rv_idx=0 retx=0 crc=OK snr=21.3 epre=
-		MAC	1	1				SBSR: lcg=0 b=0 LCID:1 len=2 LCID:1 len=29 PAD: len=67
-		RLC	1				SRB1	D/C=0 CPT=0 ACK_SN=2
16:41:27.582	+0.001	RLC	1				SRB1	D/C=1 RF=0 P=1 FI=00 E=0 SN=2
-		PDCP	1				SRB1	SN=2

Figure 32: Interface graphique d'Amarisoft callbox.

Cette capture d'écran nous montre l'activité d'un utilisateur pendant sa procédure d'attachement au réseau. Mais on remarque que le flux de données est très important il faut pouvoir extraire les informations dont nous avons besoin. On peut voir des informations importantes telles que :

- **Time** : le temps d'envoi ou de réception selon que l'on soit en UL ou en DL

- **RAN** : Nous donne la couche qui traite le message
- **UE_ID** : L'identifiant de l'UE dans le système
- **Cell** : L'identifiant de la cellule
- **SFN**: le System Frame Number
- **RNTI** : le RNTI de l'utilisateur dans la cellule
- **Info** : nous donne des informations sur l'opération effectuée
- **Message** : qui donne le contenu du message de signalisation envoyé

Ces informations ne sont pas toutes utiles pour nous. La donnée clé est le temps, par lequel nous allons inférer la latence. Il nous faut reformatter ces messages pour extraire ce que l'on veut. Pour ce faire nous avons téléchargé des fichiers de journalisation de la station de base, que nous avons fourni en entrée dans des scripts qui nous permettent d'avoir des détails plus approfondis dans les données. Le fichier de journalisation est un fichier formatté en JSON. Nous pouvons voir les caractéristiques complètes de la station de base ainsi que le format des messages de signalisation dans l'entête du fichier.

```
# lteenb version 2021-06-17, gcc 9.2.1
# Licensed to 'Télécom ParisTech ' [8a6a4cbd5be14f9b18453920b31dbc669779fc827a1d128fca]
# SMP bandwidth=10.0/40 PRACH=1 DRBs=1 RF0=1/1
# Log file format:
# time layer dir ue_id {cell_id rnti sfn channel:} message
# Cell 0x01: earfcn=3350 pci=1 mode=FDD
# DL: n_rb_dl=25 cyclic_prefix=0
# UL: n_rb_ul=25 cyclic_prefix=0 prach_config_index=4 prach_freq_offset=2 delta_pucch_shift=2 n_rb_cqi=1 n_cs_an=0
# PUCCH allocation:
# Type     RBs    n
# 2/2a/2b    1    6
# Start of PUCCH ACK/NACK=11
# RBs reserved for PUCCH:  3  3  3  3  3  3  3  3  3  3
# SR resource count=220
# CQI resource count=240
# SRS resources: offsets=8 freqs=5 total=80
# GBR limits: DL=2.356 Mre/s UL=2.492 Mre/s
# Started
```

Figure 33: Capture d'écran de l'Entête du fichier de journalisation de l'eNodeB.

Le corps du fichier commence à la connexion de l'eNodeB à l'interface S1 qui le relie avec le réseau cœur. Et la suite est constituée de l'activité des utilisateurs.

```
# Started
14:01:32.961 [S1AP] -  Connecting to 127.0.1.100:36412
14:01:33.509 [S1AP] -  Connected to 127.0.1.100:36412
14:01:33.509 [S1AP] TO - - 127.0.1.100:36412 S1 setup request
        initiatingMessage: {
          procedureCode id-S1Setup,
          criticality reject,
          value {
            protocolIEs {
              {
                id id-Global-ENB-ID,
                criticality reject,
                value {
                  pLMNidentity '09F107'H,
                  eNB-ID macroENB-ID: '1A2D0'H
                }
              },
              {
                id id-eNBname,
                criticality ignore,
                value "enb1a2d0"
```

Figure 34: Capture d'écran du début de l'activité de l'eNodeB : connexion à l'interface S1

La première étape de notre traitement reformatte le fichier de manière à ressortir uniquement les événements élémentaires (les messages de la forme « ***time layer dir ue_id {cell_id rnti sfn channel:}*** »). Une fois appliquée à notre fichier (Figure 35), on peut voir les étapes de la procédure d'attachement. Une fois ce fichier obtenu, nous calculons les latences à partir des données temporelles fournies par ce fichier de traces à partir des équations (1) et (2).

```
16:41:27.178 [MAC] -  0001 01 Allocating new UE
16:41:27.188 [PHY] UL 0001 01 003d   935.5 PUSCH: harq=3 prb=2:4 symb=0:13 CW0: tb_len=11 mod=2 rv_idx=0 retx=0 crc=OK snr=12.1 epre=-118.4 ta=0.7
16:41:27.188 [MAC] UL 0001 01 PAD: len=0 PAD: len=0 SBSR: lcg=0 b=0 LCID:0 len=6
16:41:27.188 [RRC] UL 0001 01 CCCH: RRC connection request
16:41:27.188 [RRC] DL 0001 01 CCCH: RRC connection setup
16:41:27.188 [PHY] DL 0001 01 003d   935.9 PHICH: group=2 seq=0 hi=1
16:41:27.188 [MAC] DL 0001 01 UECRI: 5c fc b6 90 5c f6 LCID:0 len=26 PAD: len=1
16:41:27.188 [PHY] DL 0001 01 003d   935.9 PDSCH: harq=0 k1=4 prb=0:7 tx=div CW0: tb_len=37 mod=2 rv_idx=0 retx=0
16:41:27.188 [PHY] DL 0001 01 003d   935.9 PDCCH: cce_index=4/12 L=4 dci=1a
16:41:27.196 [PHY] UL 0001 01    -   936.3 PUCCH: format=1A n=15 ack=1 snr=-0.1 epre=-135.3
16:41:27.213 [PHY] UL 0001 01    -   938.0 PUCCH: format=1 n=0 sr=1 snr=-0.0 epre=-135.3
16:41:27.213 [PHY] DL 0001 01 003d   938.4 PDCCH: cce_index=0/12 L=4 dci=0
16:41:27.221 [PHY] UL 0001 01 003d   938.8 PUSCH: harq=4 prb=2:5 symb=0:14 CW0: tb_len=109 mod=4 rv_idx=0 retx=0 crc=OK snr=23.5 epre=-104.9 ta=0.7
16:41:27.222 [MAC] UL 0001 01 SBSR: lcg=0 b=0 PHR: ph=30 LCID:1 len=86 PAD: len=16
16:41:27.222 [RLC] UL 0001 SRB1 D/C=1 RF=0 P=1 FI=00 E=0 SN=0
16:41:27.222 [PDCP] UL 0001 SRB1 SN=0
16:41:27.222 [RRC] UL 0001 01 DCCH: RRC connection setup complete
16:41:27.222 [NAS] UL 0001 EMM: Attach request
16:41:27.222 [PHY] DL 0001 01 003d   939.2 PHICH: group=2 seq=0 hi=1
16:41:27.222 [RLC] DL 0001 SRB1 D/C=0 CPT=0 ACK_SN=1
16:41:27.222 [MAC] DL 0001 01 LCID:1 len=2 PAD: len=4
16:41:27.222 [PHY] DL 0001 01 003d   939.2 PDSCH: harq=0 k1=4 prb=23:2 tx=div CW0: tb_len=9 mod=2 rv_idx=0 retx=0
16:41:27.222 [PHY] DL 0001 01 003d   939.2 PDCCH: cce_index=4/12 L=4 dci=1a
16:41:27.222 [NAS] DL 0001 EMM: Authentication request
16:41:27.222 [RRC] DL 0001 01 DCCH: DL information transfer
```

Figure 35: Capture d'écran du début de la procédure d'attachement pour un utilisateur.

2. LATENCE DE LA PROCEDURE D'ATTACHEMENT AU RESEAU

Après application de notre script nous pouvons avoir les résultats de la latence en fonction des différents scénarios que nous nous sommes donnés.

2.1. Latence par type d'UE

La Figure 36 ci-dessous présente la latence d'attachement pour chacun des UE dans les cas de SIMBox et de terminaux réguliers comme suit :

- Téléphone Xiaomi Redmi Note 9 (bleu)
- Téléphone Huawei Mate 8 (rouge)
- Gateway connectée au SIM Server en local (jaune)
- Gateway seule (vert)

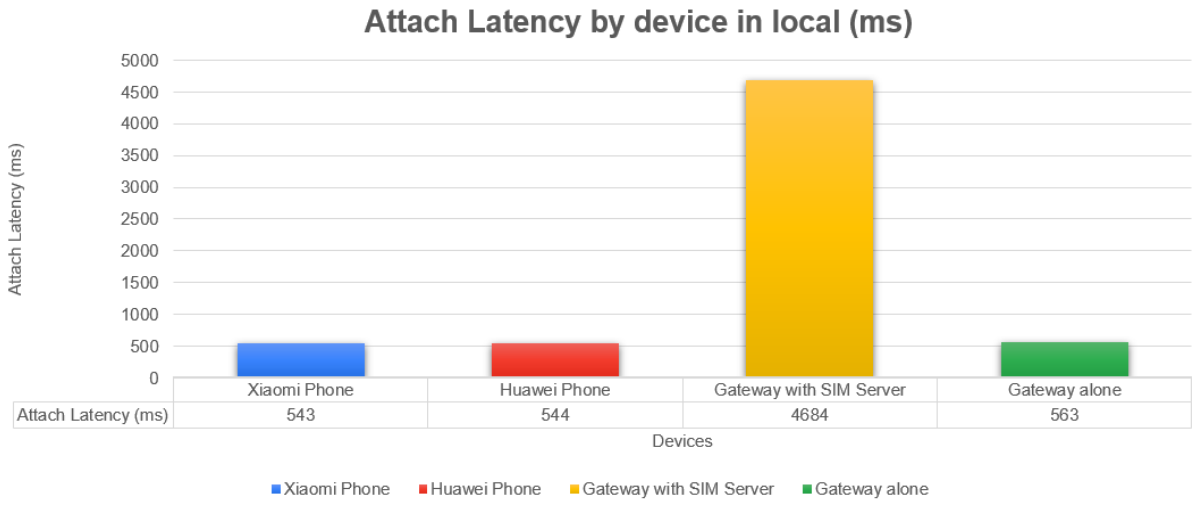


Figure 36: Latence de l'attachement par type d'UE.

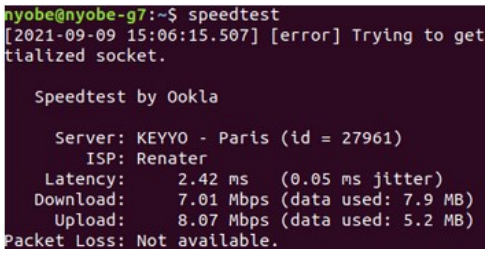
On observe une différence considérable (plus de **4000 ms**) entre le cas où il y a des communications IP entre équipements de la SIMBox, et les cas où la carte SIM est physiquement connectée.

2.2. Impact de la connexion IP entre équipements SIMBox sur la latence au niveau LTE.

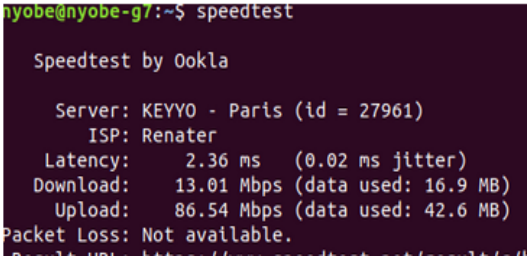
2.2.1. Impact du débit de l'interface Ethernet du SIM Server

Ici nous comparons la latence de l'attachement, pour différents débits de connexion sur l'interface Ethernet du SIM Server, pour y voir son impact sur la latence dans la communication au niveau de la station de base. Ceci serait un argument supplémentaire pour créditer la

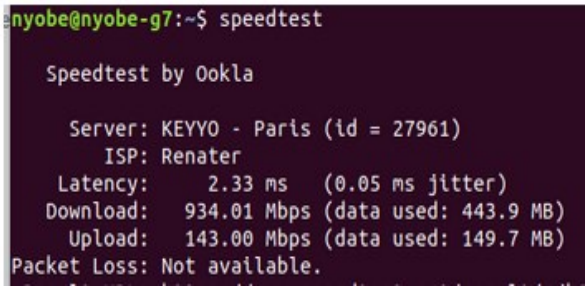
méthode utilisée. Pour ce faire nous avons fait varier ledit débit à 10, 100 et 1000 Mbps à l'aide d'**ethtool**. Nous avons observé le débit moyen réel de notre connexion à l'aide de **speedtest** un package Ubuntu.



(a) 10 Mbps



(b) 100 Mbps



(c) 1000 Mbps

Figure 37: Débits réels, moyens mesurés sur l'interface Ethernet du SIM Server pour différents débits 10, 100 et 1000 Mbps.

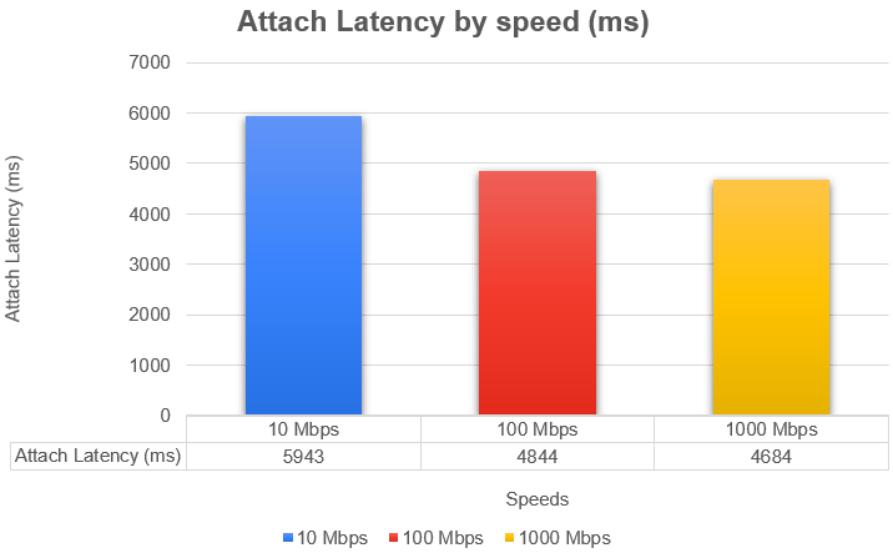


Figure 38: Evolution de la latence de la procédure d'attachement en fonction du débit.

On peut y voir que la latence croît lorsque le débit de la connexion entre équipements de la SIMBox diminue. Mais il reste toujours largement au-dessus des **4000 ms pour le meilleur débit possible** et de ce fait, toujours aussi loin de celle des terminaux réguliers.

2.2.2. Impact de l'utilisation d'internet entre équipements de la SIMBox (effet de la latence IP)

Dans ces résultats nous avons comparé pour des débits similaires la latence obtenue lorsque les équipements de la SIMBox sont connectés localement et lorsqu'ils sont connectés via internet. En effet plusieurs paramètres influencent la qualité de la connexion dont le débit, la latence, la gigue, et le séquençage des paquets.

Tableau 7: Tableau récapitulatif des caractéristiques de qualité des connexions IP

Variable	Via Internet	En local	Minimum requis
Débit(descendant/montant)	95.36/4.90 Mbps	13.01/86.54 Mbps	11 Kbps
Latence	9.38 ms	2.36 ms	300 ms
Gigue	0.17 ms	0.02 ms	/
Taux de perte de paquets	0.0%	0.0%	1%

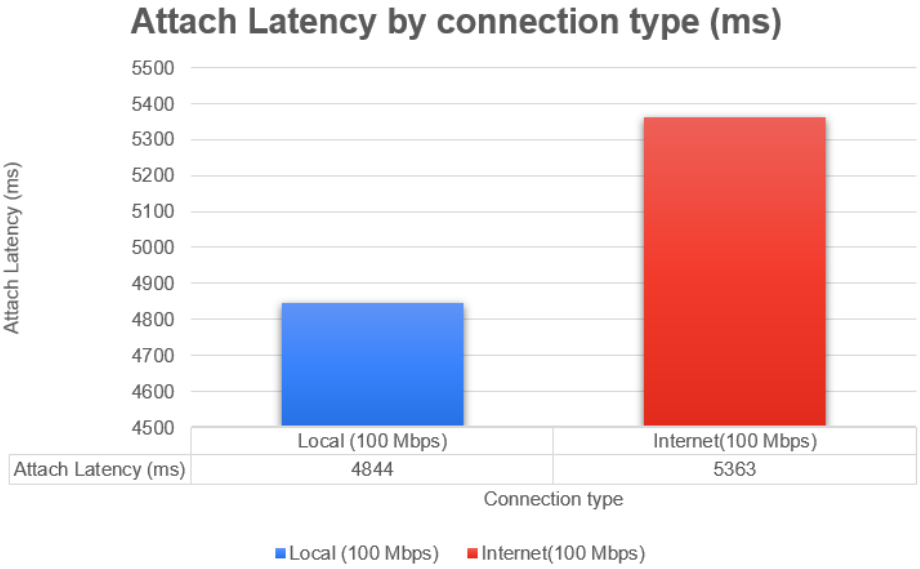


Figure 39: Latence de la procédure d'attachement dans cas de connexion en local et via internet entre équipements de la SIMBox.

On peut donc observer que quand une connexion à internet est utilisée (comme dans la plupart des cas réels d'utilisation de la SIMBox) la latence observée est beaucoup plus élevée à débit de connexion équivalent sur les interfaces. Cela du fait de l'influence des routeurs intermédiaires et de la distance entre les deux sites.

2.3. Impact de la configuration de la SIMBox

Dans cette expérience nous avons essayé de voir l'impact des configurations que les fraudeurs pourraient faire dans le but de diminuer la latence que l'on pourrait observer au niveau de la station de base. Nous avons noté deux configurations qui pourraient le faire :

- L'utilisation d'UDP pour les communications avec le SIM Server
- L'utilisation du format « short command » pour les données de carte SIM

2.3.1. Utilisation d'UDP

Nous avons observé le comportement de la latence lorsque UDP était utilisé comparativement à lorsque l'on utilisait TCP, à un même débit de 100 Mbps.

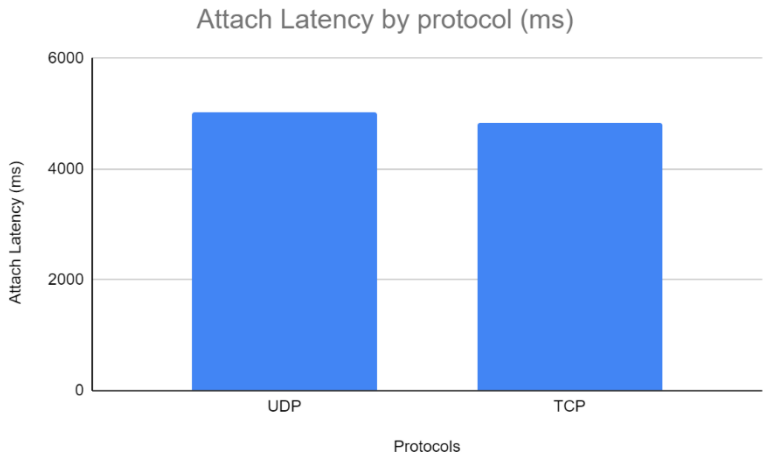


Figure 40: Impact du protocole de la couche de transport utilisé entre équipements de la SIMBox sur la latence de la procédure d'attachement

On se rend ainsi compte que la différence entre les deux latences est très faible. Ce qui rend des conclusions difficiles, mais toujours est que dans les deux cas on reste au-dessus du seuil des **4000 ms** et de ce fait largement supérieur à la latence dans le cas des terminaux réguliers.

2.3.2. Impact du format de données de carte SIM

Dans cette expérience nous avons changé le format des données de carte SIM pour observer le comportement de la latence dans chacun des cas. Il en existe deux dans le cas de la gateway Hybertone [29] que nous avons utilisé pendant l'expérience :

- **Long command** : qui envoie des instructions plus longues de la SIMBank vers la gateway. C'est l'option utilisée par défaut dans les gateways HyberTone ;
- **Short command** : qui est une alternative à format plus court qui selon le constructeur, serait plus compatible avec la commande à distance.

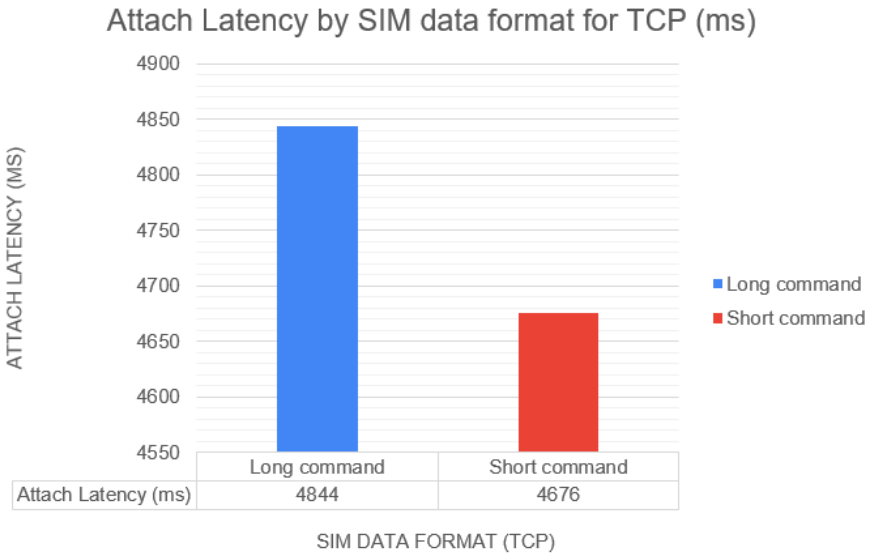


Figure 41: Impact du format de données des cartes SIM sur la latence, dans le cas de TCP.

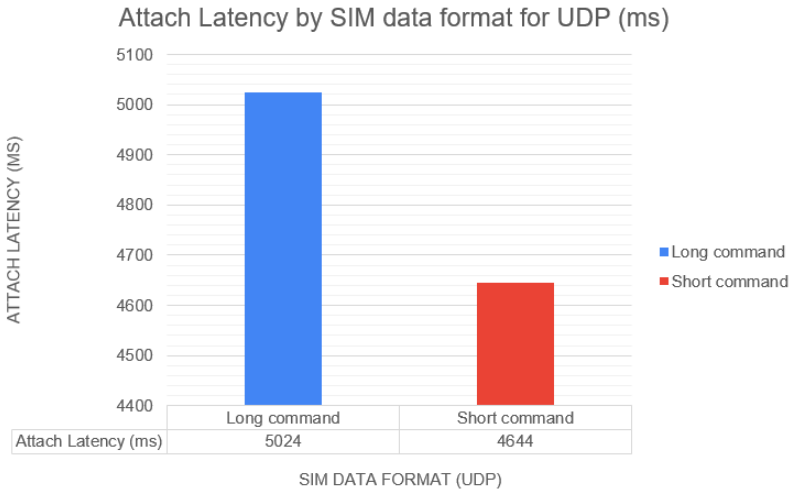


Figure 42: Impact du format de données des cartes SIM sur la latence, dans le cas de UDP.

On constate ainsi que l'utilisation du format short command peut réduire la latence, mais on remarque qu'on demeure au-dessus du seuil des **4000 ms**, toujours aussi largement supérieur au cas des terminaux réguliers.

3. OBSERVATION DETAILLEE DE LA SIGNALISATION

Dans cette partie nous présentons le résultat obtenu lorsque l'on se penche plus en détail dans chaque étape de la procédure d'attachement dans laquelle le terminal communique avec la station de base. Nous recherchons ainsi à déterminer les opérations qui créent ce décalage entre les latences dans les cas de SIMBox et dans les cas d'utilisateurs normaux.

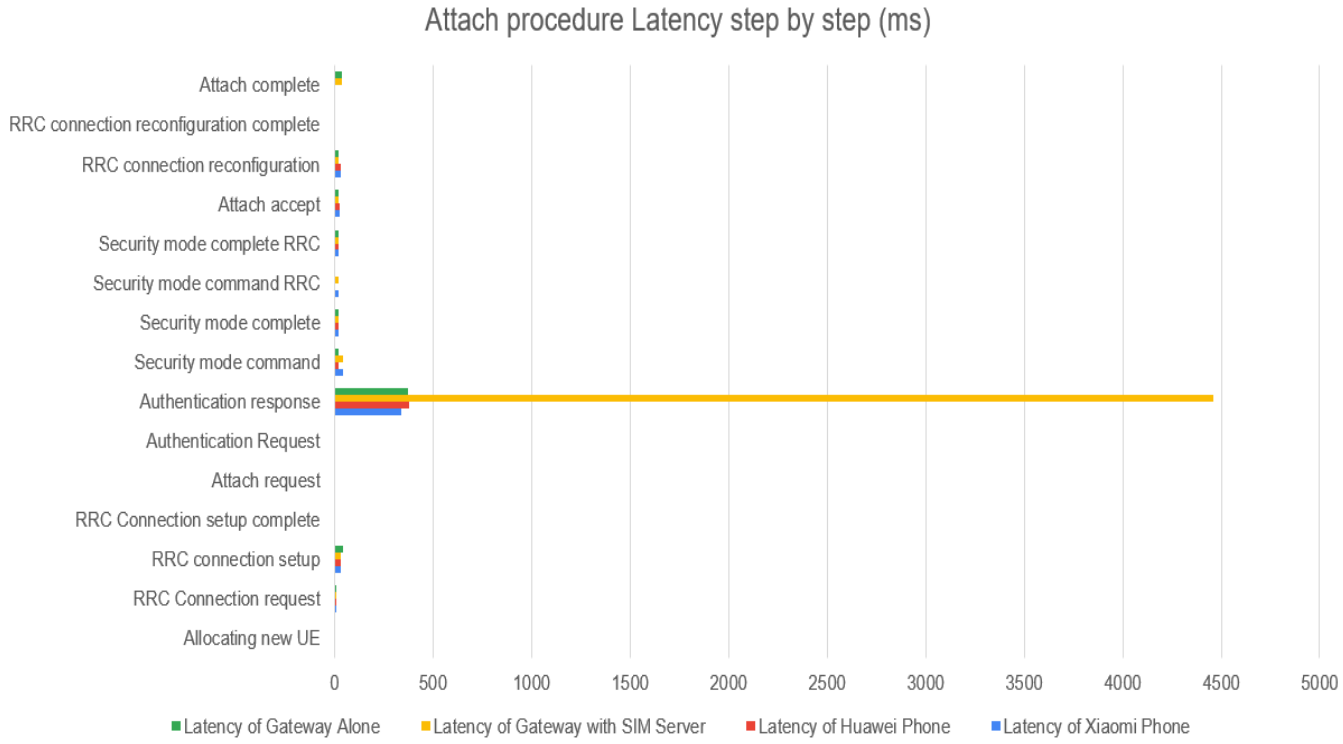


Figure 43: Latence de la procédure d'attachement étape par étape pour chaque type d'UE.

Nous pouvons ainsi observer que l'étape la plus chronophage, dans la procédure d'attachement c'est l'authentification. Cela s'observe autant pour la SIMBox que pour les terminaux ordinaires (Figure 43). On note d'ailleurs qu'il constitue plus de **80%** de la durée d'attachement.

4. BILAN DES EXPERIENCES

Le Tableau 8 , résume toutes les expériences effectuées et les résultats obtenus.

Tableau 8: Tableau récapitulatif des expériences menées

Expérience	Démarche	Résultats
Xiaomi Redmi Note 9	Test d'attachement au réseau 4G et observation de la latence.	La latence oscille autour de **550 ms.**
Huawei Mate 8	Test d'attachement au réseau 4G et observation de la latence.	➢ La latence du téléphone Huawei est sensiblement égale à celle du téléphone Xiaomi. ➢ On a ainsi un ordre de grandeur de la latence des terminaux (**moins de 600 ms**)
SIMBox complète (Variation de la qualité des liens IP)	1- Test d'attachement en local pour des débits différents (**10,100,1000 Mbps**) 2- Test d'attachement en utilisant internet (100 Mbps) pour voir l'impact de la latence IP.	➢ La latence de la SIMBox complète est largement supérieure à celle des terminaux réguliers (augmentation de **plus de 500%**) ➢ La latence au niveau LTE diminue quand le débit augmente au niveau IP ➢ La latence au niveau LTE augmente quand la latence augmente au niveau IP

SIMBox complète (Changement de protocole de la couche de transport)	Tests d'attachement en utilisant TCP puis UDP comme protocole de la couche de transport pour les communications entre équipements de la SIMBox	Aucune conclusion possible, du fait de l'encodage des données dans un protocole de la couche application inconnu.
SIMBox complète (Changement du format de données de la carte SIM)	Tests d'attachement en utilisant les formats de données de carte SIM, « short command » puis « long command ».	Le format « short command » peut réduire la latence, mais on reste dans des valeurs supérieures au seuil des **3000 ms**

SYNTHÈSE

Au terme de ce chapitre où il était question de présenter les résultats de notre travail. Il ressort que la méthode que nous avons explorée nous permet de classifier les utilisateurs de fraude à la SIMBox des utilisateurs normaux sur la base. La différence de latence pendant la période d'attachement est toujours supérieure à **4000 ms** soit 4 secondes, que l'on pourrait utiliser comme seuil de détection.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

La tâche que nous avons eu à mener, a été de déployer et de configurer une architecture matérielle composée d'équipements de la SIMBox, pour tester une méthode de détection de la fraude basée sur l'analyse de la signalisation. Dans le but de pouvoir réduire les pertes économiques chez les opérateurs de réseau mobiles. Nous avons d'abord situé le contexte en présentant l'écosystème des opérateurs de télécommunications, et celui de la fraude à la SIMBox, puis nous avons présenté les enjeux liés à ladite fraude pour les opérateurs. Il a ensuite été question pour nous de nous étendre sur le travail scientifique effectué dans la détection de la fraude à la SIMBox. Tout en présentant les limites de ces méthodes, nous avons pu mener des expériences sur la méthode de détection basée sur la signalisation afin de pouvoir montrer tout l'intérêt de cette méthode pourtant peu explorée dans la littérature.

Nous avons donc au terme de ce travail :

- Déployé et configuré la SIMBox dans un contexte expérimental ;
- Testé différentes architectures de SIMBox ;
- Analysé la signalisation entre station de base et équipements de la SIMBox ;
- Montré que la latence liée à la procédure d'attachement constitue un critère de classification fiable de la SIMBox par rapport aux utilisateurs réguliers.

En termes de perspectives pour le futur dans la recherche à ce sujet nous suggérons :

- Une étude approfondie des procédures de sécurité pendant l'attachement dans le cas de la SIMBox ;
- L'implémentation au niveau des stations de base d'algorithmes de classification basée sur la latence lors de la procédure d'attachement ;
- Une étude approfondie des communications et protocoles utilisés entre équipements de la SIMBox ;

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] GSMA, «L'Economie Mobile - Afrique Subsaharienne,» 2019.

[2] CFCA, «Communications Fraud Control Association – Fraud Loss Survey 2019,» 2019. [En ligne]. Available: https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf. [Accès le 6 Septembre 2021].

[3] CFCA, «2017 Global Fraud Loss Survey,» 2017.

[4] C. NCC Policy and E. A.Department , «An assessment of international voice traffic termination rates,» Juillet 2015.

[5] A. Ecofin, Cameroun : 22,2 milliards FCfa de pertes en 2015 sur les appels téléphoniques frauduleux par Simbox,» 9 Octobre 2015. [En ligne]. Available: https://www.agenceecofin.com/gestion-publique/0910-32980-cameroun-22-2-milliards-fcfa-de-pertes-en-2015-sur-les-appels-telephoniques-frauduleux-par-simbox. [Accès le 6 Septembre 2021].

[6] M. Yelland, *Fraud in mobile networks,* Computer Fraud & Security, vol. 2013, no. 3, pp. 5–9, 2013.

[7] L. S. R. I. (TRI), *White paper: Network protocol analysis: A new tool for blocking international bypass fraud before revenue is lost*, *Tech.Rep,* 2015.

[8] R. Kreher et K. Gaenger, *LTE Signaling : Troubleshooting and Performance Measurement (2e éd.), Wiley, 2016.*

[9] EFORT, *Architectures de Réseaux et de Services de Télécommunication Réseaux, Entités de Réseau, Technologies, Services,* 2011. [En ligne]. Available: https://sznaty2.wixsite.com/efort3/tutorial. [Accès le 6 Septembre 2021].

[10] ARCEP, *Parlons 5G : toutes vos questions sur la 5G,* 25 Mai 2021. [En ligne]. Available: https://www.arcep.fr/nos-sujets/parlons-5g-toutes-vos-questions-sur-la-5g.html . [Accès le 6 Septembre 2021].

[11] 3GPP, *ITU-R Confers IMT-Advanced (4G) Status to 3GPP LTE,* 20 Octobre 2010. [En ligne]. Available: https://www.3gpp.org/news-events/3gpp-news/1319-ITU-R-Confers-IMT-Advanced-4G-Status-to-3GPP-LTE. [Accès le 6 Septembre 2021].

[12] J. O. Oludayo, *The Future of LTE: The Femtocells perspective, School of Electrical Engineering*, Thesis submitted for examination for the degree of Master of Science in Technology Espoo 24.11.2013, 2013.

[13] EFORT, *LTE + SAE = EPS Principes et Architecture*, 2009. [En ligne]. Available: https://sznaty2.wixsite.com/efort3/tutorial. [Accès le 16 Septembre 2021].

[14] A. ABDELGHANI, *MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES COMME EXIGENCE PARTIELLE DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES, IMPACT DES INTERFÉRENCES DE LA COUCHE PHYSIQUE SUR LA COUCHE MAC,* UNIVERSITÉ DU QUÉBEC, JUIN 2011.

[15] Wikipedia, *Signalisation (télécommunication),* [En ligne]. Available: https://fr.wikipedia.org/wiki/Signalisation_(t%C3%A9l%C3%A9communication). [Accès le 16 Septembre 2021].

[16] 3GPP, *3GPP TS 24.30 l , Non-Access-Stratum (NAS) protocol for Evolved Packet Packet System (EPS),* 2014.

[17] 3GPP, 3GPP TS 36.331 , *Evolved Universal Terrestrial Radio Access (E-UTRA); RadioResource Control (RRC); Protocol specification (Release 8)*.

[18] 3GPP, *3GPP TS 36.322, Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification (Release 8)*.

[19] 3GPP, *3GPP TS 36.321 , Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (Release8)*.

[20] Wikipedia, *Voix sur IP*, [En ligne]. Available: https://fr.wikipedia.org/wiki/Voix_sur_IP. [Accès le Octobre 2021].

[21] 3CX, *Avantages d'un IPBX •• Système téléphonique VoIP,* [En ligne]. Available: https://www.3cx.fr/voip-sip/ip-pbx-overview/. [Accès le Octobre 2021].

[22] Recommendation ITU-T. H.323, *SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services,* 2009.

[23] 3CX, *Qu'est-ce que le protocole H.323 •• Définition,* [En ligne]. Available: https://www.3cx.fr/voip-sip/h323/. [Accès le Octobre 2021].

[24] E. NOUREDDINE et S. a. CHAFA , *Étude et Mise en place D'une Solution VoIP Sécurisée, Mémoire de fin d'études En vue de l'obtention Du Diplôme De Master en Electronique Option : Réseaux et Télécommunications,* Université Mouloud Mammeri De Tizi-Ouzou, 2014.

[25] 3CX, *H.323 Communication Example H323*, [En ligne]. Available: http://www.en.voipforo.com/H323/H323_example.php. [Accès le 6 Octobre 2021].

[26] F. Goffinet, *Architecture SIP,* Septembre 2020. [En ligne]. Available: https://sip.goffinet.org/sip/architecture/. [Accès le 6 Octobre 2021].

[27] B. KASSE, *Etude et mise en place d'un système de communication de VOIP: appliqué à un PABX IP open source,* Université Cheikh Anta Diop de Dakar, 2006.

[28] A. Kouam, A. Carneiro Viana et A. Tchana, *SIMBox bypass frauds in cellular networks: a survey. [Research Report], INRIA. 2021. ⟨hal-03105845v3⟩*, 2021.

[29] U. Murad et G. Pinkas, "*Unsupervised profiling for identifying superimposed fraud," in Principles of Data Mining and Knowledge Discovery*, J. M. ˙ Zytkow and J. Rauch, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 251–261.».

[30] S. Rosset, U. Murad, E. Neumann, Y. Idan et G. Pinkas, "*Discovery of fraud rules for telecommunications— challenges and solutions."* New York, NY, USA: Association for Computing Machinery Available,» 1999. [En ligne]. Available: https://doi.org/10.1145/312129.312303. [Accès le 16 Septembre 2021].

[31] I. Murynets, M. Zabarankin, R. P. Jover et A. Panaiga, *Analysis and detection of simbox fraud in mobility networks, IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, April 2014, pp. 1519–1526.*.

[32] L. Shenzhen HyberTone Technology Co., *GoIP User Manual,* 2016. [En ligne]. Available: http://www.hybertone.com/uploadfile/download/20140304125318422.pdf . [Accès le 1 Juillet 2021].

[33] L. Shenzhen HyberTone Technology Co., *User Manual for SMB32 Remote SIM Card Controller,* 2016. [En ligne]. Available: http://www.hybertone.com/uploadfile/download/20110914030122550.pdf . [Accès le 1 Juillet 2021].

[34] Telegeography, *Cellular Subscribers to Hit 9 Billion in 2026,* [En ligne]. Available: https://blog.telegeography.com/cellular-subscribers-to-hit-9-billion-in-2026 . [Accès le 16 Septembre 2021].

[35] F. Okumbor , N. Anthony et . A. A. J. Olokunde, *Grappling with the challenges of interconnect bypass fraud, IOSR Journal of Mobile Computing and Application (IOSR-JMCA), vol. 6, pp. 35 – 41, Jan - Feb 2019.*.

[36] OECD, *Access to mobile services and proof of identity 2019: Assessing the impact on digital and financial inclusion,* 2019.

[37] L. Taylor, *CFCA Administration, Founder, Lateral Alliances, " Putting telecom fraud loss into perspective…",* [En ligne]. Available: https://cfca.org/putting-telecom-fraud-loss-into-perspective/. [Accès le 16 Septembre 2021].

[38] M. R. AlBougha, *Comparing data mining classification algorithms in detection of simbox fraud,* 2016.

[39] 3GPP, *3GPP TS 36.300 V10.12.0 (2014-12),* Décembre 2014. [En ligne]. Available: https://www.arib.or.jp/english/html/overview/doc/STD-T104v3_20/5_Appendix/Rel10/36/36300-ac0.pdf. [Accès le 16 Septembre 2021].

[40] *HW Platforms – Network, Mobility and Services,* [En ligne]. Available: https://nms.telecom-paristech.fr/research/plateforms/. [Accès le 16 Septembre 2021].

ANNEXE

FABRICANTS DE SIMBOX ET SPECIFICITES

Tableau 9 : Fonctionnalités de la SIMBox en fonction des différents fabricants

Fonctionalité HBS	Rôle	Paramètre	Valeur	Fabricant proposant la function
Rotation de SIM	Trafic distribué parmi les cartes SIM	Method for selecting the next SIM card	round-robin method	Hybertone , Antrax
			random method	Hybertone , Portech
			statistic-based factor	Hybertone , Antrax , Dinstar
			statistic-based factor	Antrax
		Trigger to switch SIM cards	per time period	Hybertone , Antrax , Portech
			Threshold method	Antrax
Limitation de l'activité des SIM	Utilisation normale des carte SIM (heures, contacts, etc)	Type of limitation	Activity script method	Hybertone , Dinstar , Ejoin , Portech
			Parameter limitation	Antrax
			Parameter limitation per time period	Dinstar
			Time limitation	Hybertone , Antrax , Ejoin, Dinstar, Portech
Migration de SIM	Simulation de mouvements humains	Method for selecting the next GSM channel	Manually fixed method	Hybertone
			Any except previous	Antrax , Hybertone
			Any except previous zone	Hybertone
			Any gateway	Antrax
			Specified order	Antrax
Changement/verouillage de station de base	Simulation de micro mouvements humains	Method for selecting base station	Manually	Portech
			Default	Hybertone , Ejoin , Portech , Dinstar
			Fixed	Hybertone , Dinstar
			Random	Dinstar
			Poll	Hybertone , Ejoin
			Advanced	Hybertone Dinstar
IMEI modifiable	Une seule carte SIM par équipement	Method for changes at GSM channel	Manual editing	Hybertone
			IMEI auto change	Hybertone
		Method for changes SIM slots	Manual editing	Ejoin Antrax

			Random IMEI	Antrax , Dinstar
			Prefix IMEI	Ejoin , Antrax
			Registry IMEI	Antrax
			IMEI based on TAC	Antrax , Dinstar
Utilisation d'autres services mobiles	Utilisation normale d'autres services mobiles (data, SMS,etc)	Services used	Internet	Ejoin , Dinstar , Antrax
			USSD commands	Hybertone , Ejoin , Dinstar , Antrax , Portech , 2N voiceblue
			SMS	Hybertone , Ejoin , Dinstar , Antrax , Portech 2N voiceblue
Family list	Liste de contacts limités	Services used	SMS inter-sending	Ejoin
			Inter-calling	Ejoin
Redirection d'appels	Réponse d'un complice humain aux appels	Forwarding conditions	Unconditional	Ejoin
			Busy	Ejoin
			No reachable	Hybertone , Dinstar
			No reply	Hybertone , Dinstar