REPUBLIC ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIER ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE 20 AOUT 1955 SKIKDA
DEPARTEMENT INFORMATIQUE

Mémoire de fin d'étude en vue de l'obtention du diplôme Master

Option : Réseau et Systèmes Distribués (RSD)

THEME

UN SYSTEME DE DETECTION D'INTRUSION BASE SUR UNE APPROCHE IMMUNITAIRE ARTIFICIELLE

Réaliser par :

- **Bouteraa Djihane**
- **Boulassel Asma**

Encadré par :

Benoudina Lazhar

Session : Juin 2022

Remerciment

Tous d'abord nous remercions le Dieu, pour avoir donné la force, la volonté et le courage pour accomplir ce travail.

Nous tenons à exprimer notre profonde reconnaissance et la preuve de notre grande gratitude pour notre encadreur Lazher Benoudina, pour son aide et ses conseils qu'il nous a apporté tout au long de notre travail.

Nous tenons à remercier également les membres de jury pour avoir bien voulu examiner et avoir accepter de juger ce travail.

Nos remerciements vont également à nos familles, amis et à tous ceux qui ont participé de près ou de loin a la réalisation de ce travail et qui ont œuvré pour notre réussite par leurs soutiens, amour et précieux conseils.

Dédicace

Je dédie ce modeste travaille a :

L'homme, mon précieux offre du dieu, qui doit ma vie, ma réussite et tout mon respect mon cher père.

A ma maman qui m'a soutenu et encouragé durant ces années d'études. Qu'elle trouve ici le témoignage de ma profonde reconnaissance.

A mes deux chère frères Babi et Abdou qui m'ont soutenu et qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

Mes tantes que je n'oublierai jamais leur amour et leur soutien et tout ce qu'elles m'ont donné.

Mes grands parents, ma famille, mes proches et à ceux qui me donnent de l'amour et de la vivacité.

Mes amies Nadjet, Maria, Maroua, Amani, Ryem, Rania et Oum elkhir celles que j'aime beaucoup et qui je souhaite plein succès dans leur vie.

A tous ceux que j'aime. Merci.

Djihane

Table des matières

Chapitre 02: Les systèmes immunitaires artificiels

Chapitre 03: Analyse et conception

Chapitre 04: Réalisation et implémentation

Table des figures

Liste des tableaux

Résumé

Actuellement, La sécurité informatique est un problème majeur pour les réseaux des entreprises. Les pirates et les envahisseurs ont fait de nombreuses tentatives fructueuses pour pénétrer les réseaux des entreprises et les services Web. De nombreuses méthodes ont été développées pour sécuriser l'infrastructure réseau et la communication sur Internet, telles que les pare-feu, VPN, techniques de cryptage. Récemment, les systèmes de détection d'intrusions ou IDS sont exploitées pour améliorer la sécurité de l'hôte et du réseau. Ces systèmes offrent la possibilité de savoir si quelqu'un a pénétré ou tente de se connecter au réseau. Afin d'améliorer les performances des IDS et la précision de détection, différentes méthodes sont appliquées telles que les systèmes immunitaires artificiels ou SIA, qui ont montré une grande efficacité.

Mots clés: sécurité, réseau, IDS, systèmes de détection d'intrusions, systèmes immunitaires artificiels.

Abstract

Actually, The IT security is a big issue for enterprises networks. Hackers and intruders have made many successful attempts to penetrate companies' networks and web services. Many methods have been developed to secure the network infrastructure and communication over the Internet, such as firewalls, VPN, encryption techniques. Recently Intrusion Detection Systems or IDS are used to enhance both host and network security. These systems offer the possibility to find out if someone has gotten into or is trying to get into the network. In order to improve IDS performance and detection precision, different methods are applied such as the Artificial Immune Systems or AIS, which have shown a high efficiency.

Keywords: security, network, IDS, Intrusion detection Systems, Artificial Immune Systems.

ملخص

حاليا، يعد الأمن المعلوماتي مشكلة كبيرة لشبكات المؤسسات حيث قام الهاكرز بالعديد من المحاولات الناجحة لاختراق شبكات الشركات و خدمات الويب. من أجل هذا، تم تطوير العديد من الطرق لتأمين البنية التحتية للشبكة و الاتصالات عبر الانترنت، مثل : جدران الحماية و تقنيات التشفير. مؤخرا تم استخدام أنظمة كشف الدخلاء لتعزيز أمن كل من المضيف و الشبكة حيث توفر هذه الأنظمة إمكانية معرفة ما إذا كان شخص ما قد دخل أو يحاول الدخول الى الشبكة بغية تحسين أداء هذه الأنظمة و كذا دقة الكشف. تم الاعتماد على طرق مختلفة كأنظمة المناعة الاصطناعية التي أظهرت كفاءة عالية في هذا المجال. بالإضافة إلى ذلك يعد تطبيق نموذج العوامل المعتمدة على أنظمة اكتشاف الدخلاء أمرا مهما للغاية نظرا لمزاياه المتعددة مثل التنسيق التعاون و التوزيع فيما يتعلق بمكونات النظام.

الكلمات المفتاحية: الأمن المعلوماتي، الشبكة، أنظمة كشف الدخلاء، أنظمة المناعة الاصطناعية.

Glossaire

IDS: Intrusion Detection Systems

HIDS: Host Intrusion Detection Systems

NIDS: Network Intrusion Detection Systems

NNIDS: Node Network Intrusion Detection Systems

SIN: Systèmes Immunitaires Naturels

SIA: Système Immunitaires Naturels

SMA: Systèmes Multi Agents

DCA: Dendritic Cells Algorithm

CMH: Complexe Majeur d'Histocompatibilité

R2L : Remote to User

U2R : User to Root

KDD: Knowledge Discovery in Databases

Introduction Générale

Introduction générale

1. Domaine générale

Le développement remarquable du domaine des nouvelles technologies de l'information et de la communication (NTIC) ces dernières années, et l'utilisation de l'outil informatique à grande échelle, plus l'accessibilité du réseau internet par un grand nombre d'utilisateurs avec leurs différentes intentions qui peuvent être parfois destructifs, cela rend les données sensibles ainsi que les ressources des utilisateurs et des sociétés vulnérables au vol, ou exploités pour des raisons malveillantes. Face à toutes ces menaces, la sécurité optimale des systèmes informatiques et des réseaux est devenue un enjeu stratégique et pour assurer cette sécurité, différents outils ont été utilisés, tels que les pare-feu et les anti-virus.

Malheureusement les systèmes antivirus ou les firewalls sont la plupart du temps inefficaces face à ces nouvelles menaces sophistiquées, dont la propagation peut s'avérer extrêmement rapide. C'est pour pallier ce manque que sont apparus récemment de nouvelles solutions de sécurité appelées systèmes de détection des intrusions(IDS) qui consistent à examiner le trafic réseau, collecter tous les événements, les analyser et générer des alertes en cas d'identification de tentatives malveillantes. Ces systèmes sont devenus jour après jour très utilisés dans les stratégies de sécurité des réseaux et systèmes informatiques. Néanmoins, le défi majeur pour les systèmes de détection d'intrusions réside dans leur capacité à déterminer tout comportement malicieux que ce soit de l'intérieur ou de l'extérieur du système informatique.

2. Sous domaine

Le domaine de la détection d'intrusion est très ouvert à la recherche et au développement, où des produits logiciels et des solutions pratiques commencent à apparaitre jour après jour et qui fonctionnent selon deux principaux modes: l'approche par scénario et l'approche comportementale.

L'approche par scénario, basée sur la comparaison du comportement d'utilisation du système avec des signatures d'attaques connues préalablement et ne permet pas la détection des nouvelles attaques sans mise à jour de la base de signatures ce qui représente un inconvénient majeur de cette approche.

Par contre, l'approche comportementale consiste à construire un modèle identifiant les comportements déviants du modèle comportemental normal. Ce modèle est le résultat d'une phase d'apprentissage sur une grande base de données et son avantage principal est la possibilité de détecter de nouvelles attaques.

3. Problématique

La sécurité des systèmes informatiques est un domaine critique qui a évidemment motivé les angles divers de la recherche dont le but primordial est de fournir de nouvelles solutions prometteuses qui ne pourraient être assurées par des méthodes classiques. Parmi ces solutions est l'utilisation des IDS qui permettent la détection des utilisations non autorisées.

Afin de remplir les objectifs des IDS, diverses méthodes de détections d'intrusions ont été proposées, Le défi dans le domaine de la sécurité informatique et plus précisément dans les systèmes de détection d'intrusions s est de pouvoir déterminer la différence entre un fonctionnement normal et un fonctionnement avec intrus. Cependant, les systèmes et les réseaux à protéger sont devenus de plus en plus complexes et larges ainsi que la nature des intrusions courantes et futures nous incite à développer des outils de défense automatiques et surtout adaptatifs.

Une solution prometteuse est d'utiliser les systèmes immunitaires artificiels qui s'inspirent des systèmes immunitaires humains, lesquels sont dotés de capacités de détection et de défense d'intrus. Plusieurs travaux ont été proposés pour la détection d'intrusions qui sont basés sur les systèmes immunitaires artificiels, et qui ont intégré différents modèles immunitaires dont le modèle principal est le modèle de soi et de non soi.

L'objectif principal de ces systèmes consiste à augmenter le taux de vrai positif c'est-à-dire la détection des intrusions réelles et à minimiser le taux de vrai négatif qui reflète le taux d'erreurs du système. Afin de permettre la détection des éléments nuisibles et dangereux qui peuvent menacer la sécurité du réseau.

4. Découpage de mémoire

Ce mémoire est réparti en 5 chapitres, nous allons présenter dans le chapitre 1 une étude générale des attaques et des notions de sécurité informatique, y compris les attaques, les vulnérabilités, les intrusions, en mettant l'accent sur les systèmes de détection d'intrusions, leurs concepts, leurs types et les systèmes de détection existants.

Dans le chapitre 2, nous allons présenter le système immunitaire, commençant d'abord par la source d'inspiration le système immunitaire humain ensuite on arrive aux systèmes immunitaires artificiels avec leurs différents concepts et caractéristiques comme nous allons établir le lien entre les systèmes immunitaires artificiels et la détection d'intrusion, en focalisant sur les caractéristiques fournis par les SIA pour améliorer les performances des IDS avec une étude des travaux existants.

Le chapitre 3 concernant l'analyse et conception nous allons présenter le système proposé, son architecture, les étapes nécessaires pour sa mise en œuvre et les résultats obtenus.

Le chapitre 4 est le dernier chapitre réalisation et implémentation nous allons présenter les différentes interfaces du système.

Chapitre 1:

Sécurité informatique et système de détection d'intrusion

Introduction

Le progrès technologique, le développement des moyens de communications, l'ouverture du monde sur nouvelles technologies, et la transmission de divers types de données à travers les réseaux, ainsi que d'autre facteurs, apportent un danger d'accès et de manipulation des données par des personnes non autorisés, ou des concurrents. Donc la sécurité de l'information par une gamme de techniques et mécanismes d'authentification et de contrôle d'accès est devenue un besoin crucial afin de construire un système sécurisé déterminant et éliminant ces vulnérabilités.

Le système de détection des intrusions (IDS) est l'une de ces techniques qui offre un contrôle permanent des attaques ou suspectes et permettant ainsi de détecter toute tentative de violation de la politique de sécurité, c'est-à-dire toute intrusion.

Dans ce premier chapitre nous présentons deux parties, la première présente les principales notions de base de la sécurité informatique et les systèmes de détection d'intrusions, en commençant par les définitions des différentes notions de la sécurité informatique, puis les attaques informatiques et leurs classifications avec exemples. La deuxième partie présente les systèmes de détection d'intrusions, leur historique, définition, principe de fonctionnement, et critères de classification, ...etc.

A la fin de ce chapitre, nous citons quelques avantages et limites des systèmes de détection d'intrusions actuels.

I. La sécurité informatique

1. Définition :

La sécurité informatique: « C'est l'ensemble de technologie utilisée pour réduire les vulnérabilités du système d'information contre les attaques accidentelles ou intentionnelles et ca c'est le but d'utiliser la sécurité pour les systèmes d'information. La sécurité informatique est caractérisée généralement par les cinq propriétés ou objectifs suivants (appelés aussi les propriétés de la sécurité informatiques » **(1)**

- **Disponibilité:** Lorsqu'un utilisateur du système d'information demande des informations, la ressource doit être disponible pour répondre aux personnes autorisées uniquement.
- **Confidentialité :** assure que les informations sont cachées sur le système afin qu'elles ne puissent être lue par les personnes autorisées.
- **Intégrité :** Garantir l'impossibilité de modifier les informations relatives au système par des individus non autorisés sans l'intervention des personnes autorisées sans avoir les informer.
- **Non-répudiation:** Est de prouver la source de données pour les individus ne puissent pas nier leur participation a la communication.

- **L'authentification:** Est d'assurer l'identité de l'utilisateur, dans le sens que doit être garantir l'identité de chacune des parties impliquées dans la communication, aussi il faut également assurer le contrôle d'accès aux ressources pour les individus autorisés (l'accès au compte e-mail avec une adresse et mot de passe correcte).

On retrouve aussi dans le domaine de la sécurité informatique l'utilisation notamment des termes suivants, vulnérabilité, intrusion, menace, attaque**.** (2) (3)

- **Vulnérabilité** : faute créée durant le développement du système, ou durant l"opération, pouvant être exploitée afin de créer une intrusion.
- **Intrusion** : faute malveillante externe résultant d'une attaque qui a réussi à exploiter une vulnérabilité.
- **Menace** : possibilités et probabilités d'attaque contre la sécurité. Une menace est définie par le processus d'attaque
- **Attaque**: C'est n'importe quelle action qui a le but de menacer la sécurité des informations et de nuire au moins à l'une des propriétés de la sécurité informatique (disponibilité, Confidentialité, Intégrité, L'authentification). Il s'agit d'une tentative d'intrusion, nous abordons dans ce qui suit les différents buts et classes de ces attaques (tentatives d'intrusion).

2. Buts des attaques informatiques :

Il existe plusieurs objectifs pour les attaques:

- **Interruption**: vise la disponibilité des informations (DoS, . . .)
- **Interception**: vise la confidentialité des informations (capture de contenu, analyse de trafic,. . .).
- **Modification**: vise l'intégrité des informations (modification, rejet,. . .).
- **Fabrication:** vise l'authenticité des Informations (Masquerade). (4)

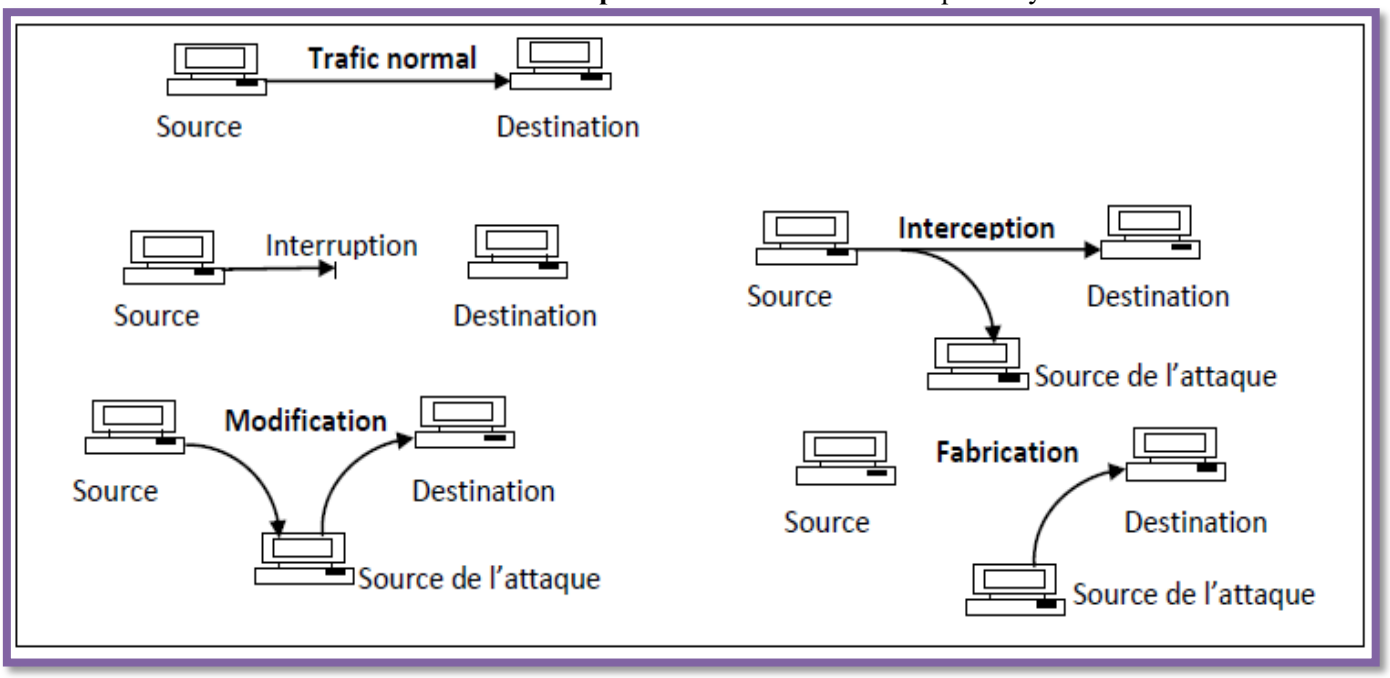

Figure 1. 1: Buts des attaques informatiques (5)

3. Les différentes classes d'attaques informatiques :

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Cette menace peut être accidentelle, intentionnelle (attaque), active ou passive, Ils existent dans la littérature plusieurs classifications d'attaques informatique selon des critères différents, parmi lesquelles :

3.1 Classification selon l'effet de l'attaque : Selon les effets résultant de l'attaque on peut classifier les attaques en deux groupes principaux : les attaques passives et les attaques actives.

- **Les attaques passives** : consistent à accéder, utiliser ou à observer le système cible sans modifier les données ou dysfonctionné les ressources de ce dernier, elles sont généralement indétectables (ex. : capture de contenu, analyse de trafic).
- **Les attaques actives** : consistent à effectuer des changements non autorisés sur les données des systèmes, à s'introduire dans des équipements réseau ou à perturber leurs fonctionnements, les attaques de ce type sont bien évidemment plus dangereuses.(ex. : mascarade et déni de service).

3.2 Classification selon la source de l'attaque : En termes de relation intrusion-victime, les attaques sont classées comme suit:

- **Les attaques internes :** provenant des employés de leur entreprise ou de leurs partenaires commerciaux ou clients,
- **Les attaques externes** : venant de l'extérieur, fréquemment via Internet.

3.3 Classification selon la cible de l'attaque:

- **Les attaques réseaux** : Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à leur implémentation. Il existe un grand nombre. Néanmoins, la plupart d'entre elles ne sont que des variantes des cinq attaques réseaux les plus connues aujourd'hui.
- **Les attaques applicatives :** Les attaques applicatives s'appuient principalement sur des vulnérabilités spécifiques aux applications utilisées.

4. Exemple d'attaque :

Il existe un nombre énorme d'attaques qui menacent les systèmes et les réseaux informatiques, néanmoins, la plupart d'entre elles ne sont que des variantes des autres. Voici des exemples d'attaques les plus connues aujourd'hui ciblant les réseaux informatiques.

4.1- Attaques de Dénis de Services :(Denial Of Service [DOS]): est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- L'obstruction d'accès à un service à une personne en particulier ;
- Également le fait d'envoyer des milliards d'octets à un box internet.

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise, les principales attaques qu"on peut trouver sont Apache2, Back,Land, Mail bomb, SYN Flood, Ping of death, Process table, Smurf, Syslogd, Teardrop,Udp storm.

4-2-Probing (Sondage) : L'attaquant de cette classe commence par un sondage de la future victime, ce que l'on appelle scan, ce sondage va balayer chaque port IP afin de connaitre les services offerts par le système (OS, topologie du réseau, protections employées,..) une fois se achevé, la machine de l'intrus (celui qui réalise l'intrusion) tente alors d'identifier le système d'exploitation utilisé par cette victime et d'exploiter les informations qu'elle a récolté. Cette classe d'attaque est la plus étendue et qu'elle requit une expertise technique minime. Les exemples de ce type d'attaque sont : Ipsweep,Mscan, Nmap,Saint, Satan.

4-3- Attaques User to Root : L'objectif de cette classe d'attaques est d'obtenir la main de l'administrateur système (Root) à partir d'un simple compte utilisateur par l'exploitation des vulnérabilités, Les exploits les plus connus sont les débordements réguliers des Buffers (buffer

overflows) dus aux erreurs de programmation, Les principales attaques de ce type sont : Eject, Ffbconfig, Fdformat, Load module, Perl, Ps, Xterm.

4-4- Attaque Remote to User : Dans cette classe d'attaque, l'attaquant essaye d'exploiter les vulnérabilités d'une machine distante afin d'avoir un accès illégal à cette dernière, Pour réussir cette attaque, l'attaquant exploite les bugs des applications installées dans la machine cible, les mauvaises configurations de celles-ci et du système qui les héberge, etc.

4-5-L'usurpation d'adresse IP(IP Spoofing) : Le principe de fonctionnement de cette attaque est d'envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été allouée à l'ordinateur qui émet ces paquets pour le but de masquer l'identité de l'attaquant lors d'une attaque d'un serveur ou n'importe quel cible dans le réseau , ou d'usurper l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

4-6-Les analyseurs réseau (sniffer): Est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent, vu que les données dans un réseau non commuté sont envoyées à toutes les machines du réseau et dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Le sniffer peut également servir cette propriété à une personne malveillante ayant un accès physique au réseau pour collecter des informations (ex : les mots de passes), Maisun sniffer peut aussi être utilisé comme un outil positif pour le but d'étudier et de capturer le trafic d'un réseau par les administrateurs réseaux et les détecteurs d'intrusion (IDS).

4.7-Balayage des ports : (port scanning) est une des activités considérées comme suspectes servant par les pirates informatiques pour découvrir les faiblesses potentiellement exploitables et chercher les ports ouverts sur un serveur de réseau en balayant les ports disponibles de la victime qui est potentiellement exécute de nombreux 'services' qui écoutent des 'ports' connus, les balayages de ports se font habituellement sur le protocole TCP pour le but d'ouvrir des connexions pour effectuer une intrusion, la même technique de balayage des ports est aussi utilisée par les administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux.

4.8-TCP Session Hijacking : Le « **vol de session TCP** » est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner, dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

4.9-Les trappes (backdoor):C'est une fonction ou un programme permettant à un pirate de prendre le contrôle d'un ordinateur à distance. Il peut être placé dans un cheval de Troie [1] ou un virus.

4.10-Attaque par virus : Il s'agit d'un programme auto-reproductible et généralement destructeur qui contamine le disque dur ainsi que tous autres supports de stockage utilisés et qui peut faire

[1] **Chevaux de Troie**: sont des programmes qui en plus d'une fonction classique, ont une fonction cachée nuisible, récupérer vos mots de passe, détruire le disque dur, etc.

exécuter à l'ordinateur des actions non désirées, le virus informatique peut donc se propager à l'intérieur même de l'ordinateur, en infectant petit à petit tous les fichiers. Il est donc destiné à modifier à notre insu le fonctionnement de l'ordinateur, certains virus peuvent simplement faire «beeper» le PC, d'autres peuvent détruire les données (formater, effacer le secteur de démarrage, voir détruire le matériel). (6)

5. Mécanismes de défense contre les attaques :

C'est l'ensemble de procédures ou dispositifs qui sont conçu pour détecter, prévenir ou récupérer les attaques qui menacent la sécurité informatique, il existe plusieurs outils de prévention contre-attaques informatiques, Nous avons cité ci-dessous quelques mécanismes**:** (5)

- **Chiffrement :** Algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature numérique**: Données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic** : Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- **Notarisation** : Utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès** : Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.
- **Antivirus** : Logiciel censé protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- **Le pare-feu** : Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le travers. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quelles sont les communications autorisées ou interdites. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- **Détection d'intrusion** : Repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.

- **Journalisation** ("logs") : Enregistrement des activités de chaque acteur. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.

- **Analyse des vulnérabilités** ("Security audit") : Identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu. (6)

Mais Aucun des mécanismes de sécurité ne suffit par lui-même, et pour cela dans la plupart du temps en vue d'atteindre un niveau acceptable de sécurité informatique plusieurs mécanismes sont utilisés en même temps.

II. Les systèmes de détection d'intrusion

1. Historique :

Les systèmes de détection ont connu une croissance rapide, le concept de système de détection d'intrusions a été introduit en 1980 par James Anderson dans l'effort d'amélioration de la vérification de la sécurité informatique et la capacité de surveillance, puis complété par le premier modèle de détection d'intrusions établit par Denning Dorothy en 1987, ensuite de nombreux prototypes sont apparus depuis 1988, et des grands budgets sont investis pour la recherche dans ce domaine. (7)

2. Définitions :

2.1 Détection d'intrusion :

Définition 1: Les outils de détection d'intrusion viennent afin de compléter les fonctions du firewall: au travers d'une surveillance de l'identité des requêtes en circulation sur le réseau, ces outils sont à même de repérer les requêtes malintentionnées, de repérer les intrus dans le flot du trafic courant transitant par les ports de communication laissés ouverts par le firewall. (8)

Définition 2: Techniques tentant de détecter une intrusion dans un ordinateur ou un réseau par l'observation d'actions, de logs de sécurité, ou de données d'audits. Détections d'intrusions (ou tentatives d'intrusions) manuellement ou en utilisant des programmes qui se servent des logs ou autres informations disponibles sur le réseau. (9)

2.2 Les systèmes de détection d'intrusion :

Les systèmes de détection sont conçus pour informer et dans certains cas pour empêcher, des accès non autorisés ou des intrusions dans les réseaux. Les pare-feu qui opèrent avec les systèmes de détection d'intrusion sont capables de détecter automatiquement les menaces venant de l'extérieur, plus rapidement qu'une vérification par un opérateur. (8)

3. Concept de base

3.1 Système : dénote un système d'information contrôlé par un système de détection d'intrusions. Cela peut être un poste de travail, un élément du réseau, une unité centrale, un pare-feu, un serveur Web, un réseau d'entreprise, etc.

3.2 Alarme: c'est la réponse générée par le système de détection d'intrusions lors de la détection d'une intrusion. Cependant les erreurs de détection peuvent être classées selon deux types:

a. Le positif faux : signifie qu'un système de détection d'intrusions détecte une intrusion là où aucune intrusion réelle n'a été commise.

b. Le négatif faux : A l'inverse de « positif faux », « négatif faux » signifie que le système de détection d'intrusions n'a pas détecté une intrusion ayant réussi. (3)

3.3 Audit de sécurité : c'est l'ensemble des mécanismes permettant la collecte d'informations sur les actions faites sur un système d'information. (3)

3.4 Log: Il s'agit d'un fichier comprenant différentes informations liées à l'utilisation d'un serveur, d'une application, d'un logiciel ou d'un système informatique. Un fichier log peut contenir certaines données confidentielles sur l'utilisateur. (10)

4. Pourquoi on a besoin des IDS

Avec la croissance rapide de l'internet, les incidents touchant à la sécurité ont augmenté. Dans ces circonstances, il y a un grand besoin d'outils logiciels qui peuvent automatiquement détecter une variété d'intrusions. Comme un gardien important du réseau, les systèmes de détection d'intrusions (IDS) doivent avoir la capacité de détecter et de défendre les intrusions de manière plus proactive dans la période plus courte. (11)

Quand une tentative est réussie en passant le par feu, il va peut-être provoquer des menaces. Alors, des fautes positives peuvent être diminuées en connaissant ces tentatives. Cette topologie permettra de vérifier que la ligne de base du par feu est suivi, ou que quelqu'un a fait une erreur en changeant une règle de par feu. Si la ligne de base du par feu proscrivent l'utilisation de ftp et l'IDS montre des alertes de ftp, alors le par feu ne bloque pas de trafic de ftp. C'est juste un effet secondaire et ne devrait pas être la seule manière pour vérifier la conformité de la ligne de base. (12)

5. Les caractéristiques des IDS :

Les systèmes de détection d'intrusions possèdent des caractéristiques liées à leurs fonctionnalités:

- **Exactitude:** elle représente le taux maximal des résultats d'IDS avec le comportement normal du système à surveiller. L'IDS ne doit pas considérer les actions légitimes des utilisateurs comme atypiques ou intrusives. Cette caractéristique peut être traduite par un taux de faux positifs minimal.

- **Performance:** elle est mesurée par le taux de traitement des traces d'audits. Si la performance d'un IDS est faible alors la détection en temps réel n'est pas possible.

- **Temps de réponse:** c'est la vitesse maximale du traitement des évènements. L'IDS doit être capable de propager son analyse de manière prompte à l'administrateur système, et/ou prendre des contres mesures dans des délais brefs.

- **Exhaustivité de détection :** un IDS idéal doit détecter toutes les attaques connues ou inconnues.

- **Tolérance aux fautes:** le système de détection d'intrusion doit résister aux attaques, particulièrement les attaques de déni de services. (13)

6. Classifications des IDS

6.1 Selon l'emplacement :

6.1.2 Les systèmes de détection d'intrusion basés hote « HIDS »

Les HIDS « Host Intrusion Detection Systems », sont placés directement sur les systèmes hôtes à surveiller. Ils analysent les fichiers, appels système ou événements réseau de la machine hôte. Ils sont par conséquent installés par l'administrateur du parc de machines ou directement par l'utilisateur. Également, la détection d'intrusions est limitée au poste en question (14). Les HIDS sont en général, intégrés au système d'exploitation qu'il protège. Ce type d'IDS est prévu pour la détection des menaces à un haut niveau de sécurité (8).

Ces IDS utilisent deux types de sources pour fournir une information sur l'activité de la machine: les logs (les journaux du système) et les traces d'audit du système d'exploitation. Les HIDS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédant des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS.

Voici quelques HIDS connus: Tripwire, WATCH, DragonSquire, Tiger,Security Manager… (15).

6.1.2 Les systèmes de détection d'intrusions basés réseau « NIDS »

Les NIDS « Network Intrusion Detection Systems » sont placés sur le réseau, à proximité des équipements réseau. Généralement en coupure du réseau, ils peuvent être directement intégrés dans les routeurs. Ils détectent les intrusions grâce à l'analyse du trafic réseau et sont capables de surveiller plusieurs systèmes (14).

L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traites éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console.

Voici quelques exemples de NIDS : NetRanger, Dragon, NFR, Snort, ISSRealSecure (15).

Le tableau ci-dessous présente les avantages et les inconvénients des deux types d'IDS:

	Avantages	Inconvénients
H I D S	✓ Il est possible de constater immédiatement l'impact d'une attaque et donc de mieux réagir. ✓ Grâce à la quantité des informations étudiées, il est possible d'observer les activités qui se déroulent sur l'hôte avec précision et d'optimiser le système en fonction des activités observées. ✓ Sont extrêmement complémentaires des NIDS. En effet, ils permettent de détecter plus facilement les attaques de type "Cheval de Troie", alors que ce type d'attaque est difficilement détectable par un NIDS. ✓ Permettent également de détecter des attaques impossibles à détecter avec un NIDS, car elles font partie de trafic crypté. ✓ Ont la capacité de fonctionner sur les traces d'audits des systèmes d'exploitation ✓ Ont une tolérance limitée aux faux positifs.	✖ Besoin de les installer sur chaque machine. ✖ Détection d'attaques locales uniquement. ✖ Ce type d'IDS est très sensible aux attaques de type DoS, qui peuvent faire exploser la taille des fichiers de logs. ✖ La taille des fichiers de rapport d'alertes à examiner est très contraignante pour le responsable de sécurité, qui peut atteindre plusieurs Mégaoctets, Et même ces fichiers sont assez gourmands en CPU et peuvent parfois altérer les performances de la machine hôte. ✖ Ils ont moins de facilité à détecter les scans.

N I D S	✓ Les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic et permettent donc une surveillance discrète du réseau. ✓ Les attaques de type scans sont facilement détectées et il est possible de filtrer le trafic. ✓ Invisibles aux attaquants, donc peut assurer une plus vaste sécurité contre les attaques. ✓ Un seul NIDS peut être utilisé pour contrôler un grand nombre de systèmes cibles en même temps ✓ Peuvent capturer le contenu de tous les paquets circulant dans le réseau. ✓ Ont la capacité de cheminer sur les traces d'audits des systèmes d'exploitation. ✓ Ont la capacité de déterminer si une tentative d'attaque est couronnée de succès.	✖ ✖ La probabilité de faux négatifs (attaques non détectées comme telles) est élevée et il est difficile de contrôler le réseau entier. ✖ Ils doivent principalement fonctionner de manière cryptée d'où une complication de l'analyse des paquets. ✖ A l'opposé des IDS basés sur l'hôte, les NIDS ne voient pas les impacts d'une attaque. ✖ Difficile de détecter des intrusions provenant de contenu chiffré. ✖ Présentent des difficultés de déploiement et de gestion face à un grand nombre d'hôtes. ✖ Ils peuvent manquer des attaques si le trafic est important sur la bande passante ou si des routes altérées sont utilisées. ✖ Détectent mais n'arrêtent pas l'intrusion.

Tableau1. 1 : Les avantages et les inconvénients des HIDS et NIDS (13) (14) (15).

6.1.3 Les systèmes de détection d'intrusions hybrides (NIDS+HIDS)

Les systèmes de détection d'intrusions hybrides rassemblent les caractéristiques de plusieurs systèmes de détection d'intrusions différents. Ils permettent, en un seul outil de surveiller le réseau et l'hôte. En pratique, on ne retrouve que la combinaison de NIDS et HIDS. Dans ce type d'IDS, les sources d'information proviennent à la fois du réseau et des machines ce qui augmente la complexité du système mais les avantages des NIDS et des HIDS sont combinés (13).

6.1 Système de Détection d'Intrusion de Noeud Réseau « NNIDS »

Ce nouveau type d'IDS (NNIDS) fonctionne comme les NIDS classiques, c'est-à-dire vous analysez les paquets du trafic réseau. Mais ceci ne concerne que les paquets destinés à un noeud du réseau (d'où le nom).

Une autre différence entre NNIDS et NIDS vient de ce que le NIDS fonctionne en mode "promiscuité ", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à destination d'une adresse ou d'une plage d'adresse. Puisque tous les paquets ne sont pas analysés, les performances de l'ensemble sont améliorées. Ce type d'IDS n'est pas encore très répandu, mais il est de plus en plus utilisé pour étudier le comportement des nœuds sensibles d'un réseau (15).

6.2 Selon la méthode de détection

6.2.1 Approche basé signature (misue detection)

Cette technique s'appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques. Elle ne tient pas compte des actions passées de l'utilisateur mais elle est basée sur la description des comportements suspects au travers des règles de description, appelées **signatures d'attaques** (ensemble de caractéristiques permettant d'identifier une activité intrusive: une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte, au niveau des paquet (jusqu'à TCP ou UDP) ou au niveau protocole (HTTP, FTP…)) (15) (16).

Les données à analyser se varient selon le type d'IDS :

- Cas **HIDS :** analyse des actions d'un utilisateur.
- Cas **NIDS :** vérification du flux d'informations sur le réseau (17).

De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion" qui consistent à maquiller les attaques utilisées. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'IDS.

Il est possible d'élaborer des signatures plus génériques, qui permettent de détecter les variantes d'une même attaque, mais cela demande une bonne connaissance des attaques et du réseau, de façon à stopper les variantes d'une attaque et à ne pas gêner le trafic normal du réseau.

La vérification des IDS est faite sur 2 niveaux :

- **Au niveau paquet**: l'analyse des différents paramètres de tous les paquets transitant et les comparer avec les signatures d'attaques connues.
- **Au niveau protocole:** elle sera réalisée si les commandes envoyées sont correctes ou ne contiennent pas d'attaque.

Cette fonctionnalité a surtout été développée pour HTTP actuellement (15).

Remarque :

Pour le Pattern Matching de nombreuses techniques et algorithmes sont utilisés tels que :

- Les algorithmes de recherche de motifs (ex : Boyer-Moore).
- Les algorithmes de comptage.
- Les algorithmes génétiques (16).

Le format standard d'une signature doit contenir les informations suivantes :

- **Nom de la signature** : le nom donné à la signature.
- **ID de signature** : un ID unique pour la signature.
- **Description de la signature :** description de la signature et ce qu'elle peut causer.
- **La description possible du faux positif :** une explication de tout « faux positif » qui peut être exploité et qui sont en fait une activité réseau normale.
- **Les Informations de vulnérabilité associées:** ce champ contient des informations de vulnérabilité associées.
- **Notes utilisateur :** ce champ permet à un professionnel de la sécurité d'ajouter des notes spécifiques liées à son réseau (18).

6.2.2 L'approche comportementale (Anomaly Detection)

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Pour cela, il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent (16).

Le comportement légitime peut être appréhendé lors d'une phase d'apprentissage, où le système de détection d'intrusions apprend en observant un hôte sain. Pour cela les IDS utilisent des méthodes différentes :

- **Systèmes experts** : Ici, c'est une base de règles qui décrit statistiquement le profil de l'utilisateur au vu de ses précédentes activités. Son comportement courant est comparé aux règles, à la recherche d'une anomalie. La base de règles est rafraîchie régulièrement. L'outil Wisdom &Sense utilise cette méthode, aujourd'hui tombée en désuétude.
- **Réseaux de neurones** : La technique consiste à apprendre à un réseau de neurones le comportement normal d'un utilisateur. Par la suite, lorsqu'on lui fournira les actions courantes, il devra décider de leur normalité. L'outil Hyperview comporte un module de ce type et plusieurs travaux de recherche vont dans le même sens. Cette méthode reste prometteuse, mais n'est pas encore industrialisée.
- **Immunologie :** Cette analogie informatique de l'immunologie biologique a été proposée par Forrest. Il s'agit de construire un modèle de comportement normal des services réseaux Unix (et non un comportement normal d'utilisateurs). Le modèle consiste en un ensemble de courtes séquences d'appels système représentatifs de l'exécution normale du service considéré. Des séquences d'appels

étrangères à cet ensemble sont alors considérées comme la potentielle exploitation d'une faille du service.

- **Le data mining**: Aussi, cette approche peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion, … (19).
- **Les méthodes statistiques:** L'approche statistique est utilisée pour la génération d'un modèle de comportement normal d'un système. Elle consiste à générer le profil de comportement normal à partir d'un ensemble de variables aléatoires, échantillonnées à des intervalles réguliers dans le temps, ces variables peuvent être par exemple :

- Le temps CPU utilisé.
- Le nombre de connexions établi durant une période de temps.
- Les fichiers les plus fréquemment utilisés.
- Les entrées/sorties effectuées (3).

6.3 Selon le type de réponse

Il existe deux types de réponses, suivant les IDS utilisés. La réponse passive est disponible pour tous les IDS, la réponse active est plus ou moins implémentée (15)**.**

6.3.1 Réponse active

La réponse active a pour but de stopper une attaque au moment de sa détection et isoler l'attaquant. Pour cela on dispose de deux techniques : la reconfiguration du firewall et l'interruption d'une connexion TCP. Cette opération peut consister à modifier l'état d'alerte de l'IDS, à fermer des connexions réseaux, en tuant des processus malfaiteurs (15) (14).

6.3 Réponse passive

La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable sécurité (15). Généralement les réponses passives des IDS aident les administrateurs réseaux à prendre des décisions sur la base des informations fournies par ces dernières, Dans ce cas le système de détection d'intrusions génère simplement des alarmes (comme afficher un message sur l'écran, générer un son spécifique ou envoi d'un email, ...).

Parmi les réponses passives :

- **L'alarme :** est produite lors d'une détection d'attaque soit par des messages d'alerte sur écran ou par téléphone ou par e-mails.
- **SNMP Trap :** le protocole SNMP (Sample Network Management Protocol) est utilisé pour la gestion du réseau. Les IDS envoient leurs rapports d'alarmes à travers ce protocole

- **L'archivage:** permet de faire des analyses et des corrélations avec l'historique d'attaques antécédentes des évènements qui se sont produits auparavant (20).

6.4 Selon la fréquence d'utilisation

Les systèmes de détection d'intrusions analysent des données pour établir si une attaque est en cours. Cette analyse peut être en temps réel ou bien réalisée après capture des événements à étudier (14).

6.4.2 Analyse continue (Temps réel)

Les IDS analysent le flux d'informations en continu. Ce mode est communément utilisé dans les IDS réseau, le trafic réseau est analysé directement après la capture. L'analyse en continue permet de prendre des actions immédiates contre toute activité malveillante détectée. Ce mode est efficace dans le cas où la vitesse de traitement des IDS est supérieure à la vitesse de transfert dans le réseau, sinon il est impossible de faire l'analyse en temps réel (21). Cela est nécessaire dans des contextes sensibles (confidentialité) et/ou commerciaux (confidentialité, disponibilité). C'est toutefois un processus coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système (19).

6.4.2 Analyse périodique

Certains systèmes de détection d'intrusions analysent périodiquement les fichiers d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans des contextes peu sensibles (une analyse journalière, par exemple) (19).

7. Classification des IDS

La figure suivante présente un schéma qui résume la classification des IDS faite précédemment :.

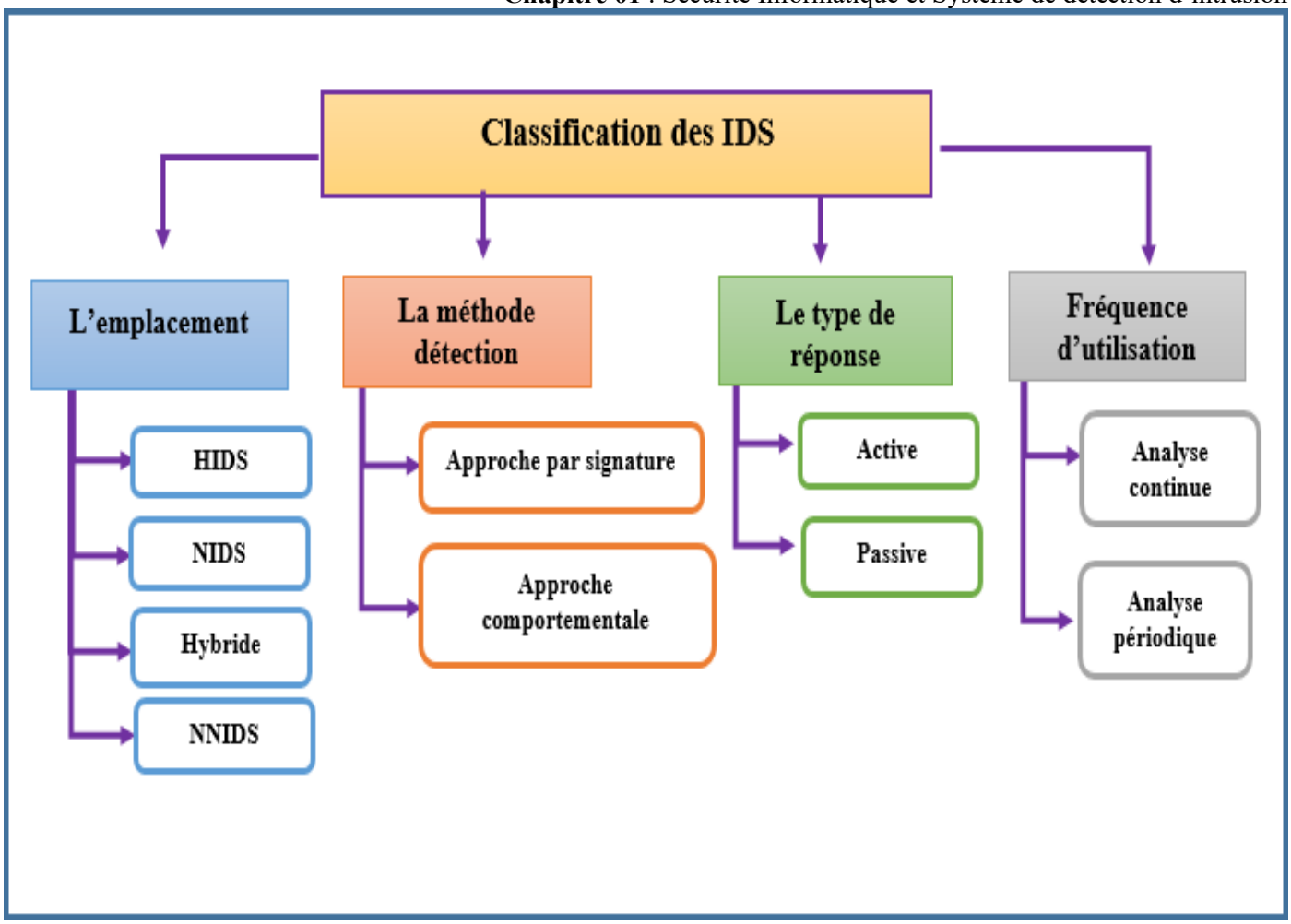

Figure 1. 2: Classification des IDS selon différents critères (19).

8. Architecture des IDS

Plusieurs architectures ont été proposées pour décrire les différents éléments intervenants dans un système de détection d'intrusion. L'architecture la plus simple est composée de trois modules : la source de données, l'analyseur des données et le module des réponses. L'architecture générale d'un IDS proposée par **IDWG (I**ntrusion **D**étection **W**orking **G**roup) est montrée dans la (Figure 1.3).

Dans l'architecture proposée par le groupe IDWG de l'IETF[2] on trouve les trois modules cités précédemment couplés avec d'autres composants, Dans cette architecture, l'objectif été la définition d'un standard de communication entre les composants du système de détection d'intrusion. Cette architecture définit un format d'échange de message pour les IDS : **I**ntrusion **D**étection **M**essage **E**xchange **F**ormat (**IDMEF**), qui contient implicitement un modèle de données. Proposée par IDWG.

[2] L'**I**nternet **E**ngineering **T**ask**F**orce, **(IETF)**: est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration des standards Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

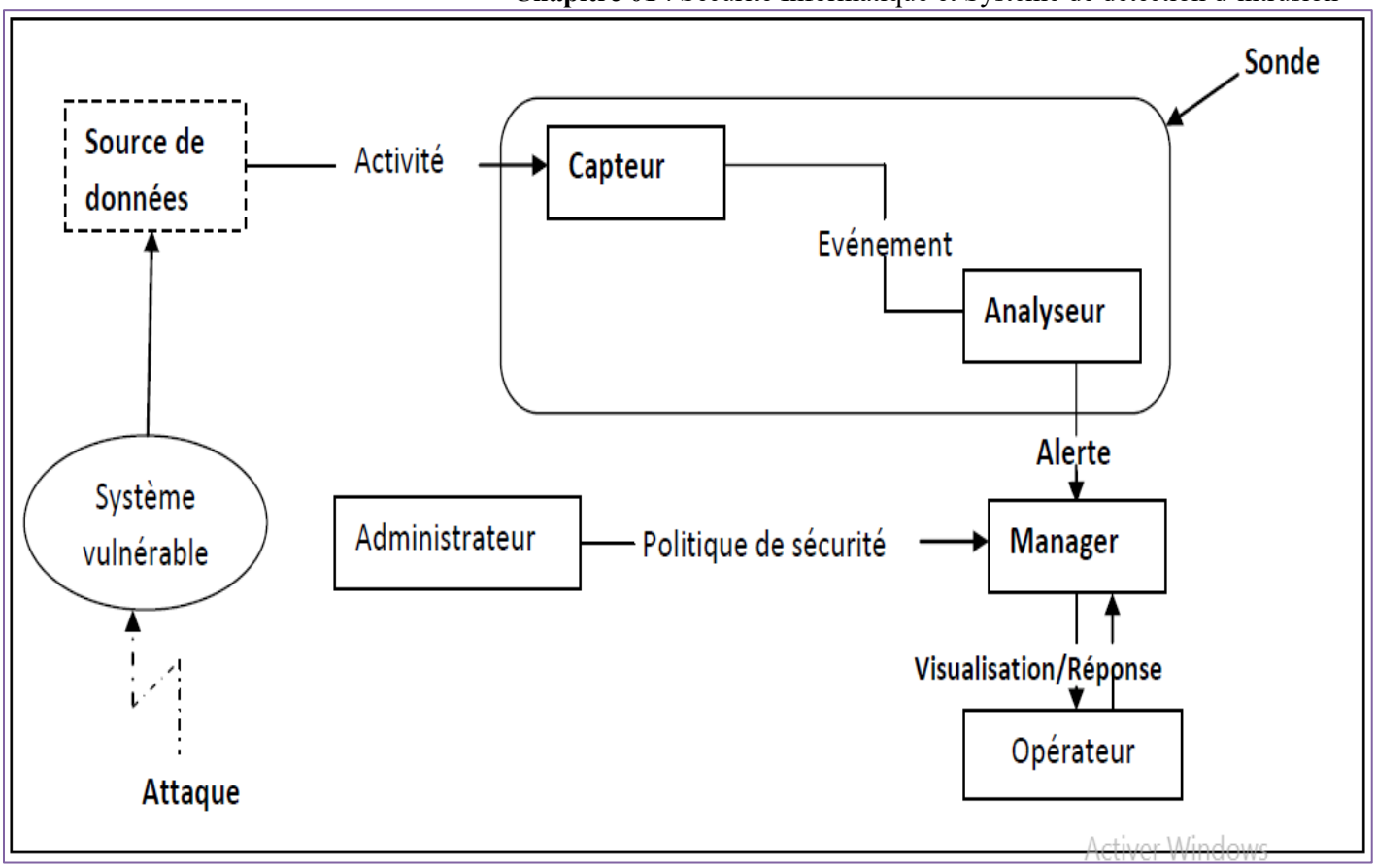

Figure 1. 3: Architecture d'un IDS proposée par IDWG (21)

Cette architecture est composée des modules suivants :

- **Source de données**: C'est l'interface entre le système surveillé et l'IDS, elle fait la collecte d'informations sur les activités du système.
- **Capteur**: Chargé de filtrer et formater les informations brutes envoyées par la source de données. Le résultat de ce traitement sera un message formaté, appelé aussi événement, il représente l'unité de base dans un scenario d'attaque.
- **Analyseur**: Permet d'analyser les événements générés par le capteur. S'il détecte une activité intrusive il émet une alerte, qui est un message sous un format standard. Dans cette architecture, le capteur et l'analyseur forment ensemble une sonde.
- **Alertes :** Lorsqu'un IDS détecte une intrusion, il doit la signaler à l'administrateur à travers les alertes, Ces dernières générées par les IDS sont généralement stockées dans les journaux du système ou utilisés pour prendre des actions contre les attaques (cela dépend du type d'IDS : à réaction active ou passive). Cependant il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité d'inter-opérer. Ce format s'appelle **IDMEF**(**I**ntrusion **D**étection **M**essage **E**xchange **F**ormat), où il est possible de les visualiser ultérieurement par un expert de sécurité.

- **Manager**: En plus de la notification des alertes, il offre à l'administrateur la possibilité de configurer une sonde et de gérer les alertes envoyées par l'analyseur.

9. Principe de fonctionnement des IDS

La Figure 1.4 illustre le fonctionnement d'un IDS et l'enchainement de ses actions lors de la détection des intrusions.

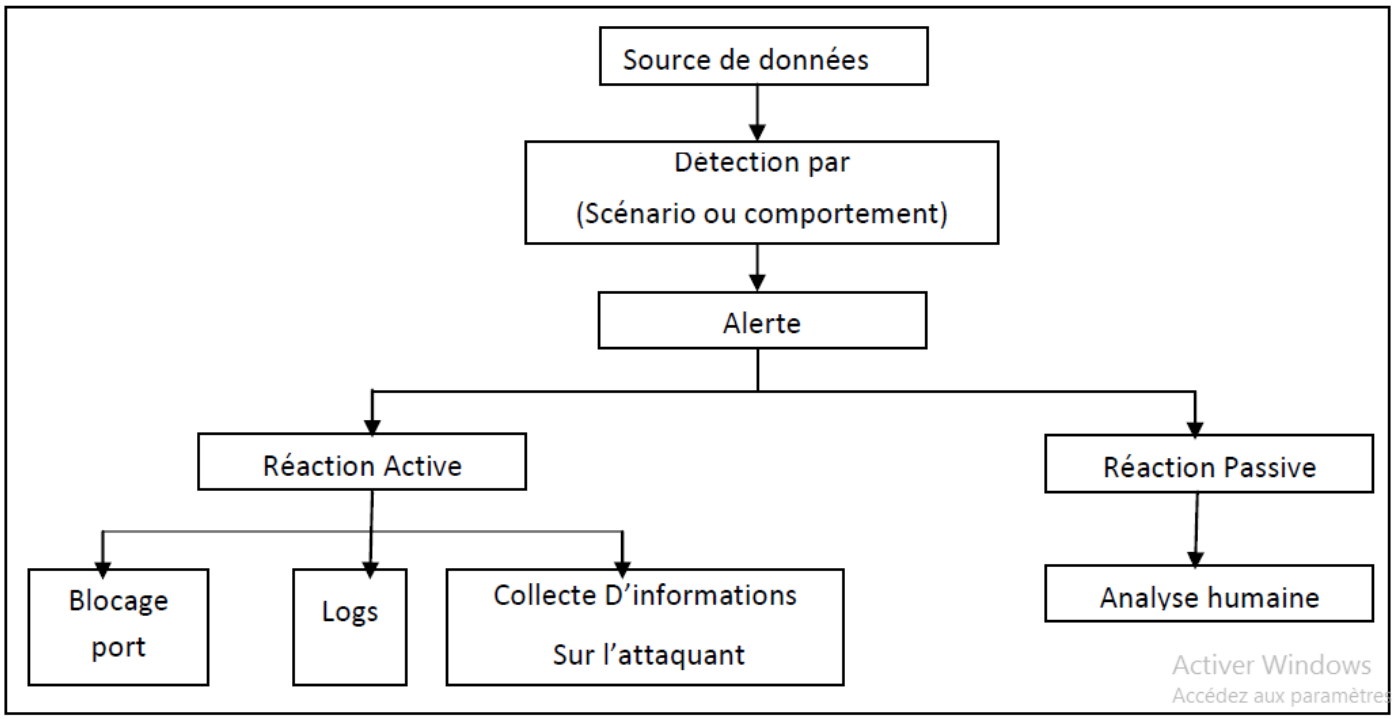

Figure 1. 4: Fonctionnement d'un IDS (22)

10. Points forts et faibles des IDS

Points fortes	Points faibles
✓ **Surveille et analyse les événements système et les comportements des utilisateurs** ✓ **Déterminer l'état de sécurité d'un système, puis suivre les modifications apportées à cet état de référence.** ✓ **Reconnaître les modèles d'événements système qui correspondent à des attaques connues.** ✓ **Gérer les mécanismes d'audit et de journalisation des systèmes d'exploitation et les données générées par ces derniers.**	✗ Ne compensent pas les mécanismes de sécurité faibles ou manquants dans la protection d'infrastructure. Ces mécanismes comprennent les pare-feu, l'identification, l'authentification, le cryptage des liens, la détection des et l'éradication. ✗ Difficile de détecter, signaler et répondre instantanément à une attaque, lorsqu'il y a un grand réseau ou une charge de traitement. ✗ Ne peuvent pas détecter les attaques récemment publiées ou les variantes d'attaques existantes.

✓ **Peut détecter les pirates externes ainsi que les attaques internes basées sur le réseau.** ✓ **S'adapte facilement pour assurer la protection de l'ensemble du réseau.** ✓ **Offre une gestion centralisée pour la corrélation des attaques distribuées.** ✓ **Fournit une défense en profondeur** ✓ **Donne aux administrateurs système la possibilité de quantifier les attaques.** ✓ **Fournit une couche de protection supplémentaire.**	✖ Ne peuvent pas résister aux attaques visant à les contourner ✖ Ne peuvent pas gérer le trafic réseau crypté. ✖ Génèrent une énorme quantité de données à analyser

Tableau1. 2: Les points forts et faibles des IDS (18) (23)

11.Conclusion

Dans ce chapitre, nous avons présenté le système de détection d'intrusions et nous avons également étudié d'une manière détaillée les différents types d'IDS selon différents critères de classification avec la présentation générale des différentes techniques utilisées pour la détection d'intrusions.

Afin d'obtenir un système de détection d'intrusions compétent et efficace, il est souhaitable d'utiliser les deux techniques de détection comportementale et basée connaissances en parallèle pour surmonter les problèmes liés à chacune de ces deux techniques de détection. Cependant, les systèmes de détection d'intrusions commercialisés emploient seulement la technique de détection basée connaissance, ce qui motive les différents efforts de recherche dans le domaine de la détection d'anomalies.

Pour cette raison, différentes approches sont utilisées pour implémenter la technique de la détection d'anomalies. Parmi ces approches diverses, nous intéresserons à l'approche immunologique qui constitue un intérêt accru des recherches actuelles vu de l'analogie qui existe entre le système de détection d'intrusions et le système immunitaire humain. Cette approche qui présente beaucoup d'aspects intéressants pour le développement d'un système de détection d'intrusions efficace.

Le deuxième chapitre sera consacré à étudier d'une manière détaillée les systèmes immunitaires artificiels. Cette approche qui s'inspire par le mécanisme de défense humain et qui présente des capacités intéressantes d'apprentissage, d'adaptation et d'évolution pour détecter les anomalies afin d'entretenir les réseaux informatiques sereins.

Chapitre 02 :
Les Systèmes Immunitaire Artificielle

Introduction

Un intérêt croissant d'utiliser la biologie comme source d'inspiration pour résoudre différents problèmes. Ce domaine de recherche se base principalement sur l'extraction des métaphores utiles à partir des systèmes biologiques afin de créer des solutions informatiques efficaces aux problèmes complexes. Les développements les plus appréciables ont été les réseaux de neurones inspirés par le fonctionnement du cerveau, et les algorithmes évolutionnaires inspirés par la théorie de l'évolution darwinienne

Cependant, plus récemment, un intérêt croissant pour l'utilisation d'un autre système biologique qui est le système immunitaire comme source d'inspiration pour résoudre des problèmes complexes. Le système immunitaire biologique est doté par des capacités de traitement de l'information y compris l'identification du modèle, l'apprentissage, la mémorisation et le traitement parallèle distribué. Pour ces dernières et d'autres raisons, le système immunitaire a suscité un intérêt significatif pour l'employer comme une métaphore d'inspiration dans le calcul. Ce domaine de recherche est connu sous l'appellation des ***systèmes immunitaires artificiels***.

Ce chapitre sera composé de deux parties principales dont la première partie sera consacrée à la présentation du système immunitaire biologique, en exhibant les différents composants immunitaires et les différents mécanismes utilisés par ce système. Enfin, nous récapitulerons les propriétés intéressantes du système immunitaire qui constituent d'un point de vue informatique une source d'inspiration très riche. Tandis que la deuxième partie sera consacrée à définir le système immunitaire artificiel (AIS) et le processus de conception d'un AIS. Ainsi, nous intéresserons à présenter les différents algorithmes et les modèles immunitaires. La dernière section de cette partie expose les tentatives d'extension du système immunitaire artificiel en intégrant une nouvelle théorie immunologique qui est la théorie de danger.

I. Les systèmes immunitaires naturel « SIN »

1. Introduction

Toutes les créatures vivantes sont dotées par un système immunitaire, par exemple quelques plantes ont des épines protectrices pour fournir la protection de prédateurs qui les attaquent. Les animaux contiennent des os (des vertébrés) qui ont développé un système immunitaire fortement efficace et complexe

Notre étude sera focalisée sur le système immunitaire de vertébrés, plus spécifiquement le système immunitaire humain. C'est dû aux caractéristiques intéressantes d'une perspective biologique et informatique et la compréhension de son fonctionnement.

2. Historique

Le terme immunité provient du latin « *immunis »* qui désignait une exemption de charges, telles que services, impôts, etc. Elle doit son nom au fait que les premiers phénomènes immunitaires ont été observés par des bactériologistes qui constataient des effets de protection contre des infections (24) .

Dès 430 av. J.-C., il a été laissé entendre que si l'on survit à une maladie, la personne devient alors « immunisée » contre toute exposition ultérieure. Cependant, cela n'a jamais été reconnu comme la preuve d'un certain type de système de défense interne jusqu'à la fin du XVIIe siècle.

Bien que la plupart des récits historiques attribuent à **Edward Jenner** le développement du premier processus de **vaccination**, une procédure similaire antérieure avait été établie en Chine en 1700. Cette technique était appelée variolation. Cela provenait du nom de l'agent infectieux - le **virus variolique**. Le principe de base de la variolation était de provoquer délibérément une légère infection par un pathogène non modifié.

En 1798, Edward Jenner a remarqué que les laitières étaient protégées de la variole si elles avaient été infectées pour la première fois par la **variole**. Ce n'était pas son intention de faire l'histoire médicale (25).

Dans les années soixante Rodney Porter et Gerald Edelman parviennent à élucider la structure des anticorps, et furent lauréats du prix Nobel de médecine en 1972.

En 1989, Charles Janeway propose un modèle selon lequel, ce serait l'immunité innée qui serait la véritable gardienne des clefs du déclenchement d'une réponse immunitaire.

Au début des années 1900, Jules Bordet et Karl Landsteiner présente leurs travaux sur la notion de « spécificité immunologique ». Il découvre que le système immunitaire est capable de produire des anticorps spécifiques contre les produits chimiques synthétisés artificiellement, sachant qu'ils n'ont jamais existé à l'état naturel (13).

Le tableau suivant résume les jalons de l'histoire de l'immunologie qui comprennent:

Année	Evénement
1798	**Edward Jenner** lance la vaccination contre la variole.
1879	**Louis Pasteur** met au point un vaccin atténué contre le choléra du poulet.
1885	**Louis Pasteur** met au point un vaccin contre la rage.
1891	**Robert Koch** explore l'hypersensibilité de type retardé.
1900	**Paul Erlich** théorise la formation d'anticorps spécifiques.
1906	**Clemens Von Pirquet** a inventé le mot allergie.
1938	**John Marrack** formule une hypothèse de liaison antigène-anticorps
1959	**Niels Jerne, David Talmage, et Macfarlane Burnet** développent la théorie de la **sélection** clonale
1957	**Alick Isaacs** et **Jean Lindemann** découvrent l'interféron (cytokine).
1962	**Rodney Porter** et son équipe découvrent la structure des anticorps.
1962	**Jaques Miller** et son équipe découvrent l'implication du thymus dans l'immunité cellulaire.
1962	**Noel Warner** et son équipe distinguent les réponses immunitaires cellulaires et humorales.
1960	**Anthony Davis** et son équipe découvrent la coopération entre **les cellules T** et les **cellules B** dans la réponse immunitaire.
1974	**Rolf Zinkernagel** et **Peter Doherty** explorent la restriction du **complexe majeur d'histocompatibilité « CMH » .**
1985	**SusumuTonegawa** , **Leroy Hood** et l'équipe identifient les gènes d'immunoglobulines.
1987	**Leroy Hood** et son équipe identifient les gènes du récepteur des lymphocytes T
1985	Les scientifiques commencent l'identification rapide des gènes des cellules immunitaires qui se poursuit jusqu'à présent.

Tableau 2. 1: Les jalons de l'histoire de l'immunologie (25).

3. Le système immunitaire naturel

Le système Immunitaire Naturel (NIS naturel immun system) est un système complexe composé d'organes, de cellules et de globules blanches ou lymphocytes. Le rôle du système immunitaire est de protéger le système contre les phénomènes étrangers appelés antigènes. (13).

Le système immunitaire permet de préserver l'organisme de dysfonctionnements internes et d'agressions externes. L'organisme est un ensemble complexe de 3 milliards de cellules et 10 milliards de bactéries, qui doivent fonctionner ensemble pour avoir une bonne santé. Pour assurer cette tâche, le système immunitaire dispose d'une batterie de processus de contrôle et de défense (26).

4. L'architecture du système immunitaire

Le corps humain est doté par plusieurs mécanismes de défense qui s'étendent à plusieurs niveaux. La première ligne de défense est composée de barrières physiques qui sont : la peau, l'urine, les membranes muqueuses, etc. Si cette première ligne échoue d'éliminer un intrus alors le système immunitaire utilise d'autres mécanismes de défense. Le système immunitaire possède une architecture multicouche [20, 25,43] qui est constituée de deux couches inter-liées qui sont ***le système immunitaire inné*** et ***le système immunitaire adaptatif ou acquis*** **(**Figure 2.1).

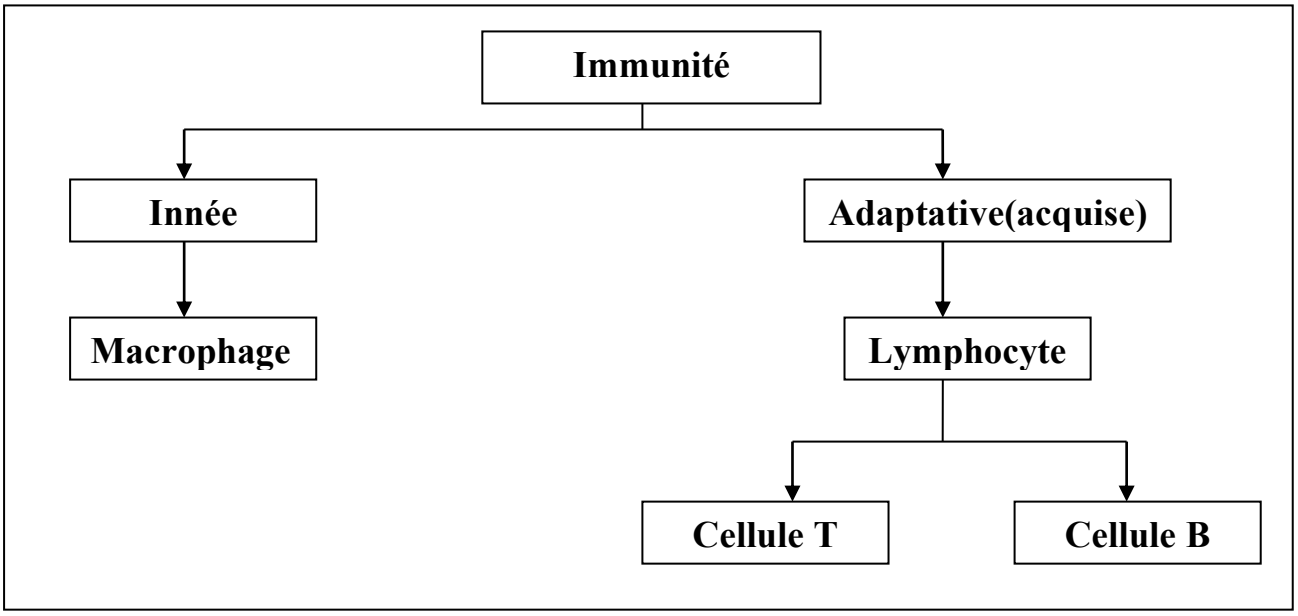

Figure 2. 1: Architecture du système immunitaire

4.1 Le système immunitaire inné :

Le système immunitaire inné est composé d'un ensemble de cellules spécialisées dont le rôle principal est la liaison avec des modèles moléculaires trouvés dans des micro-organismes. Cependant, ce système ne peut pas assurer la protection complète du corps. Il est caractérisé par (27) (28):

- Les mécanismes de détection des organismes étrangers sont constants, aussi bien pour les infections répétées.
- La réponse du système immunitaire inné est non spécifique à un type particulier d'intrus mais elle est identique contre tous les pathogènes qui envahissent le corps.
- Il joue un rôle vital pour l'initialisation et la régularisation de la réponse immunitaire adaptative.

4.2 Le système immunitaire adaptatif :

Le système immunitaire adaptatif est constitué de types différents de cellules dont chacun joue un rôle important. Le rôle central est assuré par les lymphocytes qui sont composés de deux types de cellules : ***cellule B*** et ***cellule T***. Le système immunitaire adaptatif est caractérisé par (21) :

- Le système immunitaire adaptatif s'occupe avec les intrus qui ne sont pas détectés par le système immunitaire inné.
- Le système immunitaire adaptatif est généré dynamiquement contre les organismes étrangers pendant sa durée de vie. Il fournit des mécanismes plus efficaces qui seront daptés aux changements antigéniques.
- Le système adaptatif est adressé à des intrus spécifiques.
- La présence d'une mémoire immunologique qui permet aux cellules de se souvenir des intrus déjà rencontrés lors des prochaines rencontres.

5. Les concepts immunologiques

Le système immunitaire qui nous protège des facteurs externes et internes, est un réseau complexe d'organes, de tissus et de cellules spécialisées, répartis dans tout le corps, de façon interconnectées et coordonnées.

5.1 Les organes du système immunitaire

Fonctionnellement, les organes du système immunitaire se divisent en deux catégories :

5.1.1 Les organes primaires ou centraux

Leur fonction est de fournir le microenvironnement propice à la formation et la maturation des lymphocytes. Les lymphocytes sont les principales cellules du système immunitaire, responsables de l'immunité spécifique. Les organes primaires du système immunitaire sont les suivants :

- **Le foie fœtal** est l'organe qui assure la fonction de maturation des cellules B mais il est remplacé progressivement par la moelle osseuse pendant la croissance.
- **La moelle osseuse** adulte est le lieu où se développent les lymphocytes B.
- **Le thymus** est la glande endocrine dans laquelle maturent les lymphocytes T.

5.1.2 Les organes secondaires ou périphériques

Leur fonction est de fournir aux lymphocytes un environnement adéquat pour leur permettre d'interagir entre eux, avec les cellules présentatrices d'antigènes et avec d'autres cellules, afin qu'ils entrent en contact avec l'antigène et que s'enclenche la réponse immunitaire

Les organes secondaires du système immunitaire sont les suivants :

- **Les amygdales,** des bandes de tissus lymphoïdes situés dans le pharynx constituant l'anneau de Waldeyer qui protège l'entrée des voies respiratoires de l'invasion bactérienne.
- **Les plaques de Peyer,** des agrégats de tissus lymphatiques qui recouvrent l'intérieur des muqueuses de l'intestin et des voies respiratoires.
- **La rate**, un organe situé dans le quadrant supérieur gauche de la cavité abdominale, d'une grande importance dans l'immunité cellulaire et l'immunité humorale.
- **Les tissus lymphoïdes** associés aux muqueuses (MALT), agrégats de cellules lymphoïdes sans organisation ni structure, associés à plusieurs organes du corps tels que les bronches, le tractus gastro- intestinal ou le nez.
- **La moelle osseuse**, tissu situé à l'intérieur des os longs, du bassin osseux, des vertèbres etc. fait également partie des organes secondaires de la réponse immunitaire (29).

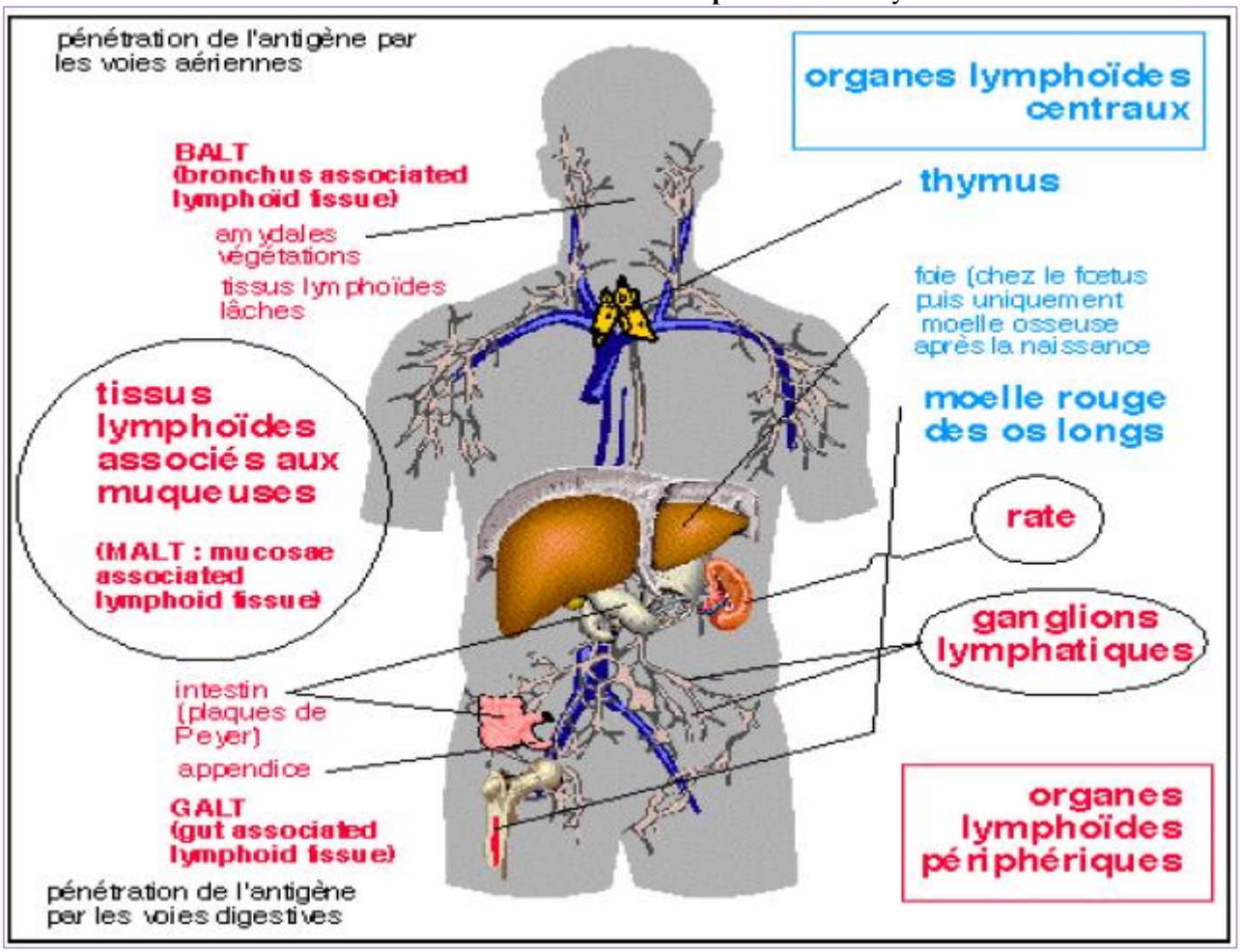

Figure 2. 2: les différents organes du système immunitaire (30)

5.2 Les cellules immunitaires

En plus des organes, le système immunitaire possède d'autres types de cellules immunitaires qui ont des rôles divers au sein de l'organisme, notamment dans la différenciation de ces cellules au niveau de la moelle osseuse, mais aussi dans la réponse immunitaire, etc.

5.2.1 Les cellules de la réponse innée

5.2.1.1 Les phagocytes

Les **phagocytes** ou **cellules phagocytaires** sont les éboueurs de l'organisme, capables d'endocyter des bactéries et des cellules mortes ; Parmi eux on compte les monocytes, macrophages et les cellules dendritiques.

a) Le monocyte

Le monocyte est une cellule sanguine immature de la famille des leucocytes, qui provient de la moelle osseuse. Cette cellule se différencie une fois dans les tissus où elles résideront et sera ainsi à l'origine des macrophages et des cellules dendritiques.

b) Le macrophage

Le macrophage est la cellule phagocytaire par excellence qui provient de la différenciation des monocytes. Il joue également le rôle de **cellule présentatrice d'antigène**.

Un des rôles principaux des macrophages est le nettoyage de l'organisme contre les poussières et les agents pathogènes. Les macrophages résidents portent chacun une appellation caractéristique suivant le tissu dans lequel il se trouve : les **cellules de Kupffer** dans le foie, les **cellules microgliales** dans les tissus nerveux, les **macrophages alvéolaires** dans les poumons…

c) La cellule dendritique (CD)

La cellule dendritique est une cellule immunitaire présentant des expansions cytoplasmiques appelées des **dendrites**, et présente dans l'ensemble des tissus de l'organisme, plus spécifiquement au niveau de l'épiderme et au niveau du thymus. Elle a deux origines, soit **myéloïde** en dérivant du monocyte, soit **lymphoïde**.

La cellule dendritique a différent rôle dans la réponse immunitaire :

- Elle joue le rôle de **cellule phagocytaire** et de **cellules présentatrice d'antigène**, lui permettant d'activer les lymphocytes (B et T) présents au niveau des organes lymphoïdes secondaires. Elle a donc un rôle principal dans l'**activation de la réponse immunitaire adaptative**. En effet une fois l'antigène phagocyté et présenté, la cellule dendritique quitte son lieu de résidence et migre vers les organes lymphoïdes secondaires.
- Au niveau du thymus elle joue un rôle essentiel dans le maintien de la tolérance au soi, dans la sélection négative des lymphocytes T.

5.2.1.2 La cellule NK (Naturel Killer)

La cellule NK fait partie des lymphocytes car elle découle du **progéniteur lymphoïde** au niveau de la moelle osseuse; Elle ne correspond cependant ni à un lymphocyte B ni à un lymphocyte T, La cellule NK peut tuer les cellules cibles de manière spontanée, en faisant intervenir les molécules de classe 1 du CMH et sont capables de faire la différence entre une cellule saine et une cellule malade (31),elles sont spécialement importantes dans la détection et l'élimination des cellules infectées par les virus et les cellules tumorales (32).

5.2.1.3 Le mastocyte

Le mastocyte est une variété de leucocytes jouant un rôle primordial dans les **allergies**. Il est habituellement situé au niveau des **tissus conjonctifs**, des **poumons**, des **ganglions lymphatiques**, de la **rate** et bien évidemment de la **moelle osseuse** où il est produit.

Le mastocyte contient des granulations contenant de l'**histamine**, de l'**héparine**, de la **sérotonine** et des **enzymes diverses**. Le mastocyte a donc plusieurs effets : activation et amplification de la réaction inflammatoire et diminution de la coagulation sanguine**.**

5.2.2 Les cellules de la réponse adaptative

Les lymphocytes sont les cellules majeures de la réponse immunitaire adaptative qui font partis des **leucocytes**. Ils sont principalement de deux types :

- D'une part les **lymphocytes B** (**LB**) ou cellule B, dont la lettre « B » provient de la « **Bourse de Fabrice** » qui est un organe d'oiseaux dans lequel les LB arrivent à maturité. Chez l'Homme, les lymphocytes B arrivent à maturité dans la **moelle osseuse**. Ils sont caractérisés par la présence d'un **BCR** qui leurs permettent de reconnaître des fragments antigéniques.
- D'autre par les **lymphocytes T** (**LT**) ou cellule T, dont la lettre « T » provient du « **Thymus** », organe humain dans lequel les LT arrivent à maturité. Ils sont caractérisés par la présence d'un **TCR** qui leurs permettent de reconnaître des fragments antigéniques.

Les lymphocytes ont différentes localisations suivant leur stade de maturité, en effet ils sont d'avantages présents aux niveaux des organes lymphoïdes secondaires, du sang et de la lymphe lorsqu'ils ne sont pas encore activé et ont une localisation ubiquitaire lorsqu'ils sont activés.

Les lymphocytes sont les seules cellules sanguines à avoir une **double différenciation** et ceci sous l'influence de l'antigène.

5.2.2.1 Le lymphocyte B

Le lymphocyte B est responsable de l'**immunité humorale**, qui vise à produire les anticorps spécifiques de l'agent pathogène. En plus du BCR, le lymphocyte B est caractérisé par des **récepteurs de cytokines**, des protéines membranaires.

Le lymphocyte B aura 2 destinées, en effet il se différenciera :

- Soit en **plasmocytes** qui sécrètent les anticorps solubles qui iront se fixer sur l'antigène facilitant ainsi la phagocytose. Ces cellules ne présentent pas d'anticorps membranaires.
- Soit en **lymphocyte B mémoire** qui expriment à leur surface les anticorps spécifique d'un antigène, permettant une réponse plus rapide si une seconde infection se présente.

Le lymphocyte B joue également le rôle de **cellule présentatrice d'antigène.**

5.2.2.2 Le lymphocyte T

Le lymphocyte T est responsable de l'**immunité cellulaire**, qui vise à détruire les cellules pathogènes, que ça soit des bactéries ou des cellules cancéreuses. Principalement les lymphocytes T ont pour reconnaitre l'antigène et mettre en marche la **réponse immunitaire adaptative** [39]. On distingue plusieurs types de lymphocytes T :

- Les **LT CD8** qui ont comme destinée leur évolution en **LT cytotoxique**.
- Les **LT CD4** qui donneront des **LT helper** (ou **auxiliaires**) qui ont un rôle de régulation de la réponse immunitaire adaptative par activation d'autres cellules immunitaires (31).

Les Lymphocytes Tueurs (LT) sont produits dans la moelle osseuse, les LT achèvent leur maturation dans le thymus où ils acquièrent leurs marqueurs membranaires spécifiques et les **récepteurs T** qui leur permettent de reconnaître directement un peptide viral associé à une molécule du CMH, des cellules infectées par un virus (ou cellule cancéreuse par exemple). L'action des cellules cytotoxiques LT caractérise la **réponse à médiation cellulaire** (33)**.**

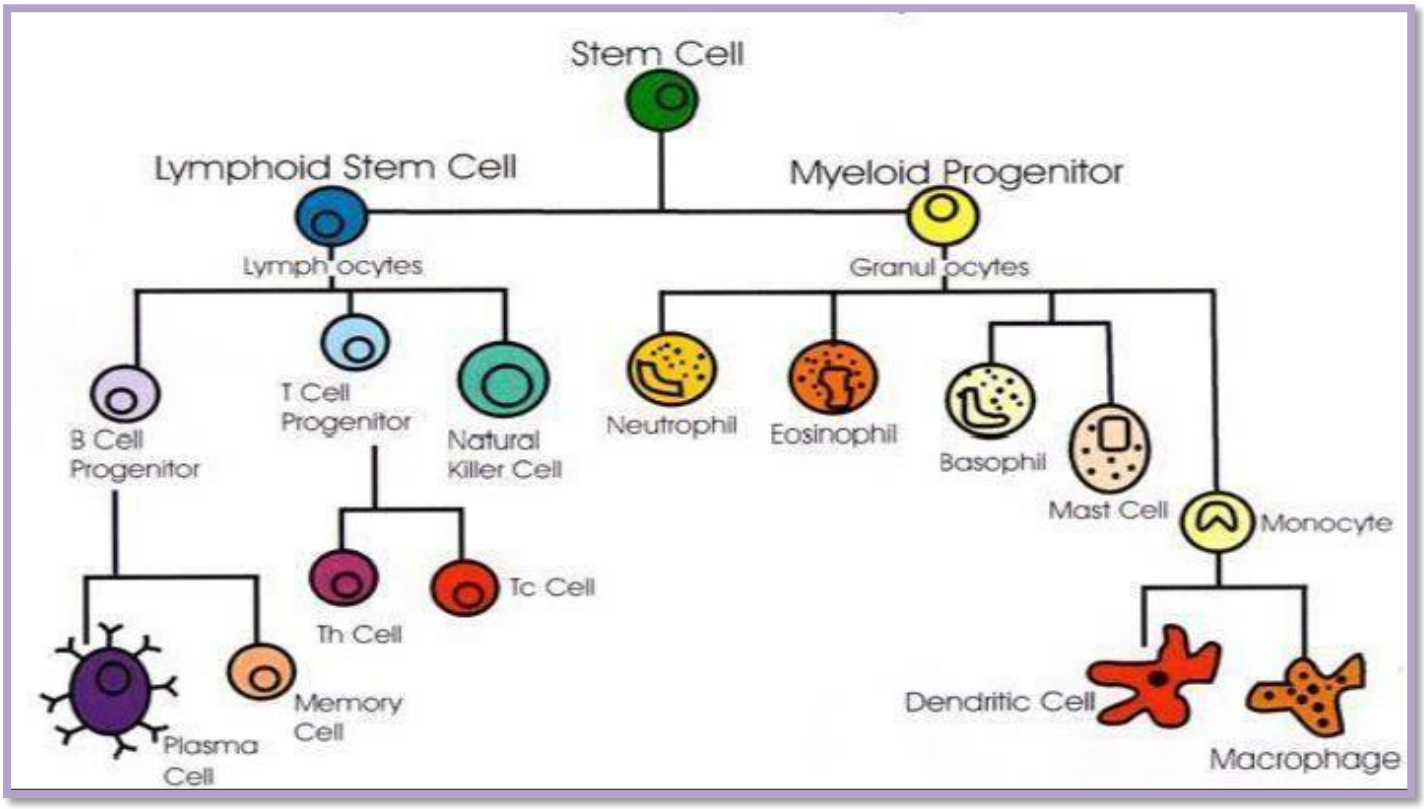

Figure 2. 3: les différentes cellules du système immunitaire (34)

5.2.2.3 Anticorps

a. La structure d'un anticorps :

Un anticorps est une molécule biologique impliquée dans l'immunité. C'est un complexe protéique. Si chaque organisme doté d'un système immunitaire code pour des milliards d'anticorps différents, ils possèdent tous les mêmes caractéristiques globales. Ce sont des glycoprotéines de la famille des immunoglobulines, formées de deux chaînes lourdes identiques (H pour *heavy*) et de deux chaînes légères identiques (L pour *light*). Ils sont souvent représentés en Y, où les deux chaînes lourdes sont reliées entre elles par un pont disulfure au niveau de la tige du Y. Les deux chaînes légères sont associées aux chaînes lourdes au niveau des bras du Y, également par des ponts disulfures.

Les anticorps contiennent des domaines constants (identiques pour tous les anticorps d'un même organisme) et des domaines variables (qui permettent la reconnaissance des corps étrangers) situés au bout des bras du Y. Les domaines variables constituent les **paratopes** de l'anticorps.

b. Les fonctions des anticorps :

Leur rôle est de reconnaître un antigène étranger afin de le neutraliser. Ils peuvent y parvenir grâce à la grande spécificité de leur **paratope**, qui ne reconnaît qu'une partie très précise de l'antigène : l'**épitope.** Dès qu'un anticorps reconnaît un épitope, le lymphocyte B qui code pour cet anticorps spécifique se multiplie et subit une maturation pour pouvoir synthétiser les mêmes anticorps, utiles, en grandes quantités (35).

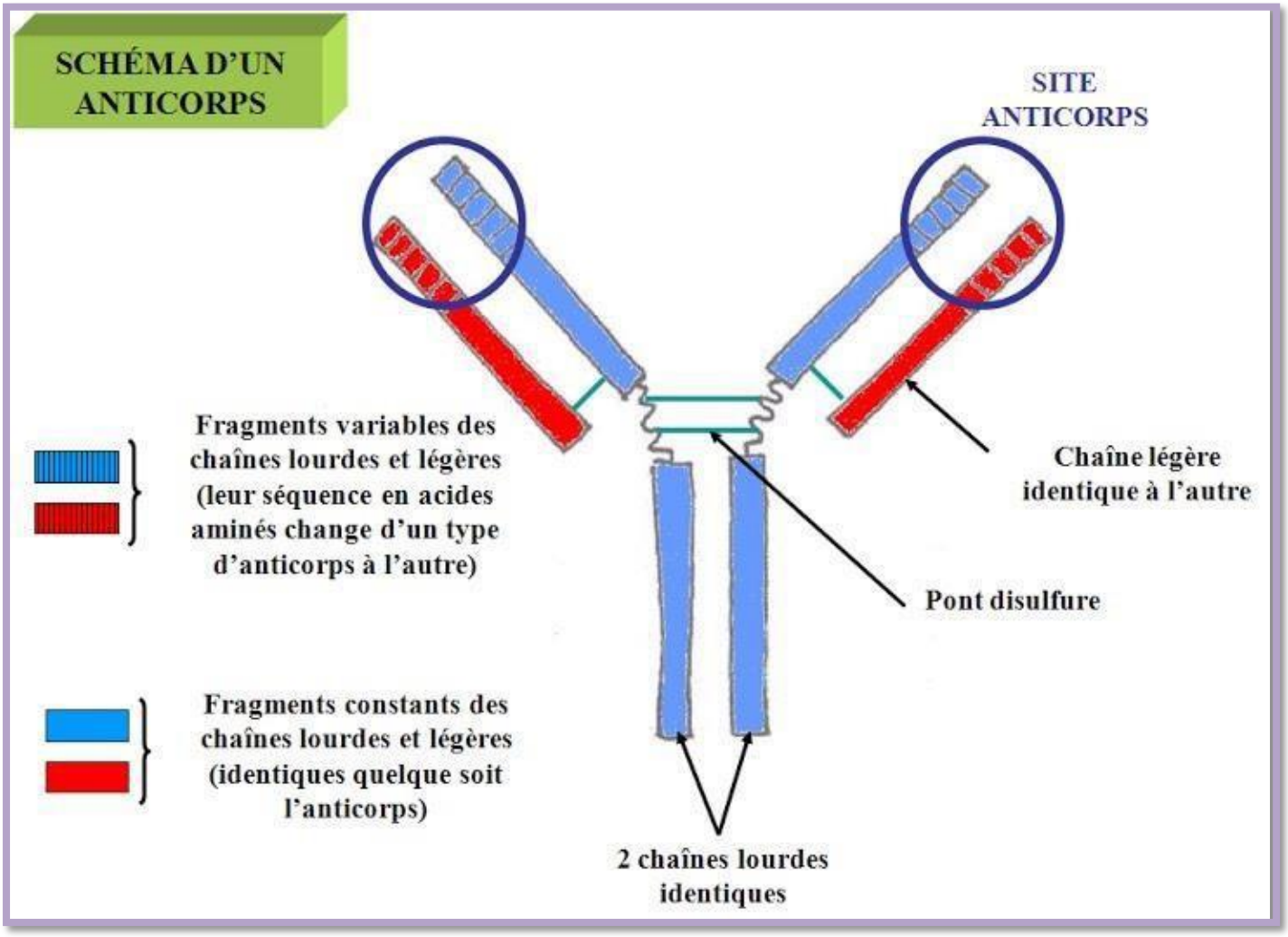

Figure 2. 4: Schéma d'un anticorps (36)

5.3 Antigènes

Un antigène est une substance microscopique, qui est étrangère à l'organisme et donc susceptible de déclencher une réaction immunitaire qui sera la production d'anticorps chargés de les neutraliser.

Toute substance étrangère, est un antigène en puissance. Il peut s'agir :

- D'un microbe comme un **virus** , une **bactérie** , un **champignon** .
- D'une molécule, à la condition qu'elle soit d'une taille conséquente (protéine en particulier), soit libre, soit fixée à une autre molécule ou un autre micro-organisme (on parle de motif antigénique).

- D'un médicament ou d'un produit toxique (37).

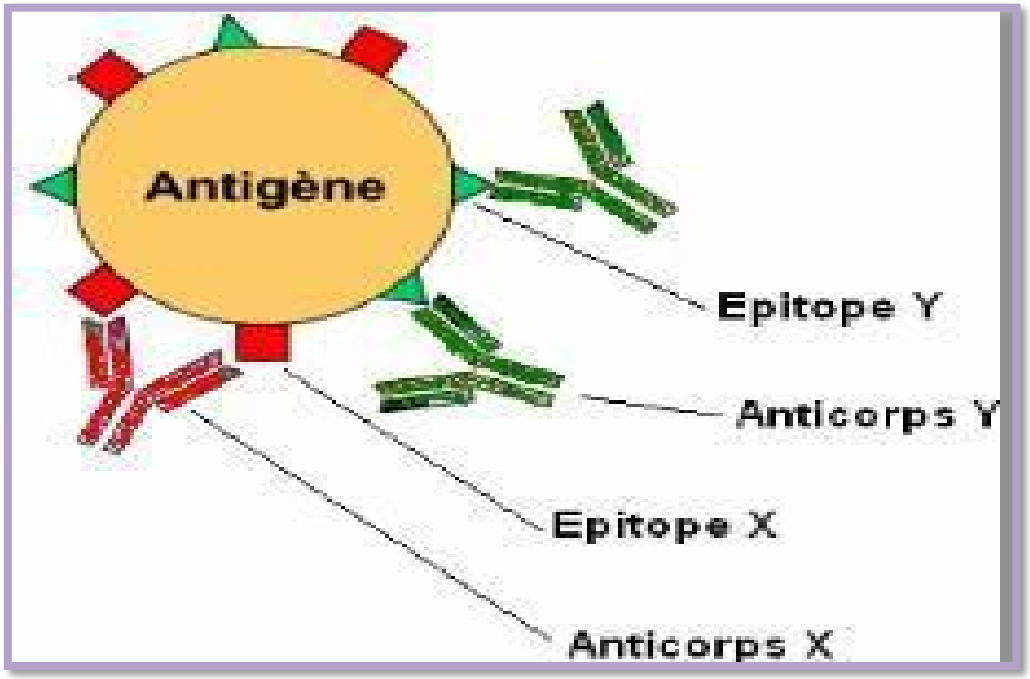

Figure 2. 5: Anticorps poly clonaux, liaison à des épitopes différents (38)

5.4 CMH

Complexe Majeur d'Histocompatibilité ou CMH, est un ensemble de gènes distribués le long d'un fragment d'ADN sur le chromosome 6 chez l'homme où il est appelé HLA (Le complexe **HLA** ou Human Leukocyte Antigens ; Partie localisée du génome humain dont les gènes codent notamment les antigènes majeurs d'histocompatibilité qui interviennent dans le contrôle de la réponse immunitaire et dans les phénomènes de rejet de greffes). Chez l'homme, il contiendrait plus de 200 gènes. Les gènes du CMH sont organisés en région codant trois classes de molécules: classe I, classe II et classe III ; les deux premières classes, impliquées dans la présentation antigénique aux cellules T, la classe III codant principalement pour des protéines sécrétées et ayant des fonctions immunitaires .En général le CMH serve à la reconnaissance des marqueurs du soi (39).

Il existe un polymorphisme important au niveau des gènes du CMH, si bien que, hormis chez les jumeaux homozygotes, il est quasiment impossible que deux personnes aient les mêmes marqueurs de CMH. Les molécules du CMH sont impliquées dans le phénomène de rejet de greffe. Les molécules du CMH de type I et II présentent les antigènes aux lymphocytes T. Le récepteur des lymphocytes T (TCR) interagit à la fois avec le peptide présenté et des acides aminés de la molécule du CMH. Il existe plusieurs types de molécules du CMH :

- **Les molécules du CMH de type I** présentes sur toutes les cellules nucléées et les plaquettes sanguines.

- **Les molécules de CMH de type II** présentes sur certaines cellules du système : macrophages, monocytes, lymphocytes B, cellules présentatrices d'antigènes...
- **Les molécules de CMH de type III** sont des molécules variées dont certaines font partie du complément ou des cytokines (35).

5.5 Tolérance et rupture de tolérance

La fonction du système immunitaire est d'assurer l'intégrité de l'organisme: pour cela, il reconnaît une variété considérable de pathogènes (microbes, parasites, virus…) sans pour autant réagir aux antigènes de l'individu (le soi). Cette absence de réponse aux antigènes du soi est appelée **tolérance immunitaire**. Elle résulte d'une éducation des lymphocytes B et T au cours de leur maturation, respectivement dans la moelle osseuse et le thymus.

L'établissement de cette tolérance a été postulé au début du 20ème siècle (1900) par le microbiologiste allemand **Paul Ehrlich**. Il est en effet le premier à avoir décrit la capacité du système immunitaire à rejeter les substances étrangères tout en laissant intactes les structures de l'organisme. Il est aussi le premier à avoir postulé que le détournement du système immunitaire pouvait aboutir à une auto-destruction de l'organisme (c'est ce que l'on observe dans les maladies auto immunes).

Il existe effectivement, des mécanismes empêchant le déclenchement de réactions immunitaires contre les molécules du soi et permettant de distinguer les antigènes du soi, des antigènes du non soi (généralement d'origine microbienne) comme L'élimination des lymphocytes très auto-réactifs, des processus de régulation immunitaire et autres (40).

6. Les théories immunitaires

Le comportement du système immunitaire est principalement régi par le processus de création des lymphocytes T pour la discrimination entre soi et le non-soi. Les lymphocytes T lors de leurs développements dans le thymus sont appeler cellules T naïves ou immatures. Ils subissent deux phase de criblage: le premier criblage par la sélection positive qui consiste à sélectionner les cellules T capables de reconnaître les peptides présentés par les molécules du CMH du soi ; A la fin de ce test leurs paratopes agréent au processus de réarrangement génétique pseudo aléatoire. Le second criblage par la sélection négative consiste à éliminer les cellules auto- réactives, qui pourraient être activées par les peptides présentés par les molécules du CMH à la surface des cellules saines. Le reste de la population est autorisé à quitter le thymus pour circuler dans le sang et effectuer leurs taches de surveillance (13).

6.1 La sélection positive

Pour acquérir la tolérance au soi, le thymus met tout d'abord en place une **sélection vis-à- vis du CMH** dite « **sélection positive** ». Seuls les lymphocytes qui expriment un TCR capable de reconnaitre une molécule HLA (c'est le CMH chez l'être humain) survivent et se multiplient. Les lymphocytes avec un TCR ne reconnaissant pas la protéine HLA sont éliminés car elles sont non fonctionnelles. Plus de 90% des cellules passant dans le thymus meurent lors de cette 1ère étape de sélection.

Cette sélection permet de conserver seulement les lymphocytes T capables de reconnaitre des antigènes dans un contexte restreint au CMH du Soi (les antigènes sont alors présentés par le CMH des cellules présentatrices comme les cellules dendritiques) (40).

6.2 La sélection négative

6.1 Pour les lymphocytes T

Les thymocytes simples positifs reconnaissent alors encore les molécules du soi comme les molécules du non-soi. Ils vont donc ensuite migrer vers la médulla au niveau de laquelle ils continueront leurs maturations et subiront la **sélection vis-à-vis du peptide** dite « **sélection négative** ». Cette dernière utilisera la caractéristique des **cellules dendritiques** à exprimer un facteur de transcription appelé **AIRE** (pour *Auto-Immune-Regulator-Element*) qui lui-même permet l'expression de peptides du soi de tissus n'ayant aucun rapport avec le thymus, eux-mêmes présentés par des molécules du CMH du soi ; ces cellules sont dites **auto-réactives**.

Ici ce sera donc les interactions entre les peptides du soi présentés par les molécules du CMH du soi exprimé à la surface des cellules dendritiques et le TCR des thymocytes au stade simple positif qui seront responsables de cette sélection négative ; on est à nouveau face à trois possibilités:

- Soit le thymocyte est capable de reconnaître le peptide présenté par les molécules du CMH avec une **forte affinité**, il sera alors considéré comme délétère pour le soi et sera **sélectionné négativement** en recevant un **signal de mort**.
- Soit le thymocyte est capable de reconnaître le peptide présenté par les molécules du CMH avec une **faible affinité**, il sera alors considéré comme acceptable et ne recevra **pas** de **signal de mort**.
- Soit le thymocyte n'interagit pas, il recevra alors un **signal de mort** (31)**.**

6.2 Pour les lymphocytes B

La sélection négative est appliquée aussi sur les cellules B dans la moelle osseuse, quand les cellules B immatures identifient les cellules du soi, elles seront éliminées. Ce mécanisme est appliqué seulement sur les cellules B immatures dans la moelle osseuse. La tolérance au soi des cellules nouvellement générées après le

processus de la sélection clonale et l'hypermutation somatique, sera assurée par l'assistance des cellules T d'aide (3).

6.3 La sélection clonale

a. Pour les lymphocytes T

Dans un état d'infection, seul un très petit nombre de lymphocytes porteurs des récepteurs spécifiques du pathogène sera activé, et après s'être divisé, se différenciera en cellules effectrices. En conséquence, tout lymphocyte stimulé par le pathogène donne naissance à une popul clonale de cellules qui toutes expriment une immunoglobuline ou un récepteur des cellules T identique à celui de la cellule initiale. Le processus par lequel les pathogènes sélectionnent des clones particuliers de lymphocytes en vue de leur expansion est appelé **sélection clonale** (41).

Chaque clone de lymphocytes T CD8 porte un seul type de récepteurs T apte à reconnaître un seul antigène présenté par les cellules dendritiques (cellules présentatrices de l'antigène : CPA) qui ont au préalable phagocyté et digéré un élément étranger.

Lorsque la reconnaissance s'effectue entre les antigènes / CMH (des CPA) et les récepteurs T (des lymphocytes T CD8), les LT CD8 sont activés et deviennent sensibles aux interleukines (facteurs stimulants) ; ils prolifèrent (par mitoses) et se transforment en cellules tueuses, les lymphocytes cytotoxiques (LTc), capables de détruire par contact une cellule infectée par un virus dont l'antigène a été reconnu (33)

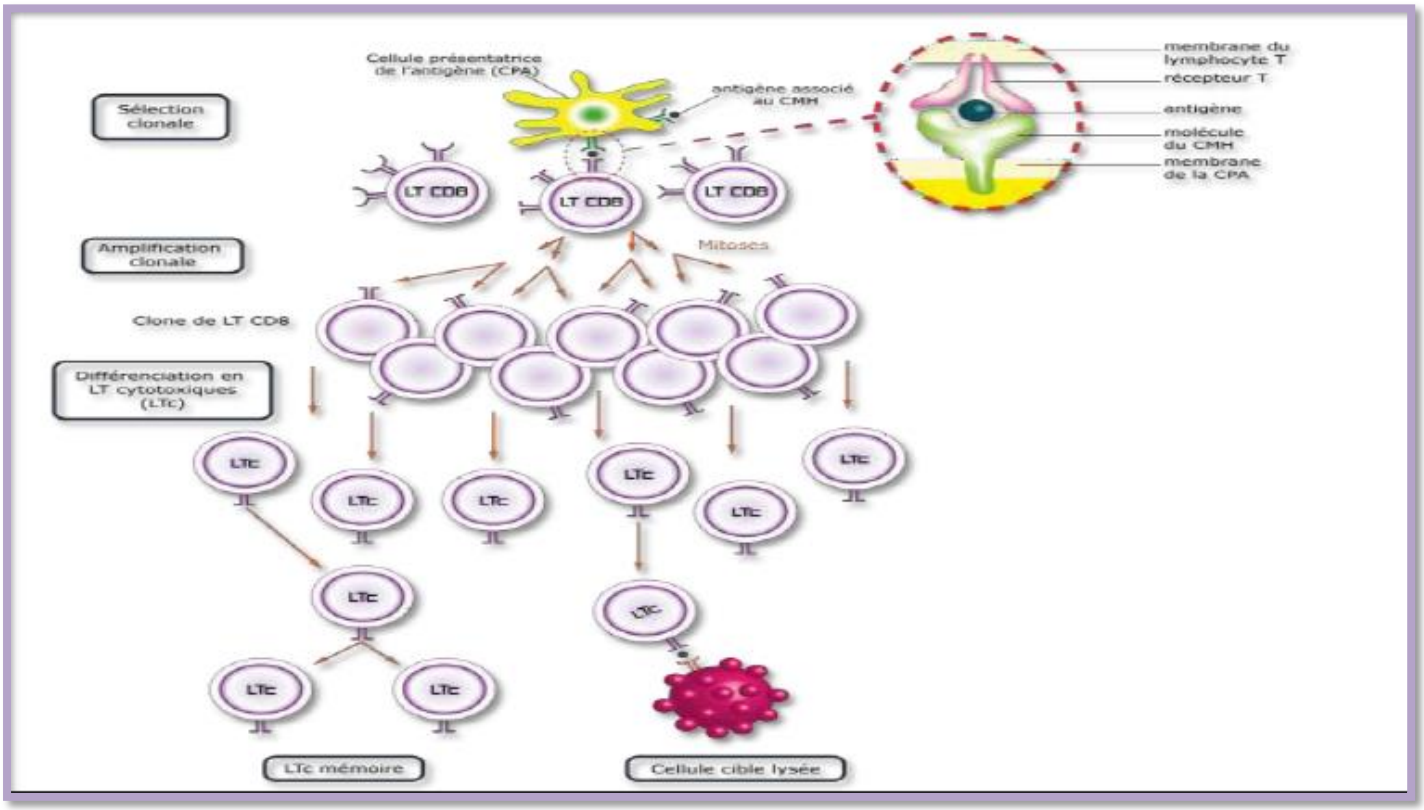

Figure 2. 6: Reconnaissance entre les LT CD8 et les cellules infectées (33).

b. Pour les lymphocytes B

La sélection clonale c'est les séquelles de la réponse immunitaire suite à un stimulus antigénique subissant des proliférations et différentiations. Quand un antigène s'infiltre dans le corps, les cellules immunitaires reconnaissent cet antigène avec des degrés d'affinité différents. L'appariement fort entre les récepteurs des anticorps et l'antigène, produit la stimulation des cellules B, c'est-à-dire la prolifération (clone) et la maturation des cellules de plasma. Le taux de prolifération d'une cellule est proportionnel par rapport à son affinité. La réponse des cellules B est la production d'un seul type d'anticorps qui est relativement spécifique à l'antigène. Les cellules qui ont les plus grandes affinités seront les plus proliférées et réciproquement. Puis, les lymphocytes qui ont une forte affinité peuvent se différencier en des cellules mémoires (13).

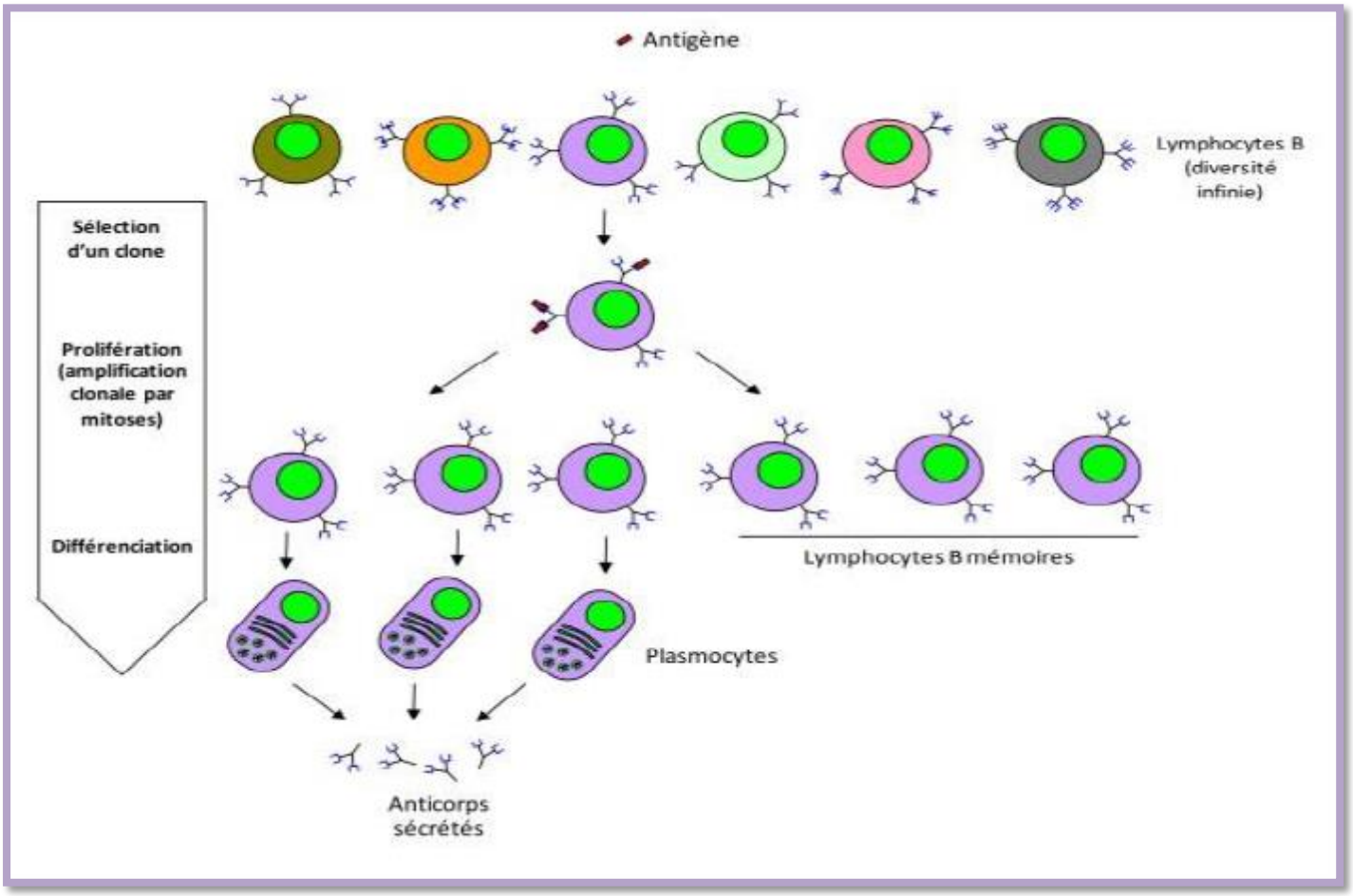

Figure 2. 7: De la détection de l'antigène à la production massive d'anticorps adaptés à cet antigène (33).

c. L'hypermutation somatique

Le résultat du processus de la sélection clonale est la reproduction de nouvelles cellules qui sont des sosies de leurs parents. Ces clones seront soumis à un mécanisme de mutation avec des taux très élevés (plus haut que des taux de mutation de cellules ordinaires). Ce mécanisme est appelé ***l'hypermutation somatique***. Le résultat est des filles de la cellule B initiale qui ont des récepteurs différents du parent et par conséquence des affinités différentes aux pathogènes.

L'hypermutation somatique est inversement proportionnelle à l'affinité d'une cellule c'est-à-dire les cellules qui ont les plus hautes affinités seront les moins mutées et réciproquement. Le mécanisme de l'hypermutation somatique permet au système immunitaire d'augmenter la capacité d'identification des anticorps par rapport à un antigène sélectif (3).

6.4 Les réseaux immunitaires

Depuis 1974 l'immunologie teste une nouvelle théorie, celle du réseau immunitaire, proposée par **Niels KajJerne**, prix Nobel de médecine en 1985. N.K. Jerne fût le premier à insister sur la nécessité de concevoir le système immunitaire comme un réseau dynamique fonctionnel, où tous les éléments, lymphocytes, plasmocytes, anticorps se reconnaissent et par là sont interconnectés. L'information peut alors recirculer dans ce réseau lympho plasmocytaire. Jusqu'alors, et encore maintenant pour la majorité, ils concevaient ce système immunitaire comme l'a conçu M.F. Burnet en 1957, c'est à dire comme un ensemble de clones de lymphocytes isolés les uns des autres. Chaque clone ayant une spécificité propre préexistante, il sera sélectionné par la structure étrangère ou étant devenue étrangère à l'organisme qu'il peut reconnaître (42).

La théorie du réseau immunitaire défini que les interactions au sein du système immunitaire ne se limitent pas entre anticorps et antigènes, mais aussi entre les anticorps en absence d'un stimulus antigénique. Cette interaction est réalisée par les récepteurs spécialisés présents sur la surface des anticorps appelés : idiotope. Les paratopes ont pour rôle de reconnaitre un ensemble d'idiotopes et les idiotopes doivent être reconnu par un ensemble de paratopes les lymphocytes stimulés peuvent répondre positivement ou négativement à un signal d'identification. La réponse positive est le résultat de l'appariement entre un anticorps et un antigène qui provoque l'activation et la prolifération des cellules. Par contre la réponse négative est le résultat de l'appariement entre un anticorps et un anticorps qui entraîne une élimination. L'enchainement de ce processus d'appariement d'antigène et suppression d'anticorps forme un réseau. Ce réseau est appelé ***le réseau immunitaire idiotypique*** (13).

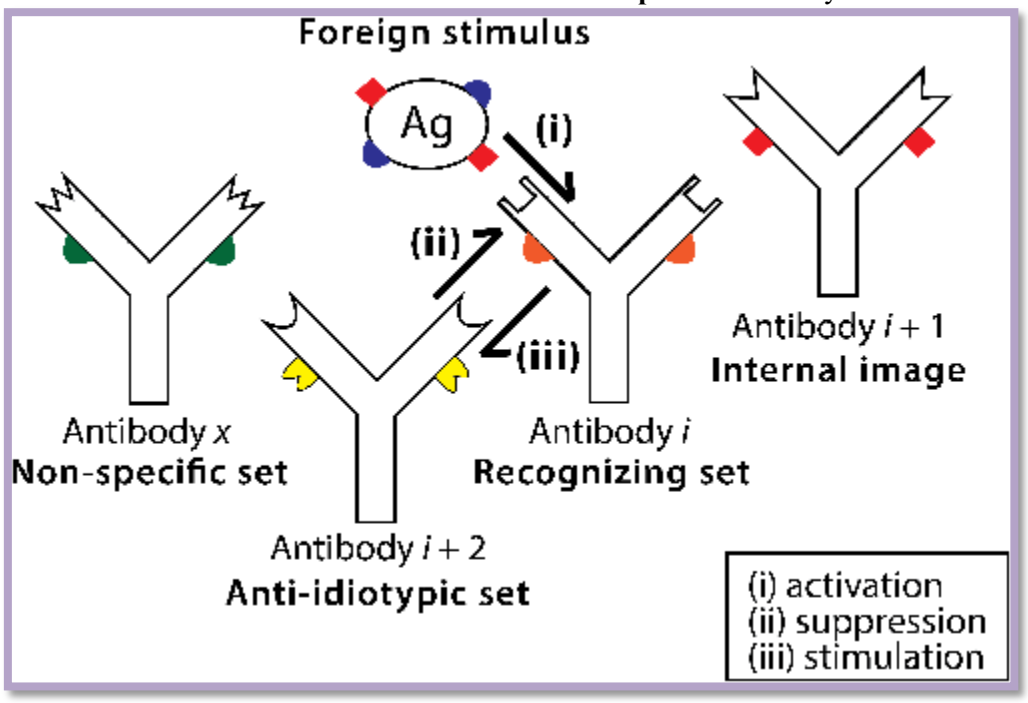

Figure 2. 8: La représentation du réseau immunitaire idiotypique (33).

6.5 La mémoire immunitaire

Lors d'un premier contact avec un antigène, le système immunitaire déclenche des mécanismes de défense, immunité innées et adaptative : il s'agit d'une réponse adaptative primaire. Celle-ci se traduit par la production d'anticorps et par la multiplication des lymphocytes spécifiques de l'antigène. Cette réponse primaire est de faible ampleur mais elle permet toutefois l'élimination de l'antigène en quelques semaines.

Lors d'un second contact avec le même antigène, le système immunitaire déclenche une réponse immunitaire plus rapide et plus efficace : c'est la réponse secondaire. Cette seconde réponse démontre l'existence d'une mémoire immunitaire (43).

6.5.1 La réponse primaire

Cette réponse est le résultat de la première exposition à un antigène qui stimule une réponse immunitaire adaptative. Cette réponse est traitée par un petit nombre de cellules B dont chacune produise des anticorps à des affinités différentes. Elle est caractérisée par un temps de latence grand et un petit nombre d'anticorps.

6.5.3 La réponse secondaire

Les prochaines expositions à des antigènes rencontrés précédemment stimulent des réponses secondaires. Ce processus est dû à une rétroaction d'événements passés aidant le système à apprendre. L'efficacité de cette réponse est augmentée par l'existence des ***cellules mémoires*** qui correspondent à un nombre de clone à forte affinité. Ces cellules mémoires sont produites lors de la première exposition à l'antigène. Cette stratégie assure que la vitesse et l'exactitude de la réponse immunitaire deviennent successivement plus élevées après chaque intrusion où le système améliore continuellement ces capacités

d'exécution des tâches. Ainsi, on peut noter que la réponse secondaire est caractérisée par un temps de latence très court, un taux d'anticorps plus élevé et une plus longue persistance des anticorps.

6.5.3 La réponse réactive croisée

Une réponse secondaire n'est pas seulement déclenchée par la réintroduction de même pathogène dans le futur. En effet, Il est possible qu'un antigène puisse se présenter avec des formes différentes qui sont des variations légères de l'antigène initial. Une caractéristique importante de la mémoire immunitaire est qu'elle est ***associative***. Cette particularité permet aux cellules B adaptées à un certain type d'antigène, par exemple l'antigène (A) de présenter également une réponse secondaire efficace et rapide aux antigènes qui sont semblables à l'antigène (A). Cette réponse est connue sous l'appellation : **la *réponse réactive croisée*** ou bien ***la réaction immunologique croisée*.**

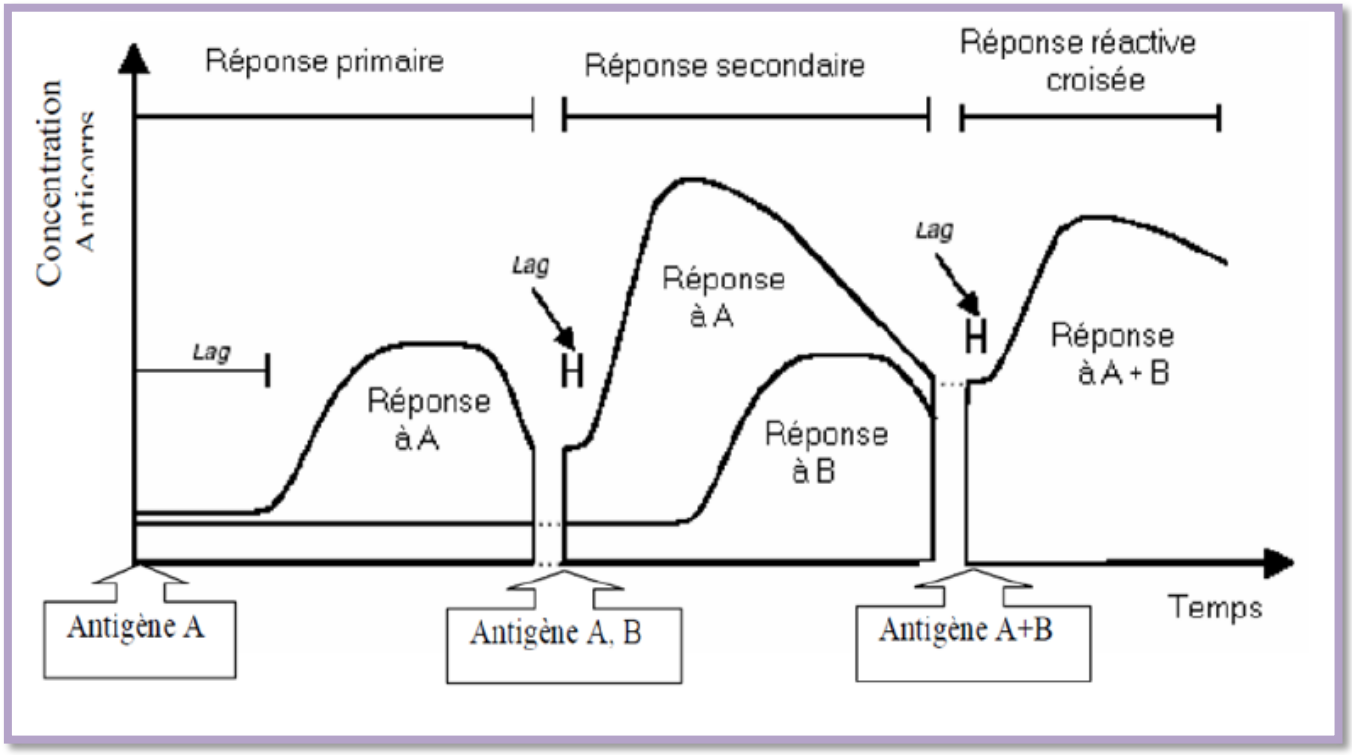

Figure 2. 9: Les différents types de réponses immunitaires (3).

7. La maturation d'affinité

La maturation d'affinité est le processus qui garantit que le système immunitaire possède de plus en plus des cellules immunitaires spécialisées pour la reconnaissance des modèles antigéniques. Ce processus est le résultat du mécanisme de l'hypermutation somatique suivi par une sélection. La mutation qui affecte les parties des récepteurs qui lient avec l'antigène suivi par une sélection qui garantit la préservation des solutions candidate de hautes qualités. Le récepteur qui possède la plus haute affinité permet d'avoir le plus fort appariement et ainsi la meilleure identification, ce qui permet d'avoir une réponse immunitaire exacte et efficace.

La réponse immunitaire est adaptative parce que l'opération de mutation suivie par une sélection permet aux récepteurs de cellules de s'y adapter à l'antigène. Cela garantit que les rencontres suivantes avec un certain type d'antigène mènent aux réponses plus puissantes.

8. Le répertoire cellulaire

La capacité du système immunitaire à identifier les antigènes est *complète.* Les récepteurs des différentes cellules immunitaires peuvent identifier les intrus externes et même les cellules du soi (la théorie du réseau immunitaire idiotypique qui sera détaillée dans les sections suivantes). La diversité des récepteurs est assurée d'une part pendant la reproduction de molécules de récepteur par la recombinaison des segments de gène à partir de la bibliothèque de gènes. D'autre part par le mécanisme de l'hypermutation somatique qui permet la génération continuelle de nouveaux récepteurs (21).

9. La discrimination entre soi / non soi

Si le système immunitaire est capable de reconnaître n'importe quel modèle antigénique qui est le complément des récepteurs de cellule immunitaire. **Comment le système immunitaire se comporte quand il est confronté avec un antigène de soi ?**

La capacité du répertoire du système immunitaire pour reconnaître les antigènes est complète. Cependant, cette propriété représente un paradoxe fondamental parce que toutes les molécules qui peuvent être reconnues incluant les cellules du corps seront considérées comme ***antigènes*** ou ***antigènes de soi***[3] (44).

Pour que le système immunitaire fonctionne correctement, il doit être capable de distinguer entre les cellules de soi et les cellules étrangères (cellules de non soi), cette capacité est appelée la ***tolérance de soi***[4]. Ce problème est reconnu sous le nom problème de discrimination entre soi / non soi (44). . Donc, il doit y avoir quelque forme de sélection négative qui empêche les cellules immunitaires de devenir auto réactives.

9.2 La sélection négative pour les cellules T

Après la production des cellules T naïves dans la moelle osseuse, elles migrent vers le thymus. Les cellules T *immatures* ou *naïves* subiront alors un processus de sélection négative dans le thymus[5]. Le processus de la sélection négative permet l'élimination des cellules T naïves qui peuvent reconnaître un antigène de soi. Les cellules T naïves qui ne reconnaissent aucun antigène du soi dans le thymus seront libérées pour la recherche éventuelle des cellules de non soi (44).

[3] Antigène de soi est une autre appellation pour les propres cellules du corps humain.
[4] Si le système immunitaire n'est pas tolérant au soi, donc une réponse immunitaire sera déclenchée contre les cellules de soi causant la maladie de l'auto-immunité
[5] Le thymus est un organe qui est doté par une barrière thymique de sang pour éviter l'assistance des antigènes du non soi.

9.2 La sélection négative pour les cellules B

La sélection négative est appliquée aussi sur les cellules B dans la moelle osseuse, quand les cellules B immatures identifient les cellules du soi, elles seront éliminées. Ce mécanisme est appliqué seulement sur les cellules B immatures dans la moelle osseuse. La tolérance au soi des cellules nouvellement générées après le processus de la sélection clonale et l'hypermutation somatique, sera assurée par l'assistance des cellules T d'aide (44).

10. La théorie du réseau immunitaire

La sélection clonale est la théorie qui explique comment le système immunitaire répond à un antigène de non soi. Tandis que la sélection négative est employée pour éliminer les cellules auto réactives. Une autre question cruciale à être répondue est comment les cellules du système immunitaire interagissent avec d'autres cellules immunitaires ? Intéressé par ce problème, Jerne a proposé la théorie du réseau immunitaire (45)qui suggère que les interactions au sein du système immunitaire ne se limitent pas entre anticorps et antigènes, mais aussi entre les anticorps même en absence d'un stimulus antigénique. Cette interaction est assurée par des récepteurs spécialisés présents sur la surface des anticorps appelés : ***idiotope***. Alors, le système immunitaire est formellement défini par un réseau énorme et complexe de paratopes qui reconnaissent un ensemble d'idiotopes et d'idiotopes reconnus par un ensemble de paratopes. Ainsi, chaque élément pourrait reconnaître aussi bien qu'être reconnu. Ce réseau est appelé ***le réseau immunitaire idiotypique*** (27).

Cette théorie synthèse la propriété de la détection distribuée des systèmes immunitaires, elle montre l'état dynamique des interactions internes des lymphocytes, des anticorps et antigènes. Les lymphocytes stimulés peuvent répondre positivement ou négativement à un signal d'identification (Figure 2.10). La réponse positive est le résultat d'une liaison entre un anticorps et un antigène qui provoque l'activation et la prolifération des cellules ainsi la sécrétion d'anticorps. Par contre la réponse négative est le résultat d'une liaison entre un anticorps et un anticorps qui entraîne une suppression. La chaîne continue de différentiation par antigène et la suppression par anticorps forme un réseau. Ce réseau peut atteindre le statut d'équilibre entre la suppression et la stimulation pour déterminer le système immunitaire complet (46). Cette théorie en particulier reflète les propriétés parallèles et distribuées de système immunitaire parce que différentes réponses locales entre un anticorps et un antigène ou un anticorps et un anticorps arrivent en parallèle et à des endroits dispersés.

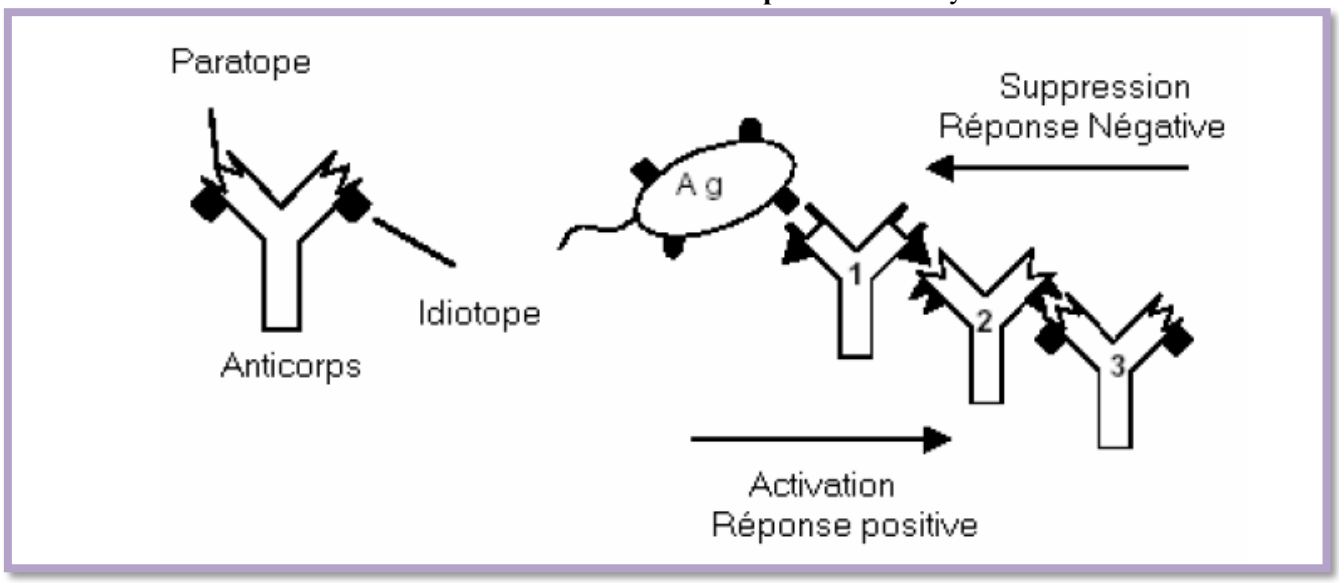

Figure 2. 10: La représentation du réseau immunitaire idiotypique (3)

11. Les caractéristiques du système immunitaire

Le système immunitaire biologique est un système robuste, complexe et adaptatif qui défend le corps contre les agents pathogènes étrangers. Il est capable de catégoriser toutes les cellules (ou Molécules) dans le corps.

Citons quelques propriétés les plus importantes du système immunitaire :

- ***Multicouche :*** Le système immunitaire possède une architecture multicouche composé de deux sous-systèmes inter-liés qui sont : le système immunitaire inné et le système immunitaire adaptatif. Ces deux systèmes combinent leurs tâches et responsabilités pour assurer la protection et la sécurité globale.
- ***Unicité :*** Chaque élément dans le système immunitaire assume ces responsabilités particulières.
- ***Autonomie :*** Le système immunitaire humain ne dispose d'aucun contrôle central. Il possède une autonomie globale dans la détection et l'élimination des intrus.
- ***Distribution :*** Les cellules immunitaires et les molécules sont distribuées dans le corps humain pour assurer la protection. Il n'existe pas un point de contrôle centralisé.
- ***Parallélisme :*** Le système immunitaire est capable de produire plusieurs réponses immunitaires en même temps à des endroits dispersés.
- ***Tolérance au soi :*** Le système immunitaire humain peut différencier entre les cellules de soi et les cellules de non-soi.
- ***Apprentissage :*** Le système immunitaire augmente la capacité d'identification des anticorps à un antigène sélectif (les réponses primaire et secondaire). Il apprend continuellement les structures de pathogènes.

- ***Adaptabilité :*** Le système immunitaire humain permet la production des cellules de plus en plus spécialisées pour l'identification des antigènes. Cela est garanti par la théorie de la sélection clonale suivie par le mécanisme de l'hyper mutation somatique.
- ***Dynamique :*** Le système immunitaire est dynamique il crée de nouvelles cellules et molécules, et élimine les cellules vieilles ou endommagées. Un bon exemple de la dynamique du système immunitaire est la théorie du réseau idiotypique.
- ***Mémorisation :*** suite à une réponse immunitaire donné, les cellules intervenantes se transforme en cellules mémoires avec une durée de vie longue afin de répondre plus rapidement à une nouvelle intrusion du même type d'antigène.
- ***Coopération :*** Les cellules immunitaires coopèrent afin de défendre le système, ainsi assurent une meilleure détection.
- ***Détection :*** Le système immunitaire est capable d'identifier et de détecter tout type d'intrusion sans aucune connaissance préalable de l'antigène.
- ***Discrimination entre soi et non-soi*****:** La plus importante propriété qui est à la base des réactions immunitaires est l'aptitude du système immunitaire à distinguer entre les cellules du Soi et les cellules du non-Soi (étrangères) ainsi que la possibilité de reconnaitre le type exact de chaque cellule étrangère (13).

II Les systèmes immunitaires artificiels

1. Introduction

Le système immunitaire biologique possède la capacité pour protéger le corps humain contre une variété énorme de pathogènes étrangers. Dans les dernières années, un nombre de chercheurs ont étudié le succès et la compétence de ce système naturel et ont proposé ***le modèle immunitaire artificiel*** pour la résolution de divers problèmes. Des approches diverses ont été proposées pour mettre en œuvre les mécanismes de base du système immunitaire humain. Cette section sera consacrée à introduire le système immunitaire artificiel avec une présentation des différents modèles qui ont été mis en œuvre.

2. Historique

Les travaux sur les systèmes immunitaires artificiels ont commencé dans le milieu des années 1980 avec l'article de **Farmer**, **Packard** et **Perelson** sur les réseaux immunitaires (1986). Cependant c'est seulement dans le milieu des années 1990 que les SIA devinrent un sujet à part entière.

Les travaux de **Forrest** sur la sélection négative commencèrent en 1994, tandis que Dasgupta menait des études sur les algorithmes de sélection négative. **Hunt** et **Cooke** commencèrent leurs travaux sur les modèles de réseaux immunitaires en 1995. **Timmis** et **Neal** continuèrent ces travaux en y apportant des améliorations. Le premier livre sur les SIA a été édité par **Dasgupta** en 1999. Les travaux de **De Castro**, **Von Zuben**, **Nicosia** et **Cutello** sur la sélection clonale (CLONALG) furent remarqués en 2002 (47).

3. Définitions

Des approches diverses ont été proposées pour mettre en oeuvre les mécanismes de base du système immunitaire humain .Cette section sera consacrée à introduire le système immunitaire artificiel avec une présentation des différents modèles qui ont été mis en œuvre :

3.1 Définition 1 :

Selon Timmis (27) : « Un système immunitaire artificiel est un système informatique basé sur les métaphores du système immunitaire naturel ».

3.2 Définition 2 :

Dasgupta a défini le système immunitaire artificiel comme suit (48) : « Le système immunitaire artificiel est la composition de méthodologies intelligentes inspirées par le système immunitaire naturel afin de résoudre des problèmes du monde réel ».

3.3 Définition 3 :

Tandis que Timmis et De Castro (27) ont donné la définition suivante : « Les systèmes immunitaires artificiels sont des systèmes adaptatifs inspirés par des théories immunologiques et des observations de fonctions immunitaires, des principes et des modèles, qui seront appliqués à la résolution des problèmes».

4. Modélisation des SIA

Le modèle commun connu sous le nom du Framework des systèmes immunitaires artificiels, définit les règles que doit respecter un SIA ainsi que les processus à suivre pour l'élaboration de nouvelles approches. Les conditions nécessaires sont :

- La représentation des composants systèmes (modèles abstraits des cellules immunitaires).
- L'utilisation des mesures d'affinité (similarité) pour évaluer l'affinité entre les composants systèmes.
- Un ensemble d'algorithmes pour contrôler l'évolution et la dynamique d'SIA.

Les trois conditions citées ci-dessus sont indispensables pour l'élaboration d'un Framework pour définir un système immunitaire artificiel (13).

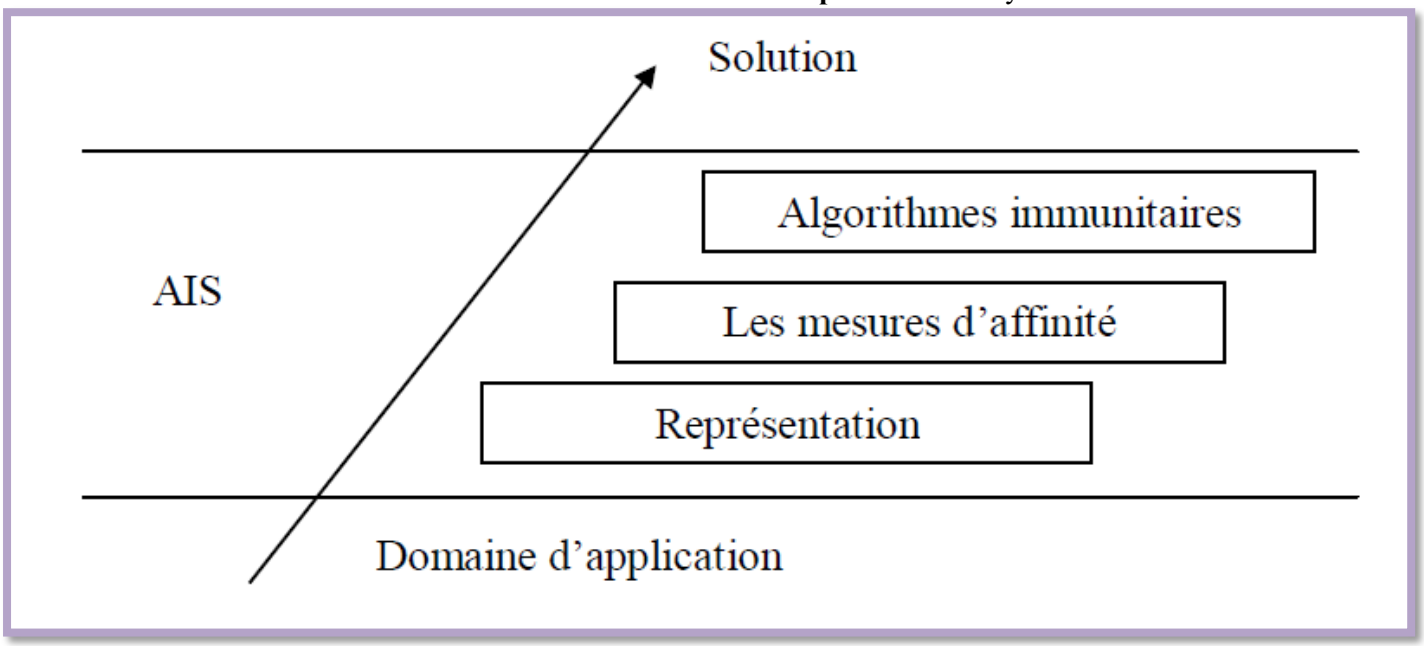

Figure 2. 11: Structure de conception d'un système immunitaire artificiel (49).

4.1 Représentation

Afin de construire un système tel qu'un SIA, un domaine d'application ou une fonction cible sont généralement exigés. A partir de cette base, la façon dont les éléments du système (cellules) seront représentés est considérée. Cette façon est appelée espace de forme (shapespace) Il existe plusieurs types d'espaces de forme, tels que Hamming, les valeurs réelles, etc. chacun porte son propre biais et doit être choisi avec précaution (49).

4.1.1 Le modèle de Shape-Space (Forme-Espace)

Le modèle Shape- Space (Forme - Espace) a été proposé par **Perelson** et **Oster** en 1979. Ce modèle permet une description quantitative des interactions de molécules, de récepteur et d'antigènes. Dans le système immunitaire biologique, le concept Forme - Espace est le degré de liaison (le degré de correspondance ou l'affinité) entre le récepteur d'anticorps (Ab ou TCR) et un antigène (Ag). Ce degré de liaison est mesuré via les régions de complémentarité entre les deux éléments (13).

4.2 Mesure de similarité

Une fois la représentation choisie, une ou plusieurs mesures d'affinité sont utilisées pour quantifier les interactions entre les éléments du système. Il y a beaucoup de mesures de similarité possibles (qui sont partiellement dépendantes de la représentation adoptée), le plus souvent on recourt à l'utilisation des métriques de distances comme la distance *Euclidienne*, **la distance de *Manhattan*** ou la **distance de *Hamming***. En intelligence artificielle, et en particulier en classification, l'affinité est appelé similarité (49).

L'affinité entre un anticorps et un antigène est relative à leur distance, Un antigène est représenté par un vecteur **Ag=<Ag1, Ag2,..., AgL>**, un anticorps est à son tour représenté par un vecteur

Ab=<Ab1,Ab2,…,AbL>. Pour mesurer le degré de complétude entre l'antigène et l'anticorps, plusieurs techniques peuvent être utilisées. Le plus souvent on recourt à l'utilisation des distances.

Plus la distance antigène-anticorps est petite, plus l'affinité entre ces derniers est grande (50). Différentes distances existent dont voici les plus utilisées :

La distance euclidienne : $D=\sqrt{\sum_{i=1}^{n}(Ab_i - Ag_i)^2}$

La distance de Manhattan : $D=\sum_{i=1}^{n}|Ab_i - Ag_i|$

La distance de Hamming : $D=\sum_{i=1}^{n}\delta^i$ où $\delta = \begin{cases} 1, & Ab_i \neq Ag_i \\ 0, & sinon \end{cases}$

Figure 2. 12: Les différentes équations pour calculer l'affinité entre un antigène et un anticorps (50)

4.3 Les algorithmes immunitaires

La couche finale implique l'utilisation d'algorithmes qui régissent le comportement (dynamique) du système. Ces algorithmes incluent ceux basés sur les processus immunitaires suivants: sélection négative, les réseaux immunitaires, et la sélection clonale (49).

4.3.1 L'algorithme de sélection négative/positive

Dans la théorie du système immunitaire naturel seules les cellules T qui ne s'attaquent pas aux cellules du soi sont autorisées à quitter le thymus et auront pour tâche de reconnaitre les cellules du non soi. **Forrest** a proposé l'algorithme de la sélection négative qui reflète le même principe. Il a considéré l'algorithme de la sélection négative comme un processus de détection d'anomalies composé de trois phases principales :

- La définition du soi
- La génération des détecteurs
- Le contrôle d'occurrence des anomalies

L'algorithme se déroule comme suit :

- **Générer un ensemble de cellules candidats aléatoirement de l'ensemble P.**
- **Calculer l'affinité entre chaque cellule C et tout l'ensemble de soi P.**
- **Si l'affinité entre un élément C et au moins un élément P est supérieur ou égal a un seuil d'affinité prédéfini,**

  Alors cet élément C sera supprimé (il est considéré comme un élément de soi).
- **Sinon il sera considéré comme un détecteur de non soi et sera ajouté a l'ensemble de détecteur M.**
- **Après avoir obtenu l'ensemble de détecteur, la prochaine étape sera de détecter la présence du modèle de non soi.**

Figure 2. 13: L'algorithme de la sélection négative.

Le schéma suivant résume l'algorithme de sélection négative :

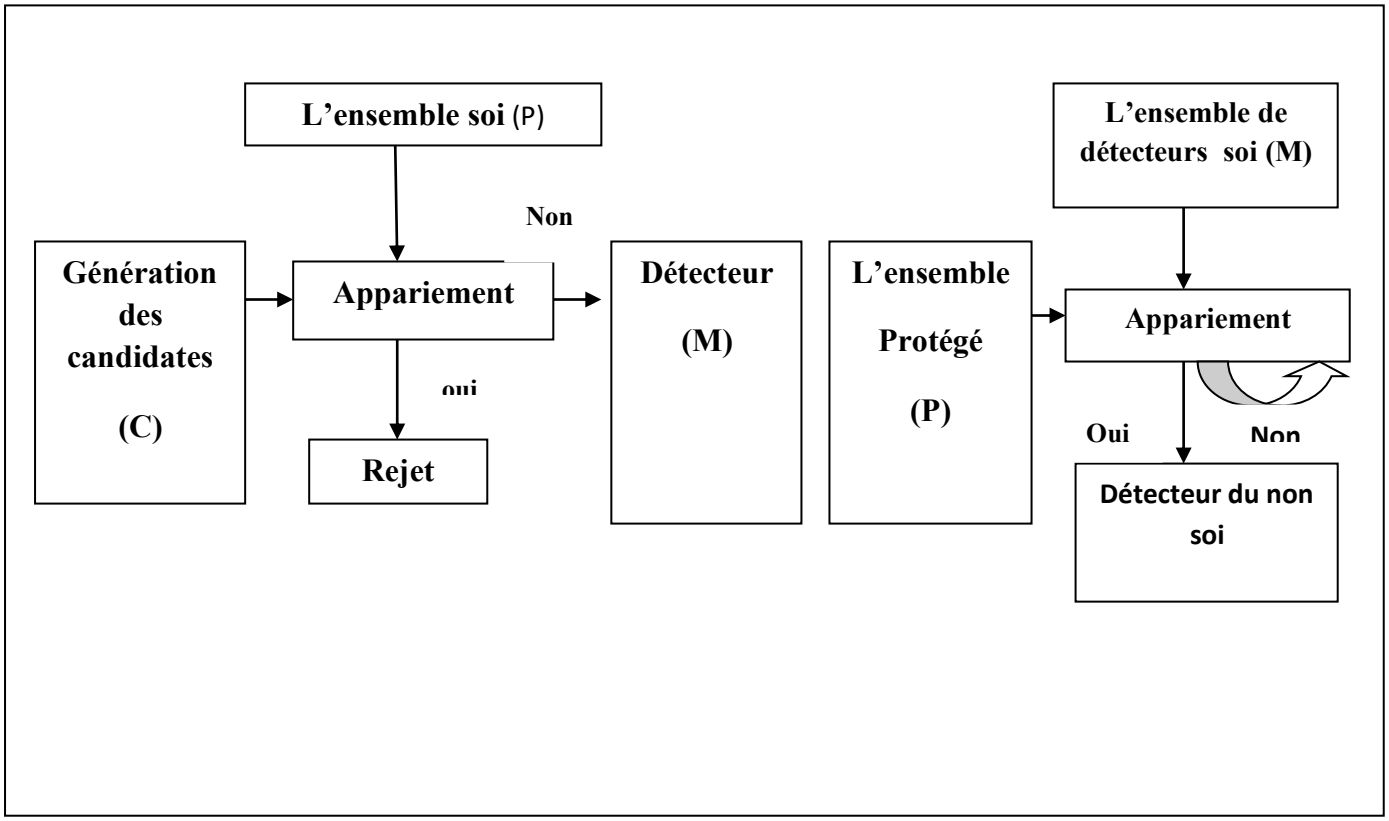

Figure 2. 14: La structure générale de l'algorithme de la sélection négative.

L'algorithme de la sélection positive est une alternative de l'algorithme de la sélection négative. La seule différence réside dans la génération des détecteurs détectant des éléments de soi au lieu de ceux qui détectent des éléments de non soi.

C'est à dire qu'un élément de non soi suspect doit être comparé avec tout l'ensemble des détecteurs de soi ; s'il n'est pas détecté alors il est considéré comme un élément de non soi.

Ces deux algorithmes sont très intéressants, pour la surveillance des systèmes et la détection d'utilisations anormales ou inhabituelles (13).

4.3.3 L'algorithme de la sélection clonale

La sélection clonale est la théorie expliquant comment le système immunitaire interagit avec les antigènes. Cette théorie est applicable aux lymphocytes B ainsi qu'aux lymphocytes T. La seule différence est que les cellules B subissent une hypermutation somatique durant leur prolifération contrairement aux cellules T. Grâce à ce procédé, le corps humain est capable de contrer un très grand nombre d'éléments externes. Les SIA s'inspirent de cette théorie. Mais vu que seules les cellules B sont capables de muter pour optimiser la réponse immunitaire, ces cellules sont les plus intéressantes. Cette optimisation est due au fait que les cellules B une fois en contact avec l'antigène, elles se multiplient et donnent plusieurs clones et chaque clone subit une mutation. Cette mutation sert à trouver des clones de la cellule mère possédant une plus grande affinité avec l'antigène (41).

De Castro & Von Zuben ont proposé l'algorithme de la sélection clonale nommé CLONALG qui accompli les tâches de base impliquées dans le processus de la sélection clonale dans le système immunitaire humain. Les étapes de base de l'algorithme CLONALG sont résumées comme suit :

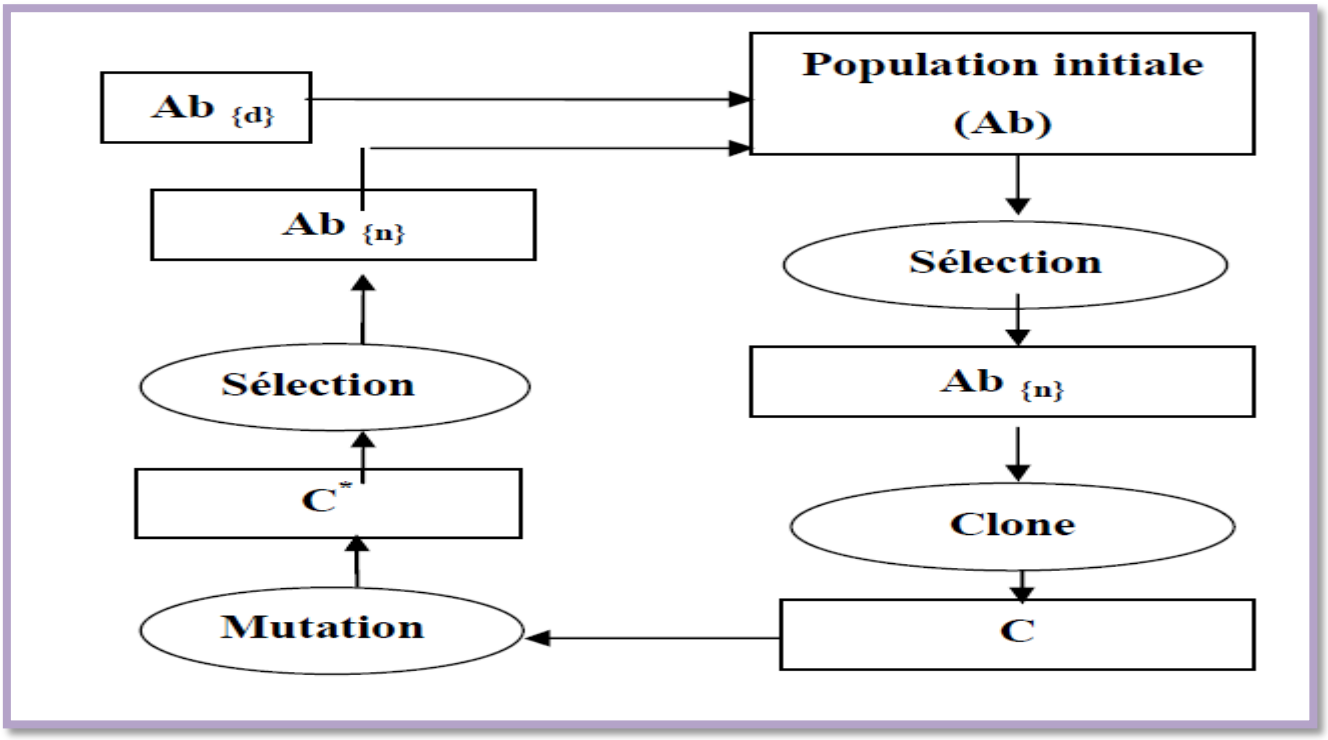

Figure 2. 16: Une représentation de l'algorithme de la sélection clonale (41).

L'algorithme se déroule comme suit :

Entrée : Un ensemble **P** de formes à reconnaitre

- Initialisation aléatoire d'une population d'individus **M**

Tantque Une forme minimale n'est pas reconnue **faire**

Pour Chaque formes de **P faire**

-Déterminer s'il y a une affinité avec chaque élément de **M**

Fin pour

-Sélectionner **n1** éléments ayant la meilleure affinité avec les éléments de M

-Générer des copier de ces éléments proportionnellement a leur affinité avec l'antigène

-Muter toutes les copies proportionnellement avec leur affinité avec les formes de l'ensemble **P** pus L'affinité est élevée, plus la mutation n'est faible)

-Ajouter les individus mutés dans la population **M**

-Choisir **n2** de ces éléments mutés (optimisé) comme mémoire

Fin Tantque

Figure 2. 17: L'algorithme de la sélection clonale (50).

4.3.3 L'algorithme du réseau immunitaire

Un réseau immunitaire artificiel (Artificial Immune Network AIN) est un modèle de calcul de la famille des SIA qui utilise les idées et les concepts de la théorie du réseau immunitaire, principalement, les interactions entre les anticorps (stimulation et suppression), et les processus de clonage et mutation. Le réseau immunitaire décrit la manière dont les cellules répondent entre elles dans le système immunitaire. Alors c'est un système immunitaire autorégulé de molécules et de cellules qui se reconnaissent entre elles, même en l'absence d'antigène.

Le déroulement d'un algorithme de réseau immunitaire peut être résumé comme suit :

1. Initialisation : créer une population initiale d'anticorps d'une façon aléatoire.

2. Présentation antigénique : pour chaque modèle antigénique faire :

2.1. Sélection clonale et expansion : pour chaque élément de réseau, déterminer son affinité avec l'antigène présenté. Sélectionner les éléments de haute affinité et les reproduire proportionnellement à leur affinité.

2.2. Maturation d'affinité : chaque clone est muté inversement proportionnel à son affinité. Sélectionner quelques clones de plus haute affinité pour constituer l'ensemble mémoire.

2.3. Interactions clonales : déterminer l'interaction réseau (affinité) de tous les éléments de l'ensemble mémoire.

2.4. Suppression clonale : éliminer ces clones mémoires dont l'affinité est moins d'un seuil prédéfini.

2.5. Méta dynamique : éliminer tous les clones mémoires dont l'affinité avec l'antigène est moins d'un seuil prédéterminé.

2.6. Construction de réseau : incorporer les clones restants de l'ensemble mémoire avec les anticorps du réseau.

2.7. Interactions de réseau : déterminer la similitude entre chaque paire d'anticorps du réseau.

2.8. Suppression de réseau : éliminer tous les anticorps du réseau dont l'affinité est moins d'un seuil prédéterminé.

3. Cycle : répéter ces pas un certain nombre d'itérations.

5. Domaines d'application des SIA

Le système immunitaire artificiel possède une variété de modèles de telle sorte que chaque modèle est basé sur une partie particulière de fonctionnement du système immunitaire humain. Cette diversité permet d'utiliser le système immunitaire artificiel dans plusieurs domaines d'application pour des buts différents. D'une manière générale, parmi ces domaines on peut citer :

- **La sécurité des ordinateurs :**

La sécurité des ordinateurs a fait l'objet de plusieurs travaux intéressants qui ont proposés d'exploiter les principes de base de la détection et l'élimination, en employant les algorithmes des systèmes immunitaires artificiels. Un travail très intéressant, considéré parmi les premières tentatives dans ce secteur de recherche et celui de **Stéphanie Forrest**.

Forest a focalisé ces recherches sur la détection et la neutralisation des virus par la réécriture des informations initiales sur le fichier infecté (13).

- **La détection et l'élimination des virus informatiques**

Okamoto et **Ishida** ont proposé un système multi agent basé SIA. Ce système de détection de virus opère dans un environnement distribué et hétérogène. L'algorithme de la sélection négative a été utilisé comme une méthode d'authentification de fichier.

La détection des virus est réalisée via l'appariement entre les informations propres d'un fichier tel que les premiers bits de l'entête du fichier, sa taille, le chemin d'accès et le fichier de l'hôte. La neutralisation des

virus est faite par la réécriture des informations initiales sur le fichier infecté. Le système est composé de quatre types d'agents qui sont :

- Les agents anticorps qui détectent les virus sur les hôtes locaux.
- Les agents tueurs qui neutralisent les virus par les réécritures des informations initiales sur les fichiers infectés.
- Les agents de copie qui copient les fichiers non infectés qui sont équivalents aux fichiers infectés à partir des différents hôtes (3).

➢ **Optimisation :**

Le problème d'optimisation consiste à trouver un ensemble absolu des meilleures conditions admissibles pour atteindre un objectif. **Castro** et **Von Zuben**, proposent un algorithme approprié pour le problème d'optimisation. Leurs travaux se focalisent sur le principe de la sélection clonale et la maturation d'affinité lors d'une réponse immunitaire adaptative afin de résoudre des problèmes complexes tels que l'optimisation combinatoire et l'optimisation multi modale.

➢ **Robotique :**

Les travaux de **Matsumoto** sont parmi les premiers travaux, il a essayé de créer un groupe de robots qui se comportent d'une façon autonome pour chercher l'alimentation sans aucun mécanisme de contrôle global. L'idée principale dans ces travaux est l'interaction entre les robots au niveau local. L'auteur emploient trois métaphores immunologiques principales. La première métaphore est les cellules B, où un robot représente une cellule B dont chaque robot possède une stratégie particulière pour trouver l'alimentation. La deuxième est le réseau immunitaire pour garantir l'interaction entre ces robots. La troisième est le calcul de stimulation des cellules B, où le robot qui est le plus stimulé alors sa stratégie est la meilleure pour être prise en considération. Suite à ce travail, plusieurs travaux ont été proposés dans ce domaine de recherche.

➢ **Autres domaines d'utilisation :**

- La maintenance des systèmes d'ordinateurs.
- La reconnaissance de formes.
- L'apprentissage.
- La classification des données.
- La planification (13).

Le tableau suivant montre les domaines d'utilisation de chaque algorithme du système immunitaire :

L'algorithme	Les domaines d'application
Algorithme de sélection négative	**La sécurité informatique :** • **La détection des spam** • **La détection d'intrusion dans un réseau**

	informatique
Algorithme de la sélection clonale	**Les problèmes de :** • **Clustering** • **Optimisation** • **Reconnaissance des formes** • **Détection d'intrusion**
Algorithme de réseau immunitaire	• **Datamining** • **Robotique** • **Ordonnancement** • **Clustering**

Tableau 2. 2: les domaines d'applications des algorithmes des systèmes immunitaires

Le tableau suivant montre quelques travaux sur les SIA :

2011Date	Auteur	Le travail	Description
1997	Lee et Sm	Robotique	Elaboration des robots en basant sur les AIS
2002	A. Secker J. Timmis A. Fretas	AISEC	Algorithme capable de classer les lettres électroniques
2001	A. Watkins J. Timmis L. Bogges	AIRS	AIRS est un algorithme puissan pour la reconnaissance des formes
2005	K.C. Tan C.K. Goh A.A. Mamun	EMQIA	Evaluation des AIS pour pour l'optimisation multi objectifs
2008	A. Secker J. Timmis A. Fretas	AISIID	Système pour la découverte intéressent de l'information sur le web

Tableau 2. 3:Des travaux sur les SIA (3).

6. Etude comparative des différents systèmes inspirés de la biologie

Le tableau suivant compare entre les différents systèmes inspirés de la biologie qui sont :

- Les systèmes immunitaires artificiels qui sont inspirés du système immunitaire humain,
- Les réseaux de neurones qui sont inspirés du fonctionnement du cerveau,
- Les algorithmes évolutionnaires inspirés par la théorie de l'évolution darwinienne.

	Algorithme génétique	Réseaux de neurones artificiels	Système immunitaire artificiel
Composants	Chaînes de chromosomes	Neurones artificiels	Chaînes d'attributs
L'emplacement des composants	Dynamique	Prédéfini	Dynamique
Structure	Composants discrets	Composant en réseaux	Composant discret / composants en réseaux
Stockage des connaissance	Chaînes de chromosomes	Connexion robuste	Concentrations des composants / réseaux
Dynamique	Evolution	Apprentissage	Evolution / apprentissage
Méta-dynamique	Incorporation / élimination des composants	Construction / élagage de la connexion	Incorporation / élimination des composants
Interaction entre les composants	Recombinaison	Connexion réseaux	Reconnaissance / connexion réseaux
Interaction avec l'environnement	Fonction de fitness	Stimulation externe	Reconnaissance / les fonctions objectives
Seuil d'activités	Surpeuplement / partage	Activation des neurones	L'affinité des composants

Tableau 2. 4: Un tableau comparatif entre les caractéristiques des différents systèmes inspirés de la biologie (50).

III Le lien entre un SIA et IDS

1. Introduction

Les approches de la sécurité des ordinateurs inspirées de la biologie sont devenues intéressantes par rapport à d'autres approches pour deux raisons à savoir :

- Les systèmes informatiques et les espèces biologiques sont souvent attaqués.
- Les systèmes informatiques deviennent de plus en plus complexes et les approches traditionnelles de la sécurité ne peuvent pas assumer le rôle de protection d'une manière parfaite, par contre les métaphores biologiques deviennent de plus en plus très puissantes.

2. L'immunologie et la sécurité des systèmes informatiques

2.1 L'immunologie

Le corps humain est constamment sous l'attaque par des micro-organismes hostiles qui sont la source de beaucoup de maladies. Le but du système immunitaire est la protection du corps contre ces pathogènes, il est face à deux aspects de problème qui sont (51) : l'identification ou la détection des pathogènes et l'élimination efficace de ces pathogènes en réduisant au minimum les dégâts causés.

2.2 La sécurité des systèmes informatiques

Le problème qui touche le système immunitaire est semblable à celui de système de sécurité des systèmes informatiques : le système immunitaire protège le corps contre les pathogènes et analogiquement le système de sécurité d'ordinateur doit protéger les systèmes informatiques contre les différentes intrusions. Cette analogie peut être bien définie en exposant les problèmes confrontés par les systèmes de sécurité des systèmes informatiques (51).

- ***Confidentialité*** : le système de sécurité doit assurer la protection contre les accès non autorisés aux systèmes et aux informations.
- ***Intégrité*** : il doit protéger les données contre les opérations non autorisées telles que : la modification, la suppression, etc.
- ***Disponibilité*** : la protection des utilisateurs légitimes contre l'indisponibilité des ressources.
- ***Responsabilité*** : si le compromis d'un système d'ordinateur a été détecté, le système de sécurité d'ordinateur doit préserver l'information suffisante pour identifier ces intrus.
- ***Justesse*** : les alarmes fausses de la classification incorrecte d'événements doivent être réduites au minimum.

La similitude entre le problème de sécurité et le problème de système immunitaire peut être montrée en traduisant la langue d'immunologie dans des termes de sécurité d'ordinateur (51) : le système immunitaire détecte les abus d'une politique de sécurité implicitement indiquée par la sélection naturelle et répond à ces abus par des contre attaques de la source de l'abus. La disponibilité permet au corps de continuer son fonctionnement même dans le cas d'existence des attaques de pathogènes. La justesse signifie que le système immunitaire ne doit pas attaquer le corps. L'intégrité signifie l'assurance que les gènes de cellule ne soient pas infectés par les pathogènes et la responsabilité signifie la recherche et l'élimination des

pathogènes responsables de la maladie. Un aspect de sécurité qui n'est pas important pour le système immunitaire est la confidentialité parce qu'il n'existe aucune notion de données secrètes dans le corps qui doit être protégé à tout prix.

3. L'analogie entre un système immunitaire et un système de détection d'intrusion

Dans cette section, l'étude de l'analogie entre le système immunitaire et le système de détection d'intrusions est basé essentiellement sur le travail établit par Kim (29) dans lequel la démonstration de cette analogie est composée de trois étapes essentielles. La première étape présente les exigences principales d'un IDS basé réseau compétent, la deuxième étape introduit les buts de conception d'un IDS pour satisfaire les exigences de la première étape. Enfin, la dernière étape analyse les propriétés significatives du système immunitaire par une comparaison avec les buts de conception d'un IDS basé réseau. Ainsi, cette démonstration est basée d'une manière générale sur un IDS basé réseau pour deux raisons principales :

- Un IDS basé hôte peut être considéré comme l'un des composants d'un IDS basé réseau.
- Un IDS basé réseau possède la possibilité de contrôler des hôtes multiples d'une manière distribuée de la même façon que le système immunitaire.

3.1 Les exigences d'un IDS basé réseau

La conception d'un IDS basé réseau compétent doit prendre en considération les fonctions suivantes:

1. ***Robustesse*** *:*

Le système de détection d'intrusions doit être doté par des points de détection multiples pour qu'il soit assez robuste contre les attaques et les fautes de système.

2. ***Configurabilité*** *:*

La configuration d'un IDS doit être facile aux exigences locales de chaque hôte et aux composants du réseau.

3. ***Extensibilité*** *:*

La facilité d'étendre la portée du contrôle d'un IDS par l'ajout de nouveaux hôtes d'une manière simple indépendamment des systèmes d'exploitation.

4. ***Incrémentabilité « Scalability »*** *:*

Il est nécessaire de réaliser l'incrémentabilité fiable pour réunir et analyser correctement le grand volume de données d'audit à partir des hôtes distribués. Dans le cas d'un IDS centralisé, la procédure de collection des données d'audit est distribuée alors que son analyse est centralisée. Cependant, il est difficile d'analyser toutes les données sur un seul IDS sans aucune perte des données.

5. ***Adaptabilité*** *:*

Les environnements de système informatique ne sont pas statiques, les utilisateurs et les administrateurs de système changent constamment et par conséquence les intrusions changent. Un IDS doit être capable de s'adapter aux changements dynamiques afin de détecter les différentes intrusions.

6. ***Analyse Globale*** *:*

Afin de détecter les intrusions issues du réseau, il est nécessaire de contrôler la corrélation entre les différents événements produits sur les différents hôtes car l'analyse établie par un seul hôte peut donner juste une erreur normale.

7. ***Efficacités*** *:*

Le système de détection d'intrusions doit être simple et assez souple pour ne pas influencer sur les activités des hôtes et le réseau ce qui peut engendrer la dégradation de performance du réseau.

3.2 Les buts de conception d'un IDS basé réseau

L'analyse des exigences identifiées ci-dessus peut être employée pour tirer trois buts de conception principaux d'un IDS basé réseau (52). Ces buts sont la distribution, l'auto organisation et la souplesse « lightweight ».

3.2.1 La distribution

Un système de détection d'intrusions basé réseau distribué délègue ses responsabilités à un nombre de composants distribués dont chacun contrôle un sous espace du système complet d'une manière concurrente et coopérative. Un IDS basé réseau distribué satisfera les exigences suivantes :

- ***Robustesse*** : pour un IDS basé réseau distribué, l'échec d'un composant de détection d'intrusions local n'endommage pas l'IDS complet bien qu'il cause la dégradation minimale de l'exactitude de la détection complète.
- ***Configurabilité*** : la facilité de configuration d'un processus de détection d'intrusions aux exigences locales d'un hôte spécifique sans considération des exigences d'autres hôtes.
- ***Extensibilité*** : si un nouvel hôte exécutant un système d'exploitation différent est ajouté à un réseau, il est facile d'ajouter des nouveaux processus de détection d'intrusions sur cet hôte, parce que les processus de détection d'intrusions sont indépendants et ne seront pas modifiés quand un nouveau processus est ajouté.
- ***Incrémentabilité « scalability »*** : puisque la collecte et l'analyse des données d'audit seront effectuées dans le même endroit dans un hôte contrôlé localement, le grand volume de données d'audit est distribué sur plusieurs hôtes locaux et par conséquence l'IDS distribué permet plus d'incrémentabilité que l'IDS basé sur un serveur local.

3.2.2 L'auto organisation

Un système de détection d'intrusions basé réseau auto organisé apprend les signatures d'intrusions qui sont inconnues et/ou distribuées sans aucune information prédéfinie. Un IDS basé réseau auto organisé satisfera les exigences suivantes :

- ***Adaptabilité*** : il est adaptatif parce qu'il n'y a aucun besoin de la mise à jour manuelle de ses signatures d'intrusions.
- ***Analyse globale*** : le système de détection d'intrusions complet fournit l'analyse globale parce qu'il est auto organisé à partir des interactions entre les différents processus de détection d'intrusions.

3.2.3 La souplesse « lightweight »

Un IDS basé réseau est souple parce qu'il n'influence pas sur les performances du système. Un IDS basé réseau souple satisfera la dernière exigence.

- ***Efficacité*** : quand chaque composant d'un IDS assure une partie minimale du contrôle, les activités principales qui doivent être exécutées par les hôtes locaux et le réseau ne sont pas défavorablement affectées par le contrôle.

3.4 Discussion

Le système immunitaire humain est distribué par son réseau immunitaire et les ensembles d'anticorps uniques. Ainsi, il est auto organisé en conséquence de trois processus évolutionnaires qui sont l'évolution de la bibliothèque de gènes, la sélection négative et la sélection clonale. Il est souple par la généralité de la liaison approximative, l'expression de gène, l'hypermutation somatique et l'efficacité des cellules mémoires. Ces propriétés significatives montrent le lien étroit entre le système immunitaire humain et le système de détection d'intrusions. Elles montrent que la réalisation des exigences principales pour la conception d'un système de détection d'intrusions basé réseau est envisageable par l'utilisation d'un système immunitaire artificiel, ce qui motive les différentes recherches exploitant les systèmes immunitaires artificiels dans le domaine de sécurité.

4. Conclusion :

Dans ce chapitre on a abordé le système immunitaire naturel avec ses différents concepts et mécanismes de défense, qui ont pour but de protéger le corps humain contre les différents envahisseurs et avec une grande adaptabilité vis-à-vis les changements que subissent les agents pathogènes et comment la mémoire immunitaire joue un rôle crucial dans la réduction de temps de réponse. Le mystère du système immunitaire a inspiré les chercheures qui ont vu dans cette métaphore la clé de voute pour la résolution des problèmes distincts de l'informatique, notamment les problèmes de sécurité informatique, l'optimisation et le clustring. L'utilisation des théories issues du système immunitaire humain a créé un nouvel axe de recherche en s'orientant vers l'étude du corps humain et ses secrets ce qui a donné naissance à une vision récente dans le domaine de l'informatique.

En effet, Les systèmes immunitaires artificiels sont considérés comme des solutions prometteuses dans le domaine de sécurité car ils ont apporté des résultats convaincants dans la détection d'intrusions. Ces systèmes sont toujours au centre d'intérêts de plusieurs chercheurs afin d'exploiter tous les concepts et les mécanismes d'identification ainsi que les méthodes de détection utilisés par le système immunitaire humain. En conséquence, plusieurs travaux ont été réalisés appliquant les différents modèles de SIA aux différentes approches des IDS.

Chapitre 3 :
Analyse et Conception

1. Introduction

Suite à la proposition de l'algorithme de la sélection négative par Stéphanie Forrest et son groupe qui ont essayé d'appliquer des métaphores du système immunitaire pour la détection des virus dans un système d'ordinateur. Ainsi, vu l'analogie entre l'objectif du système de détection d'intrusions et celui du système immunitaire humain, plusieurs travaux sont apparus dont le but principal est d'exploiter et intégrer les différents mécanismes utilisés par le système immunitaire pour la détection des intrusions.

2. Formatage et extraction d'attributs

Le trafic réseau est capturé dans un état brut (non structuré) qui donne peu d'informations sur une connexion. C'est pourquoi, une opération de formatage et d'extraction d'attributs est nécessaire, afin d'avoir des informations plus détailler qui nous permettes de distinguer entre un paquet normal ou une attaque. Cependant, tout le problème réside dans le choix et la sélection de ces attributs. Plusieurs travaux de recherches on fait l'objet de concevoir un jeu d'attributs complet, pertinents pour la majorité des attaques, cohérent, compact et rapide à extraire pour la détection d'intrusions (13). Pour notre système on a choisi le jeu de données **KDD cup 99.**

Le jeu de données KDD cup 99: L'ensemble de données de détection d'intrusion KDD 99 est basé sur l'initiative de DARPA 1998, qui fournit aux concepteurs des systèmes de détection d'intrusion (IDS) un benchmark pour évaluer les différentes méthodologies. Pour ce faire, la simulation est faite d'un réseau militaire factice composé de trois machines « cibles » exécutant des systèmes d'exploitation et des services diverses. Trois machines supplémentaires sont ensuite utilisées pour usurper des adresses IP différentes afin de générer un trafic réseau. Enfin, il existe un sniffer qui enregistre tous le trafic réseau utilisant le format de tcpdump. La période totale de simulation est sept semaines. Cette base représente des lignes TCP/IP dump, où chaque ligne est une connexion caractérisée par 41 attributs séparées par des virgules, tels que : la durée de connexion, le type du protocole, …etc. En tenant compte des valeurs de ses attributs, chaque connexion dans KDD'99 est considérée comme étant une connexion normale ou bien une attaque cela est inscrit dans un champ additionnel numéro 42. Les connexions normales sont créées pour un profil attendu dans un réseau militaire.

La base KDD'99 recense 39 attaques possibles qui peuvent être regroupées en quatre catégories :

- **Attaques par « Déni de Service » (Denial Of Service DOS) :**

Ce type d'attaques perturbe et dégrade le fonctionnement normal d'un système ou d'un réseau. Ces attaques sont à but purement "destructeur" et sont souvent très simples à mettre en oeuvre.

- **Attaques par « Utilisateur vers Administrateur » (User to Root U2R) :** L'attaquant commence à avoir un accès à un compte utilisateur normal sur le système, ensuite il essaie d'exploiter la vulnérabilité sur ce système pour obtenir un accès administrateur.

- **Attaques par « Distant vers local » (Remote to Local R2L):**

L'attaque R2L se produit quand un pirate envoi des paquets vers une machine à travers un réseau sans avoir un compte sur cette machine. Autrement dit il exploite une vulnérabilité afin d'obtenir un accès local comme utilisateur de cette machine.

- **Attaques par « Sonde » (Probing) :**

Ces d'attaques préludent d'autres types d'attaques, en scannant un réseau en vue de collecter les informations nécessaires, telle que les systèmes avec ports en écoute afin de lancer les actions constituant l'attaque proprement dite.

Le tableau suivant présente les 41 attributs de chaque enregistrement :

N°	Attribut	N°	Attribut	N°	Attribut	N°	Attribut
1	duration	12	logged_in	23	count	34	dst_host_same_srv_rate
2	protocol_type	13	num_compromised	24	srv_count	35	dst_host_diff_srv_rate
3	service	14	root_shell	25	25 serror_rate	36	dst_host_same_src_port_rate
4	Flag	15	su_attempted	26	srv_serror_rate	37	dst_host_srv_diff_host_rate
5	src_bytes	16	num_root	27	rerror_rate	38	dst_host_serror_rate
6	dst_bytes	17	num_file_creations	28	srv_rerror_rate	39	dst_host_srv_serror_rate
7	Land	18	num_shells	29	same_srv_rate	40	dst_host_rerror_rate
8	wrong_fragment	19	num_access_files	30	diff_srv_rate	41	dst_host_srv_rerror_rate
9	urgent	20	num_outbound_cmds	31	srv_diff_host_r ate		
10	Hot	21	is_host_login	32	dst_host_count		
11	num_failed_logins	22	is_guest_login	33	dst_host_srv_count		

Tableau 3. 1: les attributs de chaque ligne de connexion (14).

Le tableau ci-dessous présente les attaques des chaque classe :

Catégories d'attaques	Noms des attaques
DOS	back, land, neptune, pod, smurf, teardrop, apache2, mailbomb, processtable, udpstorm
(U2R)	buffer_overflow, perl, loadmodule, rootkit, httptunnel, ps, sqlattack, xterm
(R2)	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster, named, sendmail, snmpgetattack, snmpguess, worm, xclock, xsnoop
Probing	ipsweep, nmap, portsweep, satan, mscan, saint

Tableau 3. 2: les attaques de chaque classe (13).

3. La sélection d'attribut pertinent

Pour justifier les performances des détecteurs basés sur l'apprentissage automatique formé à partir des données de la base KDD 99. Des travaux ont été réalisés pour trouver la pertinence des attributs. À cette fin, le gain d'informations est utilisé pour déterminer les caractéristiques les plus discriminantes pour chaque classe.

Notre système proposé s'appuie sur le travail de **Wei Wang, Sylvain Gombault** et**Thomas Guyet.**

Le tableau suivant présente les attributs jugés pertinents selon leur étude :

Les attaques	Les attributs sélectionnés
DoS	3, 4, 5, 6, 8, 10, 13, 23, 24, 37
Probe	3, 4, 5, 6, 29, 30, 32, 35, 39, 40
R2L	1, 3, 5, 6, 12, 22, 23, 31, 32, 33
U2R	1, 2, 3, 5, 10, 13, 14, 32, 33, 36

Tableau 3. 3: les attributs pertinents de chaque classe d'attaque (5).

4. Conception du système proposé

4.1 Les composants immunitaires

Comme tout système immunitaire artificiel, des composants fondamentaux sont implémentés citant :

a. **Antigène (AG) :** Dans notre approche, nous considérons une intrusion tout paquet IP de type antigène, ce dernier peut être
   - **Un élément de soi :** si le paquet est considéré comme étant une connexion normale et qui n'a aucun risque sur le réseau.
   - **Un élément de non soi :** si le paquet est considérer comme une attaque sur le réseau (une connexion anormale).

b. **Anticorps :** désignent l'ensemble de détecteurs représentés sous forme de chaines de caractères combinant les attributs pertinents qui caractérisent chaque type d'attaque ayant une longueur semblable avec les antigènes, les anticorps sont constamment à la recherche des antigènes (connexion malveillante) afin de les empêcher de pénétrer le réseau.

c. **Mesure d'affinité**: Dans le but de mesurer l'affinité entre le couple Antigène /Anticorps, notre système s'appuie sur la distance de Hamming (DH). Dont :
   - Un antigène est représenté par un vecteur Ag=<Ag1, Ag2,..., AgL>,
   - Un anticorps est à son tour représenté par un vecteur Ab=<Ab1,Ab2,…,AbL>.

La distance de Hamming : $D = \sum_{i=1}^{n} \sigma i$ ou $\sigma = \begin{cases} 1, & Abi \neq Agi \\ 0, & Sinon \end{cases}$

Pour mesurer le degré de complétude entre l'antigène et l'anticorps:
La fonction d'affinité est comme suit :

Affinité : $\begin{cases} 1, & Si\ Distance\_Hamming\ (Ag, Ab) > \sigma \\ 0, & Sinon \end{cases}$

d. **Les algorithmes immunitaires :** dans le cadre de notre étude on a choisi l'algorithme de la sélection négative car il a prouvé à travers plusieurs travaux précédents son efficacité en se qui concerne la discrimination entre le soi et le non soi citant comme exemple le travail de **S.Hofmeyr**, qui a conçu un IDS nommé LYSIS basé sur l'algorithme de la sélection négative. Qu'il est prédéfini déjà.

4.2 Les classes du système :

Notre système se constitue d'un ensemble des classes qui coopèrent pour réaliser les tâches requises, la surveillance du réseau d'une part et la gestion du trafic réseau d'une autre part. Le tableau suivant présente les classes et leurs fonctions dans le système :

Classe	Fonction
Class Routeur	Assure la connectivité, en recevant les paquets de l'extérieur et les retransmettre vers les hôtes cibles si ces paquets ne présentent aucun risque sur le réseau. Il agit comme un capteur de paquets pour l'IDS.
Class PaquetGenerator	Permet la génération des paquets du trafic réseau (générer des connexions normales)
Class Client 1	Cette class simule le client numéro1 du réseau surveillé
Class Client 2	Cette class simule le client numéro 2 du réseau surveillé
Class Client 3	Cette class simule le client numéro3 du réseau surveillé

Class History	Permet l'IDS de vérifier si une connexion est anormale toute en consultant l'historique des attaques sur ce réseau.
Class Detector 1	Permet la détection d'intrusion pour les paquets ciblant du client 1 du réseau en s'appuyant sur la base d'attaques du système.la discrimination du soi et noi- soi ici est basée sur l'algorithme de la sélection négative Cette class représente l'analyseur des données d'IDS
Class Detector 2	Même principe de fonctionnement du Dector1 sauf qu'il s'occupe de la détection d'intrusion pour Le client 2
Class Detector 3	Même principe de fonctionnement du Dector1 sauf qu'il s'occupe de la détection d'intrusion pour le client 3
Class Hacker	C'est le responsable du lancement des différents attaques vers les hôtes cibles (générer des connexions malveillantes)
Class Alerte	C'est la class responsable de déclanchement d'alerte si une attaque est détecté

Tableau 3. 4: les classes du système

4.3 Le processus de déroulement

4.3.1 La construction de la base d'attaque

La base d'attaques est composée d'un ensemble de détecteurs générés en s'appuyant sur l'algorithme de sélection négative selon le processus suivant :

1. Extraction des attributs pertinents de chaque attaque à partir de la base KDD cup 99.

2. Elimination des détecteurs redondants.

3. Vérification de correspondance avec les modèles de soi avec élimination des détecteurs qui reconnaissent le soi.

4. Vérification de correspondance avec les modèles de non soi.

L'organigramme ci-dessous résume le processus de construction de la base d'attaques :

Figure 3. 1: processus de génération de détecteur (3).

4.3.2 Le processus de détection

Afin de générer un trafic réseau, la class PaquetGenerator génère des paquets et envoie ces derniers vers la class routeur comme un trafic normal. Pour lancer une attaque, la class Hacker prend place et envoie à son tour un paquet malveillant vers le routeur.

Lors de la réception d'un paquet quelconque le routeur active le processus de détection. Dans le système proposé le processus de détection se déroule en 2 phases :

- **La première phase:** la vérification est réalisée par rapport à la base d'historique d'attaques subies par le réseau surveillé dans le but de minimiser le temps et accélérer la génération de réponse tout en cherchant dans une base d'historique réduite en terme de taille par rapport à la base d'attaques. Si le

paquet existe dans la base d'historique, la class Historique va envoyer la réponse vers le routeur qui va à son tour bloquer ce paquet ainsi qu'une alerte va être déclenchée par la class Alerte. Sinon il lance la deuxième phase de détection.

- **La deuxième phase:** la class détector va vérifier le paquet entrant par rapport à la base d'attaques construite précédemment. Si il existe une corrélation entre le paquet entrant et le détecteur, la réponse va être envoyer vers le routeur, si une attaque est détectée le routeur va bloquer ce paquet ainsi qu'une alerte va être déclenchée par la class Alerte de plus la class detector va ajouter la nouvelle attaque détectée dans l'historique des attaques. Si aucune attaque n'a été reconnue alors le routeur est autorisé à transmettre le paquet vers la cible.

Enfin, pour améliorer les performances et actualiser le système, ce dernier propose aussi une mise à jour manuelle de la base d'attaques, en ajoutant des détecteurs manuellement après une vérification d'existence pour éviter des détecteurs redondants ainsi qu'une vérification de correspondance avec les modèles de soi, Cette procédure a pour but d'enrichir l'ensemble de détecteurs.

L'organigramme suivant résume le processus de détection du système :

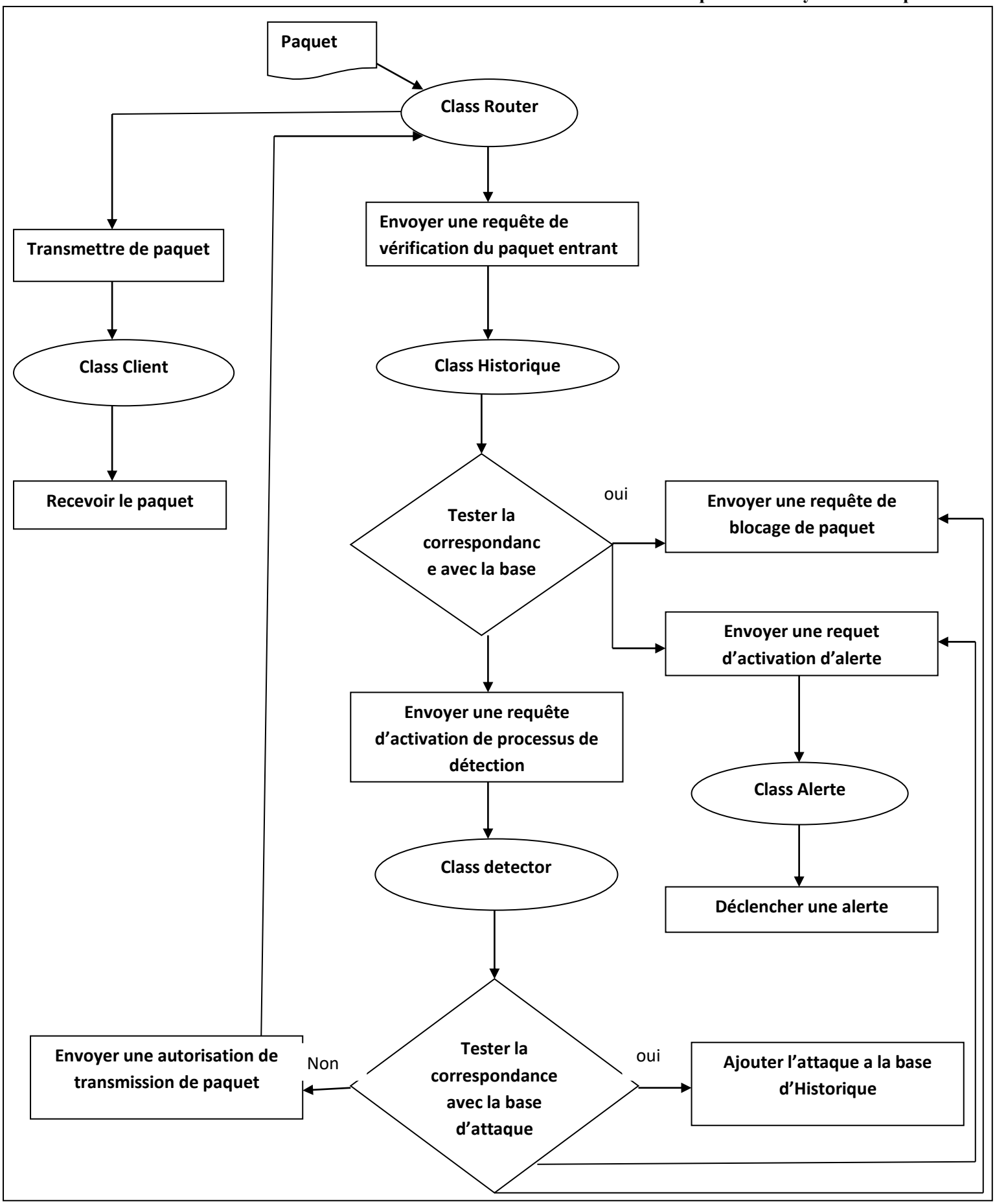

Figure 3. 2: Le processus de détection

La figure suivante présente l'architecture générale du système proposé :

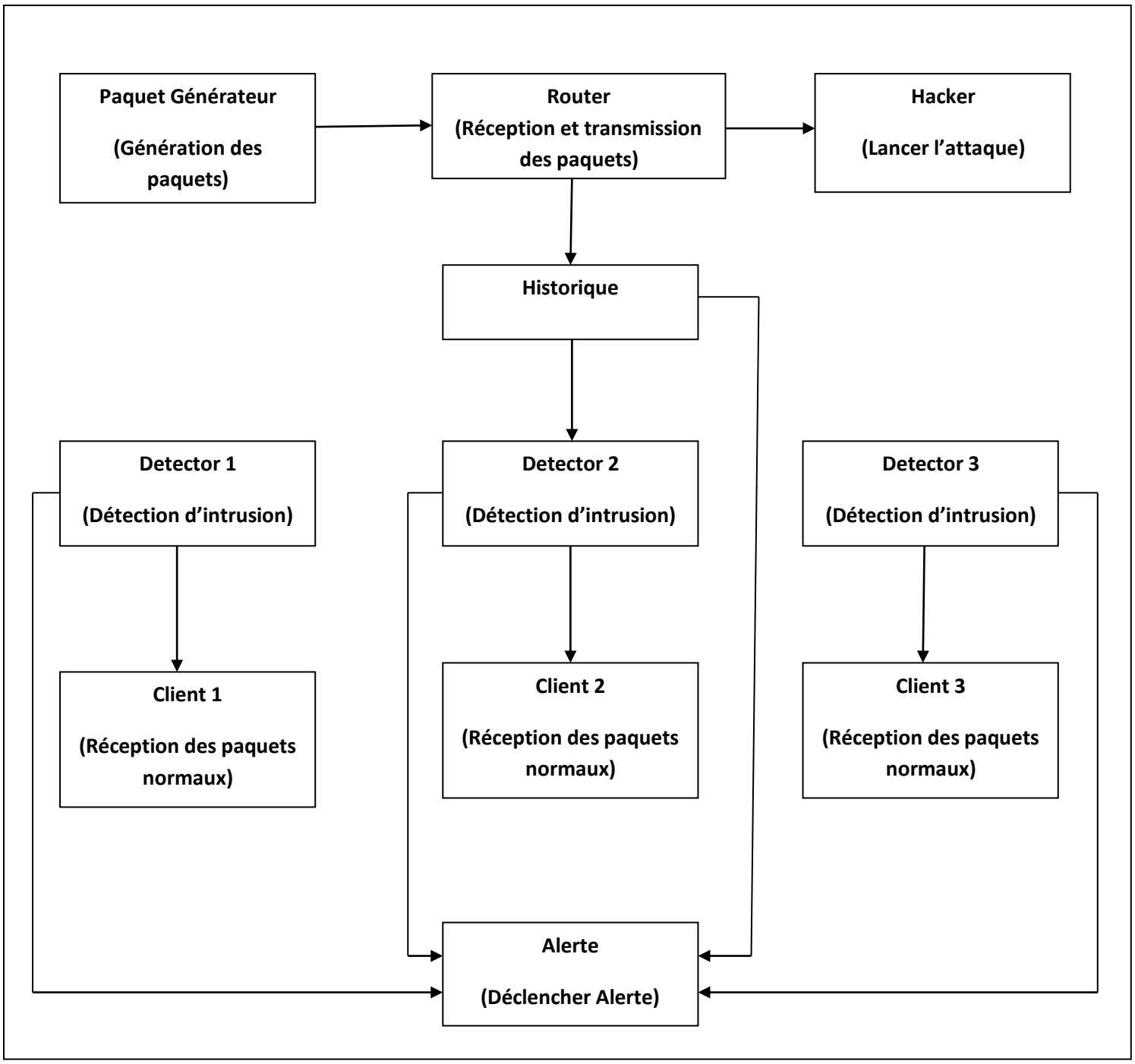

Figure 3. 3: Architecture général du système proposé

La figure suivante présente le diagramme de séquence :

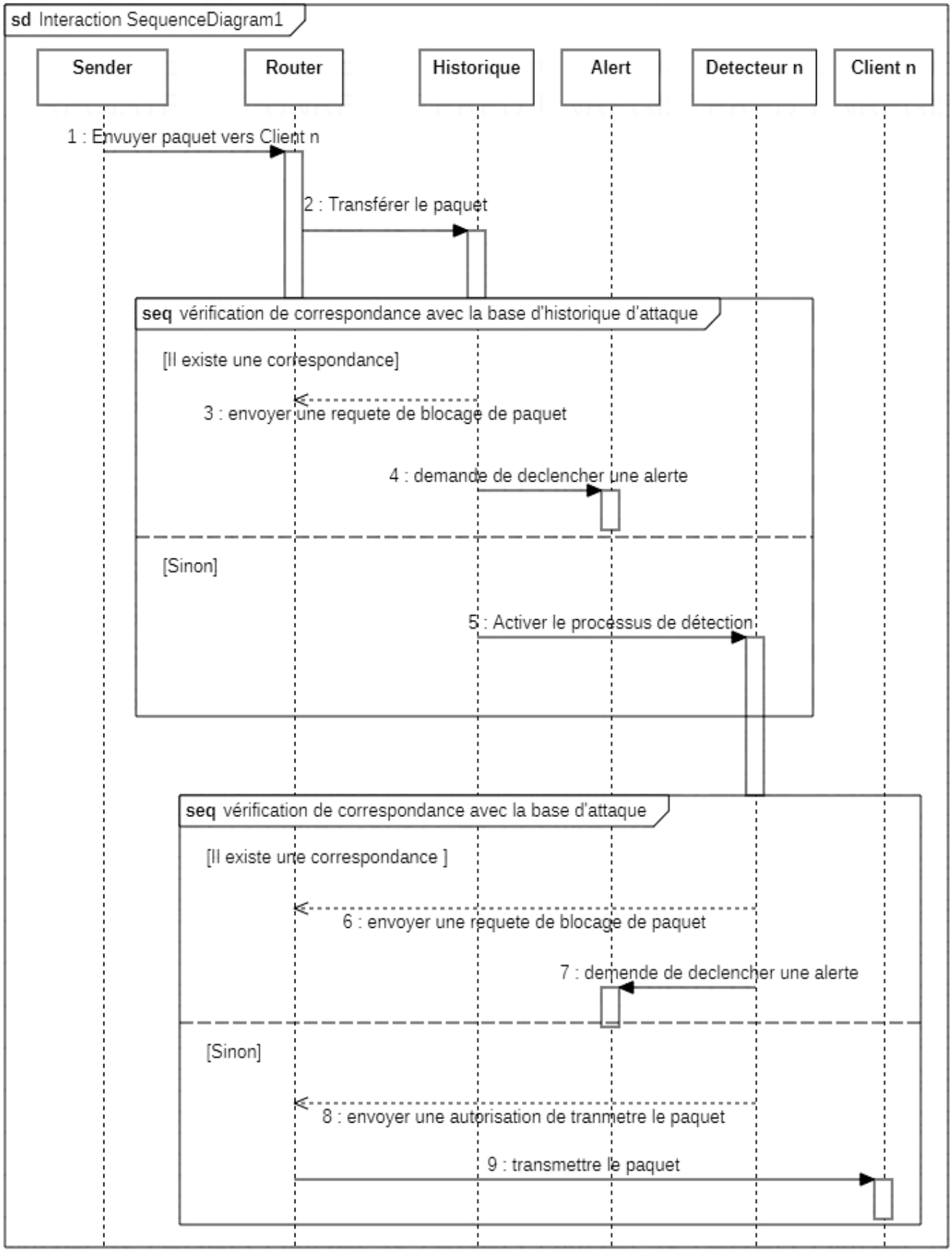

Figure 3. 4: Diagramme de séquence

Dans le diagramme précédant «Sender» désigne un émetteur de paquet, qui peut être Hacker ou le PacketGenerator mais dans les deux cas meme processus de vérification des paquets entrant va s'exécuter.

La figure ci-dessus présente le diagramme de classe du système proposé :

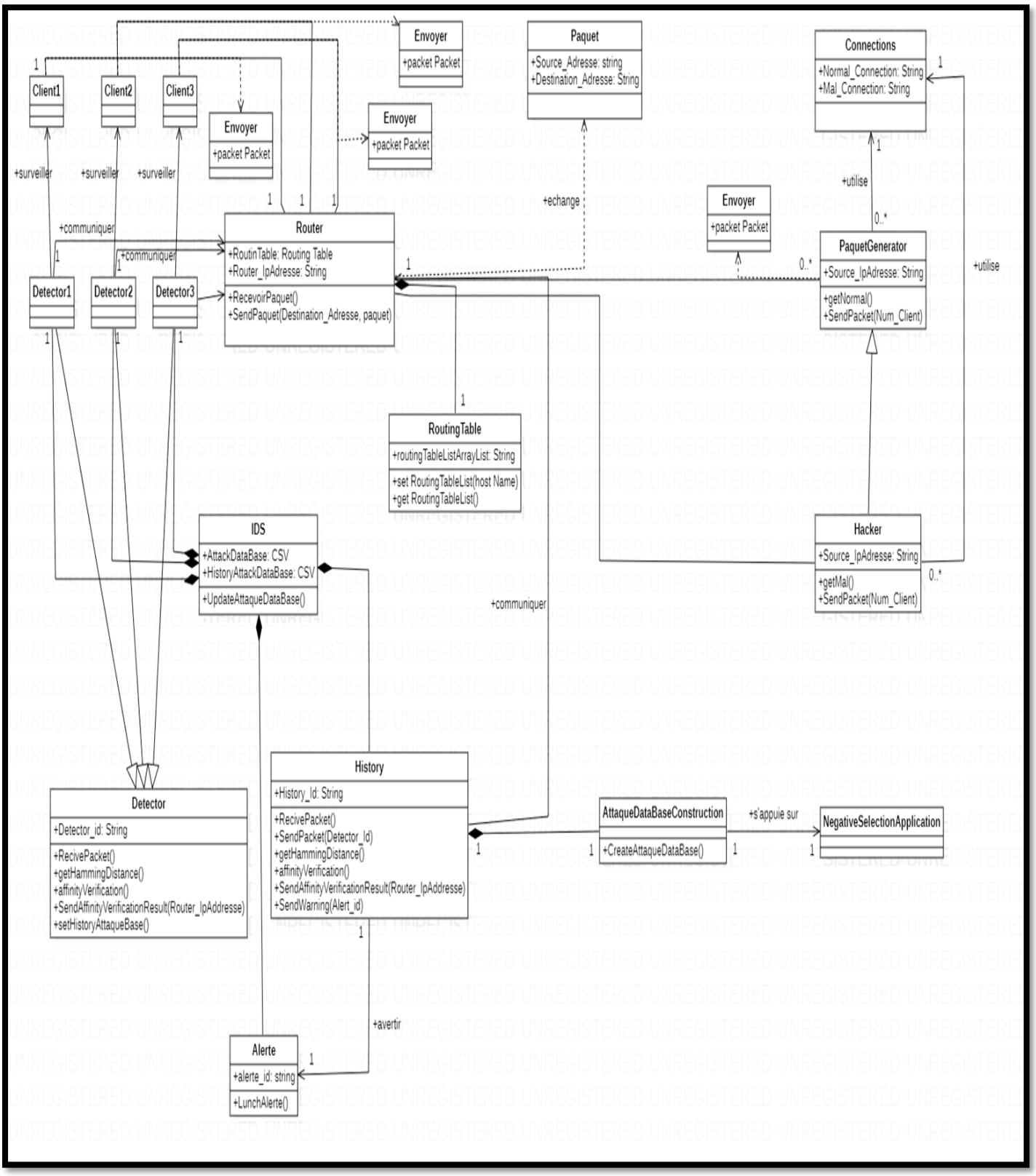

Figure 3. 5 : Diagramme de classe

5. Etude expérimentale

Pour évaluer le système proposé il faut calculé le taux de détection et le taux de fausse alerte avec :

TP : True positive (Vrai positif) événement intrusif identifié comme intrusion

TN : True Négative (Vrai Négatif) événement normal identifié comme normal

FP : False Positive (Faux Positif) événement normal identifié comme intrusion

FN : False Négative (Faux Négatif) événement intrusif identifie comme normal

Taux de détection = TP/ (TP + FN)

Taux de fausse Alerte = FP/ (FP + TN)

6. Conclusion

Dans ce chapitre, nous avons présenté la base de données utilisée, ensuite on a présenté les diagrammes du système proposée et on a détaillé les différents étapes nécessaire a la mise en ouvre. Pour la suite nous avons présenté un étude expérimentations qui ont été réalisées. Ces études qui ont prouvé l'efficacité des systèmes immunitaires artificiels pour obtenue un Taux de détection d'attaque élevé.

Chapitre 4 :
Réalisation et Implémentation

1. Introduction

Dans ce chapitre nous avons présenté les environnements de développement et les différentes interfaces du système proposé

2. Les environnements de développements

2.1 Le langage JAVA

Pour la mise en œuvre de notre système, nous allons choisir le langage de programmation orienté objet « Java » développé par Sun Microsystems. Ce langage a réussi à intéresser beaucoup de développeurs à travers le monde. En effet, Java est un langage multiplateforme disposant d'une machine virtuelle appelée JVM (Java Virtual Machine) lui permettant de s'exécuter sur n'importe quelle machine. Java est capable de tourner aussi bien sur un PC que sur un MAC, sur un téléphone ou encore sur une carte à puce.

Pour programmer avec java dans notre application, nous utilisons la version 8 du JRE (Java Runtime Environment).

2.2 ECLIPSE

Eclipse IDE est un environnement de développement intégré libre (le terme Eclipse désigne également le projet correspondant, lancé par IBM) extensible, universel et polyvalent, permettant potentiellement de créer des projets de développement mettant en oeuvre n'importe quel langage de programmation. Eclipse IDE est principalement écrit en Java (à l'aide de la bibliothèque graphique SWT, d'IBM), et ce langage, grâce à des bibliothèques spécifiques, est également utilisé pour écrire des extensions.

La spécificité d'Eclipse IDE vient du fait de son architecture totalement développée autour de la notion de plug-in (en conformité avec la norme OSGi) : toutes les fonctionnalités de cet atelier logiciel sont développées en tant que plug-in.

Plusieurs logiciels commerciaux sont basés sur ce logiciel libre, comme par exemple IBM Lotus Notes 8, IBM Symphony ou Websphere Studio Application Developer.

De nombreux langages sont d'ores et déjà supportés (la plupart grâce à l'ajout de plug-ins), parmi lesquels : Java, RPG pour system I, C#, C++, C, Objective Caml, Python, Perl, Ruby, COBOL, Pascal, PHP, Javascript, XML, HTML, XUL, SQL, ActionScript, Coldfusion[6].

3. NSL-KDD DataSet :

NSL-KDD est un ensemble de données proposé pour résoudre certains des problèmes inhérents au KDD'99 dataset. Bien que cette nouvelle version d'ensembles de données KDD pose encore quelques problèmes et ne soit pas un représentant idéal des réseaux réels actuels, nous pensons qu'elle peut toujours

[6] https://www.techno-science.net/definition/517.html

être utilisée comme un dataset de référence efficace pour aider les chercheurs à comparer différentes méthodes de détection (6).

3.1 Les avantages de NSL-KDD

Le NSL-KDD dataset présente les avantages suivants par rapport au KDD'99 dataset d'origine (18):

- Il n'inclut pas les enregistrements redondants dans l'ensemble d'apprentissage, de sorte que les classificateurs ne seront pas orientés vers des enregistrements plus fréquents.
- Il n'y a aucun enregistrement en double dans les ensembles de tests proposés; par conséquent, les performances des apprenants ne sont pas biaisées par les méthodes qui ont de meilleurs taux de détection sur les enregistrements fréquents.
- Le nombre d'enregistrements dans l'ensemble d'apprentissage et les tests est raisonnable, ce qui permet de réaliser des expériences sur l'ensemble complet sans qu'il soit nécessaire de sélectionner au hasard une petite partie. Par conséquent, les résultats d'évaluation de différents travaux de recherche seront cohérents et comparables.

4. Matériel

Notre application a été réalisé sous le système exploitation Windows 10 64 bits. Le développement a été fait sur une machine dotée d'un processeur Intel (R) Core (TM) i3 @2.00GHz 2.00 GHz RAM 4 GO.

5. Les interfaces du système :

Figure 4. 1: Premier interface du système

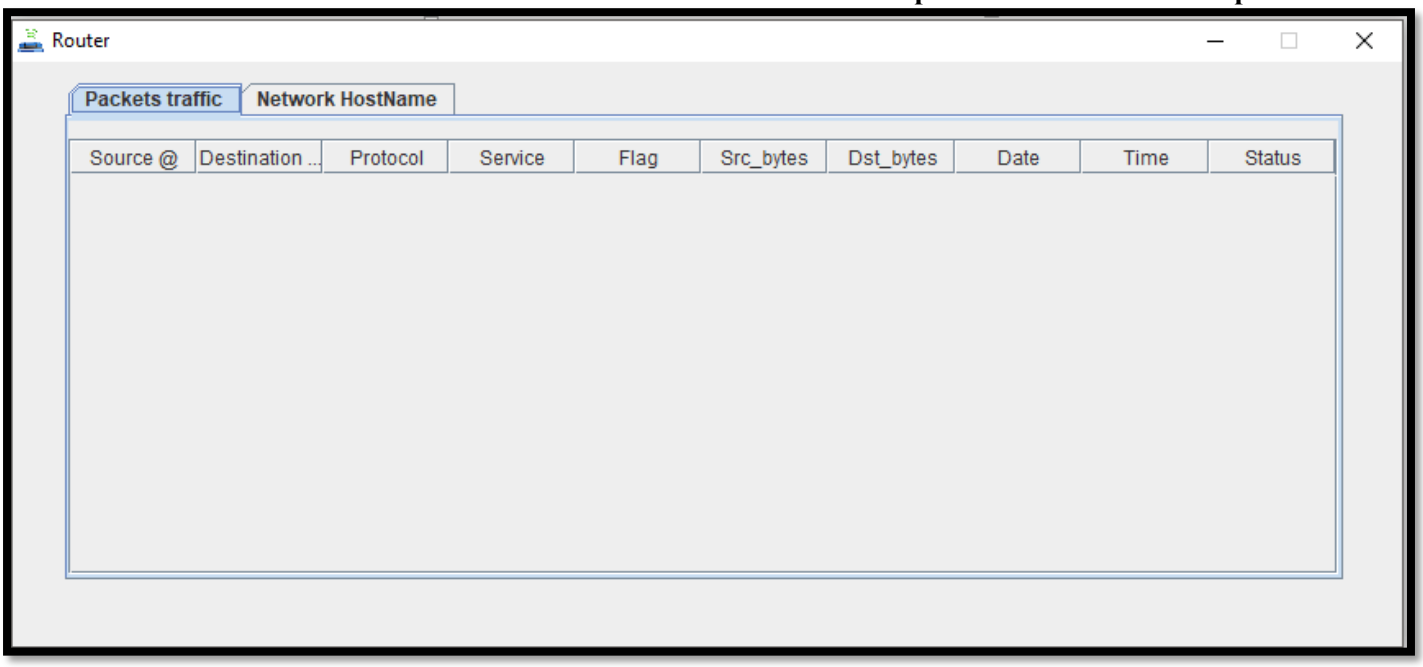

Figure 4. 2: Interface du routeur

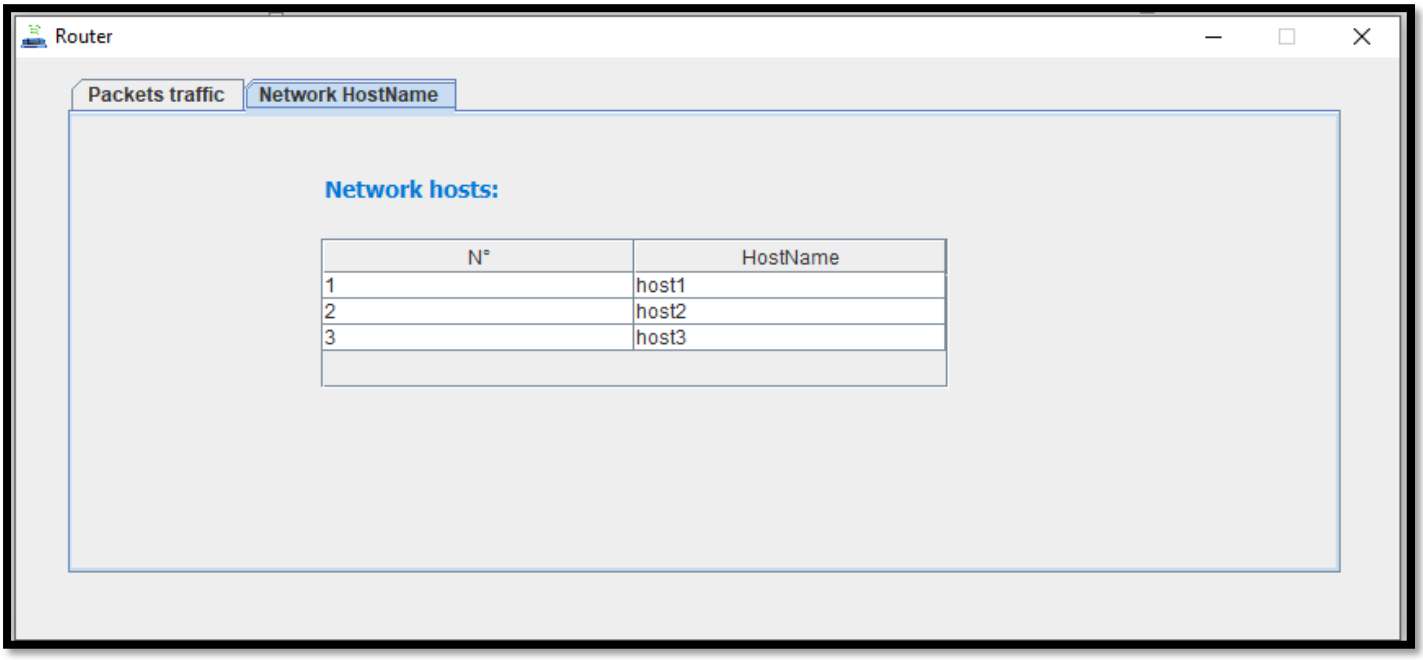

Figure 4. 3: Table du routage

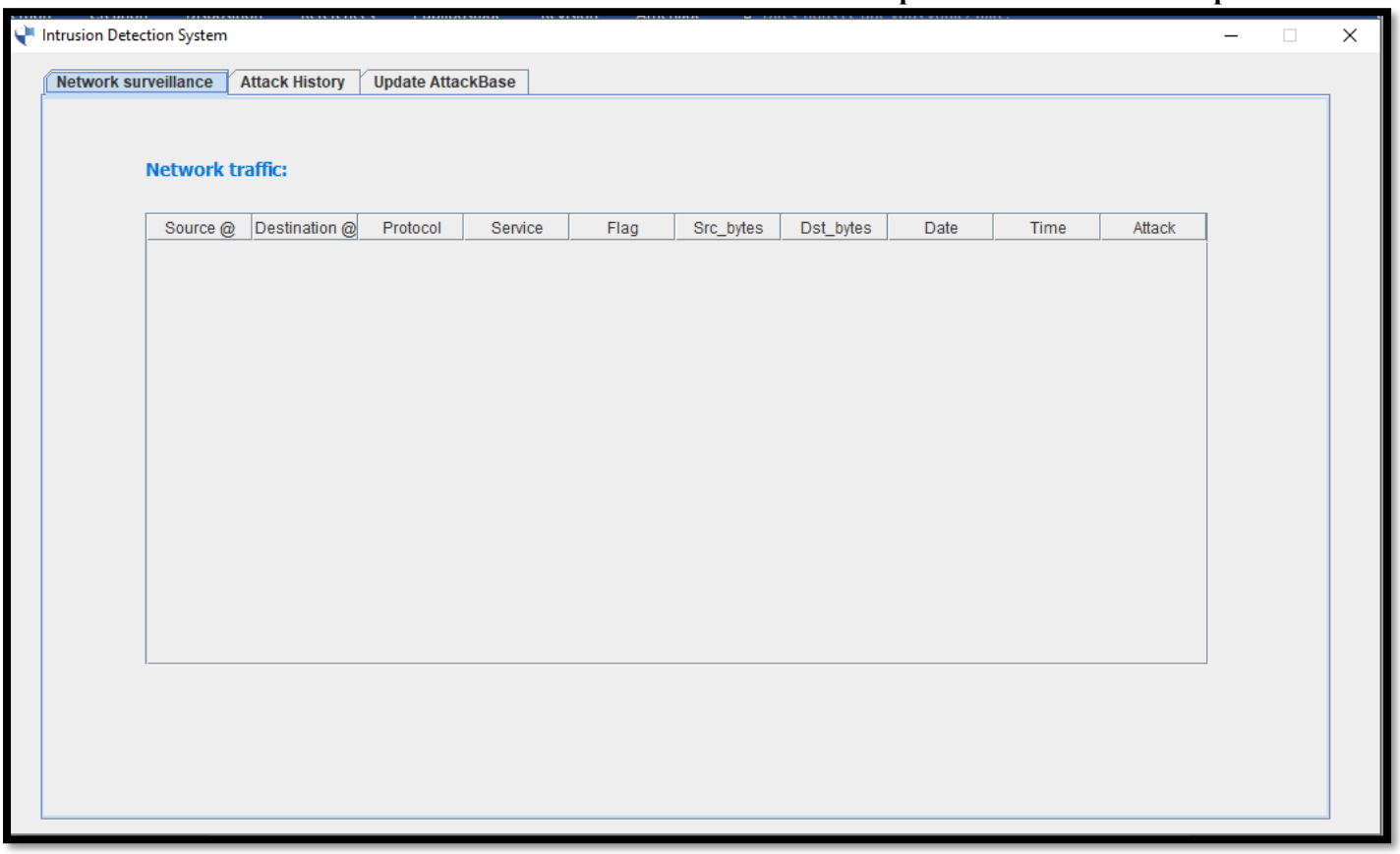

Figure 4. 4: Interface d'IDS

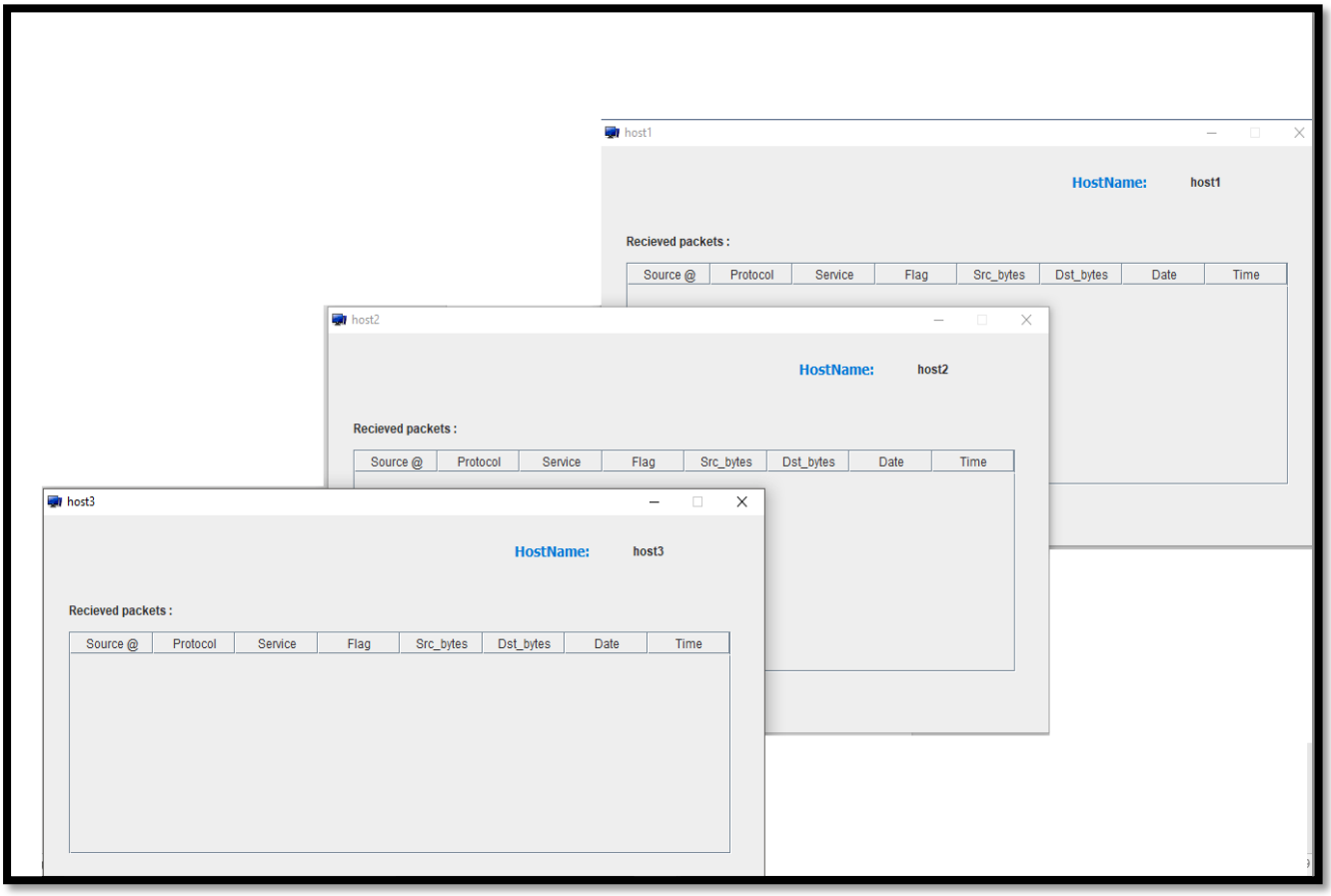

Figure 4. 5: Lancement des 3 hôtes

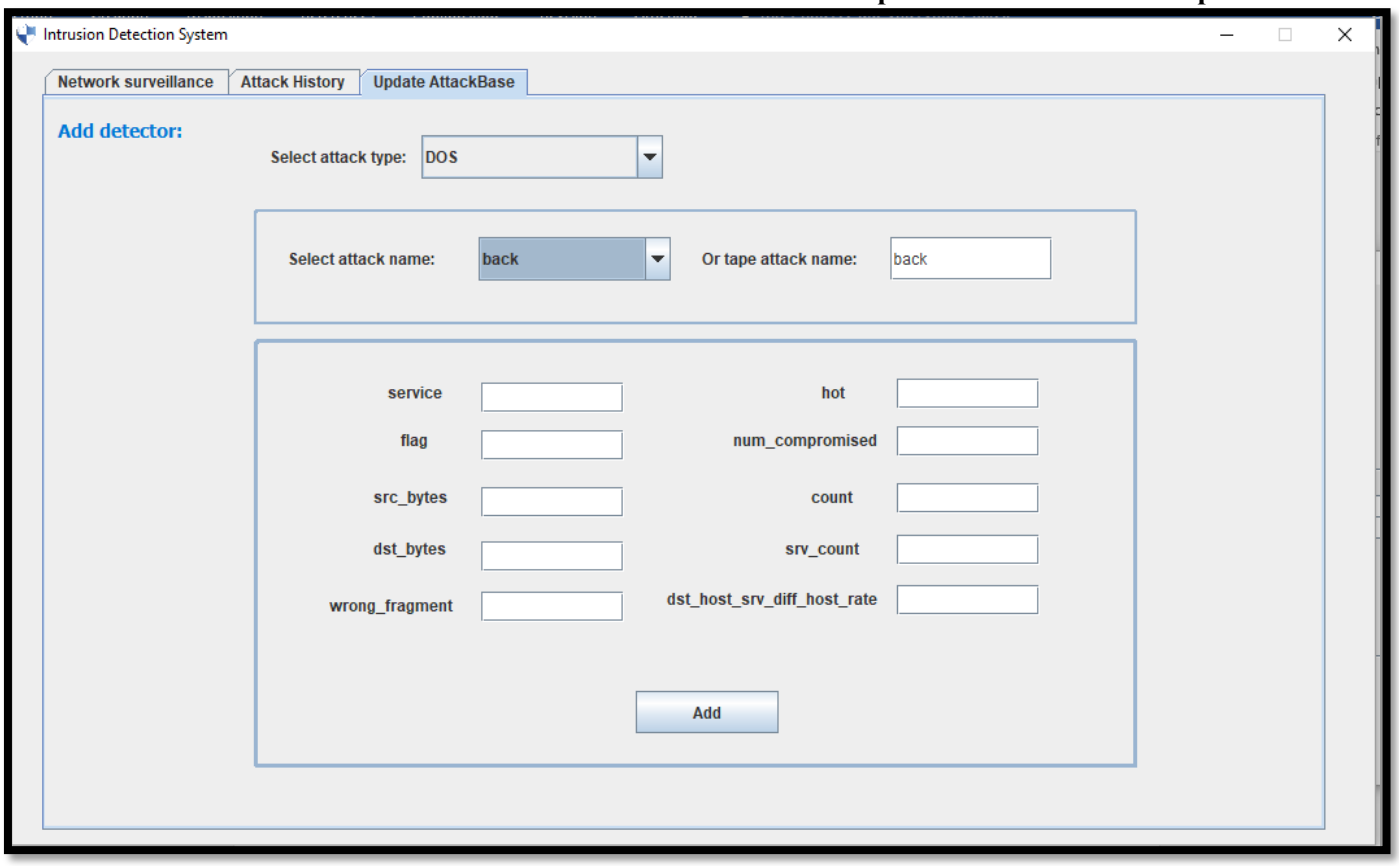

Figure 4. 6: Interface de la mise à jour manuelle du système

Figure 4. 7: Interface de l'attaquant

Conclusion

Dans ce dernier chapitre réalisation et implémentation nous avons présenté les différentes interfaces du système proposé qui est un système de détection d'intrusion basé sur une approche immunitaire artificiel basé sur l'algorithme de la sélection négative.

Conclusion général

Vu l'analogie entre l'objectif du système immunitaire naturel et l'objectif des systèmes de détection d'intrusions. Ainsi, la capacité puissante du système immunitaire humain à assurer la protection du corps contre les différents intrus qui envahissent le corps. Les systèmes immunitaires artificiels présentent des solutions prometteuses pour assurer la protection des systèmes informatiques. Ce domaine de recherche constitue toujours le centre d'intérêt des différentes recherches afin d'exploiter tous les concepts et les mécanismes d'identification et de détection utilisés par le système immunitaire humain.

Les résultats expérimentaux effectués sur cet algorithme montrent la possibilité de détecter les éléments de soi qui peuvent provoquer des dégâts dans le système dont le système est initialement tolérant. Ainsi, l'algorithme détecte les éléments de non soi dangereux qui ont établi des intrusions réelles.

Nous espérons dans l'avenir d'intégrer d'autres concepts inspirés du système immunitaire humain et en particulier les fonctionnalités proposées par la théorie de danger comme par exemple la zone de danger qui est établie au tour de signaux d'alarme déclenchés, cette zone qui peut être intégrée dans le système immunitaire artificiel en terme temporelle. Ainsi, l'intégration des molécules de costimulation produisent par les cellules dendritiques qui ont un effet amplifiant sur les signaux d'alarme produits dans le système.

A la fin de ce travail, le système immunitaire naturel constitue toujours une source d'inspiration très riche dont le but principal des différentes recherches est la compréhension et l'extraction des mécanismes clefs utilisés par ce système dans l'identification, la détection et l'élimination des intrus afin de construire des systèmes immunitaires pour protéger les systèmes et les réseaux d'une manière efficace.

Bibliographie

1. **Gunadiz Safia, Algorithmes d‟intelligence artificielle pour la classification d‟attaques réseaux a partir de données TCP, université de boumerdes,2011.** 27/02/2017, https://www.securiteinfo.com/conseils/choix_ids.shtml:le.

2. **M Thibaut Probst : évaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing, 2015.**

3. **Mme LABED Ines : Proposition d‟un système immunitaire artificiel pour la détection d‟intrusions, universite de Constantine, 2006.**

4. **Rodrigue Mpyana Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP. Cas de Mecelco, 2011.**

5. **William Stallings, network security essentials: applications and standards fourth edition,2011.**

6. **Aissaoui Sihem, Apprentissage automatique et sécurité des systèmes d‟information :Application :un système de détection d‟intrusion basé sur les (SVM),Université d‟oran,2008.**

7. **Yousef Farhaoui, «Evaluation des systèmes de détection et de prévention des intrusions et la conception d‟un BIDS », thèse de doctorat, Université Ibn Zohr, 2012.**

8. **CARPENTIER, Jean-François. La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques. Edition ENI, 2009. [En ligne]. Disponible.** *https://books.google.com/books?hl=fr&lr=&id=dsn7gsgbEZYC&oi=fnd&pg=PA11&dq=disponibilit%C3.*

9. **SecuriteInfo.com, Lexique de la Sécurité Informatique. [En ligne]. Disponible:.** *https://www.securiteinfo.com/divers/lexique.shtml.*

10. **Gabriel Dabi-Schwebel, Fichier LOG : Définition. [En ligne]. Disponible :.** *https://www.1min30.com/dictionnaire-du-web/fichier-log-definition.*

11. **El mostapha CHAKIR, Youness IDRISSI KHAMLICHI,Mohammed MOUGHIT,Contribution à la Nouvelle Génération des Systèmes de Détection d'Intrusion : Une approche basée sur les Agents Mobiles. [En ligne]. Disponible :.** *https://www.academia.edu/24434474/Contribution_%C3%A0_la_Nouvelle_G%C3%A9n%C3%A9ration.*

12. **M. Tran Van Tay, Le Système De Détection Des Intrusions t Le Système D'empêchement Des Intrusions. [En ligne]. Disponible :.** *https://repo.zenksecurity.com/Protocoles_reseaux_securisation/IDS%20intrusion%20detections%20snort.pdf .*

13. **Benyettou Noria, Modélisation des Systèmes Immunitaires Artificiel par les Systèmes Multi-Agents Pour la Détection d'intrusion dans les réseaux informatique, thèse en vue de l'obtention du diplôme de Doctorat, département d'informatique, université de Moh.**

14. **Damien Riquet, Une architecture de détection d'intrusions réseau distribuée basée sur un langage dédié, thèse en vue de l'obtention du diplôme de Doctorat, département d'informatique, université Lille 1,2015. [En ligne]. Disponible :.** *https://hal.archives-ouvertes.fr/tel-01757859/document.*

15. **Nicolas Baudoin, Marion Karle,NT Réseaux IDS et IPS, .[En ligne].Disponible:.** *http://igm.univ-mlv.fr/~duris/NTREZO/20032004/Baudoin-Karle-IDS-IPS.pdf.*

16. **David Burgermeister, Jonathan Krier,, Les systèmes de détection d'intrusions. [En ligne]. Disponible :.** *https://dbprog.developpez.com/.*

17. **Odile PAPINI, Les systèmes de détection d'intrusions. [En ligne]. Disponible :.** *http://odile.papini.perso.luminy.univ-amu.fr/sources/SECURITE/cours-SSI-5.pdf.*

18. **Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, Edition McGraw-Hill 2004.**

19. **Kaoutar EL KABDANI, Sécurité Informatique au sein de l'entreprise. [En ligne]. Disponible :.** *https://wikimemoires.net/2012/08/les-systemes-de-detections-dintrusions-securite-des-reseaux/.*

20. **Rebiha HADAOUI, Un IDS basé sur un algorithme inspiré du fonctionnement de colonies des fourmis, mémoire en vue de l'obtention du diplôme de magister, département d'informatique, université de M'hamed Bougara, Boumerdes, ,2008-2009. [Enligne]. Disponible:.** *http://dlibrary.univ-boumerdes.dz:8080/handle/123456789/911.*

21. **Abdelhalim Zaidi. Recherche et détection des patterns d'attaques dans les réseaux IP _a hauts débits. Réseaux et télécommunications [cs.NI]. Université d'Evry-Val d'Essonne, 2011.**

22. **Nathalie Dagorn. D´etection et pr´evention d"intrusion : pr´esentation et limites. [Rapport de recherche], Université de Nancy1, France,2006.**

23. **Rebecca Bace1, Peter Mell Intrusion Detection Systems. . [En ligne]. Disponible :.** *https://pdfs.semanticscholar.org/44b0/95940e9b8ed827d633ab8f7ea4abd9033478.pdf.*

24. **Joseph ALOUF, Pierre GRABAR, Immunologie. [En ligne]. Disponible :.** *http://www.universalis.fr/encyclopedie/immunologie.*

25. **Encyclopedia.com, Monde de microbiologie et d'immunologie : Histoire de l'immunologie. [En ligne]. Disponible:https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/history- immunology.**

26. **Le CEA, Organisme public de la recherche, (2015),Le système immunitaire.**

27. **J. Timmis & T. Knight & L.N. De Castro & E.Hart, «An overview of Artificial.**

28. **intrusion, J. Kim & P. Bentley « Towards an artificial immune system for network.**

29. **Mon Système Immunitaire, Les organes du système immunitaire (11 juin 2014).** *https://www.monsystemeimmunitaire.fr/les-organes-du-systeme-immunitaire/.*

30. **Pierre Stouff, Le système immunitaire: des cellules et des organes. [En ligne]. Disponible : http://pst.chez-alice.fr/ts2tp.htm.**

31. **Matthieu SIMON, 07 septembre 2009, Immunologie. Les cellules immunitaires et les organes lymphoïdes.**

32. **Mon Système Immunitaire, Système Immunitaire. Vue Générale Des Cellules Du Système Immunitaire, 23 Juin 2016. [En ligne]. Disponible :.** *https://www.monsystemeimmunitaire.fr/vue-generale-des-cellules-du-systeme-immunitaire/.*

33. **Elisabeth Planchet, Sébastien Maugenest, CORPS HUMAIN ET SANTÉ. Août 2014.** *http://ressources.unisciel.fr/DAEU-biologie/P2/co/P2_chap5_c02.html.*

34. **Kenneth Todar, Immune Defense against Bacterial Pathogens: Adaptive or Acquired Immunity. [En ligne].** *http://textbookofbacteriology.net/adaptive_2.html.*

35. **Futura Santé, Anticorps. [En ligne]. Disponible :.** *https://www.futura-sciences.com/sante/definitions/medecine-anticorps-93/.*

36. **Floriane et Léa, Fonctions d'anticorps. [En ligne]. Disponible :.** *https://sites.google.com/site/asthmendr/le-mecanisme/fonctionnement-de-l-anticorps.*

37. **Doctreurclic, Antigène. [En ligne]. Disponible :https://www.docteurclic.com/encyclopedie/antigene.aspx.**

38. **Géraud Chancelin Hellow Tejiozem, Utilisation Des Produits Biologiques D'origine Equine En Thérapeutique Humaine, Thèse en vue de l'obtention du diplôme le grade de Docteur Vétérinaire, Ecole Inter - Etats Des Sciences Et Médecine Vétérinaires, Université.** *Https://Www.Memoireonline.Com/01/08/863/Utilisation-Produits-Biologiques-Origine-Equine-.*

39. **Katia Mayol, MICROBES, IMMUNITÉ ET VACCINATION, publié le 26/02/2014, mise à jour le 14/03/2018.2009. [En ligne]. Disponible :.** *http://acces.ens-lyon.fr/acces/thematiques/immunite-et-vaccination/thematiques/cellules-immunes-et- organes-lymphoides/fiches-organes-et-tissus-lymphoides/le-thymus.*

40. **Marion MATHIEU, Frédérique FORQUET, Dominique BLANC, MALADIES AUTO-IMMUNES [CLES DE COMPREHENSION],2009. [En ligne]. Disponible :.** *https://www.inserm.fr/sites/default/files/2017-10/Inserm_SKS_2009-2010-2011_AutoImmuniteMaladies_Dossier.pdf.*

41. **Mokhtar GHARBI, Optimisation grâce aux Systèmes Immunitaires Artificiels, Le 3 février 2006. [En ligne]. Disponible : https://docplayer.fr/1869644-Optimisation-grace-aux-systemes-immunitaires-artificiels.html.**

42. **Jacques Dewaele, Le Concept De Réseau Idiotypique Une Nouvelle Façon De Penser Le Système Immunitaire. [En ligne]. Disponible.** *http://documents.irevues.inist.fr/bitstream/handle/2042/9132/ASTER_1990_10_57.pdf;sequence=1.*

43. **Jugirault.free, Réponse primaire et réponse secondaire. [En Ligne]. Disponible.** *http://jugirault.free.fr/chapitre3,immuno/co/module 2.html?mode=html.*

44. **theory, De Castro .L.N & Von Zuben .F.J «Artificial Immune Systems: Part I - Basic.**

45. **Jerne. N. K «Towards a Network theory of the immune system », Ann. Immunol.**

46. **J. Kim « Integrating Artificial Immune Algorithms for Intrusion Detection », PhD.**

47. **ABERKANE Sabrina Amina Développement d'un système immunitaire artificiel pour le traitement des données médicales », mémoire en vue de l'obtention du diplôme d'Ingénierie des Systèmes d'Information, département de Mathématiques et d'Informatique, universi.** *http://e-biblio.univ-mosta.dz/bitstream/handle/123456789/9469/MINF123.pdf?sequence=1&isAllowed=y.*

48. **D. Dasgupta «Artificial Immune Systems and Their Application », Springer-Verglas,.**

49. **Rima Daoudi, Classification du cancer du sein par des approches basées sur les Systèmes Immunitaires Artificiels, thèse en vue de l'obtention du diplôme de Doctorat.**

50. **LOUATI Nour El-Houda, Réalisation d'un Système de Détection D'intrusion Basé Système immunitaire.**

51. **Lanutrition.fr (Publié le 01/12/2008 Mis à jour le 15/02/2017), Immunité innée et immunité adaptive. [En ligne]. Disponible :.** *https://www.lanutrition.fr/outils/glossaire/immunite-innee-et-immunite-adaptive.*

52. **Philippe Biondi, Architecture expérimentale pour la détection d‟intrusions dans un système informatique,2001.**

53. **Ridha GHAYOULA, Contribution à l‟Optimisation de la Synthèse des Antennes Intelligentes par les Réseaux de Neurones,2008].**

54. **YOUSSEF FATAICHA, RECHERCHE D'INFORMATION DANS LES IMAGES DE DOCUMENTS, MONTRÉAL, LE 27 DÉCEMBRE 2005.**

55. **Patrice Wira, Réseaux de neurones artificiels : Architecture et applications.**

56. **Cédric Michel, Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène, Université de Rennes 1,2003.**

57. **Claude Touzet, LES RESEAUX DE NEURONES ARTIFICIELS, INTRODUCTION AU CONNEXIONNISME, 2016.**

58. **theory, De Castro .L.N & Von Zuben .F.J «Artificial Immune Systems: Part I - Basic.**

59. **Jerne. N. K «Towards a Network theory of the immune system », Ann. Immunol.**