République algérienne démocratique et populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 20 Aout-1955-SKIKDA

Faculté des sciences

Département d'informatique

Mémoire de fin d'études en vue de l'obtention du diplôme

De master académique-Option : Réseau et Systèmes Distribués (RSD)

Thème

Un système immunitaire artificiel pour la détection des intrusions Dans un réseau local

Réalisé par :

- Alioua Miada
- Zouiti Amani

Encadré par

Mr.Benoudina lazher

Année Universitaire 2022-2023

Remerciement

Tous d'abord et avant tout, nous remercions Dieu Tout-Puissant de nous avoir donné la capacité et la patience de surmonter les difficultés de la vie et d'atteindre ces succès.

Deuxièmement, nous tenons à exprimer notre grande gratitude à notre encadreur M. Benoudina Lazhar, pour les orientations et les conseils qu'il nous a prodigués lors de son encadrement.

Nous remercions infiniment nos chers parents de nous avoir accordé confiance et encouragements et d'avoir fait de nous ce que nous sommes aujourd'hui, d'être le soutien constant vers lequel nous nous tournons.

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

Amani & Miada

Dédicace

Je tiens avant tout à remercier dieu le tout

puissant de nous avoir donné la force et la volonté pour achever ce modeste travail.

Je dédie ce présent mémoire

A l'homme qui m'a toujours encouragé, travaillé dur pour moi et soutenu : mon cher père Halim

A la femme qui a souffert sans me laisser souffrir et qui m'a encouragé tout au long de mon parcours universitaire : ma mère adorée Hassiba

A ma chère sœur et cher frère : Ahlem et Hocine , qui m'ont soutenu

A tous ceux qui m'ont aidé et soutenu pour réaliser ce travail de près ou de loin.

A tous ceux que j'aime. Merci.

Amani

Dédicaces

Je dédie ce modeste travail à l'homme que je porte son nom et je suis fière d'être sa fille, à celle qui a travaillé dur et lutté pour que j'arrive ici mon cher père Djamel.

A mon modèle dans la vie, à la plus grande femme que mes yeux aient jamais vue, à mon soutien et ma source de force, à la femme la plus belle et la plus tendre du monde, ma chère mère Monia.

Au plus beau cadeau que m'ont fait mes parents, mon cher frère Mouhamed et mes deux sœurs Meriem et Malake 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.

A tous les membres de la famille ALIOUA

A ma seule et meilleure amie Rania qui était parmi les personnes qui n'ont pas cessé de me soutenir durant cette période.

A tous ceux qui m'ont aidé et soutenu pour réaliser ce travail de près ou de loin.

A tous ceux que j'aime. Merci.

Miada

Résumé

L’informatique c’est un domaine vaste, ces points faible actuelle dans le système peut-être très importante, les attaques et menaces contre ces points et divers et à gros risques.

Pour protéger ces informations pendant leur transfert, il faut que ce système les préservent en appliquant certain mesures de protection de système d’informatique ce dernier à améliorer certain moyen de protection parmi eux « Le système de détections des intrus » ce méthode utile on l’utilise pour préserver le réseau et détecter toute activité non autorisée ou anormale.

Afin d'améliorer ces systèmes, ainsi que la précision de la détection, diverses méthodes ont été utilisées, telles que des systèmes immunitaires artificiels qui dépendent du système immunitaire humain capable de détecter des infiltrations connues et inconnues, qui évoluent rapidement.

Mots clés : l’informatique automatisée, réseau, système immunitaire artificiel, détection d'intrusion.

Abstract

Media automated is a vast domain, and the weaknesses in the system is important because the attacks against them can be variable and dangerous. For the protection of data during the transferring, the system must be secured.

In addition to ensure the application of the security policy for automated media it developed many security ways such as intrusion detection join , and it's an important way to protect and reveal all unallowed activities.

To improve these protective applications it depends on many ways such as artificial immune systems that depend on the human immune system that is able to detect previously known and unknown infiltration, which is rapidly evolving.

Key words: automated information, network, artificial immune system, intrusion detection.

ملخص

الإعلام الآلي هو مجال واسع، وعدد نقاط الضعف الحالية في النظام قد تكون مهمة وهكذا فإن الهجمات ضد هذه النقاط يمكن أن تكون متنوعة وخطيرة. لحماية البيانات أثناء الإرسال يجب أن يكون هذا النظام آمن. من أجل ضمان تطبيق السياسة الأمنية لأنظمة الإعلام الآلي طورت العديد من الوسائل الأمنية المتعددة من بينها أنظمة كشف التسلل، وهي وسيلة هامة تستخدم لحماية الشبكة والكشف عن أي نشاط غير مصرح به أو غير طبيعي.

من أجل تحسين هذه الأنظمة وكذا دقة الكشف تم الاعتماد على طرق مختلفة كأنظمة المناعة الاصطناعية التي تعتمد على جهاز المناعة البشرية القادرة على كشف التسلل المعروفة سابقا والغير معروفة والتي تتطور بسرعة.

الكلمات المفتاحية: الإعلام الآلي، الشبكة، نظام المناعة الاصطناعية، كشف التسلل.

Table de matière

Chapitre 02 : Les systèmes immunitaires artificiels

Chapitre 03 : Analyse et Conception

Chapitre 04 : Réalisation et Implémentation

Liste des figures

Liste des tableaux

Glossaire

IDS: Intrusion Detection Systems

HIDS: Host Intrusion Detection Systems

NIDS: Network Intrusion Detection Systems

SIN: Systèmes Immunitaires Naturels

SIA: Système Immunitaires Naturels

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

De nos jours, Le monde connaît des avancées très significatives dans le domaine informatique ; les besoins en matière de sécurité sont un peu plus impérieux, et la prédisposition n'est forcément pas à la baisse. Depuis quelques années déjà, on participe à un changement constant des techniques, qu'il s'agisse des techniques visant à sécuriser l'échange des données ou des techniques de mises au point pour contourner les systèmes sécurisés. D'où, la sécurité des données tend à s'améliorer. Et comme prône ce proverbe chinois : « l'art de la guerre est basé sur la tromperie », de même par analogie, la sécurité informatique doit représenter une stratégie qui éradique cette tromperie.

La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés.

Les systèmes de détection d'intrusions sont l'une de ces contre-mesures les plus efficaces. Leur rôle est de reconnaitre des intrusions ou des tentatives d'intrusions par des comportements anormaux des utilisateurs ou par la reconnaissance d'attaque à partir du flux des données du réseau. Différentes méthodes et approches ont été adoptées pour la conception de systèmes de détection d'intrusions. Parmi ces méthodes, l'une est inspirée de la nature, notamment des systèmes immunitaires, qui présentent des propriétés et une grande similarité avec les systèmes de détection d'intrusions.

Le système immunitaire biologique avec ses propriétés remarquables est une source d'inspiration pour la résolution de problèmes. L'étude des systèmes immunitaires est un nouvel axe de recherche très prometteur, qui a donné naissance à une nouvelle branche de l'intelligence artificielle, à savoir, les systèmes immunitaires artificiels. Ces derniers sont en fait la modélisation, l'implémentation et l'adaptation des concepts et méthodes des systèmes immunitaires biologiques pour la résolution de problèmes.

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. Vu que les intrusions sont générées non seulement par les membres externes mais aussi par ses membres internes, alors il est nécessaire d'améliorer les systèmes de détection

d'intrusions qui sont basés sur le modèle de soi et non soi afin de permettre la détection des éléments nuisibles et dangereux qui peuvent être de soi ou de non soi ce qui permet l'augmentation du taux vrai positif et la minimisation du taux vrai négatif. Ainsi, pour la réalisation de ce but, certains systèmes de détection d'intrusions proposés, exigent l'intervention continue de l'opérateur de sécurité après chaque détection dont le but principal est l'obtention d'un ensemble de détecteurs permettant la détection des intrusions réelles.

Le mémoire est organisé en quatre chapitres qui peuvent être résumés comme suit :

Le premier chapitre représente une introduction générale au domaine de la sécurité informatique d'une façon générale, aussi nous allons présenter les systèmes de détection d'intrusions (IDS), avec une classification générale des systèmes de détection d'intrusions selon plusieurs critères. Ainsi qu'une étude comparative entre certains types d'IDS sera présentée. Puisque cette étude se focalise sur l'approche comportementale, les différentes approches utilisées par cette approche seront exposées avec une vue d'ensemble sur les différentes architectures d'implémentation d'un IDS. La dernière section de ce chapitre sera consacrée à l'exposition de quelques systèmes de détection d'intrusions existants.

Le deuxième chapitre décrit les systèmes immunitaires artificiels (AIS). Afin de comprendre les différents algorithmes proposés dans le domaine des systèmes immunitaires artificiels, ce chapitre commence par une présentation générale du système immunitaire naturel et les différents mécanismes utilisés dans l'identification et la détection des intrus. La partie consacrée aux systèmes immunitaires artificiels expose les différents algorithmes immunitaires disponibles ainsi que les différents domaines d'application des systèmes immunitaires artificiels.

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

Chapitre 01 :

La sécurité informatique et les systèmes de détection des intrusions

Introduction

Les systèmes et les réseaux informatiques ne cessent de subir des attaques, de plus en plus ingénieuses et discrètes. Ces attaques peuvent même être d'une complexité technologique extrême, ce qui les rendent difficile à détecter de la part du système ciblé par les attaques, En conséquence l'amélioration des mécanismes de défense est une opération indispensable en fonction de l'émergence de nouvelles attaques. En effet les entreprises subissent des attaques qui peuvent entraîner des pertes conséquentes. Le besoin des entreprises en sécurité informatique est de plus en plus crucial, un élément essentiel d'une bonne politique de sécurité est l'utilisation des IDS. Un système de détection d'intrusions (IDS) est un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative [1].

I. La sécurité informatique

1. Définition

Ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service.

La sécurité informatique comporte trois aspects : la protection physique des installations, la protection des données contre la consultation, la modification ou la dégradation, effectuée de façon volontaire ou accidentelle par des personnes non autorisées, et la protection de la fiabilité de ces données (c'est-à-dire la conservation de leur contenu au fil du temps ou lors de leur traitement).

La sécurité informatique ne résulte pas d'une accumulation de moyens, mais est plutôt associée à une démarche méthodique d'analyse et de réduction des risques. Ainsi, de nombreuses techniques sont mises en œuvre pour réduire la vulnérabilité vis-à-vis des risques informatiques, elles concernent notamment l'organisation de l'entreprise, le contrôle des accès aux systèmes d'information, la protection des télécommunications, le plan de secours, les consignes de sécurité, la qualité des logiciels, les sauvegardes, le chiffrement, etc [2].

2. Services et mécanismes de sécurité

De façon générale, les mécanismes de sécurité permettent de mettre en œuvre des services de sécurité. Ces services peuvent être la confidentialité (des données ou du flux de données), l'authentification (d'une entité ou de l'origine des données), le contrôle d'accès, l'intégrité ou encore la non répudiation (avec preuve de l'origine ou preuve de la remise). Les mécanismes peuvent être le chiffrement, l'authentification, l'intégrité, la signature numérique, et d'autres encore [3].

2.1. Les services de sécurité

Les principaux besoins de sécurité que peut avoir l'émetteur d'un message sont les suivants :

- E1 : le message ne doit être connu que de son destinataire,
- E2 : le message doit parvenir au bon destinataire,
- E3 : le message reçu doit être identique au message émis,
- E4 : le destinataire ne doit pas pouvoir nier avoir reçu le message.

Et les besoins du destinataire peuvent être :

- D1 : le message ne doit être connu que de lui (et de l'émetteur),
- D2 : l'émetteur du message doit être connu avec certitude,
- D3 : le message reçu doit être identique au message émis,
- D4 : l'émetteur ne doit pas pouvoir nier avoir émis le message.

Les besoins E1 et D1 sont identiques. Ils sont satisfaits par la mise en œuvre d'un service de confidentialité, définie dans la norme 7498-2 comme la "propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés".

Les besoins E2 et D2 sont symétriques. Chaque entité doit s'assurer de l'identité de l'autre, ce qui implique de mettre en œuvre un service d'authentification, défini comme la "confirmation qu'une entité homologue d'une association est bien l'entité déclarée", et même dans le cas du destinataire, un service d'authentification de l'origine des données, ou "confirmation que la source des données est telle que déclarée".

Les besoins E3 et D3 sont identiques. L'égalité entre le message émis et le message transmis est assurée par un service d'intégrité (des données), qui est la "propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée".

Enfin, les besoins E4 et D4 sont symétriques. Le service correspondant est la non répudiation, qui empêche la répudiation, c'est-à-dire "le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie". Dans un cas il s'agira de non répudiation avec preuve de l'origine, dans l'autre de non répudiation avec preuve de la remise.

A tout cela s'ajoute le service de contrôle d'accès, ou "précaution prise contre l'utilisation non autorisée d'une ressource", et qui peut s'appliquer à divers types d'accès (utilisation de ressources de communication, lecture, écriture ou suppression d'une ressource d'information, exécution d'une ressource de traitement).

Parfois, la simple observation du flux de données fournit de l'information à un ennemi. C'est ce qu'on appelle l'analyse de trafic, qui permet de détecter la présence, l'absence, la quantité, la direction, ou la fréquence de telles ou telles données, qu'elles soient compréhensibles ou non. On peut alors renforcer la confidentialité des données en assurant également la confidentialité du flux de données, c'est-à-dire un "service de confidentialité fournissant une protection contre l'analyse de trafic". La confidentialité, tout comme l'intégrité, peut être sélective par champ, c'est-à-dire ne s'appliquer qu'à une partie des champs contenus dans le message transmis [3].

2.2. Les mécanismes de sécurité

Les différents services de sécurité décrits précédemment sont mis en œuvre grâce à des mécanismes, dont la plupart sont de nature cryptographique. La cryptographie est la "discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée" [3].

Afin d'assurer la confidentialité des données et/ou du flux de données, on fait appel à un mécanisme de chiffrement, qui est la "transformation cryptographique de données produisant un cryptogramme", unité de données dont "le contenu sémantique n'est pas compréhensible".

L'opération inverse du chiffrement est le déchiffrement. Lorsqu'il est effectué de bout en bout, le chiffrement a lieu "à l'intérieur ou au niveau du système extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination".

S'il n'est effectué qu'à chaque liaison du système (dans quel cas les données sont en clair à l'intérieur des entités relais), il s'agit de chiffrement de liaison. La confidentialité du flux de données exige en outre un mécanisme de bourrage de trafic, consistant à produire des "instances de communications parasites, des unités de données parasites et/ou des données parasites dans des unités de données". Cet échange continu de données, transportant ou non de l'information, permet d'éviter qu'un tiers ne sache quand deux entités sont entrées en communication.

Le service d'authentification (d'entité homologue) est fourni par un mécanisme d'échange d'authentification, "destiné à garantir l'identité d'une entité par échange d'informations". (Typiquement, cet échange est constitué d'un nombre choisi au hasard envoyé par l'entité qui souhaite authentifier l'autre, et d'une réponse de cette dernière obtenue en appliquant un mécanisme cryptographique à ce nombre et à un secret connu d'elle seule). L'authentification de l'origine des données peut être obtenue grâce à un mécanisme de signature numérique. Il s'agit de "données ajoutées à une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)". Le même terme désigne aussi la transformation cryptographique qui produit ces données. Pour produire une signature, il faut une information privée, c'est-à-dire connue du seul signataire. Pour la vérifier, il suffit d'une information publique. Il doit cependant être matériellement impossible de déduire l'information privée de l'information publique correspondante.

L'intégrité des données est assurée par un mécanisme du même nom. Un tel mécanisme peut consister à produire une valeur de contrôle cryptographique, à partir des données à protéger et d'un secret partagé par les entités en communication. Dans ce cas, la vérification par le destinataire consiste à recalculer cette valeur et à la comparer avec celle reçue. Si elles sont égales, il y a présomption d'intégrité. Mais on peut également utiliser un mécanisme de signature numérique qui, en plus de l'origine des données, garantit également leur intégrité. Par ailleurs, il peut être nécessaire de recourir en outre à des mécanismes visant à éviter le rejoue (répétition frauduleuse de tout ou partie des données), tels que la numérotation, l'horodatage ou le chaînage cryptographique des données.

Pour obtenir le non répudiation avec preuve de l'origine, on peut utiliser un mécanisme de signature numérique. En effet, la caractéristique essentielle de ce mécanisme est que la signature ne peut être produite qu'en utilisant l'information privée du signataire. On peut donc, en vérifiant la signature, prouver à tout moment à une tierce partie (par exemple un

juge ou un arbitre) que seul le détenteur unique de l'information privée peut avoir produit la signature. Il est cependant possible d'utiliser aussi des mécanismes de chiffrement ou d'intégrité.

La non répudiation avec preuve de la remise peut aussi reposer sur un mécanisme de signature, produite cette fois par le destinataire du message. Les deux services de non répudiation, et plus particulièrement le second, peuvent aussi faire appel à un mécanisme de notariat. Ce mécanisme .

met en jeu une tierce partie, appelée notaire, qui garantit certaines propriétés relatives à des données communiquées entre deux ou plusieurs entités, telles que leur intégrité, leur origine, l'heure d'émission, etc. Le notaire s'interpose alors entre les entités communicantes.

Les mécanismes de contrôle d'accès peuvent utiliser des éléments variés tels que l'identité authentifiée de l'entité, une information sur cette entité, une liste de droits d'accès, des "étiquettes" de sécurité spécifiant des niveaux de sensibilité, etc. La politique de contrôle d'accès choisie peut être de type discrétionnaire (l'utilisateur définit les droits d'accès aux informations dont il a la responsabilité) ou de type par mandat (l'autorisation d'accès dépend des droits du demandeur, du niveau de sensibilité des informations et d'attributs spécifiques).

Le contrôle de routage permet d'acheminer l'information à travers des sous réseaux, liaisons ou relais considérés comme sûrs. Il peut, soit spécifier explicitement les chemins autorisés, soit tenir compte du niveau de sensibilité des informations dans le choix des chemins utilisés.

3. Quelques possibilités en matière de sécurité réseau

Actuellement, toute une série d'outils et de techniques permettent à un administrateur de sécuriser facilement son réseau et les machines qui le composent. Chacune de ces techniques se base sur des principes fondamentalement différents, mais celles-ci ont un but commun : permettre une connexion entre Internet (réseau non sécurisé) et le réseau de l'entreprise concernée, en assurant la sécurité des équipements et des informations disponibles sur ce réseau, tout en tenant compte des contraintes de plus en plus présentes, telles que les interconnexions de réseaux, les besoins de « contacts électroniques » pour le personnel (mails, transferts de fichiers, accès Web, etc.), les systèmes d'informations complexes, et autres [4].

Nous allons citer et expliquer brièvement quelques outils de sécurité courants, pour nous permettre par la suite de distinguer entre les systèmes de détection d'intrusions (IDS), l'objectif de cette thèse, et les Firewalls, à cause de la confusion qui peut exister entre eux.

3.1. Les Firewalls

Le mot Firewall (Pare-feu) signifie qu'on instaure une série de protections en un point particulier entre deux entités connectées, en l'occurrence entre Internet et le réseau interne d'une entreprise. En pratique, le Firewall consiste en une architecture, plutôt qu'un matériel ou un logiciel précis. Cette architecture intègre alors une série de composants matériels et logiciels, qui tentent précisément d'assurer le niveau de sécurité requis [5].

L'architecture la plus utilisée actuellement est basée sur une « Zone démilitarisée», communément appelée DMZ (Demilitarized Zone). Elle consiste à placer un réseau intermédiaire entre l'accès Internet et le réseau interne (éventuellement plusieurs). Cette DMZ sera isolée, aussi bien vis-à-vis de l'Internet que du réseau local, par des systèmes de filtrage (filtres de paquets entrant et sortant). Ensuite, les éventuels serveurs nécessaires à l'entreprise devant continuer à être accessibles de l'extérieur seront connectés directement sur cette DMZ, de manière à les séparer du réseau interne. Par exemple, on pourra y trouver un serveur Web, un serveur DNS (Domain Name Service), un serveur de mails, un serveur FTP (File Transfer Protocol), etc. Dans le cas où l'un de ces serveurs serait compromis, le filtrage entre la DMZ et le réseau interne doit être capable d'assurer une protection suffisante au réseau interne.

Bien évidemment, cette architecture doit être adaptée plus précisément à la structure d'une entreprise précise, et éventuellement intégrer des composants supplémentaires, tels que des Proxys (machine intermédiaire entre les ordinateurs d'un réseau local et le Web) et autres dispositifs.

3.2. Les filtres de paquets

Un filtre de paquet, tout comme son nom l'indique, permet de filtrer les paquets circulant sur un réseau. Plus précisément, on peut même dire que le filtrage s'effectue sur les paquets traversant une interface réseau. Celui-ci fonctionne en analysant le contenu de ces paquets, principalement en observant les valeurs de certains champs des en-têtes des protocoles IP (Internet Protocol), ICMP (Internet Control Message Protocol), UDP (User Datagramme Protocol) et TCP (Transmission Control Protocol). Cela permet par exemple d'interdire des paquets provenant d'une source précise, étant destinés à une destination précise, des paquets

réceptionnés sur une interface précise, des paquets avec des ports sources ou cibles précis, d'intégrer des contraintes d'heures éventuelles d'après l'horaire d'une entreprise, etc [5].

Au niveau de la configuration, on fait établir une série de règles de filtrage qui reflète la politique de sécurité de l'entreprise. Les paquets ne satisfaisant pas aux règles de filtrage seront alors bloqués (supprimés), et peuvent entraîner éventuellement la génération d'un message d'erreur (via un protocole comme ICMP).

3.3. Les scanners et les outils relatifs à la sécurité

Etant donné que les hackers (pirates informatique) trouvent de plus en plus les outils nécessaires à la réalisation de leurs attaques, les entreprises travaillant dans le domaine de la sécurité ont petit à petit.

Commencé à proposer leurs propres outils de vérification de vulnérabilités. C'est ainsi qu'on commence à avoir apparaître toute une série de scanners, qui offrent de nombreuses possibilités. Il est primordial à l'heure actuelle d'effectuer de nombreux tests de sécurité réguliers, car ces tests permettent de mettre en avance des modifications dans l'architecture et dans la configuration du réseau et des machines qui le composent. Ces outils sont décomposés en toute une série de catégories, dont notamment : [5]

- Les scanners de vulnérabilités.
- Les scanners orientés réseaux.
- Les scanners orientés hosts (machines).
- Les sniffers.
- Les vérificateurs de mots de passe.

3.4. Les systèmes de détection d'intrusion

Un IDS a pour fonction d'analyser en temps réel ou différé les évènements en provenance des différents systèmes à travers le réseau, de détecter et de prévenir les attaques. Les IDS ont donc un rôle d'alarme (la comparaison avec une alarme anti-vol placée dans le hall d'une maison, qui détecte des mouvements ou des ouvertures de portes, correspond d'ailleurs assez bien). Les buts sont nombreux :

- Collecter des informations sur les intrusions.
- Gestion centralisée des alertes.
- Effectuer un premier diagnostic sur la nature de l'attaque permettant une réponse rapide et efficace.

- Réagir activement à l'attaque pour la ralentir ou la stopper.

4. 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) [6]

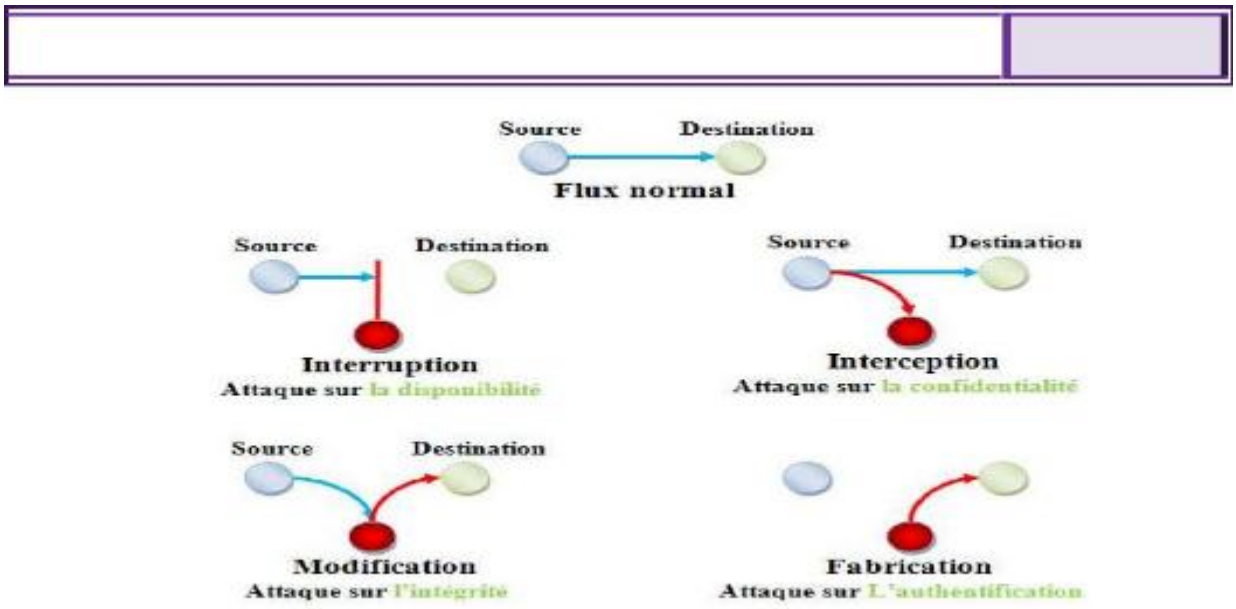

Figure 01 : Buts des attaques informatiques [7].

5. 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 :

5.1. 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).

5.2. 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.

5.3. 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**.**

6. Exemples d'attaques

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.

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

6.5. 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.

6.6. 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).

6.7. 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.

6.8. 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.

6.9. 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 ou un virus.

6.10. 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 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) [8].

II. Les systèmes de détection d'intrusion :

1. Définition

1.1. Détection d'intrusion

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].

1.2. Le système 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 [10].

2. Efficacité des systèmes détection d'intrusion :

Philip définit trois critères pour évaluer l'efficacité des systèmes de détection d'intrusion:

- **L'exactitude (accuracy) :** on parle de l'exactitude quand le système de détection d'intrusion déclare comme malicieux une activité légale. Ce critère correspond au faux positif.
- **La performance (performance) :** la performance de système de détection d'intrusion est le taux de traitement des évènements. Si ce taux est faible, la détection en temps réel est donc impossible.
- **La complétude (completeness) :** on parle de la complétude quand le système de détection d'intrusion rate la détection d'une attaque. Ce critère est le plus difficile, parce qu'il est impossible d'avoir une connaissance globale sur les attaques. Ce critère correspond au vrai négatif [11].

Debar a rajouté également les deux critères suivants :

- **La tolérance aux fautes (Fault tolérance) :** le système de détection d'intrusion doit lui-même résisté aux attaques, particulièrement au déni de service. Ceci est important, parce que plusieurs systèmes de détection d'intrusion s'exécutent sur des matériels ou logiciels connus comme vulnérables aux attaques.

- **La réaction à temps (Timeliness) :** le système de détection d'intrusion doit s'exécuter et propager les résultats de l'analyse le plus tôt possible, pour permettre à l'officier de sécurité de réagir avant que des graves dommages n'aient lieu. Ceci implique plus qu'un calcul de performance, parce qu'il ne s'agit pas seulement de temps de traitement des évènements, mais aussi le temps nécessaire pour la propagation et la réaction à cet évènement [12].

3. Que doit assurer la détection d'intrusion :

La détection d'intrusion permet aux organisations de protéger leurs systèmes contre les menaces qui ne cessent de croître à cause de l'augmentation de la connectivité du réseau public (Internet), et la confiance accordée aux systèmes informatiques qui comportent des bugs [13].

La question pour les professionnels de sécurité ne devraient pas être s'il faut utiliser la détection d'intrusion, mais quels dispositifs utiliser et quelles sont leur capacité de détection d'intrusion.

Les systèmes de détection d'intrusion ont gagné l'acceptation d'être un élément nécessaire dans l'infrastructure de la sécurité informatique de chaque organisation. En effet, il y a plusieurs raisons pour acquérir et utiliser les systèmes de détection d'intrusion :

- ✓ Pour détecter les attaques et autres violations de sécurité qui ne sont pas empêchées par d'autres outils de sécurité.
- ✓ Pour documenter les menaces existantes dans une organisation, c'est-à-dire découvrir les vulnérabilités avant qu'elles ne soient exploitées par un attaquant.
- ✓ Pour agir en tant que contrôle de qualité pour la conception de sécurité, particulièrement dans les grandes et complexes entreprises.
- ✓ Pour fournir des informations utiles au sujet des intrusions qui ont eu lieu, et faire des diagnostics, recouvrement, et corrections des facteurs causatifs.
- ✓ Pour arrêter les intrusions afin de limiter les dégâts. Malheureusement cela n'est pas toujours possible à cause de la complexité et la diversité des intrusions, et la naissance de nouveaux types d'intrusions liées au développement des nouvelles technologies d'information. Les contre-mesures actives sont souvent optionnelles dans la quasi-totalité des systèmes de détection d'intrusion.

4. Le modèle de processus de la détection d'intrusion :

La majorité des systèmes de détection d'intrusion peuvent être décrits en termes de trois composants fonctionnels fondamentaux [14] :

- **La source d'informations (sonde) :** Les différentes sources des évènements utilisées pour déterminer les intrusions qui ont eu lieu. Ces sources peuvent être fournies par les différents niveaux du système d'information : les réseaux, les hôtes, et les applications.
- **L'analyse :** La partie du système de détection d'intrusions qui réellement organise et donne un sens aux évènements dérivés des sources d'informations, décidant quand ces évènements indiquent que des intrusions se produisent ou ont déjà eu lieu. Les principales approches communes d'analyse sont : détection d'abus (The misuse detection) ou encore dite approche par scénarios et détection d'anomalie (Anomaly detection) ou encore dite approche comportementale qui seront expliquées par la suite.
- **La réponse :** L'ensemble de contre-mesures que le système prend une fois qu'il détecte des intrusions. Celles-ci sont typiquement groupées dans des mesures actives et passives, les mesures actives comportent une certaine interposition automatisée de la part du système, alors que les mesures passive rapportent des résultats issus de l'analyse aux responsables, qui sont alors prévenus pour agir et prendre une action basée sur ces rapports.

5. Classification des systèmes de détection d'intrusion :

Le domaine de la détection d'intrusions est encore jeune mais en plein développement. Nous dénombrons à l'heure actuelle environ une centaine de systèmes de détection d'intrusions, que ce soit des produits commerciaux ou du domaine public [4]. Il est donc devenu très utile d'utiliser des critères pour classifier ces systèmes de détection d'intrusion, c'est ce que nous allons présenter dans cette section.

5.1. Selon la méthode de détection

La détection d'intrusions repose sur deux approches de base :

- ✓ L'approche comportementale.
- ✓ L'approche basée connaissance.

5.1.1. L'approche comportementale

Cette approche est connue aussi par l'approche de détection d'anomalies. Elle consiste à définir un profil de l'activité normale d'un utilisateur et à considérer les déviations significatives de l'activité d'utilisateur courante par rapport aux profils de comportement normaux comme anomalie.

5.1.2. L'approche basée connaissance

Cette approche définit des signatures soupçonneuses basées sur les vulnérabilités connues de système et la politique de sécurité. Une intrusion est signalée lorsque la trace d'une attaque connue est présente dans les traces d'audit.

Ces deux méthodes d'analyse constituent la partie importante des systèmes de détection d'intrusions.

5.2. Selon le type de réponse

Le comportement d'un IDS après la détection d'une intrusion est l'ensemble des actions prises par le système lorsqu'il détecte une attaque. Ces réponses peuvent être actives ou bien passives.

5.2.1. Réponse active

La réponse active implique des actions automatisées prises par un IDS quand le système détecte une intrusion. Par exemple interrompre le progrès d'une attaque pour bloquer ensuite l'accès suivant de l'attaquant.

5.2.2. Réponse passive

Dans ce cas, quand une attaque est détectée, le système de détection d'intrusions ne prend aucune action. Il génère seulement une alarme pour notifier l'administrateur de système qui va prendre des mesures en se basant sur les rapports générés par le système de détection d'intrusions.

5.3. Selon la nature des données analysées

Les systèmes de détection d'intrusions sont classés en fonction de l'origine des données qui seront exploitées pour détecter des actions intrusives. La source de données utilisée est une caractéristique essentielle pour classer les systèmes de détection d'intrusions. On distingue trois catégories de sources d'informations :

- ✓ Les audits systèmes.
- ✓ Les sources d'information réseau.
- ✓ Les audits applicatifs.

5.3.1. Les audits systèmes

Les audits systèmes sont produits par le système d'exploitation d'un hôte. Ces données permettent à un IDS de contrôler les activités d'un utilisateur sur un hôte. Elles peuvent être également de plusieurs types, par exemple :

- **Historique des commandes systèmes :** tous les systèmes d'exploitation possèdent des commandes pour obtenir des informations instantanées sur les processus actifs courants dans un ordinateur. Grâce à ces commandes, l'IDS peut avoir des informations précises sur les événements système.
- **Accounting :** l'accounting fournit des informations sur l'usage des ressources partagées par les utilisateurs. Ces ressources sont par exemple : le temps processeur, la mémoire, L'espace disque, les applications lancées, etc.
- **Systèmes d'audit de sécurité :** les systèmes d'exploitation sont dotés par ce service pour définir des événements, les associer à des utilisateurs et assurer leurs collectes dans un fichier d'audit. L'IDS possède potentiellement des informations sur toutes les actions effectuées par un utilisateur.

L'avantage de ces données systèmes réside dans leur fiabilité et leur granularité fine, qui permettent un diagnostic précis des actions effectuées sur un hôte par un attaquant. Cependant, le volume d'événements généré par les audits systèmes est très volumineux ce qui implique un impact très important sur les performances de la machine surveillée. Les IDS qui se basent sur cette catégorie des sources de données sont appelés : Les IDS basés hôte « Host Based Intrusion Detection System ».

5.3.2. Les sources d'information réseau

Ce sont des données du trafic réseau. Cette source d'informations est prometteuse car elle permet de collecter et analyser les paquets de données circulant sur le réseau. Les IDS qui exploitent ces sources de données sont appelés : Les IDS basés réseau « Network Based Intrusion Detection System ».

5.3.3. Les audits applicatifs

La troisième catégorie de source de données est constituée des audits applicatifs. Les données à analyser sont produites directement par une application, par exemple des fichiers logs générés par les serveurs ftp et les serveurs Web. L'avantage de cette catégorie est que les données produites sont très synthétiques, elles sont sémantiquement riches et leur volume est modéré. On note que ces types d'informations sont généralement intégrés dans les IDS basés

hôte. Vu de l'importance des IDS basés hôte et basés réseau, une étude détaillée de ces deux types d'IDS sera exhibée dans les prochaines sections.

5.4. Selon la fréquence d'utilisation

La fréquence d'utilisation d'un système de détection d'intrusions peut exister selon deux formes :

5.4.1. Surveillance périodique

Ce type de système de détection d'intrusions analyse périodiquement les différentes sources de données à la recherche d'une éventuelle intrusion ou une anomalie passée.

5.4.2. Surveillance en temps réel

Les systèmes de détection d'intrusions en temps réel fonctionnent sur le traitement et l'analyse continue des informations produites par les différentes sources de données. La détection d'intrusions en temps réel permet de limiter les dégâts produits par une attaque car elle permet de prendre des mesures qui réduisent le progrès de l'attaque détectée.

5.5. Selon l'emplacement

5.5.1. Les systèmes de détection d'intrusion basé hôte « 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 [15]. 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 [10].

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 possédantes des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS. Voici quelques HIDS connus: Tripwire, WATCH, Dragon Squire, Tiger,Security Manager… [16].

5.5.2. Les systèmes de détection d'intrusion basé réseau « NIDS »

Un N-IDS« Network-Based Intrusion Detection System » nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs lien(s) réseau dans le but de découvrir si un acte malveillant ou anormal a lieu. Le N-IDS place une ou plusieurs cartes d'interface réseau du système dédié en mode promiscuité (promiscuous

mode), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP. Elles n'ont pas non plus de pile de protocole attachée. Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau et en particulier de placer une sonde à l'extérieur du réseau afin d'étudier les tentatives d'attaques ainsi qu'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu ou bien menée depuis l'intérieur. Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Les NIDS étant les IDS plus intéressants et les plus utiles du fait de l'omniprésence des réseaux dans notre vie quotidienne, ce document se concentrera essentiellement sur ce type d'IDS [17].

5.5.3. Les systèmes de détection d'intrusion 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 let des machines ce qui augmente la complexité du système mais les avantages des NIDS et des HIDS sont combinés [18].

5.5.4. Les systèmes de détection d'intrusion immunitaire

Le système immunitaire constitue un intérêt croissant des recherches vu de sa capacité de traitement des informations. En particulier, il assure des calculs d'une manière distribuée et parallèle. Il peut apprendre des nouvelles informations et identifier les différents modèles d'une manière décentralisée. Il détecte et répond aux envahisseurs étrangers d'une façon distribuée. L'approche immunologique est une solution prometteuse pour la détection d'anomalies vue l'analogie puissante qui existe entre l'objectif du système immunitaire humain et celui du système de détection d'intrusions ainsi que la capacité du système immunitaire humain à protéger le corps contre les intrus. Ce système présente un intérêt croissant des différents travaux existants pour exploiter ces méthodes d'identification et de détection dans des systèmes de détection d'intrusions [13].

Pour cette raison, dans ce travail nous nous intéresserons par ce domaine de recherche.

6. l'architecture d'implémentation des IDS

L'architecture d'implémentation d'un système de détection d'intrusions qui est considérée comme une stratégie de contrôle décrit la manière de contrôle effectuée par les éléments d'un système de détection d'intrusions. Nous distinguons trois approches d'implémentation [19]: Monolithique, hiérarchique et coopérative.

6.1. L'approche monolithique (centralisée) :

Les premières mises en œuvre des systèmes

de détection d'intrusions ont employé une architecture monolithique sous laquelle les données rassemblées seront analysées à un point central. Puisque le contrôle de l'activité des utilisateurs d'un seul hôte ne révèle pas les attaques impliquant des hôtes multiples. L'IDS basé réseau a été développé, qui analyse le trafic de réseau pour déduire les anomalies venant du réseau.

Bien qu'un IDS basé réseau avec un serveur central a montré des résultats prometteurs pour des réseaux à petite échelle. Cependant, cette approche ne peut pas supporter un grand réseau à cause de la quantité énorme des données des différents hôtes qui doivent être analysée par le serveur central, ce qui engendre une dégradation sévère des performances de réseau. Un exemple d'un système de détection d'intrusions qui se base sur l'approche monolithique est le système NADIR [20].

6.2. L'approche hiérarchique :

Cette approche a été proposée pour surmonter les problèmes de l'approche monolithique. Elle est caractérisée par l'existence des secteurs de contrôle hiérarchiques. Chaque IDS contrôle un secteur avec l'élimination du transfert des données d'audit rassemblées par les hôtes locaux à un point central. Chaque IDS à n'importe quel niveau de contrôle exécute une analyse locale et envoie ses résultats d'analyse au niveau suivant dans la hiérarchie. L'approche hiérarchique montre la meilleure incrémentabilité « scalability » en permettant des analyses locales aux secteurs de contrôle distribués. Cependant, les problèmes vus précédemment demeurent toujours. En plus, le changement de la topologie du réseau cause un changement aussi bien dans la hiérarchie de réseau et dans les mécanismes de rassemblement des rapports d'analyse locaux. Ainsi, la difficulté de détecter les attaques qui visent le niveau le plus haut de la hiérarchie. Un exemple de système de détection d'intrusions hiérarchique : GrIDS, EMERALD [21].

6.3. L'approche coopérative (distribuée) :

Cette approche a été suggérée pour résoudre les problèmes de l'approche précédente. Elle essaye de distribuer les responsabilités d'un serveur central à un nombre de systèmes de détection d'intrusions coopératifs. La différence de cette approche avec l'approche hiérarchique est qu'il n'y a aucune hiérarchie entre les IDS distribués ce qui signifie que l'échec de n'importe quel IDS n'empêche pas la détection d'attaques coordonnées [22]. Parmi les systèmes de détection d'intrusions coopératifs nous pouvons citer par exemple le système CSM et le système AAFID.

7. Emplacement de l'IDS

Le choix de l'IDS est très influencé par son éventuel emplacement au sein du réseau. En effet, la topologie réseau impose quelques règles à respecter si on veut l'IDS soit efficace. L'emplacement de l'IDS doit également tenir compte du type d'intrusions à détecter (internes, externes, les deux). Si dans un réseau, il existe un seul point de connexion à internet, le meilleur emplacement de l'IDS est qu'il soit juste après le routeur. Si dans un autre réseau, différents points de connexions à internet existent, un IDS est placé pour chaque point de connexion comme nous pouvons le voir dans la Figure 1. Par contre pour détecter les intrusions internes un IDS doit être placé à chaque segment du réseau [13].

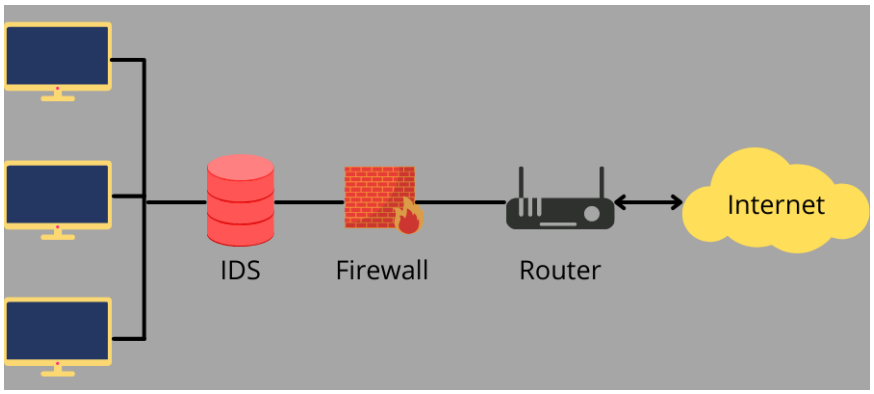

Figure 02 : Emplacement de l'IDS au sein d'un réseau.

8. Évaluation de l'IDS

Des mesures permettent de comparer et de mesurer l'efficacité des IDS. Les IDS sont des éléments très importants dans une stratégie de sécurité, pour cela le choix de l'IDS est très décisif et doit être basé sur les caractéristiques de ce dernier, les tâches qu'il devra accomplir, son emplacement …etc. mais également selon des mesures qui permettent d'évaluer son

efficacité. La technique la plus utilisée pour évaluer un IDS est le scanner de vulnérabilités. Cependant, ce dernier reste peu fiable.

Les mesures permettant de mieux choisir son IDS et mesurer son efficacité sont :

- Qualité des informations fournies par l'IDS : le taux de faut positif.
- Réponse de l'IDS dans un environnement surchargé.
- La possibilité de mettre à jour la base des signatures ou de modifier certaines signatures.
- La séparabilité des fonctions d'administration (architecture distribuée) …etc.

Les IDS à leurs tours peuvent faire l'objet d'attaques et certaines de leurs faiblesses sont liées au système d'exploitation (saturation de la mémoire ou de la carte réseau) [13].

9. Quelques systèmes de détection d'intrusions existants :

9.1. AAFID :

Le système AAFID (Autonomous Agent for Intrusion Detection) a été proposé par (Balasubramaniyan, Garcia-Fernandez, Isacoff, Spafford, & Zamboni, 1998) à l'université de Purdue. C'est une approche de détection d'intrusions multicouche avec des agents stationnaires et autonomes organisés sous forme d'une architecture hiérarchique. Chaque couche de la hiérarchie s'occupe de la détection des attaques spécifiques [23].

9.2. CSM :

(Cooperating Security Manager) est un système de détection d'intrusions qui peut être utilisé dans un environnement de réseau distribué. Son principal objectif est de détecter les activités intrusives de façon non centralisée car utiliser un directeur central qui coordonnerait toutes les activités limiterait la taille du réseau « le problème d'incrémentabilité ». Pour cela, CSM doit s'exécuter sur chaque hôte connecté au réseau. Ainsi, au lieu de reporter les activités anormales à un directeur central, les CSM communiquent entre eux pour détecter d'une manière coopérative les intrusions réseaux. Les composants principaux de ce système de détection d'intrusions sont [24] :

- Un système de détection d'intrusions local (IDS) ;
- Un gestionnaire de sécurité ;
- Un gestionnaire d'intrus.

9.3. GrIDS :

(Graph-Based Intrusion Detection System) a été conçu pour détecter des attaques à grande échelle. GrIDS considère les réseaux larges comme une agrégation de sous réseaux. Les données concernant l'activité des hôtes et le trafic réseau entre ces hôtes sont rassemblées dans des graphes d'activité qui révèlent la structure causale de l'activité réseau [25].

9.4. NIDES :

(Next- Generation IDES) est une version améliorée du système de détection d'intrusions IDES. Il assure la détection d'intrusions sur plusieurs hôtes (distribuées) en se basant toujours sur les données d'audit. Il n'y a aucune analyse du trafic réseau. Il utilise les mêmes algorithmes qu'IDES [24].

9.5. NADIR :

(Network Anomaly Detection and Intrusion Reporter) est un système expert qui a été conçu pour le réseau ICN (Integrated Computing Network) du Laboratoire National Los Alamos. Son but est d'analyser les activités réseaux des utilisateurs et d 'ICN en se basant sur les règles du système expert qui définissent la politique de sécurité et les comportements suspects. L'inconvénient majeur de ce système est qu'il ne peut être porté sur d'autres réseaux, étant donné que les protocoles réseaux d'ICN ne sont pas standards [24].

Conclusion :

Les réseaux constituent la plateforme de toutes les activités quotidiennes du monde entier, cette technologie présente des vulnérabilités qui peuvent causés plusieurs types d'attaques touchant à l'un des services de sécurité comme la confidentialité, l'intégrité des données, la disponibilité.

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.

Le chapitre suivant sera consacré à étudier les systèmes immunitaires artificiels. Cette approche s'inspirant du mécanisme de défense humain, présente des capacités intéressantes d'apprentissage, d'adaptation et d'évolution pour détecter les anomalies présentes dans les réseaux informatiques.

Chapitre 02 :

Les systèmes immunitaires artificiels

Introduction

Ces dernières années, la biologie est devenue une source d'inspiration pour résoudre certains problèmes informatiques complexes, basés sur l'extraction de métaphores utiles des systèmes biologiques. Les développements les plus notables étaient les réseaux neuronaux inspirés par la façon dont le cerveau fonctionne, et les algorithmes évolutifs inspirés par la théorie de l'évolution darwinienne.

Le système immunitaire a suscité un intérêt considérable pour son utilisation comme métaphore de l'inspiration. Ce domaine de recherche est connu sous le nom de systèmes immunitaires artificiels. Il s'agit d'un modèle moderne qui tente de saisir les propriétés des systèmes immunitaires naturels, comme la conservation et l'apprentissage, les compétences en adaptation et la détection des intrusions.

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. Tandis que la deuxième partie sera consacrée à la description du système immunitaire artificiel (AIS) en définissant le processus de conception d'un AIS. Ainsi, nous intéresserons à présenter les différents théories et algorithmes immunitaires.

I. Les systèmes immunitaires naturel « SIN »

1. Introduction

Le corps humain est un ensemble de systèmes complexes et très divers, chacun accomplissent une tâche ou une fonction spécifique. Le corps humain est constamment exposé à des micro-organismes pathogènes et /ou des substances nocives dans l'environnement. C'est pourquoi le système immunitaire agit comme une défense contre ces envahisseurs. La capacité du corps à se défendre est appelée résistance et dépend de nombreux mécanismes. Notre étude portera davantage sur le système immunitaire humain, les concepts de base des systèmes immunitaires naturels et leur fonctionnement.

2. Le système immunitaire

Le système immunitaire est une collection de cellules, des molécules et des organes. Il représente un mécanisme d'identification capable de percevoir et de combattre le

dysfonctionnement de ses propres cellules et les micro-organismes exogènes infectieux qui envahissent le corps [26].

3. Le système immunitaire naturel

Le système immunitaire naturel (système immunitaire naturel NIS) est un groupe d'organes, de tissus, de cellules et de molécules qui assurent l'immunité de l'organisme. Les interactions complexes entre les entités à tous les niveaux conduisent à un système complexe capable de protéger notre corps de toute entité dangereuse appelée antigène. Les éléments de base des SIN sont les globules blancs ou lymphocytes. Pour pouvoir identifier les autres molécules, des lymphocytes particuliers appelés cellules B produisent des récepteurs appelés anticorps [27].

4. L'architecture du système immunitaire

La défense de l'organisme contre le milieu extérieur comporte une immunité dite innée ou naturelle. En absence de tout contact avec un antigène, cette immunité dite adaptative ou acquise, c'est-à-dire apparaissant après contact de l'organisme avec des molécules étrangères qui sont des antigènes.

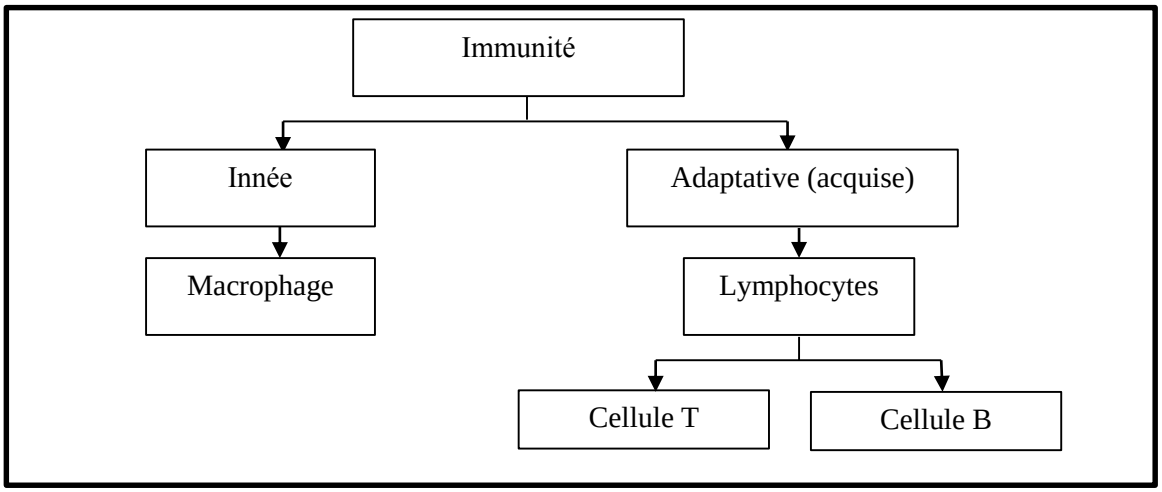

Figure 03 : Architecture du système immunitaire.

4.1. L'immunité innée

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 [28,29] :

- 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 [28,29] :

- 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 adaptés 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.

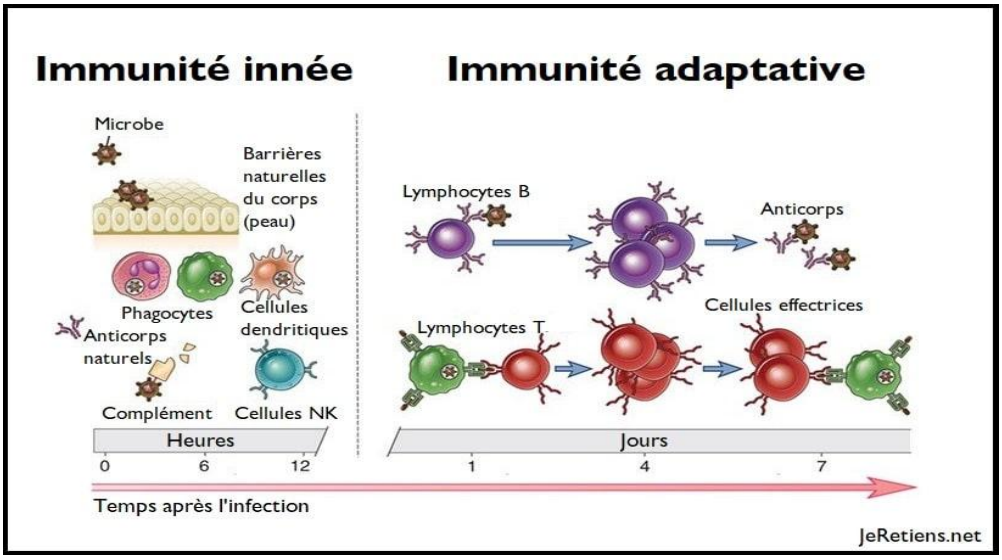

Figure 04 : immunité innée et immunité adaptive [30].

5. Éléments fonctionnels du système immunitaire

Le système immunitaire sert à protéger notre organisme contre les attaques extérieures mais aussi contre des cellules anormales voire cancéreuses." En permanence, il veille, identifie, réagit, s'organise puis élimine les agents pathogènes ou les corps étrangers" [31].

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, un processus appelé lymphopoïèse. 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 ganglions lymphatiques ou nœuds lymphatiques**, des cumuls de tissu lymphatique isolés ou regroupés en grappes, répartis dans tout le corps qui agissent comme des filtres pour capturer les antigènes.
- **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[32].

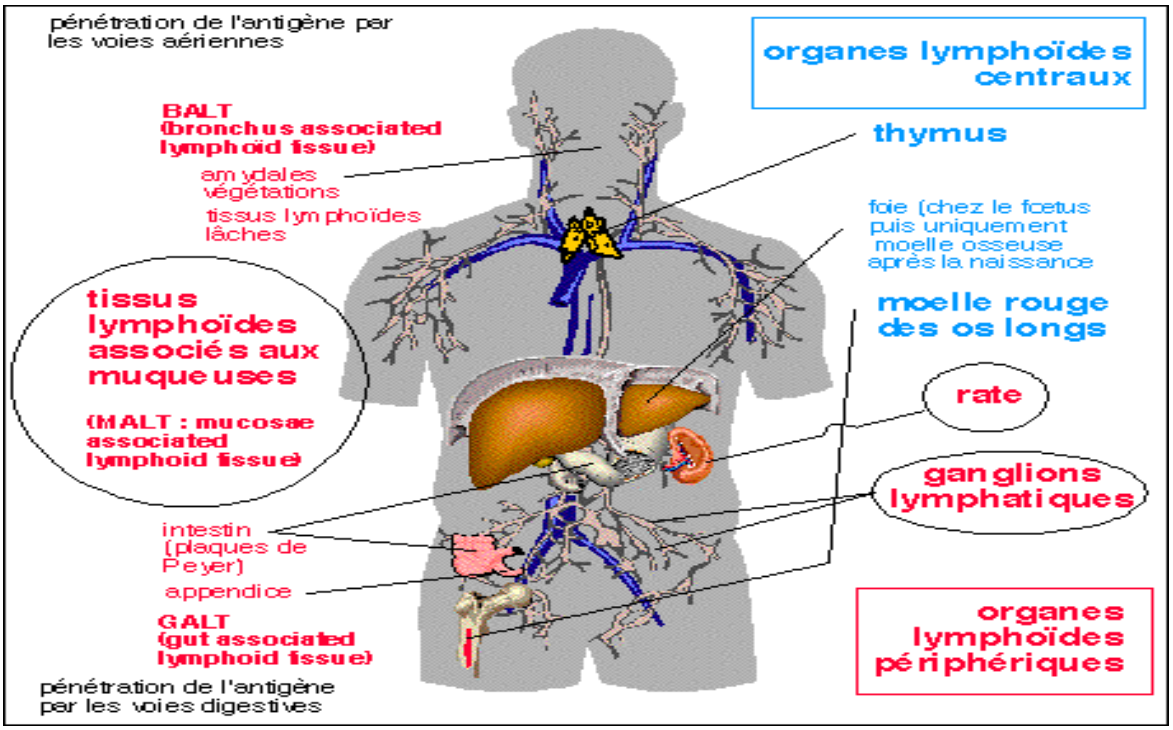

Figure 05 : les différents organes du système immunitaire [33].

5.2. Les cellules immunitaires

Les cellules immunitaires sont caractérisées par les clusters de différenciation. Ils ont des rôles divers au sein de l'organisme, notamment dans la différenciation de ces cellules au niveau de la moelle osseuse, mais encore 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 ; on parle de phagocytose Parmi eux on compte les macrophages, les cellules dendritiques, et les polynucléaires.

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

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.
- 52Au 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 [34],elles sont spécialement importantes dans la détection et l'élimination des cellules infectées par les virus et les cellules tumorales[35].

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 [34]. Principalement les

lymphocytes T ont pour reconnaitre l'antigène et mettre en marche la réponse immunitaire adaptative [35]. 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 [34].

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 [36].

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 [37].

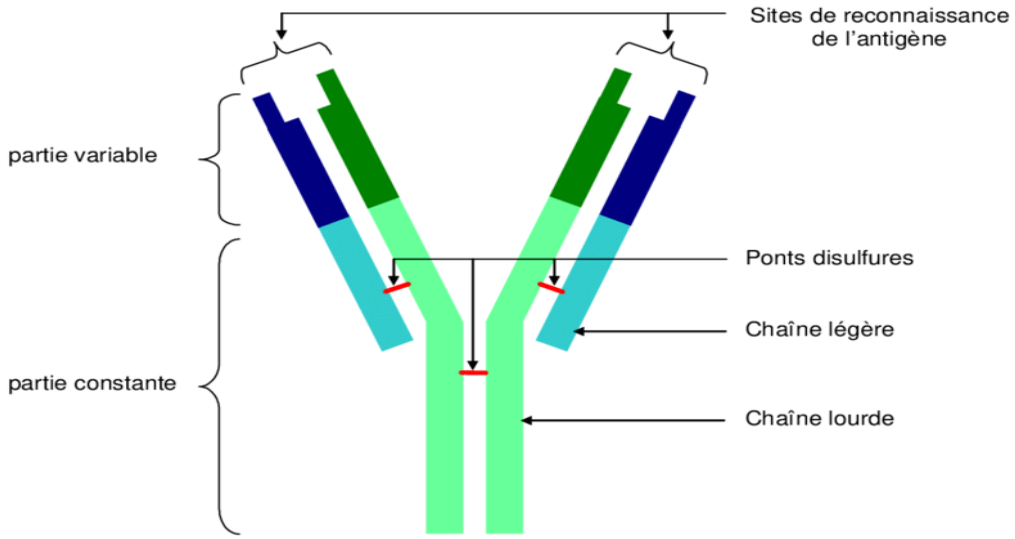

Figure 06 : Schéma d'un anticorps [38].

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 [39].

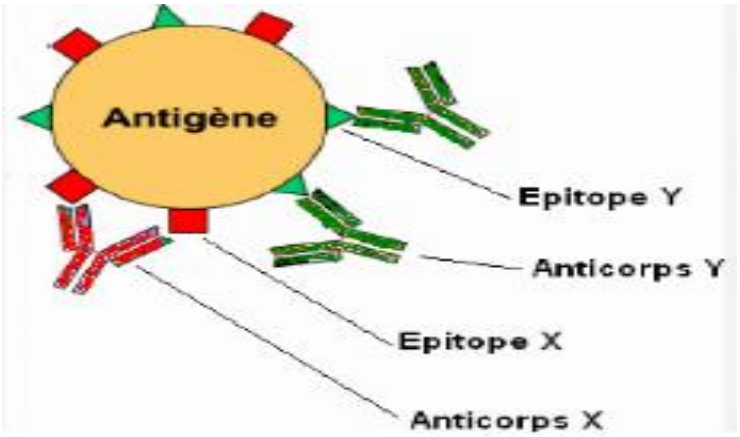

Figure 07 : Anticorps poly clonaux, liaison à des épitopes différents [40].

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 [41].

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** sont des molécules variées dont certaines font partie du complément ou des cytokines [37].

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 [42].

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 développement dans le thymus sont appeler cellules T naïves ou immatures. Ils subissent deux phases de criblage : le premier criblage par la sélection positive qui consiste a sélectionné 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 [43].

6.1. Théorie de la sélection positive/négative

Cette théorie gère le processus de création des lymphocytes. Plus précisément, cette théorie gère le processus de création au niveau de la discrimination entre soi et non soi. Les lymphocytes ont sur leurs surfaces des récepteurs (paratopes), Les lymphocytes issus de la moelle osseuse migrent vers le thymus, à ce stade ils sont appelés cellules T naïves ou immatures. Leurs paratopes subissent un processus de réarrangement génétique pseudo aléatoire, puis un test très important est mis en place [44]. Le test en question consiste à vérifier si les nouveaux récepteurs s'attaquent aux cellules du soi, dans ce cas lymphocytes sont détruits et purgés de la population des nouveaux lymphocytes, on parle de sélection négative. Le reste de la population est autorisé à quitter le thymus pour circuler dans le sang et effectuer leurs taches de surveillance. Ce processus est illustré par la figure 08.

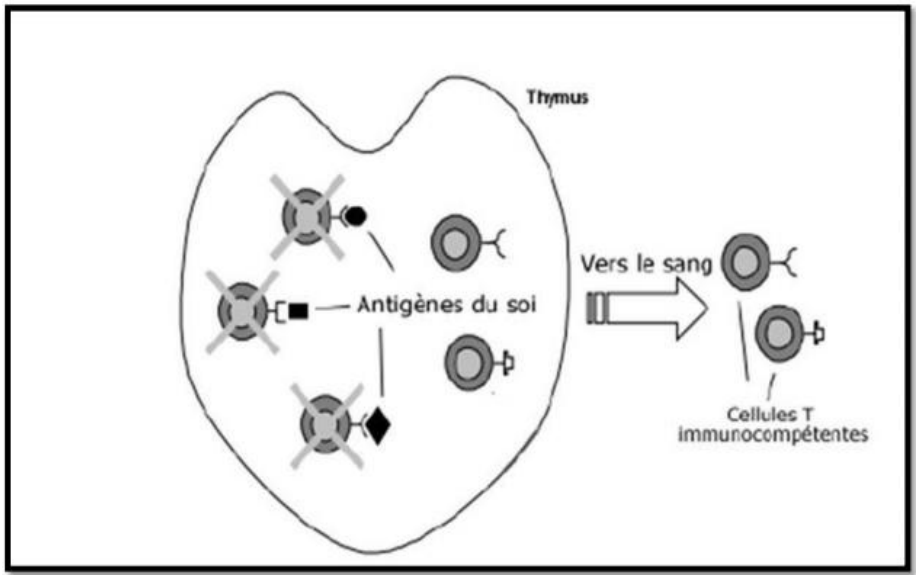

Figure 08 : Processus de sélection Négative/Positive.

6.2. Théorie de la sélection clonale

Une autre théorie tout aussi importante que la sélection négative c'est la théorie de la sélection clonale. Cette théorie a été exposée en 1959 par Burnet [45]. Elle met en avant la réaction du système immunitaire à une stimulation antigénique [46]. La théorie de la sélection clonale explique les deux processus de prolifération et de maturation d'affinité. L'idée de cette théorie est la suivante : Dès la reconnaissance d'un antigène par les lymphocytes B, ces derniers produisent des anticorps spécifiques (chaque cellule sécrète un seul type d'anticorps). L'anticorps s'associe à l'antigène à l'aide des récepteurs (épitopes-paratopes) puis à l'aide des cellules telles que les T aideuses, les cellules B sont stimulées et un processus de prolifération (division cellulaire) permet aux cellules B de se reproduire en créant des clones d'elles-mêmes [45]. Un second processus permettra de sélectionner parmi les nouvelles cellules celles présentant une grande affinité afin d'en faire des cellules mémoires [47].

Les cellules mémoires circulent à travers le sang, la lymphe, et à la présence d'un antigène précédemment reconnu, une réaction rapide et efficace est immédiatement lancée [48]. Cette théorie est particulièrement utilisée dans les domaines tels que l'optimisation, la reconnaissance de formes et l'apprentissage-machine (intelligence artificielle).

6.3. Théorie du danger

Proposée initialement par **Polly Matzinger**, cette théorie est une nouvelle vision qui diffère de l'approche classique. La théorie du danger gère le comportement du système et sa réaction selon les nouvelles conditions suivantes :

- Le système immunitaire ne doit pas réagir contre le soi, sauf si ce dernier est dangereux.
- Le système immunitaire réagit contre le non soi, sauf si ce dernier n'est pas dangereux.

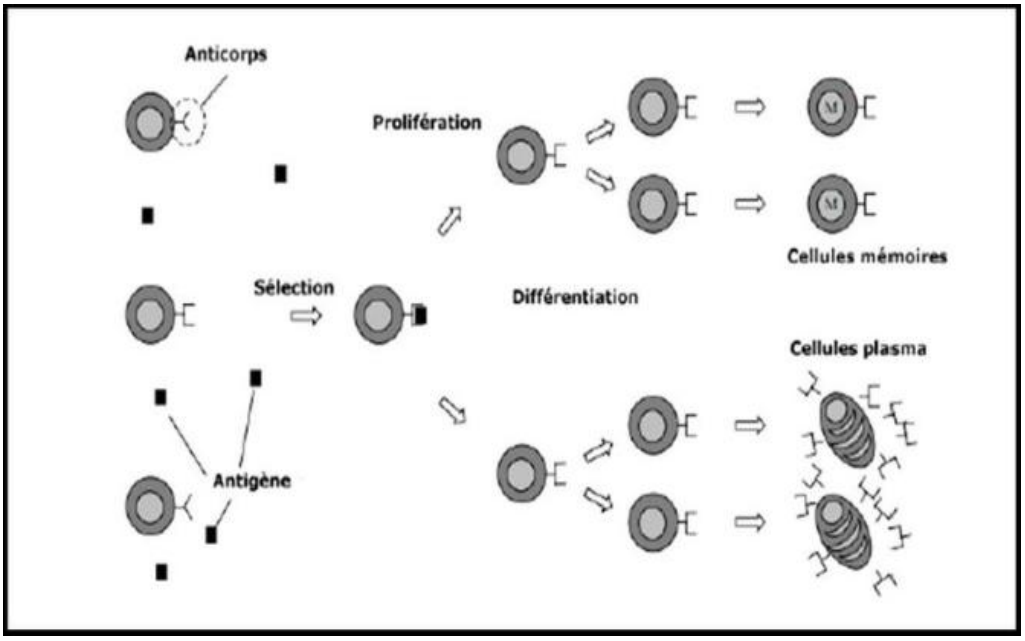

Figure 09 : Processus de sélection clonale [49].

Nous constatons que dans la théorie du danger il y a une corrélation entre les signaux d'alarmes. Il ne suffit pas de détecter les cellules étrangère, il faudrait également savoir si ces dernières sont dangereuses ou pas [48].

7. 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 [50].

Pour que le système immunitaire fonctionne correctement, il doit être capable de distinguer entre

Tolérance de soi. Ce problème est reconnu sous le nom problème de discrimination entre soi / non soi [50]. Donc, il doit y avoir quelque forme de sélection négative qui empêche les cellules immunitaires de devenir auto réactives.

7.1. 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. 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 [50].

7.2. 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 [50].

8. Comment le système immunitaire assure-t-il la protection du corps humain ?

Notre corps est protégé par une collection diverse des cellules et des molécules qui collaborent contre n'importe quelle molécule étrangère comme les bactéries ou d'autres envahisseurs. La figure ci-dessous présente une version simplifiée des mécanismes de base de défense immunitaire (figure 10), et qui peuvent être résumés par les étapes suivantes :

1- Quand un intrus envahit le corps, les cellules de présentation antigénique (APC1) comme les macrophages procèdent à l'ingestion et la digestion de l'antigène rencontré pour le présenter comme des fragments de peptides antigéniques
2- Ces peptides seront avec les molécules MHC pour permettre leurs liaisons avec les cellules T qui ont la capacité de reconnaître la combinaison de peptide / MHC.
3- Les cellules T activées par cette identification produisent et sécrètent des lymphokines ou des signaux chimiques pour mobiliser d'autres composants du système immunitaire.

4- Les cellules B qui ont aussi des molécules de récepteur complémentaires répondent à ces signaux. À la différence des récepteurs de cellules T, ceux de cellules B peuvent reconnaître les parties d'antigènes libres sans les molécules MHC.

5- Après cette activation, les cellules B prolifèrent et se différencient et sécrètent des protéines d'anticorps.

6- La liaison entre les anticorps et les antigènes disponibles mènent à la destruction et la suppression des antigènes.

7- Un nombre de cellules B et T deviennent des cellules mémoires qui ont une durée de vie illimitée, en permettant l'élimination rapide de l'antigène s'il se présente une autre fois dans l'avenir [14].

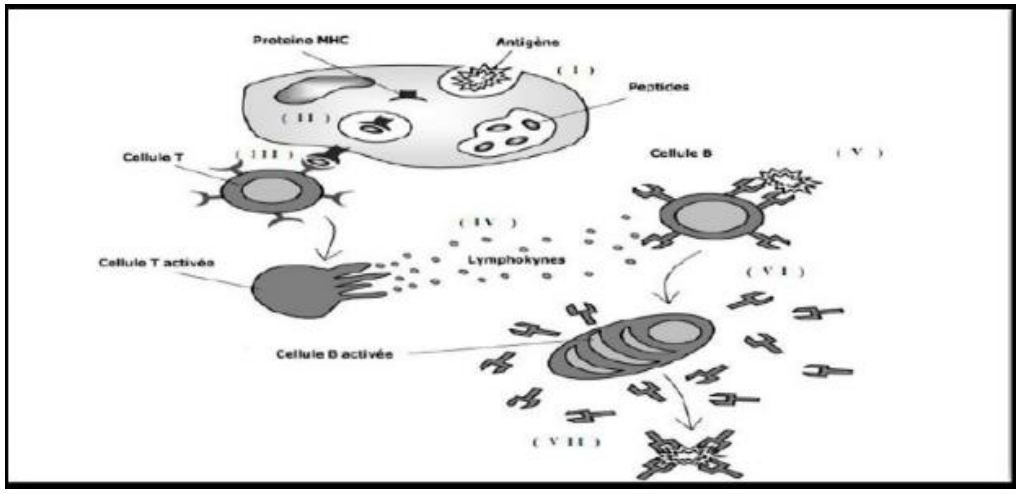

Figure 10 : Le processus de base de défense immunitaire.

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 [51]. Cette section sera consacrée à introduire le système immunitaire artificiel avec une présentation des différents modèles qui ont été mis en œuvre.

2. Définitions

Def 01 :

Un système immunitaire artificiel est un système informatique basé sur les métaphores du système immunitaire naturel [52].

Def 02 :

Dasgupta a défini le système immunitaire artificiel comme suit : « Le système immunitaire artificiel est la composition de méthodologies intelligentes inspirées par le système immunitaire naturel afin de résoudre des problèmes du monde réel [53].

Def 03 :

Tandis que Timmis et De Castro 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 » [54].

3. Structure de conception d'un système immunitaire artificiel

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 [43].

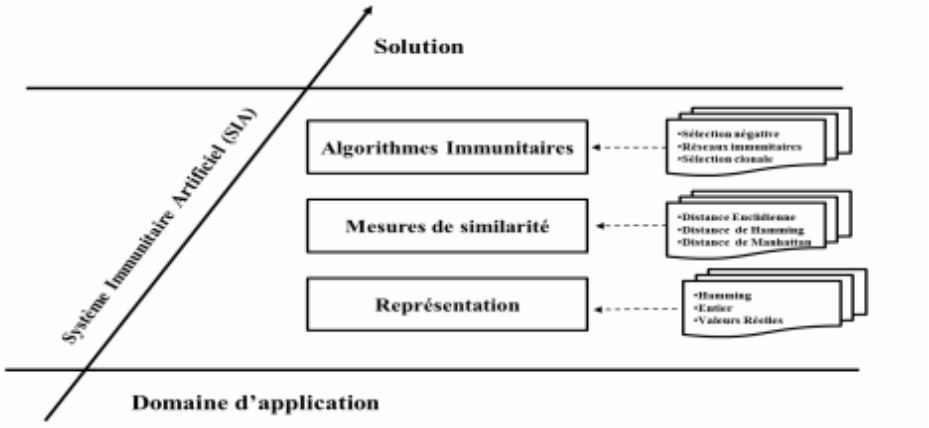

Figure 11 : Le processus de base de défense immunitaire.

3.1. Représentation

Afin de construire un système tel qu'un SIA, un domaine d'application ou une fonction cible sont généralement exigés. À 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 [55].

3.1.1. 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 [43].

3.2. Les mesures d'affinités

L'affinité entre un anticorps et un antigène est relative à leur distance [44]. Elle peut être estimée via n'importe quelle mesure de distance entre deux chaînes (ou vecteurs) par exemple par l'utilisation de la distance Euclidienne, la distance de Manhattan ou la distance de Hamming [44]. Si on considère un anticorps Ab = <Ab1, Ab2, …AbL> et un antigène Ag =<Ag1, Ag2, … ,AgL>, alors la distance D peut être calculée selon l'une des distances précédentes qui seront

Présentées respectivement dans la figure suivante :

La distance Euclidienne	$D = \sqrt{\sum_{i=1}^{L}(Ab_i - Ag_i)^2}$
La distance de Manhattan	$D = \sum_{i=1}^{L}\lvert Ab_i - Ag_i\rvert$
La distance de Hamming	$D = \sum_{i=1}^{L}\delta_i \; ou \; \delta = \begin{cases} 1 & si \; Ab_i \neq Ag \\ 0 & sinon \end{cases}$

Figure 12 : Les différentes équations pour calculer l'affinité entre un antigène et un anticorps [56].

4. Les algorithmes du système immunitaire artificiel

4.1. L'algorithme de la sélection négative/positive

La sélection négative (ou détection négative) est une abstraction des mécanismes qui permettent aux systèmes immunitaires naturels de distinguer entre le soi et le non soi. Elle se concentre sur la génération de détecteurs de changements, ces détecteurs sont censés détecter qu'un élément d'un ensemble de chaînes (le soi) a changé [57]. Ils ont 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 :

- Produire aléatoirement des anticorps et les placez dans un ensemble P,
- Déterminer l'affinité de tous les anticorps dans P avec toutes les cellules de l'individu S.
- Si l'affinité d'un anticorps de P avec au moins une cellule de S est supérieure ou égal à un seuil donné S', alors l'anticorps identifie l'individu et doit être éliminée, si non l'anticorps est accepté [58].

Le schéma suivant résume l'algorithme de sélection négative :

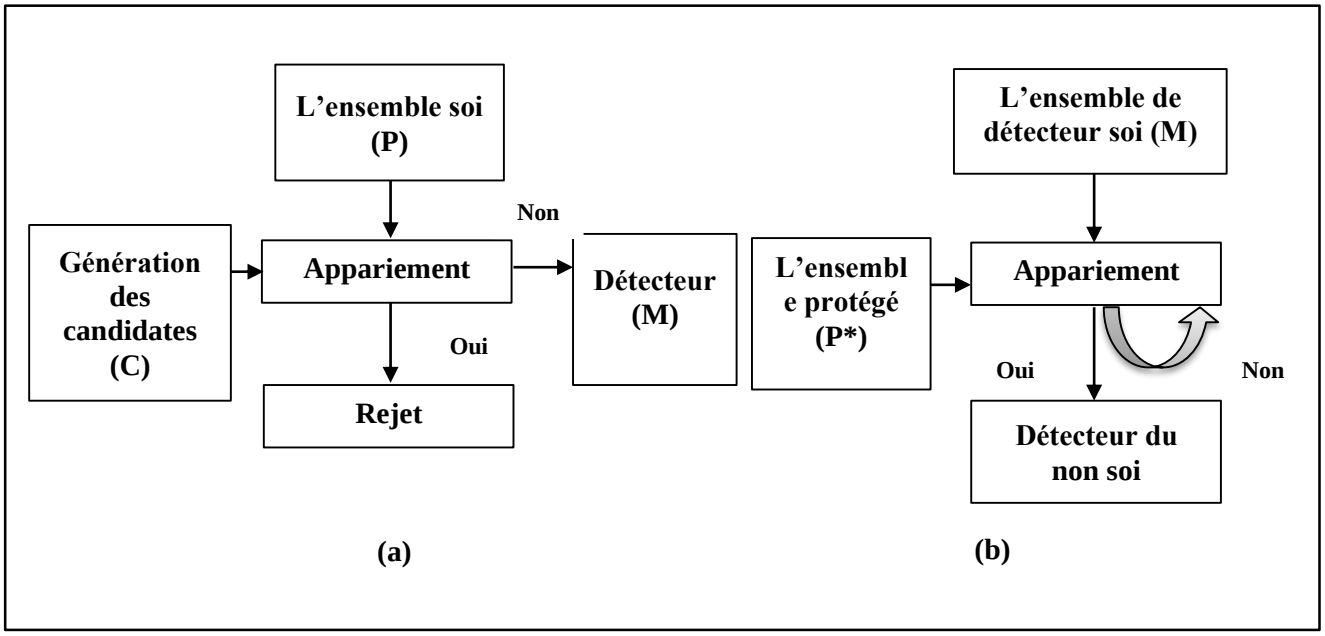

Figure 13 : La structure générale de l'algorithme de la sélection négative [14].

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 [43].

4.2. 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 [59].

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 :

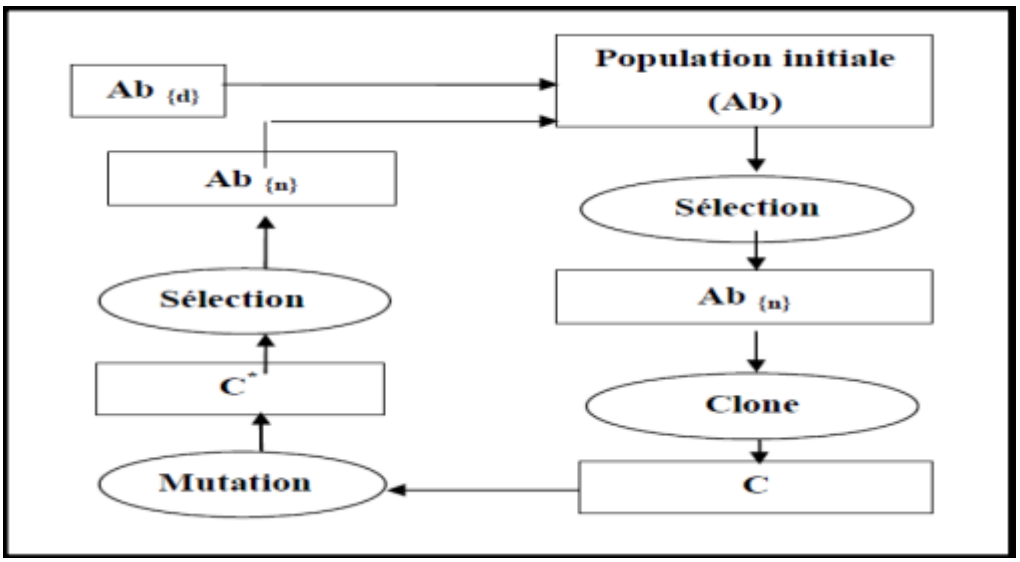

Figure 14 : Une représentation de l'algorithme de la sélection clonale [59].

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 15 : L'algorithme de la sélection clonale [60].

4.3. 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 [55]. 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 :

Algorithme de Réseau immunitaire

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

Entrée : Un ensemble **N** de détecteurs aléatoire

Entrée : **n** le nombre de meilleures récepteurs

Sortie : **M** un ensemble de détecteurs générés capable de reconnaitre les formes entrantes

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

Pour Chaque forme à reconnaitre **faire**

-Calculer l'affinité pour chaque membre de **B** avec chaque détecteur de **N**

-Sélectionner les **n** membres de **B** ayant la meilleure correspondance avec les formes

-Cloner et muter chaque **n** selon le degré d'affinité

-Placer l'élément **n** ayant la plus forte affinité et l'ajouter a l'ensemble **M**

-Parcourir l'ensemble **M** et retirer les membres les plus faibles (la plus faible affinité)

-Générer des éléments **b** et les ajouter a l'ensemble **B**

Fin pour

Figure 16 : L'algorithme du réseau immunitaire [60].

5. Domaines d'application des SIA

Comme vu dans les sections précédentes, 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 à plusieurs secteurs d'application pour des buts différents. D'une manière générale, parmi ces secteurs 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 [43].

- **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 [14].

- **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 emploie 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 [43].

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'intrusions 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 01 : 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 02 : Des travaux sur les SIA [14].

6. Étude 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.

Systèmes / Caractéristiques	**Système immunitaire Artificiels(AIS)**	**Réseaux de neurones artificiels (RNA)**	**Algorithme Génétique(AG)**
Composants	Chaîne d'attribut	Neurones artificiels	Chaînes de Chromosomes
Endroits des composants	Dynamique	Prédéfini	Dynamique
Structure	Composant discret/composants en réseaux	Composant en réseaux	Composants discrets
Stockage de la connaissance	Concentration des Composants/ réseau	Connexion robuste	Chaîne Chromosomiques
Dynamique	Apprentissage / Evolution	Apprentissage	Evolution
Méta-dynamique	Incorporation/ élimination des composants	Construction/ élagage de la connexion	Incorporation / élimination des composants
Interaction entre l'environnement	Reconnaissance/ connexion réseaux	Connexion réseaux	Recombinaison
Interaction avec l'environnement	Reconnaissance/ les fonction objectives	Stimulation externe	Fonction de fitness
Seuil d'activités	L'affinité des composants	Activation des Neurones	Surpeuplement/ Partage

Tableau 03 : Un tableau comparatif entre les caractéristiques des différents systèmes inspirés de la biologie [60].

III. Le lien entre in 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.

Comme vu dans la section précédente, le système immunitaire artificiel a été appliqué aux différents domaines de recherche. Parmi ces domaines, la sécurité et la détection d'intrusions sont le secteur d'application qui est le plus étroitement lié avec le système immunitaire humain.

Puisque les deux systèmes ont un but commun qui consiste à assurer la protection contre les intrus.

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 [61] : 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 dé finie en exposant les problèmes confrontés par les systèmes de sécurité des systèmes informatiques [61].

- **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 [61] : 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 [32] 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 [14]:

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 [62]. 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.

3.3. 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 gêne, 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.

Conclusion :

Les systèmes immunitaires artificiels sont des programmes dont le principe de fonctionnement est inspirés de la biologie et plus précisément du système immunitaire humain qui est considéré l'un des systèmes de défense les plus efficaces.

Cependant, le cerveau de ces systèmes consiste en un algorithme qui implémente les techniques de détection : soi/non soi, sélection négative,...

Nous aborderons dans le prochain chapitre la partie analyse et conception de notre système de détection d'intrusions qui est basé sur les algorithmes immunitaires artificiels.

Chapitre 03 :

Analyse et Conception

Introduction

Les systèmes de détection d'intrusions basés sur les systèmes immunitaires artificiels ont encore des points à explorer. Ils peuvent adopter des concepts et des aspects plus larges inspirés d'immunologie comme : la théorie de danger et la bibliothèque de gènes.

Dans ce chapitre, nous avons proposé un algorithme exploiter le fonctionnement de base du système immunitaire naturel pour la détection d'intrusions, en ajoutant quelques améliorations sur l'algorithme de la sélection négative qui se base sur le modèle de soi et de non soi, à travers d'intégration de la notion de danger pour permettre la détection des intrusions réelles causées par des utilisateurs internes ou externes qui endommagent le système .

1. 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 [43]. 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 œuvre.
- **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 ci-dessous présente les types de chaque attaque :

S/N	Nom	Type	S/N	Nom	Type
1	Back	Dos	20	Worm	R2l
2	buffer_overflow	U2r	21	Smurf	Dos
3	ftp_write	R2l	22	Spy	R2l
4	guess_passwd	R2l	23	Teardrop	Dos
5	Ps	U2r	24	Warezclient	R2l
6	Imap	R2l	25	Warezmaster	R2l
7	Ipsweep	Probe	26	Apache2	Dos
8	Land	Dos	27	Named	R2l
9	Loadmodule	U2r	28	Httptunnel	U2r
10	Multihop	R2l	29	Mailbomb	Dos
11	Neptune	Dos	30	Processtable	Dos
12	Nmap	Probe	31	Sendmail	R2l
13	Snmpgetattack	R2l	32	Xterm	U2r
14	Perl	U2r	33	Udpstorme	Dos
15	Phf	R2l	34	Snmpguess	R2l
16	Sqlattack	U2r	35	Xclock	R2l
17	Pod	Dos	36	Xsnoop	R2l
18	Portsweep	Probe	37	Mscan	Probe
19	Rootkit	U2r	38	Saint	Probe

Tableau 04 : les types d'attaques.

Le tableau suivant présente les 41 attributs de chaque enregistrement :

No.	Network attributes	No.	Network attributes	No.	Network attributes
1	duration	15	su_attempted	29	same_srv_rate
2	protocol_type	16	num_root	30	diff_srv_rate
3	service	17	num_file_creations	31	srv_diff_host_rate
4	flag	18	num_shells	32	dst_host_count
5	src_bytes	19	num_access_files	33	dst_host_srv_count
6	dst_bytes	20	num_outbound_cmds	34	dst_host_same_srv_rate
7	land	21	is_host_login	35	dst_host_diff_srv_rate
8	wrong_fragment	22	is_guest_login	36	dst_host_same_src_port_rate
9	urgent	23	count	37	dst_host_srv_diff_host_rate
10	hot	24	srv_count	38	dst_host_serror_rate
11	num_failed_logins	25	serror_rate	39	dst_host_srv_serror_rate
12	logged_in	26	srv_serror_rate	40	dst_host_rerror_rate
13	num_compromised	27	rerror_rate	41	dst_host_srv_rerror_rate
14	root_shell	28	srv_rerror_rate		

Tableau 05 : les attributs de chaque ligne de connexion [63].

2. La Sélection D'attributs pertinents

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**
U2R	**1, 2, 3, 5, 10, 13, 14, 32, 33, 36**
R2L	**1, 3, 5, 6, 12, 22, 23, 31, 32, 33**
Probe	**3, 4, 5, 6, 9, 29, 30, 32, 35, 39, 40**

Tableau 06 : les attributs pertinents de chaque classe d'attaque.

3. Conception du système proposé

3.1. Les composants immunitaires

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

3.1.1. 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).

3.1.2. 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.

3.1.3. 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 : $\mathbf{D}=\sum_{i=1}^{n} \boldsymbol{\sigma i}\ \boldsymbol{ou}\ \boldsymbol{\sigma} = \begin{Bmatrix} \mathbf{1}, \boldsymbol{Abi \neq Agi} \\ \mathbf{0}, \boldsymbol{sinon} \end{Bmatrix}$

Pour mesurer le degré de complétude entre l'antigène et l'anticorps:

La fonction d'affinité est comme suit :

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

3.1.4. 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 ce 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.

3.2. Les classes du système :

Notre système se constitue d'un ensemble des classes qui coopèrent pour réaliser les tâches requises, lasurveillance 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 aucunrisque sur le réseau. Il agit comme un capteur de paquets pour l'IDS.
Class PaquetGenerator	Permet la génération des paquets du traficréseau (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 iciest 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 07: les classes du système.

3.3. Le processus de déroulement

3.3.1. 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 :

- Extraction des attributs pertinents de chaque attaque à partir de la base KDD cup 99.
- Elimination des détecteurs redondants.
- Vérification de correspondance avec les modèles de soi avec élimination des détecteurs qui reconnaissentle soi.
- Vérification de correspondance avec les modèles de non soi.

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

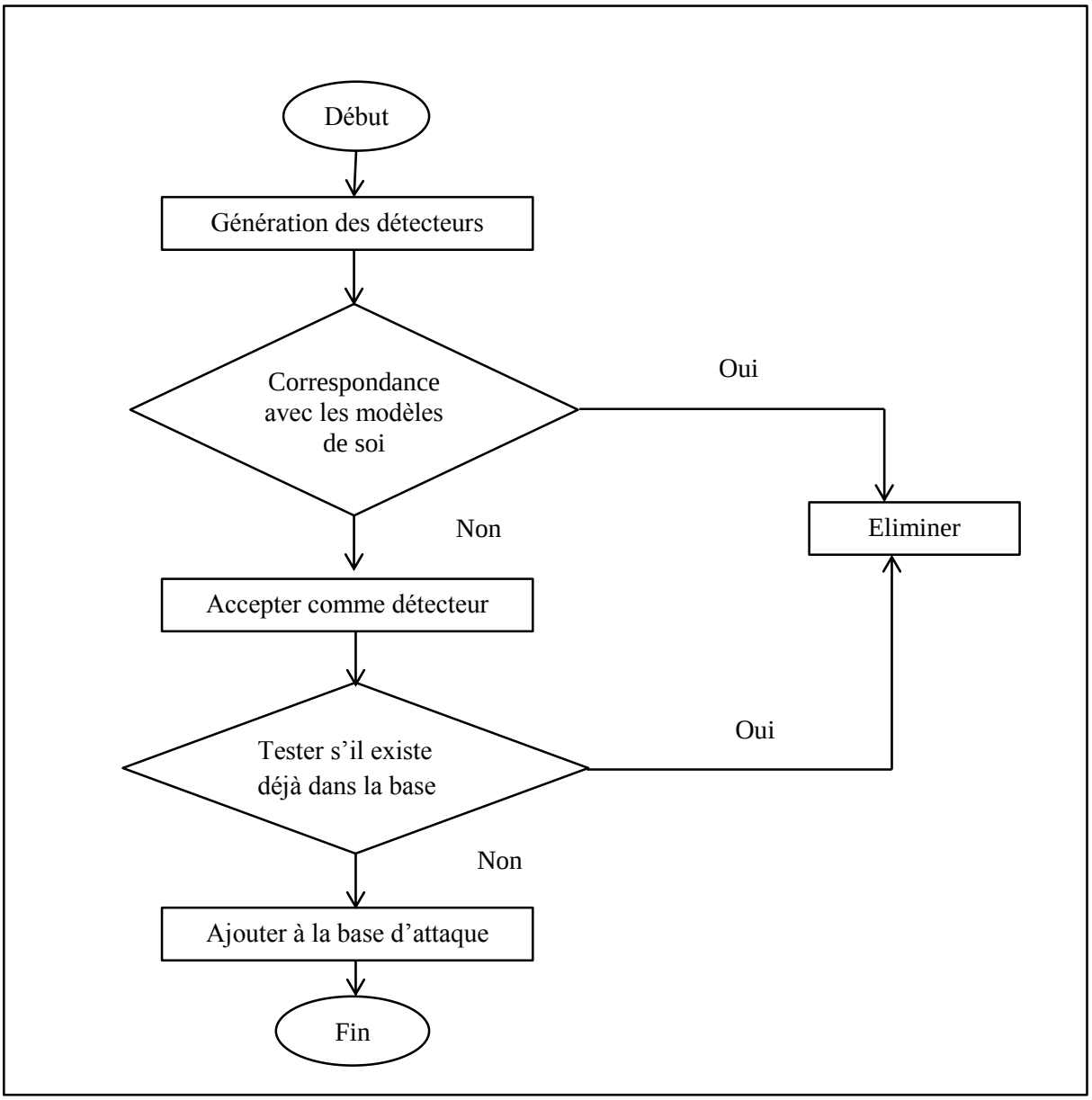

Figure 17 : processus de génération de détecteur (14).

3.3.2. 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 envoyé 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 :

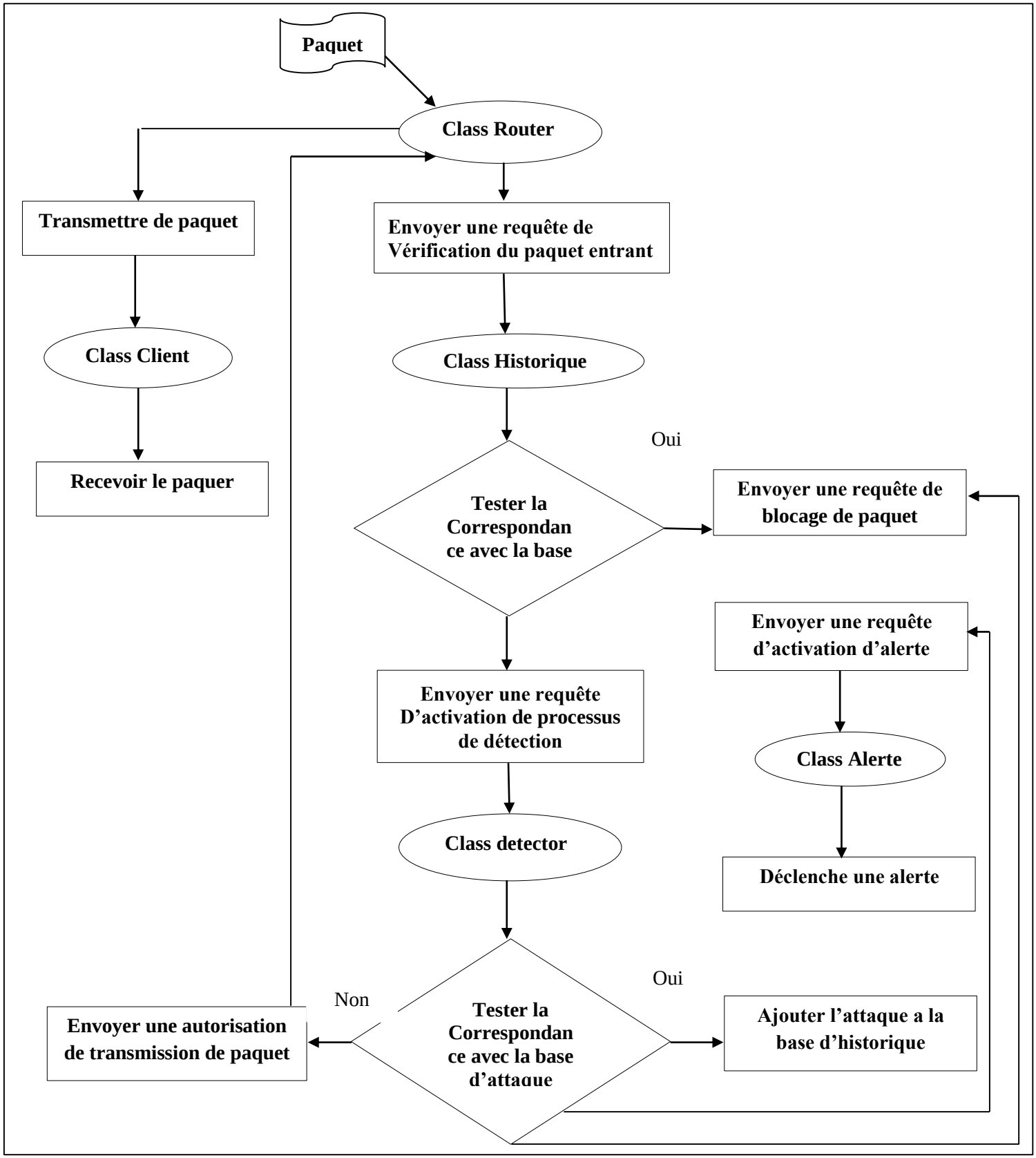

Figure 18 : Le processus de détection.

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

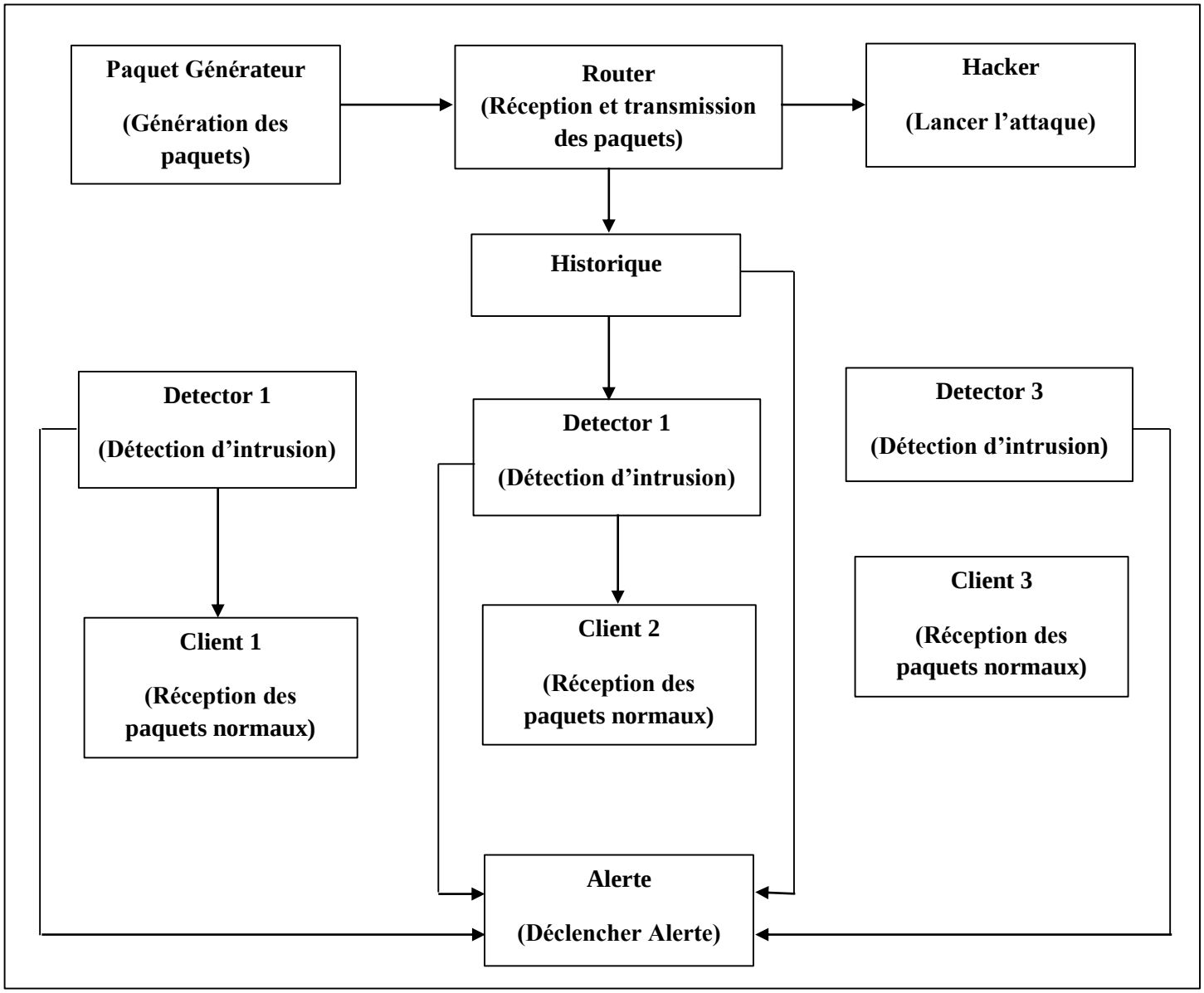

Figure 19 : L'architecture générale du système proposé.

La figure suivante présente le diagramme de séquence :

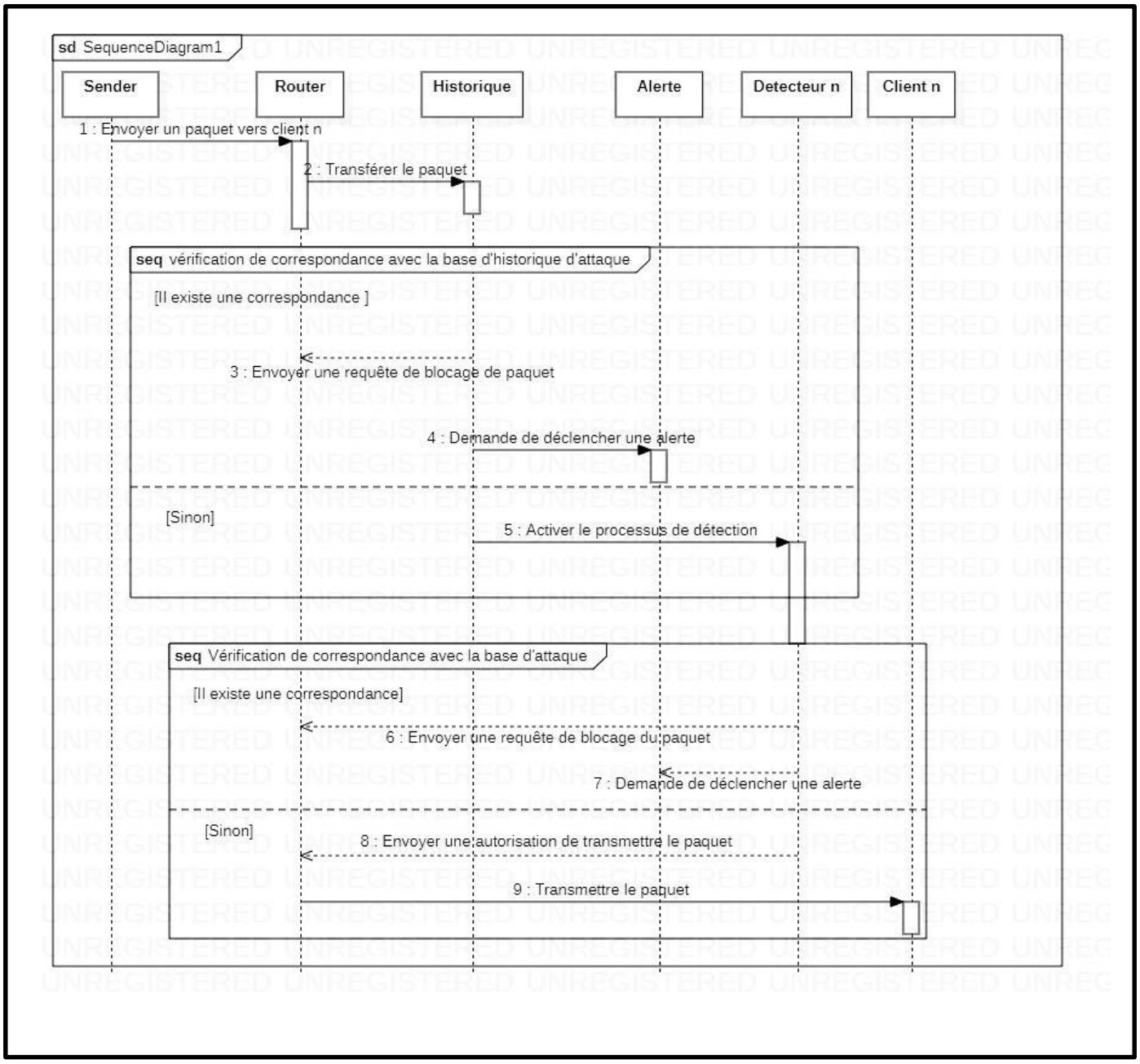

Figure 20 : Diagramme de séquence.

Remarque

Dans le diagramme précédant « Sender » désigne un émetteur de paquet, peut être Hacker ou PackGenerator mais dans les 2 cas le même processus de vérification des paquets entrants va s'exécuter.

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

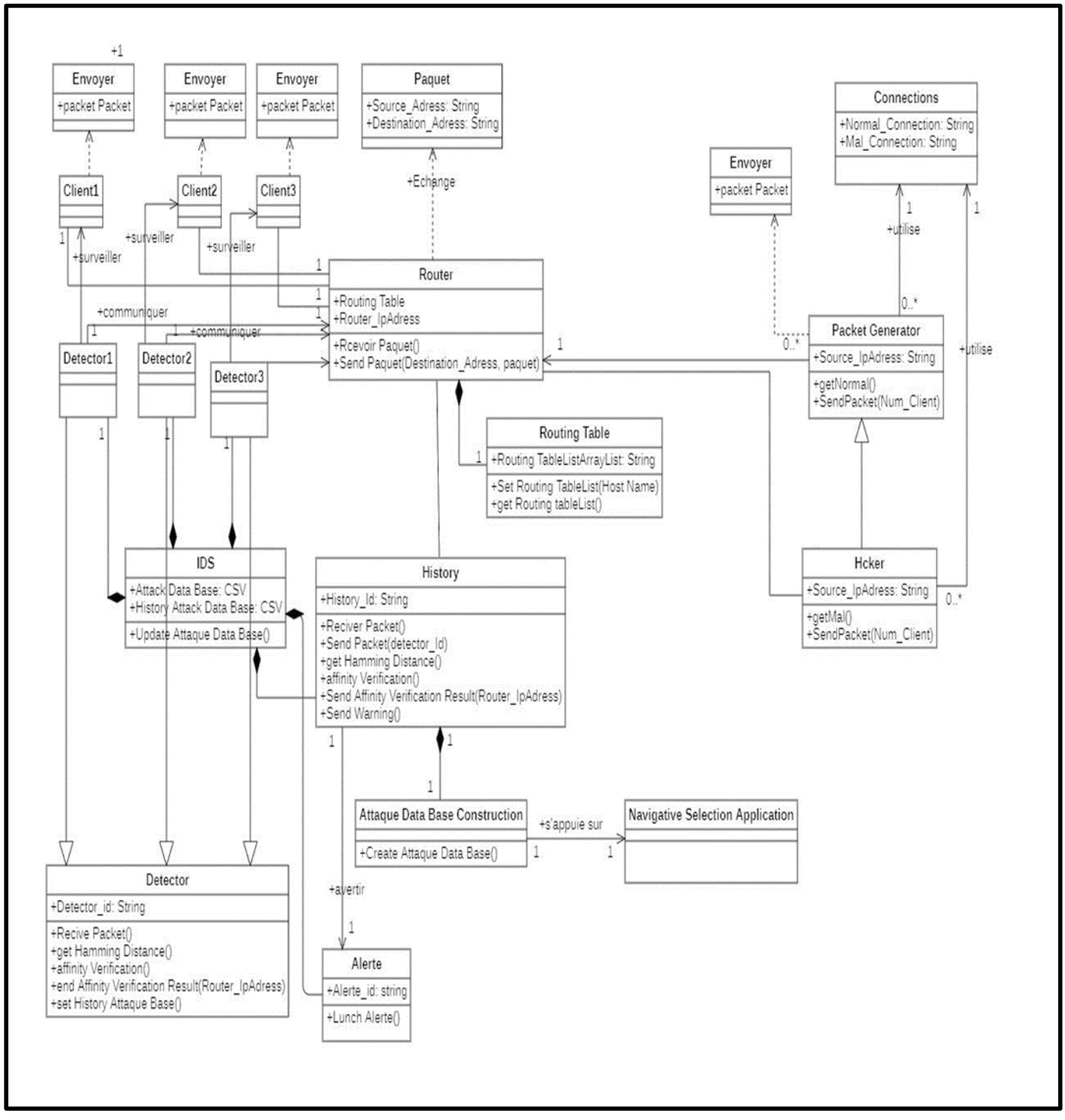

Figure 21 : Diagramme de classe.

4. Étude expérimentale

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

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

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

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

FN : False Négative (Faux Négatif) évènement intrusif identifié comme normal

Taux de détection = TP/ (TP + FN)

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

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 différentes étapes nécessaires à la mise en œuvre. Pour la suite nous avons présenté une 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 04 :

Réalisation et Implémentation

1. Introduction

Dans ce chapitre nous allons aborder la cote technique de notre projet, et précisément l'implémentation de notre système.

Nous commençons par détailler les outils de développement de l'application ainsi que la présentation des principales interfaces graphiques ergonomiques qu'il offre.

2. Les environnements de développements

2.1. Le langage Pascal

Pascal est un langage de programmation impératif qui se caractérise par une syntaxe claire, rigoureuse et facilitant la structuration des programmes. Cette clarté et cette rigueur font que Pascal était encore récemment souvent utilisé dans l'enseignement.

2.2. Delphi

Delphi a son origine de Pascal et est souvent appelé Delphi Pascal. Il est un produit de Borland et est entré sur le marché en 1995 sous le nom de Delphi 1, ajoutant des capacités orientées objet au langage Pascal.

Delphi est un langage de haut niveau prenant en charge la conception orientée objet. Il s'agit d'un développement rapide d'application utilisé pour développer des applications allant des solutions de base de données aux applications mobiles et est utilisé sur Windows ainsi que Linux.

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

3.1. Les avantages de NSL-KDD

Le NSL-KDD dataset présente les avantages suivants par rapport au KDD'99 dataset d'origine [64]:

- 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) i3-4005U CPU @ 1.70GHz 1.70 GHz RAM 4 GO.

5. Les interfaces du système

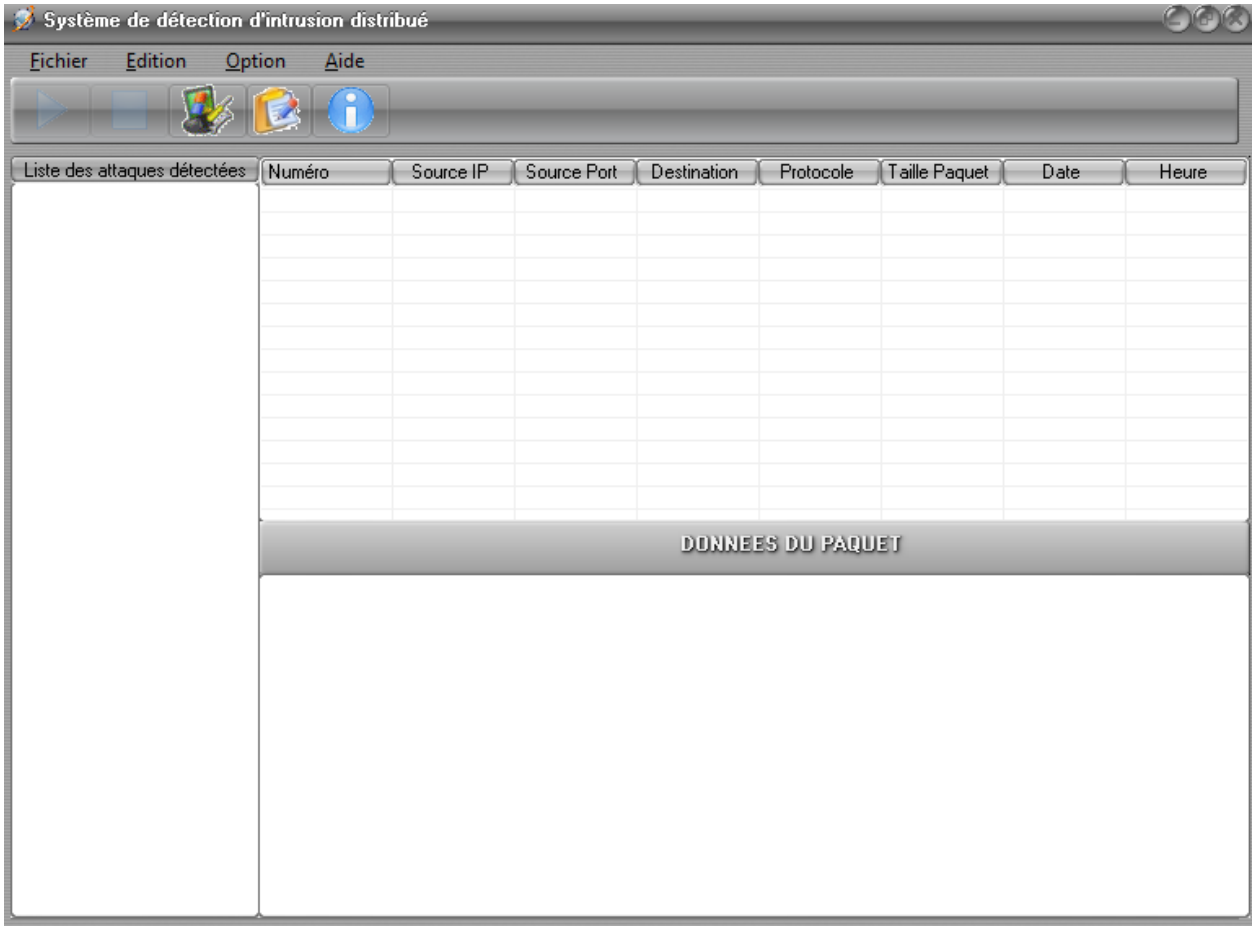

Figure 22 : Premier interface du système

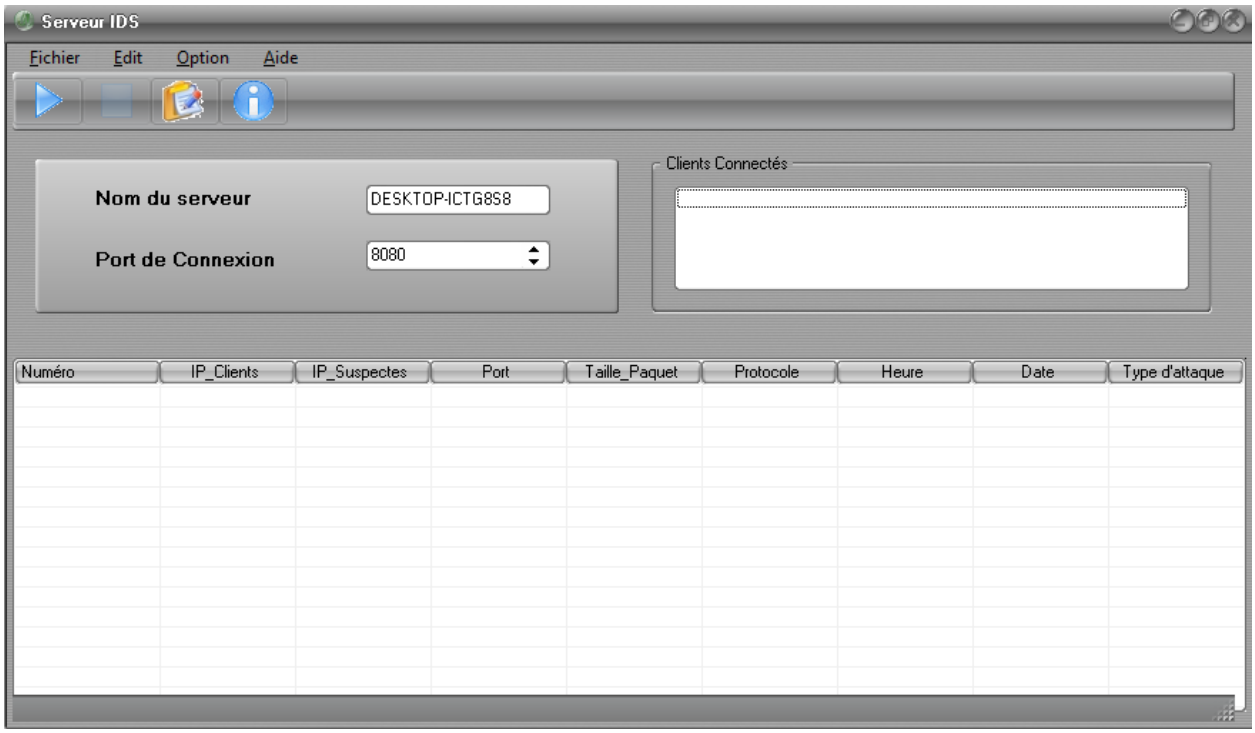

Figure 23 : L'interface de serveur IDS.

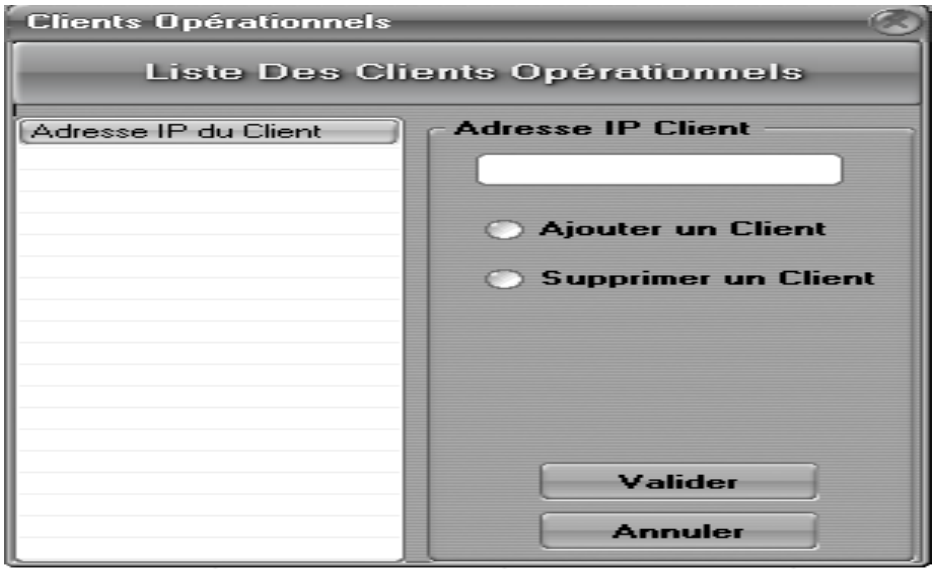

Figure 24 : L'interface du client.

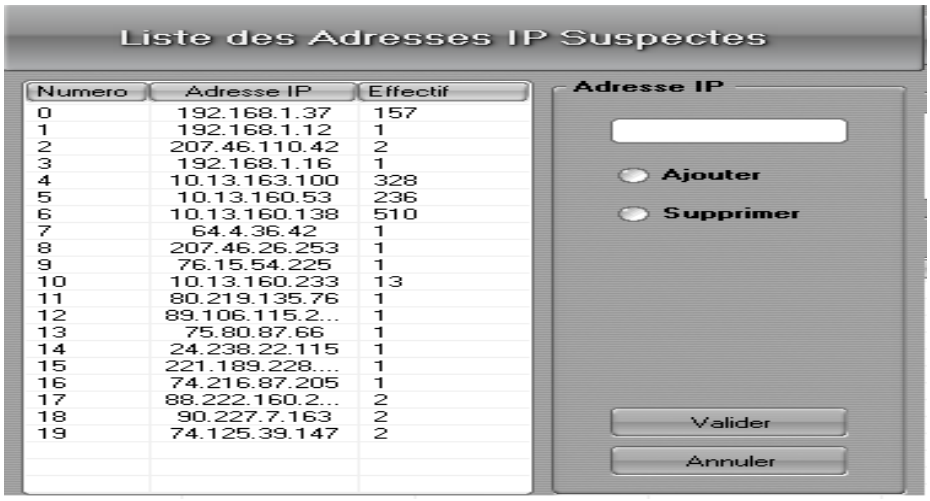

Figure 25 : L'interface des adresses IP suspectes.

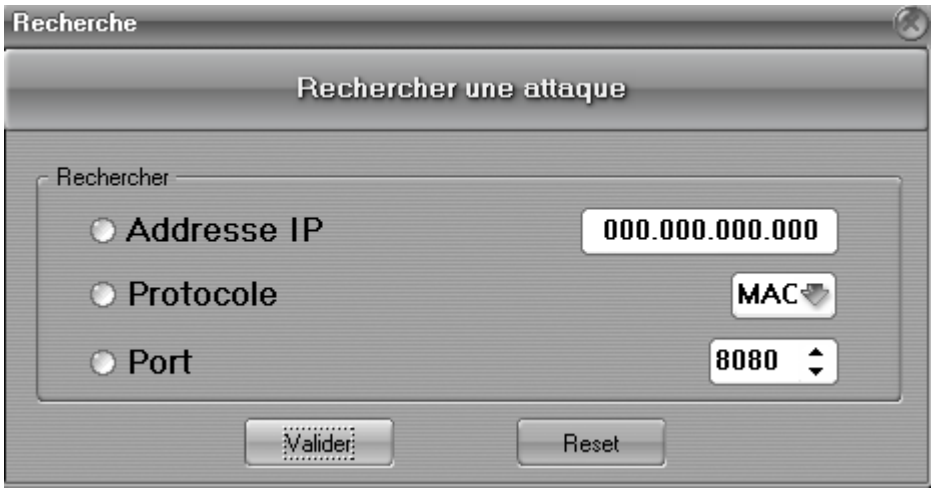

Figure 26 : Rechercher une attaque.

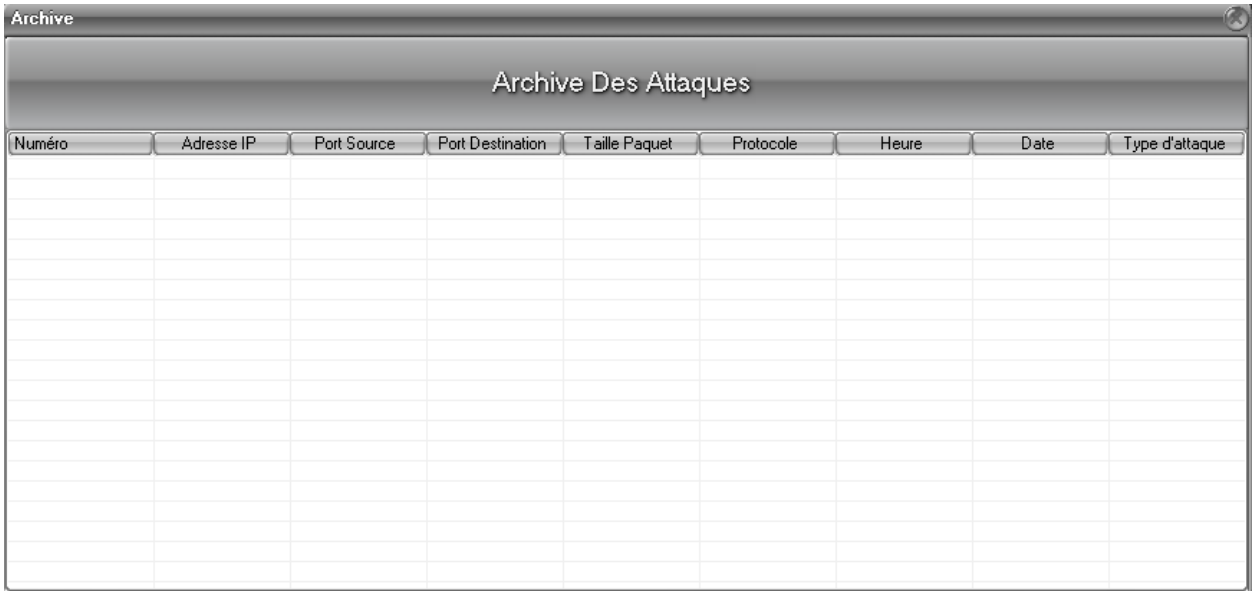

Figure 27 : L'interface d'archive des attaques.

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 Générale

Conclusion générale

La détection d'intrusion est un sujet de recherche particulièrement intéressant avec la complexité croissante des réseaux, des systèmes informatiques et des solutions inspirées de la biologie. Ce domaine de recherche constitue toujours le centre d'intérêt de diverses recherches afin d'exploiter tous les concepts et mécanismes d'identification et de détection utilisés par le système immunitaire humain.

L'application des solutions bio-inspirées telles que les systèmes immunitaires artificiels ne cesse de croître, car ces derniers se sont avérés très efficaces dans le domaine de la sécurité, notamment la détection des failles par rapport aux méthodes traditionnelles.

Notre travail proposé était une combinaison de différente approche, dont la détection d'intrusion est basée sur l'application de l'algorithme de sélection négative, 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.

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] 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

[2] Fiche du terme - Sécurité informatique. [En ligne]. Disponible : https://www.thesaurus.gouv.qc.ca/tag/terme.do?id=11543

[3] International Standards Organization. Information Processing Systems - OSI – Basic Reference Model - Part 2: Security Architecture. ISO 7498-2, February 2000.

[4] Rebecca Bace and Peter Mell. Intrusion Detection Systems. NIST Special Publication on Intrusion Detection Systems ,2000.

[5] David Burgermeister, Jonathan Krier. Les systèmes de détection d'intrusions http://dbprog.developpez.com

[6] Stéphan GUIDARINI, Sébastien DESSE, État de l'art de la sécurité informatique. [En ligne]. Disponible: https://slideplayer.fr/slide/1796910/

[7] Nadia Bounegta. Approche distribuée pour la sécurité d'un réseau de capteurs sans fils (RCSF), 2010. [En ligne].Disponible : https://www.memoireonline.com/08/10/3831/m_Approche-distribuee-pour-la-securite-dun-reseau-de-capteurs-sans-fils-RCSF2.html

[8] Techopedia Attack. [En ligne].Disponible : https://www.techopedia.com/definition/6060/attack

[9] Systèmes de traitement de l'information-Interconnexion de systèmes ouverts -Modèle de référence de base -Partie 2: Architecture de sécurité, Norme ISO 7498-2,1989. [En ligne]. Disponible: https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:fr

[10] SecuriteInfo.com, Introduction et initiation à la Sécurité Informatique. [En ligne]. Disponible: https://www.securiteinfo.com/conseils/introsecu.shtml

[11] A. Phillip, Porras and Alfonso Valdes. Live traffic analysis of tcp/ip gateways. Proc. ISOC Symposium on Network and Distributed System Security (NDSS98). (San Diego, CA, March 98), Internet Society.

[12] H. Debar, M. Dacier & A. Wespi. "A revised taxonomy for intrusion detection systems. Annales des télécommunications''. July–August 2000.

[13] Mémoire en vue de l'obtention du diplôme de Magister sous le thème « Application des systèmes immunitaires artificiels à la détection d'intrusion »réaliser par SLIMANI Ahmed

[14] LABED Ines «Proposition d'un système immunitaire artificiel pour la détection d'intrusions » thèse de magister informatique université mentouri de Constantine 2006.

[15] Guy Bruneau, The History and Evolution of Intrusion Detection, 2001. [En ligne]. Disponible: https://www.sans.org/reading-room/whitepapers/detection/paper/344

[16] Saraydaryan Jacques, Détection d'anomalies comportementales appliquée à la vision globale, thèse en vue de l'obtention du diplôme de Doctorat, Informatique et Information pour la Société L'Institut National des Sciences Appliquées de Lyon, ,2007-2008.[En ligne]. Disponible :https://www.researchgate.net/publication/38320555_Detection_d'anomalies_comportementales_appliquee_a_la_vision_globale

[17] Karen Scarfone, Peter Mell «Guide to Intrusion Detection and Prevention Systems (IDPS) », February 2007

[18] Mohan Vijayarani. Intrusion Detection System-A Study, 2015. [En ligne]. Disponible: https://www.researchgate.net/publication/339551603_INTRUSION_DETECTION_SYSTEM_-A_STUDY

[19] W. Jansen, P. Mell, T.Karygiannis , D.Marks «Mobile Agents in Intrusion Detection And Response », 2000

[20] Mykerjee. B, Heberlein. L.T , Levitt .K.N « Network Intrusion Detection », IEEE Network, Vol 8, No 3, pp .26-41, 1994

[21] S. Staniford-Chen & S. Cheung & R. Crawford & M. Dilger & J. Frank & J.Hoagland & S. Templeton & K. Levitt & S. Walnum & C. Wee, & R. Yip. « GrIDS-A Graph-Based Intrusion Detection System for Large Network »s. Proc of the 19th National Information Systems Security Conference, 1996.

[22] B. White & E. A. Fisch, U. W. Pooch. « Cooperating Security Managers: A Peer- Based Intrusion Detection System ». IEEE Network Journal, pp. 20-23, January/February 1996.

[23] KAZAR Okba, OUENDJEN Mohammed El Fateh «Une approche agent pour la sécurité de système industriel distribué » thèse de magister informatique université de Ouargla 2016. [En ligne]. Disponible : http://dspace.univ-ouargla.dz/jspui/handle/123456789/10347

[24] K.Price « Intrusion Detection Pages ».Purdue University, 1998. [En ligne]. Disponible : http://www.cs.purdue.edu/coast/intrusion-detection/ids.html

[25] S. Staniford-Chen , « GrIDS Outline Design Document ». GrIDS Project Home Page at UC Davis'sComputer Science Department, 1997. [En ligne]. Disponible : http://olympus.cs.ucdavis.edu/arpa/grids/design.html

[26] De Castro .L.N & Von Zuben .F.J «Artificial Immune Systems: Part I - Basic theory and applications », Technical re port, TR-DCA-01/99, December 99.

[27] Larousse, Système Immunitaire. [En ligne]. Disponible : https://www.larousse.fr/encyclopedie/divers/syst%C3%A8me_immunitaire/60053#:~:text=.

[28] J. Timmis & T. Knight & L.N. De Castro & E.Hart, «An overview of Artificial immune Systems », Natural computation series, pages 51-86, Springer, 2004.

[29] J. Kim « Integrating Artificial Immune Algorithms for Intrusion Detection », PhD Thesis, University College London, 2002.

[30] Mirandole, 11 septembre 2020. Différence entre immunité innée et immunité adaptative. [En ligne]. Disponible : https://jeretiens.net/difference-entre-immunite-innee-et-immunite-adaptative/

[31] Système immunitaire. [En ligne]. Disponible : https://sante.journaldesfemmes.fr/fiches-sante-du-quotidien/2694047-systeme-immunitaire-definition-fonction-maladies-schema/

[32] Mon Système Immunitaire, Les organes du système immunitaire (11 juin 2014). [En ligne]. Disponible : https://www.monsystemeimmunitaire.fr/les-organes-du-système-immunitaire/

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

[34] Mathieu SIMON, 07 septembre 2009, Immunologie. Les cellules immunitaires et les organes lymphoïdes. [En ligne]. Disponible : https://www.cours-pharmacie.com/immunologie/les-cellules-immunitaires-et-lesorganes-lymphoides.html

[35] 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/

[36] Elisabeth Planchet, Sébastien Maugenest, CORPS HUMAIN ET SANTÉ. Août 2014. [En ligne]. Disponible :https://ressources.unisciel.fr/DAEU-biologie/P2/co/P2_chap5_c02.html

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

[38] Schema de la structure anticorps. [En ligne]. Disponible : https://www.researchgate.net/figure/Schema-de-la-structure-dun-anticorps_fig11_335460067

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

[40] Geraud CHANCELIN, Utilisation des produits biologique d'origine équine en thérapeutique humaine, 2007. [En ligne]. Disponible : https://www.memoireonline.com/01/08/863/m_utilisation-produits-biologiques-origine-equine-therapeutique-humaine16.html

[41] Katia Mayol, MICROBES, IMMUNITÉ 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-etvaccination/thematiques/cellules-immunes-et-organes-lymphoides/fiches-organes-et-tissus-lymphoides/lethymus.

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

[43] 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 deDoctorat, département d'informatique, université de Mohamed Boudiaf, Oran, 2016-2017.[En ligne]. Disponible: http://www.univ-usto.dz/theses_en_ligne/doc_num.php?explnum_id=2242

[44] L.N DE CASTRO, J I TIMMIS, Artificial immune system as a Novel Soft Computing paradigm, Computing laboratory, University of Kent at Canterbury, Soft Computing Journal, Vol 7 July, 2003.

[45] L. N. DE CASTRO, J. TIMMIS In Artificial Neural Networks in Pattern Recognition Artificial Immune Systems: A Novel Paradigm to Pattern Recognition, University of Paisley, UK, pp. 67-84, 2002.

[46] S. A. HOFMEYR, STEPHANIE FORREST, Immunity by Design; An Artificial Immune System, Dept. of Computer Science University of New Mexico, 2004.

[47] L N DE CASTRO, F J VON ZUBEN, Artificial immune systems: Part I – Basic theory and applications, Technical Report TR – DCA, Dec 1999.

[48] U. AICKELIN, P. BENTLEY, S. CAYZER, J. KIM, J. MCLEOD, Danger Theory: The Link between AIS and IDS?. Proceedings ICARIS-2003, 2nd International Conference on Artificial Immune Systems, pp 147-155, 2003

[49] Ammar Haboussi, Processus de sélection clonale, jun 2012. [En ligne]. Disponible : https://www.researchgate.net/figure/Processus-de-selection-clonale-37_fig7_3331058947

[50] theory, De Castro .L.N & Von Zuben .F.J «Artificial Immune Systems: Part I – Basic

[51] D. Dasgupta & Z.Ji & F.Gonzalez « Artificial Immune System (AIS) Research in the Last Five Years », IEEE.2003.

[52] Leandro Nunes De Castro and Jonathan Timmis.Artificial immune sys-tems : a new computational intelligence approach. Springer Science & Bu-siness Media, 2002.

[53] TIMMI S« artificial imm une systems: a novel data analysis tech nique inspired by the immune network theory », PhD thesis, university of wales, 2001.

[54] D. DASGUPTA«artificial immune systems and their application », pringer-verglas, 1999.

[55] 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, département des Sciences et technologies de l'information et de la communication, université PARIS-SACLAY, Paris,2016. [En ligne]. Disponible :
https://www.biblio.univ-evry.fr/theses/2016/2016SACLE026.pdf

[56] Pr. Philippe KOURILSKY, Immunologie moléculaire, Académie des SciencesCollège de France, 2007.

[57] S. FORREST, A. S. PERELSON, L. ALLEN, R. CHERIKURI, "self-nonself discrimination on a computer". in proceedings of IEEE symposium research in security and privacy, pp. 132-143, 1994.

[58] Meroua Yahiaoui, L`algorithme de la sélection négative. [En ligne]. Disponible : https://studylibfr.com/doc/3542742/l-algorithme-de-la-sélection-négative

[59] Mokhtar GHARBI, Optimisation grâce aux Systèmes Immunitaires Artificiels, le 3 février 2006. [En ligne]. Disponible :
https://docplayer.fr/1869644-Optimisation-grace-aux-systemes-immunitairesartificiels.html

[60] LOUATI Nour El-Houda, Réalisation d'un Système de Détection D'intrusion Basé Système immunitaire Artificiel, mémoire en vue de l'obtention du diplôme de Master, département de Mathématique et Informatique, université de 20 Aout 1955, Skikda ,2005-2006.

[61] Steven Hofmeyr « An immunological model of distributed detection and its application to computer security ». PhD thesis, University Of New Mexico, 1999.

[62] Philippe Biondi, Architecture expérimentale pour la détection d"intrusions dans un système informatique, 2001.

[63] IntrusionDetection System Using Feature Selection and classification Technique-Scientific Figure on ResearchGate, [accessed 9 Jun, 2023]. [En ligne].Disponible :
https://www.researchgate.net/figure/THE-41-FEATURES-IN-KDD99-DATASET_tbl1_275578491

[64] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, Edition McGraw-Hill 2004.