République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université larbiTebessi - Tébessa

FACULTE DES SCIENCES EXACTES ET DES SCIENCES DE LA NATURE ET DE LA VIE

DEPARTEMENT DE MATEMATIQUE ET INFORMATIQUE

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

Spécialité : réseau et sécurité informatique

Thème

Système de détection d'intrusion basé sur un système immunitaire artificiel

Présenté par :
- TOBBA Aicha
- ZEMALI Sana

Encadré par :
Dr. AHMIM Ahmed

Jury de soutenance :

Président TAG Samir

Examinateur MAHMOUDI Rachid

Promotion2016/2017

REMERCIEMENT

On remercie ALLAH le tout puissant, qui m'a donné la force et la patience pour l'accomplissement de ce travail.

Nous exprimons notre reconnaissance et remerciements à notre encadreur **Dr AHMIM Ahmed** pour son encadrement. Son expérience et ses qualités scientifiques ont toujours été sources d'enrichissement me permettant de mener à bien ce travail.

Aussi à tous les PROFESSEURS qui nous ont enseignés au cours des années universitaires pour l'obtention du diplôme master.

Nous remercions particulièrement avec gratitude l'Examinateur qui nous a fait l'honneur de prendre notre modeste travail en considération et en suite de le juger.

Nous tenons également à remercier les membres du jury **Mr MAHMOUDI Rachid**, **Dr TAG Samir** d'avoir accepté d'examiner et d'évaluer ce travail.

Enfin que tous ceux qui ont contribué de prés ou de loin, par leurs encouragements et conseils à l'accomplissement de ce travail, trouvent ici l'expression de ma profonde reconnaissance.

SANA & AICHA

ملخص

الإعلام الآلي هو مجال واسع جدا، وعدد نقاط الضعف الحالية في النظام قد تكون مهمة. وهكذا، فان الهجمات ضد نقاط الضعف يمكن أن تكون متنوعة وخطيرة جدا، لحماية البيانات أثناء الإرسال، يجب أن يكون هناك نظام أمني .

الأمن لا يمكن ضمانه مئة بالمئة، و هذه الأدوات ليست مثالية. لديهم دائما العيوب. لذلك تحتاج إلى استخدام أدوات أكثر فعالية لحماية أنظمة الكمبيوتر مثل أنظمة كشف التسلل. وهي وسيلة هامة تستخدم لحماية أنظمة الكمبيوتر.

الهدف الرئيسي من نظام كشف التسلل هو الكشف عن الاستخدام غير المصرح به وسوء الاستخدام وسوء المعاملة من أنظمة الكمبيوتر من قبل كل من المطلعين على النظام والمتسللين من الخارج والداخل. نظام كشف التسلل تحدد التوقيعات المشبوهة القائمة على عمليات الاقتحام وتحقيقات المعروفة.

الحل واعد هو استخدام جهاز المناعة الاصطناعية التي تعتمد على جهاز المناعة البشرية القادرة على كشف التسلل المعروفة سابقا وغير المعروفة والتي تتطور بسرعة.

في هذا العمل استخدمنا مفهوم الخطر والتفاعلات المناعية بين نظام المناعة الفطري وجهاز المناعة التكيفية القائمة لتحسين خوارزمية اختيار السلبية التي تقوم على نموذج الذاتية وغير الذاتية، للحصول على القدرة على الكشف عن العناصر الخطرة في النظام، يمكن للمتسلل تكون مكونات النظام إما داخلية أو خارجية.

الكلمات المفتاحية :حماية شبكة المعلومات، نظرية الخطر، نظام المناعة الاصطناعي، اكتشاف التدخلات.

.

Résumé

L’informatique étant un domaine très vaste, le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, les attaques visant ces failles peuvent être à la fois très variées et très dangereuses. Pour protéger les données durant leur transmission, il doit y avoir système de sécurité.

la sécurité ne peut pas être assurée à cent pour cent, et que ces outils ne sont pas parfaits. Ils possèdent toujours des failles. pour cela il faut utiliser outils plus efficaces pour protéger les systèmes informatiques tel que les systèmes de détection d’intrusion . les systèmes de détection d’intrusion est une méthode importante utilisée pour protéger les systèmes informatiques.

L'objectif principal de IDS est de détecter l'utilisation non autorisée, la mauvaise utilisation et l'abus des systèmes informatiques à la fois par les initiés du système et les intrus externes et internes. Les IDS les plus récents définissent des signatures suspectes fondées sur des intrusions et des sondes connues.

Une solution prometteuse est d’utiliser les systèmes immunitaires artificiels qui s’inspirent des systèmes immunitaires humains qu'il soit capable de détecter des intrusion préjudiciables précédemment connus et inconnus et en évolution rapide.

Dans le cadre de ce travail nous avons utilisé la notion de danger et les interactions immunitaires existantes entre le système immunitaire inné et le système immunitaire adaptatif pour améliorer l’algorithme de la sélection négative qui est fondé sur le modèle de soi et de non soi,afin d’obtenir la possibilité de détecter les éléments dangereux dans le système, ces intrus qui peuvent être soient des éléments internes ou externes du système.

Mots clés : sécurité informatique, théorie de danger, systèmes immunitaires artificiels,

Détection d’intrusions.

Abstract

Because computing is a very large domain, the number of vulnerabilities on a system can be significant. Thus, attacks against these faults can be both very varied and very dangerous. To protect data during transmission, there must be a security system.

Security can not be ensured one hundred percent, and these tools are not perfect. They always have flaws. For this you need to use more effective tools to protect computer systems such as intrusion detection systems. An intrusion detection system is an important method used to protect computer systems.

A promising solution is to use the artificial immune systems (AIS) inspired from the human immune system, which can detect and defend against harmful and previously unseen invaders.

The purpose of this work is the design and the realization of an IDS inspired from natural immune systems. We used the notion of danger and the existing immune interactions between the innate immune system and the adaptive immune system to improve the algorithm of negative selection that is based on self-model and non-self, In order to obtain the possibility of detecting the dangerous elements in the system, these intruders which can be either internal or external elements of the system.

Keywords: computer security, artificial immune systems, danger theory, intrusion detection.

LISTE DES FIGURES

LISTE DES TABLEAUX

GLOSSAIRE

Abréviation	signification
DNS	Domain Name System
IDS	Intrusion detection system
HIDS	Host Based Intrusion Detection System
NIDS	Network-based Intrusion Detection System
IDES	Intrusion Detection Expert System
MIDAS	Système de détection et d'alerte d'intrusions Multics
CPU	Central Processing Unit
NIDES	Next-generation Intrusion Detection Expert
SIB	Système immunitaire biologique
APC	Cellule de présentation antigène
MHC	Complexe Majeur Histocompatibilité
HLA	Human Leucocyte Antigène
APC	Cellules de présentation antigénique
SIA	Système immunitaire artificiel
AIS	Artificial immune system
Ag	Antigène
Ab	Antibody
AINET	Artificial Immune NETwork
BoW	Bag-of-Words
SBPH	Sparse Binary Polynomial Hashing
OSB	Orthogonal Sparse Bigrams

Problématique

Aujourd'hui, les systèmes informatiques occupent une place prédominante dans les entre prises, dans les administrations et dans le quotidien des particuliers. Ce phénomène a été catalysé, entre autres, par l'essor de l'Internet qui séduit chaque jour de plus en plus d'internautes par les nombreux avantages et la diversité des services rendus accessibles. Ils peuvent ainsi bénéficier à moindre coût de moyens de communication rapides, partager des ressources de traitement et de stockage de grandes capacités (Cloud Computing), faciliter les échanges commerciaux et financiers (e-Commerce, e-Banking), fournir et utiliser de nombreux services en ligne(e-Administration, e-Health, e-Learning, etc.), participer à des communautés virtuelles et à des réseaux sociaux, se divertir (e-Gaming, e-Television, etc.) et, plus généralement, partager et accéder à l'information. Notre dépendance croissante aux systèmes informatiques dans divers aspects de la vie quotidienne et leur omniprésence soulèvent inévitablement des questions quant à leur sécurité et à la sécurité des informations qui leurs sont confiées.

En dépit des efforts conséquents qui ont été investis depuis un certain nombre d'années pour tenter d'endiguer les problèmes de sécurité, force est de constater que le nombre de vulnérabilités dans les systèmes informatiques et, de surcroît, les activités malveillantes qui essaient et qui réussissent à les exploiter, continuent régulièrement à se multiplier. L'importance de sécurité des systèmes informatiques motive les angles divers de la recherche dont le but principal est de fournir de nouvelles solutions prometteuses qui ne pourraient être assurées par des méthodes classiques. Les systèmes de détection d'intrusions sont l'une de ces solutions qui permettent la détection des utilisations non autorisées, les mauvaises utilisations et les abus dans un système informatique par les utilisateurs externes ainsi que ses utilisateurs internes.

INTRODUCTION GÉNÉRALE

Introduction générale

Historiquement, internet a débuté par un réseau privé connectant les gouvernements, les militaires et les chercheurs académiques. C'est pourquoi il y avait de faibles besoins de protocoles sécurisés. A la base, on ne pensait pas au virus, au vers, au spam, au phishing, aux zombies, auxs pywares, aux attaques par déni de service, ... De plus, le coût de subir une telle attaque n'était pas significative. Petit à petit, le réseau s'est ouvert au monde et sa taille a empêché la création d'un mécanisme totalement sécurisé. De plus, une facilité venant des programmes tout faits et supportant une automatisation des attaques a permis de réaliser rapidement des agressions par n'importe qui.

Une attaque peut se faire par un individu ou un groupe de personnes, contre l'ordinateur d'un individu ou d'un groupe de personnes morale ou physique. La dépendance contemporaine de l'humain aux réseaux informatiques 1 a généré une motivation non seulement pour le goût de la réussite de l'exploit, mais aussi pour le gain d'argent, pour des convictions politiques, pour des buts militaires et pour la curiosité. La cause d'une faille dans un système peut être due à un manque de budget, de temps d'installation, de personnes qualifiées, de politique de sécurité, de protections efficaces sur le marché, . . . Néanmoins, de nos jours, le coût d'une attaque et de sa réparation 2 peut être très élevé. C'est pourquoi les entreprises et l'ensemble des organisations s'intéressent de près à la sécurité informatique.

Le concept de système de détection d’intrusions a été introduit en 1980 par James Anderson **[James P,Anderson,1980]**. Mais le sujet n’a pas eu beaucoup de succès. Il a fallu attendre la publication d’un modèle de détection d’intrusions par Denning en 1987 **[Dorothy E ,Denning,1987]** pour marquer réellement le départ du domaine.

La recherche dans le domaine s’est ensuite développée, le nombre de prototypes s’est énormément accru. Le gouvernement des États-Unis a investi des millions de dollars dans ce type de recherches dans le but d’accroître la sécurité de ses machines.

La détection d’intrusion est devenue une industrie mature et une technologie éprouvée :à peu près tous les problèmes simples ont été résolus, et aucune grande avancée n’a été effectuée dans ce domaine ces dernières années, les éditeurs de logiciels se concentrant plus à perfectionner les techniques de détection existantes.

Quelques voies restent cependant relativement inexplorées :

- Les mécanismes de réponse aux attaques,
- Les architectures pour les systèmes de détection d'intrusions distribués,
- Les standards d'interopérabilités entre différents systèmes de détection d'intrusion,
- La recherche de nouveaux paradigmes pour effectuer la détection d'intrusion.

Une des approches de la sécurité informatique est de créer un système complètement sécurisé, c'est la prévention. Mais il est très rarement possible de rendre un système complètement inattaquable pour plusieurs raisons.

- La plupart des systèmes informatiques ont des failles de sécurité qui les rendent vulnérables aux intrusions. Les trouver et les réparer toutes ne sont pas possible pour des raisons techniques et économiques.
- Les systèmes existants ayant des failles connues ne sont pas facilement remplacés par des systèmes plus surs, principalement parce qu'ils ont des fonctionnalités intéressantes que n'ont pas les systèmes plus surs, ou parce qu'ils ne peuvent pas être remplacés pour des raisons économiques.
- Déployer des systèmes sans failles est très dur voire impossible car des failles sont inconnues ou inévitables
- Même les systèmes les plus sûrs sont vulnérables aux abus de la part d'utilisateurs légitimes qui profitent de leurs privilèges où souffrent de la négligence des règles de sécurité par ceux-ci.

En réponse à ces difficultés pour développer des systèmes sécurisés, un nouveaumodèle de gestion de la sécurité des systèmes a émergé.

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

L'objectif principal de ces systèmes consiste à augmenter le taux de vrai positif c'est-à-dire la détection des intrusions réelles et à minimiser le taux de vrai négatif qui reflète le taux d'erreurs du système. 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.

PARTIE I ÉTAT DE L'ART

CHAPITRE 1 : SYSTÈME DE DÉTECTION D'INTRUSION

1.Introduction

De nos jours l’outil informatique est omni présent dans notre vie quotidienne. Que cesoit pour l’achat d’articles, faire des transactions bancaires, l’envoi de courrier ou encore laréservation de places de cinéma, nous dépendons énormément de cette technologie et nous nepouvons plus nous en passer.

L’arrivée d’Internet est définie comme l’âge d’or de l’informatique. Historiquement, internet a débuté par un réseau privé connectant les gouvernements, lesmilitaires et les chercheurs académiques. C'est pourquoi il y avait de faibles besoins de protocolessécurisés. A la base, on ne pensait pas au virus, au vers, au spam, au phishing, aux zombies, auxspywares, aux attaques par déni de service.... De plus, le coût de subir une telle attaque n'était pas significative. Petit à petit, le réseau s'est ouvert au monde et sa taille a empêché la créationd'un mécanisme totalement sécurisé. Par conséquent unecommunauté de gens malveillants s’est fondée et de nouveaux objectifs se sont créés tel que ledétournement d’informations, la percée des secrets personnels et cela peut aller jusqu'à ladestruction d’informations vitales.

L'idée intuitive de la sécurité informatique est de limiter l'accès à un systèmeinformatique. Avec une sécurité parfaite, les informations ne sont jamais compromises puisqu'un utilisateurnon-autorisé n'y a jamais accès. Néanmoins, la sécurité parfaite n'est pas réaliste. C'est pourquoion va essayer de prévenir, détecter et répondre à une attaqueafin de ne pas permettre qu'unemême agression se reproduise. La prévention permet de limiter les cas où une offensive se produit.

2. La sécurité informatique

De nos jours, La sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux a se connecter a Internet. et le transfert d'informations sensibles et le désir d'assurer la confidentialité d'un tel point essentiel dans le développement des réseaux informatiques**[jeanet al, 2000]**.

2.1. Définition :

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information.

« La raison principale de l'existence de l'industrie de la sécurité informatique est que les produits et services informatiques ne sont pas naturellement sûrs. Si les ordinateurs étaient protégés des virus, il n'y aurait pas besoin de produits antivirus. Si le mauvais trafic réseau ne pouvait être utilisé pour attaquer les ordinateurs, personne ne s'inquiéterait d'acheter un pare-feu. S'il n'y avait plus de dépassement de tampon, personne n'aurait besoin d'acheter des produits pour se protéger contre leurs effets. Si les produits informatiques que nous achetons étaient sûrs par défaut, nous n'aurions pas besoin de dépenser des milliards chaque année pour les rendre plus sûrs. » **[Bruce Schneider, 2007]**

2.2. Les fonctions principales de la sécurité informatique

Actuellement, l'information dans l'entreprise est une importance primordiale, ce qui rend sa protection est une fonction préliminaire. La sécurité des systèmes informatiques est devenue un défi majeur dont l'objectif est d'assurer la disponibilité des services, la confidentialité et l'intégrité des données et des échanges.

La sécurité informatique dépend de :

- **La confidentialité :** assurer que l'information n'est pas mise à disposition à des personnes, des entités ou des processus non autorisés.
- **L'intégrité :** assurer l'exactitude et la complétude de l'information pour éviter la modification non autorisée de données.

- **La disponibilité :** assurer que l'information est accessible et utilisable sur demande par une entité autorisée.
- **Le non répudiation** : assurer qu'une action d'une entité peut être liée uniquement à son initiateur**[OSI – Basic ,2000]**.

3. Les attaques

L'informatique étant un domaine très vaste, le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, les attaques visant ces failles peuvent être à la fois très variées et très dangereuses. C'est pourquoi nous allons dans un premier temps définir ce que nous appellerons « une attaque », puis dans un second temps, nous caractériserons ces attaques et observerons leur déroulement.

3.1. Une attaque, de quoi s'agit-il ?

Une attaque définie comme ensemble d'action qui peut porter atteinte à la sécurité des informations d'un système ou d'un réseau informatique**[Hung-Jen et al,2012].**

3.2. Classification des attaques

Tout acte sur un système dont l'intention est de nuire au moins à l'une des propriétés desécurité est qualifié de malveillant et constitue, de ce fait, une attaque surce système. Nous trouvons dans la littérature des manières différentes de classer les attaques **[James P,Anderson,1980].**

Certaines taxonomies les organisent en fonction d'un unique critère. Parmi ces critères, les plusrécurrents sont :

3.2.1. Première classification

Les attaques peuvent être classées en deux grandes catégories :

a. Les attaques passives :

Elles consistent à écouter sans modifier les données ou le fonctionnement du réseau. En généralement les attaques passives indétectables mais une prévention est possible.

b. Les attaques actives:

Elles consistent à modifier des données ou des messages, pour s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Une attaque active peut être exécutée sans écoute **[Johnet al,2012]**.

3.2.2. Deuxième classification

a. **Les attaques internes** :

Ce type d'attaque est causé :

- Soit par les utilisateurs autorisés du système qui essayent d'utiliser des privilègescomplémentaires dont ils n'ont pas le droit.
- Soit par les utilisateurs autorisés qui emploient improprement les privilèges dontils ont le droit.

b. Les attaques externes:

Ce type d'attaque est causé par des utilisateurs externes quiessayent d'accéder à des informations ou des ressources d'une manière illégitime et nonautorisée.

3.2.3. Troisième classification

a. Attaques agissant au niveau des systèmes logiciels

Les systèmes logiciels constituent un premier niveau d'abstraction à partir duquel un attaquantpeut mettre en défaut la sécurité d'un système informatique. Dans ce contexte, le termesystème logiciel doit être pris dans son sens le plus général. Il désigne tous types de logicielsdans un système informatique, couvrant aussi bien les programmes d'application, le systèmed'exploitation et son noyau, que les logiciels implantés (en anglais, firmware) dans les composantsmatériels. Une attaque, à ce niveau d'abstraction, repose alors soit sur l'utilisation d'unefonctionnalité logicielle légitime du système (éventuellement accessible grâce à une erreur dansla configuration logicielle), soit sur l'exploitation d'une fonctionnalité logicielle vulnérable àdes fins malveillante

b. Attaques agissant au niveau des systèmes matériels

Les systèmes matériels constituent un second niveau d'abstraction à partir duquel il estpossible de nuire à la sécurité d'un système informatique. Bien qu'il soit plus simple pour unattaquant de cibler directement les systèmes logiciels, nous observons qu'actuellement de plusen plus d'attaques s'appuient sur les systèmes matériels pour impacter indirectement le systèmelogiciel. Nous discernons deux raisons principales à cela. La première est que le fonctionnementdes systèmes logiciels repose sur les systèmes matériels. Ainsi, corrompre un systèmematériel signifie potentiellement corrompre tous les systèmes logiciels qui en dépendent pourleur exécution. Le fait que les systèmes matériels sont souvent soumis à des restrictions moinsdrastiques que les systèmes logiciels constitue une seconde raison. En effet, au niveau du matériel, il n'existe plus de notion de privilèges, d'isolation de processus, etc. Une attaque au niveaudes systèmes matériels agit alors soit sur les fonctionnalités matérielles qui ont été implémentéesen logique câblée, soit sur leur configuration matérielle.

c. Attaques agissant au niveau des canaux de communication

Les canaux de communication constituent un autre niveau d'abstraction à partir duquel unattaquant peut mettre en défaut la sécurité d'un système informatique. La notion de canal decommunication désigne ici tout type de médium de transmission d'information dont le rôle estd'acheminer des messages entre des systèmes qui interagissent, et couvre aussi bien les canauxde communication physiques que les canaux de communication logiques (par exemple, les mémoirespartagées, les fichiers partagés, etc.).

Une attaque, à ce niveau d'abstraction, repose alorssur des vecteurs d'attaque liés aux messages échangés entre les systèmes logiciels ou matérielsqui interagissent. Nous distinguons alors quatre vecteurs d'attaque possibles qui nécessitentpour l'attaquant un accès au canal de transmission : la destruction, la modification, la captationet l'insertion de messages, ces messages pouvant être soit cohérents, soit incohérents par rapportau protocole de communication.

d. Attaques agissant au niveau des canaux auxiliaires

L'environnement d'un système informatique constitue un dernier niveau d'abstraction àpartir duquel un attaquant peut porter atteinte à la sécurité de ce système. En particulier, unattaquant peut agir au niveau des canaux auxiliaires, c'est-à-dire les canaux autres que ceux généralementutilisés pour la transmission d'information. Une attaque, à ce niveau d'abstraction, peut alors consister à

analyser les canaux de fuite ou à injecter des fautes dans le système informatiquevia les canaux auxiliaires**[Landwehr et al. 1994]**.

3.3. Anatomie d'une attaque

Fréquemment appelés « les 5 P » dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate, Paralyze.

- **Probe** : consiste en la collecte d'informations par le biais d'outils comme whois, Arin, DNS lookup. La collecte d'informations sur le système cible peut s'effectuer de plusieurs manières, par exemple un scan de ports grâce au programme Nmap pour déterminer la version des logiciels utilisés, ou encore un scan de vulnérabilités à l'aide du programme Nessus.

- **Penetrate** : utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme le brute force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe. Une autre possibilité pour s'infiltrer dans un système est d'utiliser des failles applicatives que nous verrons ci-après ;

- **Persist** : création d'un compte avec des droits de super utilisateur pour pouvoir se ré-infiltrerultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex. : un cheval de Troie) ;

- **Propagate** : cette étape consiste à observer ce qui est accessible et disponible sur le réseau local ;

- **Paralyze** : cette étape peut consister en plusieurs actions. Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

Après ces cinq étapes, le pirate peut éventuellement tenter d'effacer ses traces, bien que cela ne soit rarement utile. En effet, les administrateurs réseau sont souvent surchargés de logs à analyser. De plus, il est très difficile de supprimer entièrement des traces**[Jonathan Krier, 2006]**.

3.4. Dispositifs destructeurs

Les dispositifs destructeurs sont utilisés pour paralyser, saturer ou détruire un système d'information. Ils constituent l'espèce la plus nuisible dans le domaine de la sécurité car ils peuvent être la source de perte de données.

3.4.1. Craquage des mots de passe.

Le cassage de mot de passe (en anglais : password cracking) est un procédé de recouvrement de mots de passe d'un système informatique.

Ce procédé permet ponctuellement d'aider un utilisateur du système à retrouver un mot de passe perdu ou d'obtenir le mot de passe d'une tierce personne. On se sert aussi de ce procédé pour obtenir des statistiques de fiabilité et de robustesse des mots de passe utilisés lors d'audits de sécurité.

3.4.2. Le virus

Le virus est un programme dont le seul but est de consommer ou de paralyser des ressources système. Le virus s'auto duplique pour mieux infecter le système, il se propage en infectant tour à tour les fichiers. Les effets d'une contamination varient : fichiers effacés, disque dur formaté, saturation des disques, etc.

La grande majorité d'entre eux existent sur les plates-formes Microsoft, ils infectent en particulier les fichiers COM ou EXE. De plus, de nouvelles formes sont apparues comme les macro-virus qui attaquent les fichiers de données (word ou excel).

Les systèmes UNIX ne sont pas épargnés ! Les administrateurs UNIX doivent faire face à des virus comme Winux. Néanmoins, la gestion des droits sous UNIX se révèle être un facteur limitant pour la propagation de virus.

Les virus sont de plus en plus évolués, ils peuvent s'automodifier pour échapper à une éventuelle détection (virus polymorphes). D'autres types peuvent tenter de leurrer le système en s'installant dans des secteurs défectueux ou non utilisés (virus furtifs) ...

3.4.3. Les vers

Les vers sont du même acabit que les virus, sauf qu'ils n'utilisent pas nécessairement un fichier pour se propager. Ils sont aussi capables de se dupliquer et de se déplacer au travers d'un réseau informatique. Les vers utilisent différents supports pour se propager.

Les vers simples utiliseront des failles propres à certains logiciels (exemple du ver de Morris en 1988 qui paralysa une grande partie de l'Internet).

Les macro-vers utiliseront les pièces jointes contenant des documents bureautiques infectés (exemple du ver Nimda).

Les vers d'email sont contenus dans une pièce jointe comprenant un code malicieux exécuté automatiquement par le logiciel de courrier électronique ou manuellement par l'utilisateur.

3.4.4. Les bombes logiques

Les bombes logiques sont aussi néfastes que les virus ou les vers et sont la cause de dégâts similaires. La différence est que la bombe logique a besoin d'un détonateur pour s'activer, c'est-à-dire qu'elle attend une date ou une action bien précise de l'utilisateur pour exploser.

3.4.5. Les attaques de déni de service (Denial of service)

Elles ont pour but de paralyser le serveurcible pour qu'il devienne inaccessible, au moins pour une durée de temps. De trèsnombreuses techniques existent pour épuiser les ressources d'un hôte cible, par exemple : ICMPFlooding, smurf, SYN flood, etc.

3.4.6. IP spoofing

Dans ce cas l'attaquant change son adresse IP par une autre adresse deconfiance afin d'obtenir des droits d'accès.

3.4.7. Les scans

Qui servent principalement à obtenir des informations sur un hôte, un réseau (pour préparer une attaque plus élaborée). Les informations qu'un attaquant peut obtenirsur le réseau sont par exemple : le type de système d'exploitation de la machine, les portsouverts, etc.

3.4.8. Les chevaux de Troie

Le principe du « Cheval de Troie» est facile à comprendre. Un programme ou un code malveillant est intégré à une application par ajout ou par modification de son code. Ainsi lors de l'exécution de ce programme inoffensif, le bout de code malveillant pourra exécuter des commandes spécifiques (récupération de fichiers de mot de passe, altération du système, etc.) à l'insu de l'utilisateur [**P.Kazienko, P. Dorosz ,2004**].

4. Système de détection d'intrusion

L'intrus est généralement vu comme une personne étrangère au système informatique qui a réussi à en prendre le contrôle, mais les statistiques montrent que les utilisations abusives proviennent le plus fréquemment de personnes internes ayant déjà un accès au système **[Richard heady et al.1990].**

La détection d'intrusion est le processus de surveillance des événements se produisant dans un système informatique ou un réseau et de les analyser pour les signes d'intrusions, définies comme des tentatives de compromettre la confidentialité, l'intégrité, la disponibilité ou de contourner les mécanismes de sécurité d'un ordinateur ou réseau. Les intrusions sont causées par les attaquants qui accèdent aux systèmes à partir d'Internet, les utilisateurs autorisés des systèmes qui tentent d'obtenir des privilèges supplémentaires pour lesquels ils ne sont pas autorisés et les utilisateurs autorisés qui abusent des privilèges qui leur sont donnés**[Rebecca Bace et Peter Mell,2001].**

4.1. Définition d'un système de détection d'intrusion

Le système de détection d'intrusion IDSest défini comme le produit logiciel ou matériel, qui concentre et identifie les incidents probables causés par les attaquants, surveille les informations sur ces intrusions, tente de les terminer et produit un rapport pour les administrateurs de sécurité en temps réel. Ainsi, le système de détection d'intrusion peut être considéré comme une opération de sécurité qui complète la protection, par exemple, pare-feu. Il contribue également à assurer la sécurité et la prévention contre les diverses intrusions causées par les attaquants**[Hussain Ahmad et al,2014].**

L'IDS (Intrusion Detection System) peut être vue comme un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Le premier modèle de détection d'intrusions générique a été proposé par Dorothy Denning en 1987. Il est indépendant de tout système et environnement d'application, les types d'intrusions et les vulnérabilités de système. Ce modèle se compose des éléments :

- **Sujets :** sont les initiateurs des activités sur le système, normalement les utilisateurs.
- **Objets:** sont les ressources gérées par les fichiers système tel que les commandes, les périphériques, les fichiers, les messages, etc.
- **Enregistrements audit :** généré par le système en réponse aux actions effectuées ou tentées par des sujets sur les objets, tel que connexion utilisateur, exécution de la commande, accès aux fichiers, etc.
- **Profils :** sont des structures qui caractérisent le comportement des sujets en termes de métriques statistiques et de modèles d'activité observée. Les profils sont automatiquement générés et initialisés à partir de modèles.
- **Les enregistrements d'anomalie :** ils sont générés quand un comportement anormal est détecté.
- **Les règles d'activité :** sont des actions à entreprendre lorsque de conditions sont satisfaites sur les enregistrements d'audit ou les enregistrements d'anomalies générés**[Dorothy E, Denning,1987].**

4.2. Modèle de processus de la détection d'intrusion

Il existe plusieurs types d'IDS disponibles aujourd'hui, caractérisés par différentes approches de suivi et d'analyse. Chaque approche présente des avantages et des inconvénients distincts. De plus, toutes les approches peuvent être décrites en termes de modèle générique de processus pour les IDS.**[Labed Ines.2006].**

IDS peuvent être décrits en termes de trois composants fonctionnels fondamentaux :

- **Sources d'information** : les différentes sources d'information sur les événements utilisées pour déterminer si une intrusion a eu lieu. Ces sources peuvent être tirées à partir de

différents niveaux du système, avec le réseau, hôte et la surveillance des applications les plus courantes.

- **Analyse :** la partie des systèmes de détection d'intrusion qui réellement organise et fait sens des événements dérivés des sources d'information, en décidant quand ces événements indiquent que des intrusions se produisent ou ont déjà eu lieu. Les méthodes d'analyse les plus courantes sont la détection basée connaissance et comportementale.

- **Réponse :** Ensemble d'actions que le système effectue lorsqu'il détecte les intrusions. Ceux-ci sont généralement regroupés en mesures actives et passives, avec des mesures actives impliquant une intervention automatisée de la part du système et des mesures passives impliquant la déclaration des résultats IDS aux humains, qui sont alors censés prendre des mesures sur la base de ces rapports**[LabedInes, 2006].**

4.3. Composants et architecture

Cette section décrit les principaux composants des solutions IDS et illustre les architectures de réseau les plus courantes pour ces composants.

4.3.1. Capteur ou Agent :

Les capteurs et les agents surveillent et analysent l'activité. Le terme de capteur est généralement utilisé pour les IDS qui surveillent les réseaux, y compris les réseaux, sans fil, et les technologies d'analyse de comportement réseau. Le terme agent est généralement utilisé pour les technologies IDS basées sur l'hôte.

4.3.2. Serveur de gestion :

Un serveur de gestion est un dispositif centralisé qui reçoit des informations des capteurs ou des agents et les gère. Certains serveurs de gestion effectuent une analyse sur les informations d'événement que les capteurs ou agents fournissent et peuvent identifier des événements que les capteurs ou agents individuels ne peuvent pas. L'association d'informations d'événement à partir de plusieurs capteurs ou agents, comme la recherche d'événements déclenchés par la même adresse IP, est appelée corrélation. Les serveurs de gestion sont disponibles en tant que produits d'appliance et de logiciels uniquement. Certains petits déploiements IDS n'utilisent pas de serveurs de gestion,

mais la plupart des déploiements IDS le font. Dans les déploiements IDS plus importants, il existe souvent plusieurs serveurs de gestion et, dans certains cas, il existe deux niveaux de serveurs de gestion.

4.3.3. Serveur de base de données :

Un serveur de base de données est un référentiel d'informations d'événements enregistrées par des capteurs, des agents et / ou des serveurs de gestion. De nombreux IDS prennent en charge les serveurs de base de données.

4.3.4. Console :

Une console est un programme qui fournit une interface pour les utilisateurs et les administrateurs de l'IDS. Le logiciel de console est généralement installé sur des ordinateurs de bureau ou portables standard. Certaines consoles sont utilisées uniquement pour l'administration IDPS, telles que la configuration de capteurs ou d'agents et l'application de mises à jour logicielles, alors que d'autres consoles sont utilisées strictement pour la surveillance et l'analyse. Certaines consoles IDS fournissent à la fois des capacités d'administration et de surveillance **[Karen Scarfone, Peter Mell,2007].**

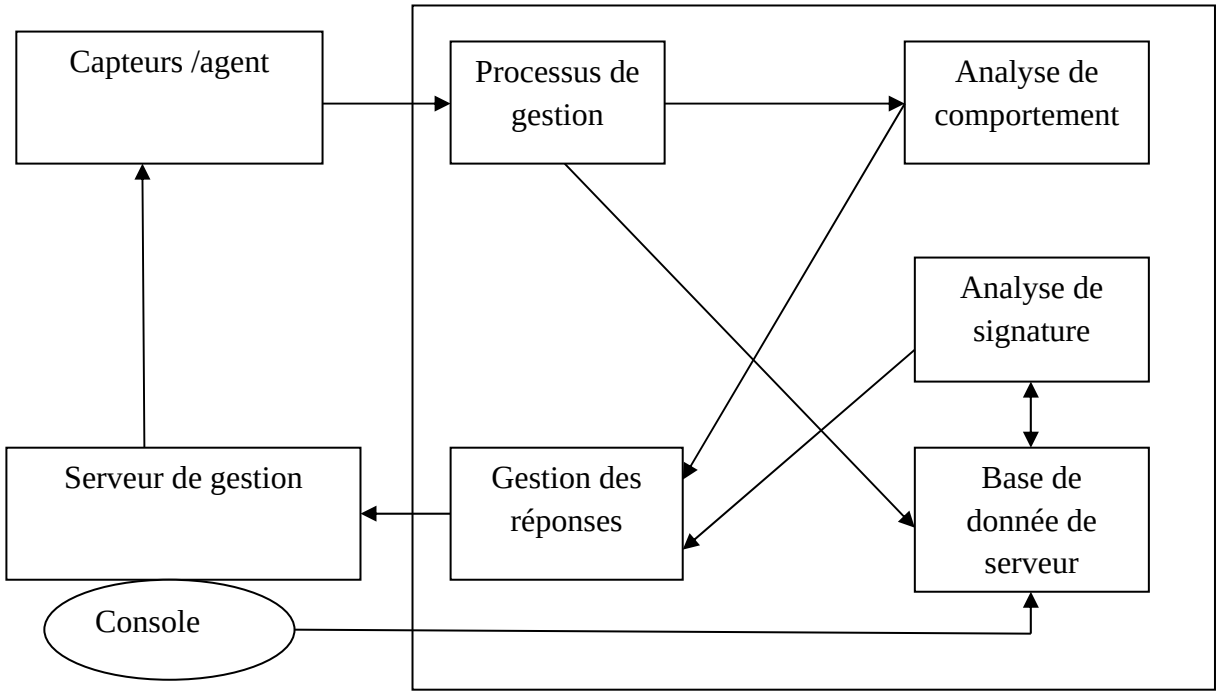

Figure 1.1: Architecture IDS**[F.Sabahi, A.Movaghar,2008].**

4.3.5.Analyse de signature et comportementale :

Les systèmes de détection d'intrusions peuvent être classés suivant leur approche d'analyse des données. Deux grandes approches ont été proposées dans la littérature : la détection d'intrusions par signature et la détection d'intrusions comportementale.

Ces deux approches s'opposent dans leur principe de détection : l'approche par signature se fonde sur la recherche de traces d'attaques ou d'intrusions alors que l'approche comportementale recherche les déviations du comportement de l'entité observée par rapport à un modèle du comportement normal de cette entité. Bien que la première approche proposée par Anderson en 1980 soit de type comportementale, nous allons d'abord présenter les approches par signature qui ont les faveurs des industriels de la sécurité mais présentent des inconvénients, inhérents à l'approche, difficilement contournables [**Dado, Guillaume,2003**].

4.4. Les fonctions de détection d'intrusion

Les fonctions de détection d'intrusion sont :

- **Observer et Surveiller**: Utilisé pour observer et surveiller les activités utilisateur, réseau et système pour les événements suspects.
- **Reconnaître les modèles**: a la capacité de reconnaître les modèles d'attaques.
- **Rapports sur les intrusions**: Préparer un rapport détaillé sur les événements capturés. Les administrateurs système utilisent ces rapports pour analyser les modèles d'activité anormaux, les configurations système et la configuration de sécurité pour déterminer les vulnérabilités.
- **Suivi de la violation des règles utilisateur**: permet de suivre les violations des règles utilisateur, d'évaluer l'intégrité des systèmes et des fichiers.
- **Enregistrement des événements**:
- en rencontrant une activité méfiante, l'IDSenregistre l'information rattachée à l'activité observée.
- **Alerte des Administrateurs de Système** : l'IDS envoient des alertes à l'Administrateur de Système via les pages Web, les e-mails, les messages etc., quand tout événement méfiant survient sur une base de données**[Hussain Ahmad et al,2014]**.

5. Classification des systèmes de détection d'intrusion

Il existe plusieurs critères qu'on peut utiliser pour classifier les différents systèmes de détection d'intrusion, dont les principaux sont résumés dans la **Figure 1.2.**

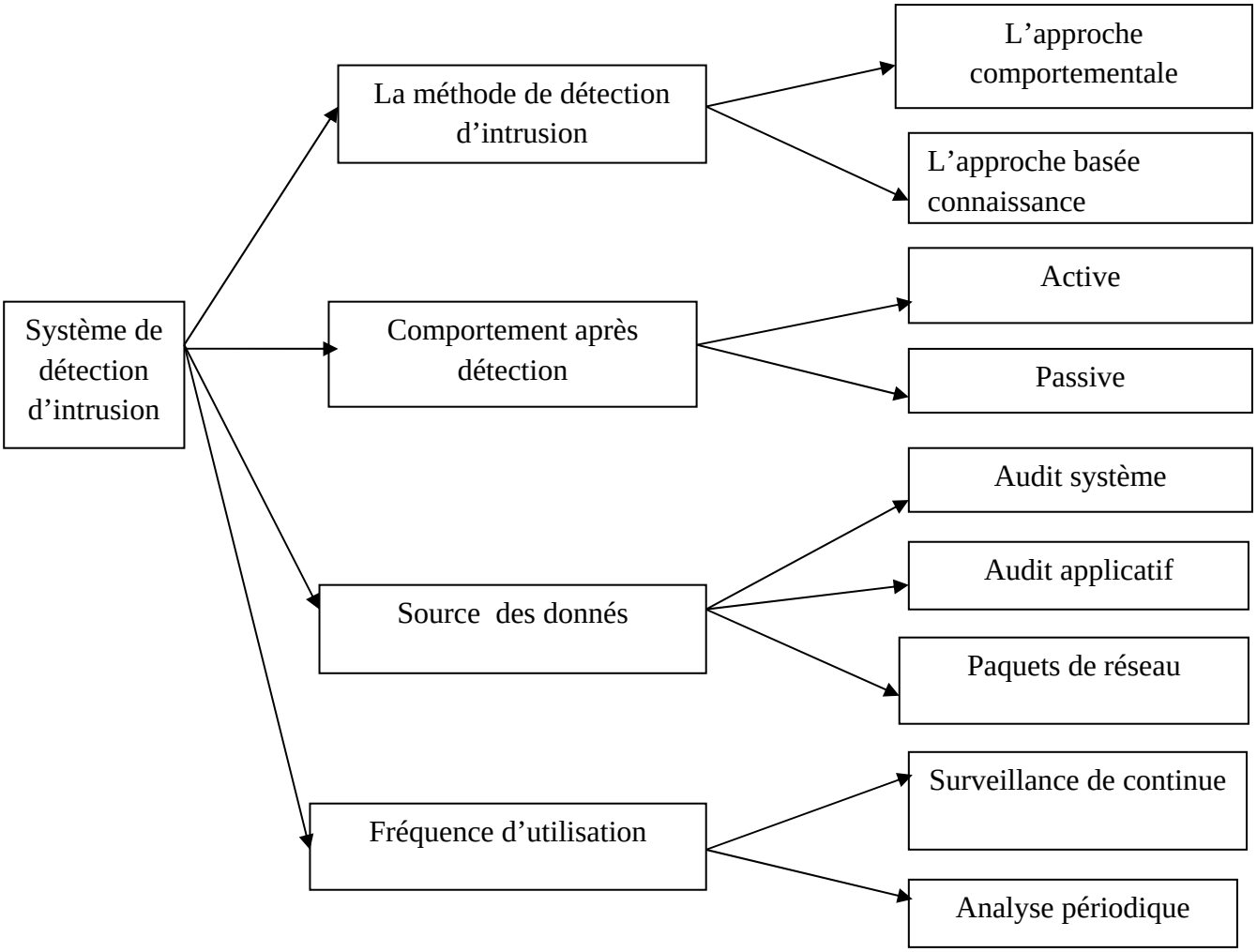

Figure 1.2: Taxonomie des systèmes de détection d'intrusion [**H. Debar et al, 2000]**

5.1. La méthode de détection

Les méthodes de détection d'intrusion sont classées en deux catégories principales :

5.1.1. L'approche basée connaissance

L'approche basée connaissance est également appelée détection basée sur une signature ou sur une règle, qui compare les signatures des menaces connues à des événements observés pour identifier les incidents. Ceci est très efficace pour détecter les menaces connues **[Hussain Ahmad et al,2014]** Mais il échoue facilement lorsqu'on fait face à des intrusions inconnues. La meilleur façon de résoudre ce problème est de mettre à jour régulièrement la base de connaissances manuellement, ce qui prend un temps et est laborieux, ou automatiquement avec l'aide d'algorithmes d'apprentissage supervisés. **[F.Sabahi, A.Movaghar,2008].**

a.Les avantages de l'analyse basée connaissance

- La méthode la plus simple et la plus efficace pour détecter les attaques connues.
- Une analyse contextuelle détaillée.

b. Les inconvénients de l'analyse basée connaissance

- Inefficace pour détecter des attaques inconnues, des attaques d'évasion et des variantes d'attaques connues.
- Peu de compréhension des états et des protocoles.
- Difficile de garder les signatures et les modèles à jour.
- Consommer du temps pour maintenir les connaissances **[Hung-Jen Liao et al,2012].**

5.1.2. L'approche comportementale

L'approche comportementale est également appelée détection anomalie, qui compare les définitions de ce que l'activité est considérée comme normale contre les événements observés pour identifier les écarts significatifs. Cette méthode utilise des profils qui sont développés en surveillant les caractéristiques de l'activité typique sur une période de temps. L'IDS compare alors les caractéristiques de l'activité courante aux seuils liés au profil. Les méthodes de détection basées sur les anomalies peuvent être très efficaces pour détecter des menaces précédemment inconnues

[Hussain Ahmad et al,2014].

a. Les Avantages de l'analyse comportementale

- Efficace pour détecter les vulnérabilités nouvelles et imprévues.
- Moins dépendant du système d'exploitation.
- Faciliter la détection des abus de privilège.

b. Les inconvénients de l'analyse comportementale

- Précision des profils faibles en raison de l'évolution constante des événements observés.
- Indisponible lors de la reconstitution des profils de comportement.
- Difficile de déclencher des alertes au bon moment**[Hung-Jen Liao et al,2012].**

5.2. Le comportement après la détection d'intrusions

5.2.1. Réaction active:

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

5.2.2. Réaction passive:

Dans ce cas, quand une attaque est détecter, le système de détection d'intrusion génère seulement une alarme pour notifier l'administrateur d'un événement malveillant ,sans aucune contre-mesure**[F.Sabahi, A.Movaghar,2008].**

5.3. La nature des données analysées

La source de données utilisée est une caractéristique essentielle pour classer les IDSs, Ces données peuvent être utilisées pour confirmer la validité des alertes, enquêter sur les incidents et corréler les événements entre l'IDS. On distingue trois de sources d'informations :

5.3.1. Les audits systèmes:

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

a. 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 systèmes.

b. Accounting :

L'Accounting fournit des informations sur l'usage des ressources partagées par les utilisateurs. Ces ressources sont par exemple : l'espace disque, le temps processeur, les applications lancées, la mémoire, etc.

c. Systèmes d'audit de sécurité :

Les pistes d'audit de sécurité représentent des enregistrements qui contiennent toutes des événements importants sur toutes les actions effectuées par un utilisateur, les associer à des utilisateurs et assurer leurs collectes dans un fichier d'audit.

5.3.2. Les sources d'informations réseau

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

5.3.3. Les audits applicatifs

Dernier 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. Généralement ils sont intégrés dans les IDS basés hôte « host based intrusion systems » Le trafic réseau **[NIST, 2001].**

5.4. Temps de détection

Pour détecter une intrusion les IDS besoin le temps, ce dernier est divise en deux groupes principaux:

5.4.1. Surveillance en temps réel

Tentent de détecter les intrusions en temps réel ou presque en temps réel. Ils fonctionnent sur des flux de données continues provenant de sources d'information et analysent les données pendant

que les sessions sont en cours (par exemple, des sessions réseau pour la détection d'intrusion réseau, des sessions de connexion pour la détection d'intrusion basée sur l'hôte). Les IDS en temps réel doivent déclencher une alarme dès qu'une attaque est détectée, de sorte qu'une action qui affecte la progression de l'attaque détectée peut être prise. La plupart des IDS commerciales revendiquent une capacité de traitement continu.

5.4.2. Surveillance périodique

Effectuent une analyse post-analyse des données d'audit. Cette méthode d'analyse des données d'audit est courante chez les analystes de la sécurité qui examinent souvent le comportement du réseau, ainsi que le comportement des différents attaquants, en mode hors ligne (batch). Beaucoup de premiers IDS basés sur l'hôte ont utilisé ce schéma de synchronisation, puisqu'ils utilisaient des pistes d'audit de système d'exploitation qui étaient enregistrées en tant que fichiers **[H. Debar et al, 1999]**

6. Types de systèmes de détection d'intrusions

6.1. Host Based Intrusion Detection System (HIDS)

Le H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Solaris, Linux, HP-UX, Aix, etc… Le H-IDS se comporte comme un démon ou un service standard sur un système hôte. Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs (syslogs, messages, lastlog, wtmp…) et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de troie, tentatives d'accès non autorisés, exécution de codes malicieux, attaques par débordement de buffeurs…).

Un HIDS se base sur une unique machine, n'analysant cette fois plus le trafic réseau, mais l'activité se passant sur cette machine. Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.

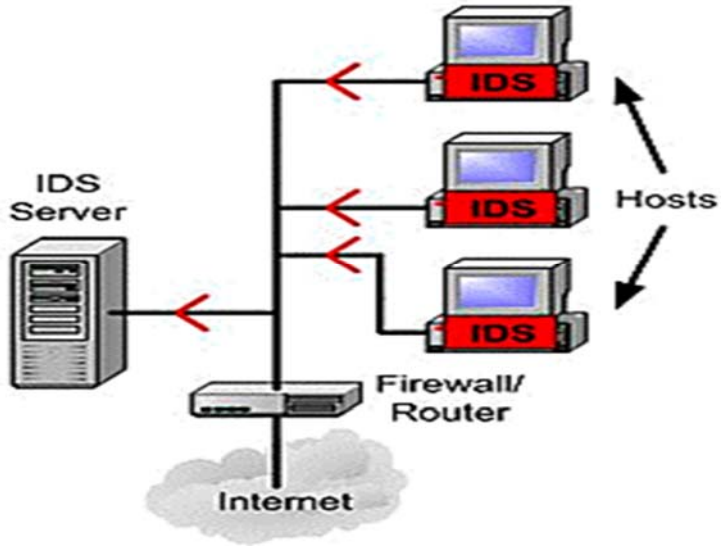

Figure1.3:L'architectureHost Based Intrusion Detection System**[Seth Fogie,Cyrus Peikari, 2002]**

6.2. Network-based Intrusion Detection System (NIDS)

Un N-IDS 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.**[Karen Scarfone,Peter Mell,2007]**

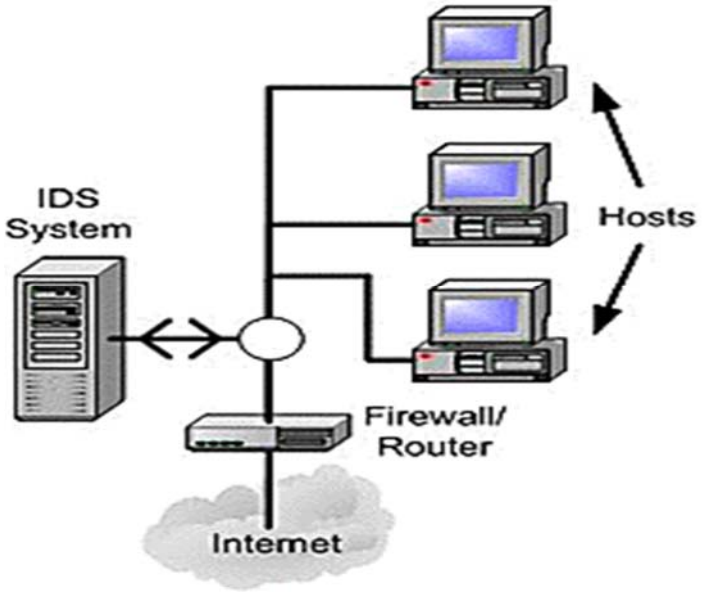

Figure1.4:l'architectureNetwork-based Intrusion Detection System (NIDS)**[Seth Fogie,Cyrus Peikari, 2002]**

7. Les architectures 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 **[W. Jansen et al, 2000]**: **centralisée, hiérarchique** et **distribuée.**

7.1. L'approche centralisée

Les premières mises en œuvre des systèmes de détection d'intrusions ont employé une architecturecentralisée 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 **[Mykerjee et al,1994].**

7.2. L'approche hiérarchique

Cette approche a été proposée pour surmonter les problèmes de l'approche centralisée. 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. **[S. Staniford-Chen,1997]**

7.3. L'approche 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 **[B. White et al, 1996]**.

8. Les méthodes de détection

Pour bien gérer un système de détection d'intrusions, il est important de comprendre comment celui-ci fonctionne. Une question simple se pose alors : comment une intrusion est-elle détectée par un tel système ? Quel critère différencie un flux contenant une attaque d'un flux normal ?

Ces questions nous ont amenés à étudier le fonctionnement interne d'un IDS. De là, nous en avons déduit deux techniques mises en place dans la détection d'attaques. La première consiste à détecter des signatures d'attaques connues dans les paquets circulant sur le réseau. La seconde, consiste quant à elle, à détecter une activité suspecte dans le comportement de l'utilisateur.

Ces deux techniques, aussi différentes soient-elles, peuvent être combinées au sein d'un même système afin d'accroître la sécurité.

8.1. L'approche par scénario (misusedetection)

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IDS est purement réactif ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour fréquentes. De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniquees dites "d'évasion" qui consistent à maquiller les attaques utilisées. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'IDS**[Dado et Guillaume,2003]**.

8.1.1. Techniques basées sur des règles

Système expert basé sur la règle est l'une des premières techniques utilisées pour la détection de mauvaise utilisation (L'approche par scénario). Les systèmes experts encodent les scénarios intrusifs sous la forme d'un ensemble de règles, qui sont comparées aux données d'audit ou de trafic réseau. Tout déviation dans le processus d'appariement des règles est signalé comme une intrusion. Les exemples de systèmes à base de règle incluent MIDAS (système de détection et d'alerte d'intrusions Multics), le système IDES (Intrusion DetectionExpert System) et le système expert NIDES (Next-generation Intrusion Detection Expert)**[Ghorbani et al ,2010].**

8.1.2.Analyse des transitions d'états

Les techniques basées sur l'état détectent les intrusions connues en utilisant des expressions de l'état du système et des transitions d'état. Les modèles d'état simplifient la spécification des patterns pour les attaques connues et peuvent être utilisés pour décrire les scénarios d'attaque plus facilement que les langages basés sur des règles. Dans les techniques basées sur l'état, les activités contribuant aux scénarios d'intrusion sont définies comme des transitions entre les états du système, et donc les scénarios d'intrusion sont définis sous la forme de diagrammes de transition d'état. La figure représente un diagramme d'état générique; Un nœud représente un état du système et un arc représente une action.

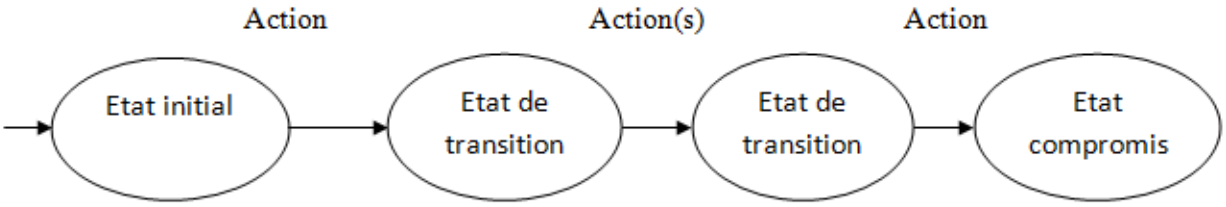

Figure 1.5: Diagramme générique de transition d'état**[Ghorbani et al,2010].**

L'état du système est fonction des utilisateurs ou des processus. Les scénarios d'intrusion définis par le diagramme de transition d'états incluent trois types d'états, à savoir l'état initia, l'état de transition et l'état compromis. Un état initial se réfère au début de l'attaque, alors qu'un état compromis représente l'achèvement réussi de l'attaque. Les états de transition correspondent aux états successifs se produisant entre un état initial et un état compromis. Une intrusion se produit si et seulement si un état compromis est finalement atteint **[Ghorbani et al,2010].**

8.2. L'approche comportementale (AnomalyDetection)

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

Cette technique peut être appliquée non seulement à des utilisateurs, mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion.

Cependant elle possède quelques inconvénients :

- **Peu fiable** : tout changement dans les habitudes de l'utilisateur provoque une alerte ;
- **Nécessite une période de non-fonctionnement** pour mettre en œuvre les mécanismes d'autoapprentissage : si un pirate attaque pendant ce moment, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement mis en place ;
- **L'établissement du profil doit être souple** afin qu'il n'y ait pas trop de fausses alertes : le pirate peut discrètement intervenir pour modifier le profil de l'utilisateur afin d'obtenir après plusieurs jours ou semaines, un profil qui lui permettra de mettre en place son attaque sans qu'elle ne soit détectée.

Plusieurs approches peuvent être utilisées pour la méthode de détection comportementale :

8.2.1. Approche probabiliste

Cette approche est quelquefois qualifiée de bayésienne : les réseaux bayésiens permettent de modéliser des situations dans lesquelles la causalité joue un rôle, mais où la connaissance de l'ensemble des relations entre les phénomènes est incomplète, si bien qu'il est nécessaire de les décrire de manière probabiliste. Ainsi, pour chaque élément du profil, on spécifie la probabilité de chaque évènement susceptible de se produire par la suite. Les indications obtenues progressivement sur l'état du système modélisé influent sur la confiance que l'on accorde à une proposition donnée.

Une alerte pourra être générée quand le nombre d'évènements ne correspondant pas aux probabilités définies aura dépassé un certain seuil sur une période donnée. Il est capital pour l'administrateur d'un système utilisant cette méthode de suivre l'évolution du gabarit dans le temps et de s'assurer que celui ci se conforme aux habitudes de travail des utilisateurs, sans quoi le taux de

faux positifs (alerte remontée ne correspondant pas réellement à une attaque) risque d'être très élevé**[Didier Marcant et Cédric, 2005].**

8.2.2. Approche statistique

Dans cette approche, le profil est établi en observant la valeur de certains paramètres du système considéré comme des variables aléatoires. Pour chaque paramètre du système, un modèle statistique est utilisé pour établir la distribution de la variable aléatoire correspondante. Une fois le modèle établi, un vecteur distance est calculé entre le flux d'événements observés et le profil. Si la distance dépasse un certain seuil, une alerte est émise.

Les premiers IDS utilisant un modèle statistique comme, par exemple, celui proposé par Anderson ou IDES (Intrusion Detection Expert System) ciblent la détection de comportements anormaux d'utilisateurs en étudiant des paramètres comme le temps processeur, la durée des sessions, le nombre de tentatives de login, etc. NIDES (Next Intrusion Detection Expert System) propose des améliorations par rapport à IDES en combinant les approches comportementales et par signature et étend cette approche à la modélisation statistique d'applications**[Frédéric Majorczyk , 2008].**

8.2.3. Réseaux de neurones

Les réseaux neuronaux sont utilisés pour leur rapidité de traitement et leur relative résistance aux informations incomplètes ou déformées. les utilise de deux manières différentes. Ils sont d'abord utilisés comme filtres pour filtrer et sélectionner les parties suspectes dans les données d'audit. Celles-ci sont ensuite analysées par un système expert. On peut ainsi réduire les fausses alarmes, et on peut même augmenter la sensibilité du système expert car il ne travaille que sur des données suspectes. Puis ils sont utilisés de façon à prendre seuls la décision de classer une séquence d'événements comme malveillante**[Philippe Biondi, 2001].**

8.2.4. Approche immunologique

L'approche immunologique tente de calquer le comportement du système immunologique pour faire la différence entre ce qui est normal (le soi) et ce qui ne l'est pas (le non-soi). Le système immunologique montre en effet beaucoup d'aspects intéressants comme son mode d'opération distribué (il n'y a pas de système de contrôle central) qui lui permet de continuer à fonctionner

même après des pertes, sa capacité à apprendre automatiquement de nouvelles attaques pour mieux réagir les prochaines fois qu'elle se présente, sa capacité à détecter des attaques inconnues, etc.

On peut voir l'approche immunologique de la détection d'anomalies comme une méthode de détection d'anomalie où l'on utilise les techniques de détection des malveillances. En effet, les techniques de détection d'anomalie connaissent ce qui est bien et vérifient en permanence que l'activité du système est normale, alors que les techniques de détection de malveillance connaissent ce qui est mal et sont à sa recherche. L'approche immunologique propose de rechercher ce qui est mal en connaissant ce qui est bien. On devrais même dire que l'approche propose de rechercher ce qui n'est pas bien, et l'on peut se permettre la comparaison avec la notion de tiersexclus en logique : on n'obtient pas ce qui est mal en prenant la négation de ce qui est bien. Cependant, les résultats obtenus sont satisfaisants**[philippeBiondi, 2001].**

8.3. Les méthodes répandues / Hybrides

Cette approche consiste en la sérialisation d'un IDS comportemental suivi d'un IDS par signature. L'IDS comportemental permet de filtrer les requêtes normales et ainsi seules les requêtes anormales sont passées à l'IDS par signature. Bien que l'IDS comportemental utilisé soit simple, ceci permet de réduire le nombre de faux positifs générés globalement. La source d'entrées est le fichier d'audit du serveur web. Cet IDS est donc soumis aux mêmes problèmes que les autres utilisant cette source de données **[Frédéric Majorczyk , 2008].**

9. Conclusion

Les réseaux constituent la plateforme de toutes les activités quotidiennes du mondeentier, cette technologie présente des vulnérabilités qui peuvent causés plusieurs typesd'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 nousavons également étudié d'une manière détaillée les différents types d'IDS selon différentscritères de classification avec la présentation générale des différentes techniques utiliséespour la détection d'intrusions.

Chaque jour de nouvelles techniques d’attaques apparaissent, et avec chaque évolutiontechnologique dans le domaine des réseaux et systèmes. Et cela à donner la nécessité dediversifier les dispositifs de protection contre ces menaces. De dispositif de sécurité passif(filtres, alarmes, proxy), à des dispositifs de sécurité actifs (systèmes de surveillance, systèmes de détection d’intrusion).

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

CHAPITRE 2 : LE SYSTÈME IMMUNITAIRE ARTIFICIEL

1. Introduction

Toutes les créatures vivantes sont dotées par un système immunitaire, par exemple quelquesplantes ont des épines protectrices pour fournir la protection de prédateurs qui les attaquent.

Le système immunitaire biologique constitue une arme contre des intrus dans un corps donné. Pour ce faire, il existe plusieurs cellules qui contribuent à éliminer ces intrus nommé antigènes. Ces cellules participent pour ce qu'on appelle une "**Réponse Immunitaire Biologique**" **[Hiba Khelil,A. Benyettou ,2010**].

Le système immunitaire protège l'organisme contre l'invasion de corps étrangers. Il est constitué de cellules différentes réparties dans tout l'organisme. Chaque catégorie de cellules à une fonction spécifique et se déplace dans l'organisme selon les besoins.

Le système immunitaire naturel est assez compliqué pour qu'une simulation artificielle soit réalisée d'une façon complète. Par contre, les chercheurs ont réussi à simuler les fonctions les plus pertinentes dans un système immunitaire biologique pour que l'artificiel hérite le maximum des fonctionnalités naturelles dans le domaine de la reconnaissance des formes **[Goodman D et al,2002].**

2. Vocabulaire et définition

- **Cellule** :

  C'est l'unité structurale et fonctionnelle de tous les êtres vivants.

- **Antigène :**

Toute molécule capable de stimuler le système immunitaire.

- **Thymus** :

C'est un organe situé dans la région supérieure de la poitrine et à laquelle certains globules blancs (cellules T) migrent après avoir été produits par la moelle osseuse **[De castro L.N,Von Zuben .F.J ,2000].**

- **Cellule de présentation antigène (APC)**:

C'est un type particulier de globine blanc du sang dont le rôle principal est la digestion des intrus caches a l'intérieur des cellules pour les présenter aux lymphocytes.

- **ComplexeMajeur Histocompatibilité (MHC)** :

Le rôle de la molécule MHC consiste à rassembler les fragments de protéines cachés à l'intérieur des cellules pour les présenter sur la surface de cette cellule infectée afin de permettre leur identification par les cellules T.

- **Antigène de soi :**

C'est représenté par l'ensemble des molécules résultant de l'expression de son génome. L'individualité biologique de l'être vivant est surtout définie par la présence, dans les membranes cellulaires, de molécules le plus souvent protéiques. Ces marqueurs cellulaires forment le système **HLA**(Human Leucocyte Antigène) et sont le résultat de l'expression des antigènes d'histocompatibilité**.**

- **Antigène de non soi :**

C'est l'ensemble des molécules différentes du soi qui, présentes dans l'organisme, vont déclencher des réactions immunitaires. Elles peuvent être issues du milieu extérieur (vers, virus, bactéries, toxines…) ou être simplement des molécules du soi modifiés (ex : cancer).

- **Tolérance de soi :**

Si le système immunitaire n'est pas tolérant au soi, donc une réponse immunitaire sert déclenchée contre les cellules de soi causant la maladie de l'auto-immunité**[De castro.LN,2001].**

- **Affinité**:

C'est le degré de liaison entre le récepteur d'une cellule et l'antigène.

- **Clonage :**

Dans le domaine de biotechnologie, le clonage désigne la reproduction en laboratoire de gènes, cellules ou organismes à partir d'une même entité originale.

3. Système immunitaire biologique (SIB)

3.1. Définition

Le système immunitaire est un système de défense remarquablement adaptatif qui nousprotège des pathogènes aussi variés que les virus, les bactéries, les champignons et lesparasites. Il est composé d'une multitude de cellules et de molécules composant un réseaudynamique capable de reconnaître spécifiquement et d'éliminer un grand nombre de microorganismesétrangers **[Ying Tan,2016].**

Le système immunitaire sert de défense contre les organismes étrangers s'introduisant à l'intérieur d'un individu. Ce système de défense est capable de discriminer entre ce qui lui appartient et ce qui doit être détruit. Ilreprésente un mécanisme d'identification capable de percevoir et de combattre ledysfonctionnement de ses propres cellules et les micro-organismes exogènes infectieux quienvahissent le corps **[De Castro .L.N & Von Zuben .F.J,1999].**

3.2. Classification des systèmes immunitaires biologiques

Bien que l'on fasse référence au système immunitaire, il est important de mentionnerqu'il existe deux systèmes de l'immunité, l'immunité innée et l'immunité adaptative qui nécessite de collaborer pour protéger l'organisme. **[Timmis et al.2000].**

3.2.1. L'immunité innée

L'immunité innée est l'ensemble des mécanismes cellulaires et moléculairespréexistants à une infection dans un organisme.

Cette première ligne de défense, très efficace, empêche la plupart des infections de sepropager et permet ainsi d'éliminer l'agent infectieux dans les quelques heures qui suivent sarencontre avec l'organisme. Il est phylogénétiquement le plus ancien mécanisme de défense contre les microbes et est présent dans tous les organismes multicellulaires, y compris les plantes et les insectes. L'immunité innée sert deux fonctions principales.

De prime abord, le système immunitaire utilise ses barrières physiques. En effet, lepremier obstacle rencontré par les pathogènes sont les barrières anatomiques protectrices del'hôte. C'est l'exemple de la peau et de la surface des muqueuses qui constituent des barrièresefficaces contre l'entrée de la plupart des microorganismes. L'acidité de l'estomac et de latranspiration empêche également le développement des organismes incapables de sedévelopper dans des conditions acides. Les enzymes, comme le lysozyme, qui sont présentesdans les larmes peuvent également contribuer à cette défense en altérant la paroi cellulaire decertaines bactéries.

Le système immunitaire inné est caractérisépar **[J. Kim,2002] [J. Timmis et al,2004]** :

- Les mécanismes de détection des organismes étrangers sont constants, aussi bien pour lesinfections répétées.
- La réponse du système immunitaire inné est non spécifique à un type particulier d'intrusmais 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 immunitaireadaptative.

3.2.2. L'immunité adaptative.

Cependant, il arrive que l'immunité innée ne soit pas suffisante et que le pathogèneparvienne à échapper à cette première ligne de défense. Ainsi, afin de reconnaître etd'éliminer cette fois-ci sélectivement les pathogènes, il existe une seconde forme d'immunité, connue sous le nom d'immunité adaptative, dépendante de l'immunité innée, qui se met enplace quelques jours après l'infection initiale.

Le système immunitaire adaptatif se compose des cellules extrêmement spécialisées qui ont la capacité de s'adapter à la menace de micro-organismes pathogènes nouveaux et divergents. On croit que l'immunité adaptative a évolué dans les vertébrés sermonnés, puisqu'il n'est pas trouvé dans les espèces évolutionnettement lointaines, qui possèdent seulement un système immunitaire inné. Les principaux types de cellule qui constituent l'immunité adaptative sont **des cellules T** tirées de thymus et **des cellules B** tirées de la moelle osseuse. Ces cellules sont capables de reconnaître une

multitude de différents antigènes étrangers d'une façon très précise, qui a mené certains à appeler le système immunitaire adaptatif comme le système immunitaire spécifique **[Anass khanouss et al, 2005].**

Le système immunitaire adaptatif estcaractérisé par **[J. Timmis et al ,2004] [J. Kim,2002].**

- Le système immunitaire adaptatif s'occupe avec les intrus qui ne sont pas détectés par lesystème immunitaire inné.
- Le système immunitaire adaptatif est généré dynamiquement contre les organismesétrangers pendant sa durée de vie. Il fournit des mécanismes plus efficaces qui serontadaptés 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 desintrus déjà rencontrés lors des prochaines rencontres.

3.3. Comment le système immunitaire protège le corps humain?

Notre corps est protégé par une collection diverse des cellules et des molécules quicollaborent contre n'importe quelle molécule étrangère comme les bactéries ou d'autresenvahisseurs. La figure ci-dessous présente une version simplifiée des mécanismes de base dedéfense immunitaire (figure 2.1), et qui peuvent être résumés par les étapes suivantes :

- Quand un intrus envahit le corps, les cellules de présentation antigénique (APC[1]) commeles macrophages procèdent à l'ingestion et la digestion de l'antigène rencontré pour leprésenter comme des fragments de peptides antigéniques.
- Ces peptides seront liées avec les molécules MHC pour permettre leurs liaisons avec lescellules T qui ont la capacité de reconnaître la combinaison de peptide / MHC.
- Les cellules T activées par cette identification produisent et sécrètent des lymphokines oudes signaux chimiques pour mobiliser d'autres composants du système immunitaire.
- Les cellules B qui ont aussi des molécules de récepteur complémentaires répondent à cessignaux. A la différence des récepteurs de cellules T, ceux de cellules B peuventreconnaître les parties d'antigènes libres sans les molécules MHC.

[1]**APC** est un type particulier de globine blanc du sang dont le rôle principal est la digestion des intruscachés à l'intérieur des cellules pour les présenter aux lymphocytes.

- Après cette activation, les cellules B prolifèrent et se différencient et sécrètent desprotéines d'anticorps.
- La liaison entre les anticorps et les antigènes disponibles mènent à la destruction et lasuppression des antigènes.
- 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 foisdans l'avenir **[De Castro L. N, 2001].**

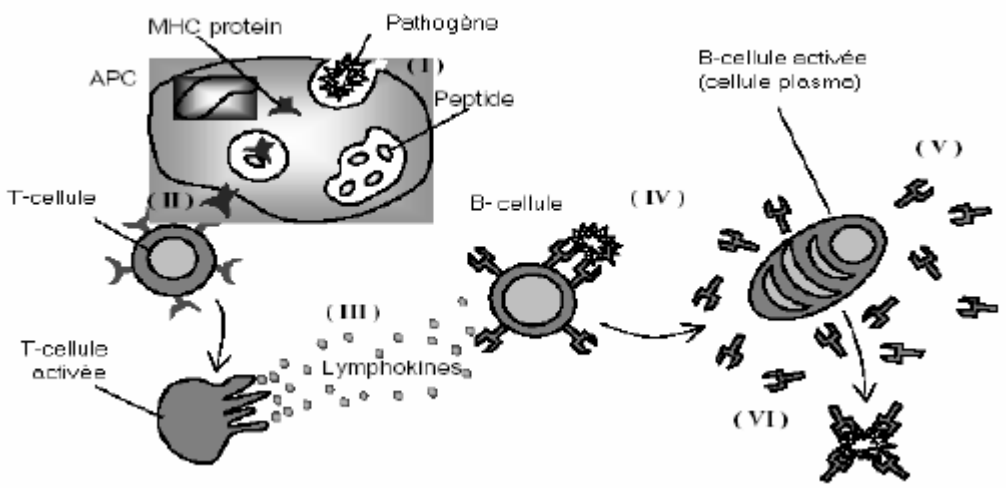

Figure 2.1 : Le processus de base de défense immunitaire [De Castro L. N, 2001]

3.4. Les processus de base d'un système immunitaire

3.4.1. L'identification dans le système naturel

Les lymphocytes sont des globules blancs produits dans la moelle osseuse et sont responsables de l'identification pathogènes. Ces lymphocytes ont des récepteurs situés sur leur surface responsables de la reconnaissance des antigènes. **[Anass De Castro .L.N & Von Zuben .F.J,99]** Les antigènes et les récepteurs cellulaires doivent avoir des formes complémentaires pour pouvoir se lier ensemble. C'est la liaison du récepteur avec les antigènes qui déclenchent une réponse immunitaire.

Les cellules B et T ont une structure semblable mais elles ont une manière de reconnaissance différente :

a) Reconnaissance d'un antigène par un récepteur de cellule B.

b) les cellules T ont la possibilité de reconnaître l'antigène qui est présenté par les molécules MHC**[De castroL.N, Von Zuben .F.J ,2000].**

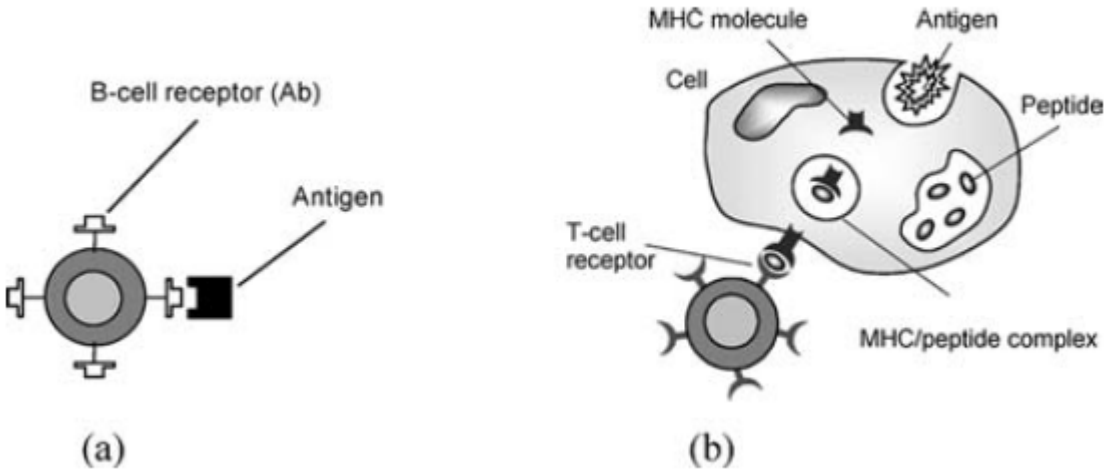

Figure 2.2 :L'identification dans le système immunitaire[De castro L.N ,Von Zuben .F.J ,2000].

3.4.2. L'activation

La reconnaissance antigène est la première condition préalable à l'activation du système immunitaire pour déclencher une réponse contre le pathogène qui présente l'antigène reconnu. L'appariement entre un récepteur cellulaire et un l'antigène détermine l'affinité, et cette appariement se produit force proportionnelle à cette affinité. Si l'affinité est supérieure à un seuil donné, appelé "seuil d'affinité", alors le système immunitaire est activé. La nature de l'antigène, le type de cellule reconnaissante et le site de reconnaissance influencent également l'issue d'une rencontre entre un antigène et un récepteur cellulaire.

Le système immunitaire humain contient un organe appelé thymus, qui joue un rôle dans la maturation des cellules T. Après cellules T Sont générés, ils migrent dans le thymus où ils mûrissent. Pendant cette maturation, toutes les cellules T qui reconnaissent les auto-antigènes sont exclues et cette processus appelé sélection négative. Si une cellule B rencontre un antigène non-soi avec une affinité suffisante, elle prolifère et se différencie en cellules mémoire et effectrices et cette processus nommé sélection clonale. En revanche, si une cellule B reconnaît un auto-antigène, elle pourrait entraîner la suppression, comme proposé par la théorie du réseau immunitaire **[De castro L.N ,Von Zuben .F.J ,2000].**

3.5. Caractéristique du système immunitaire

- **Reconnaissance :** le système immun est capable de classifier et de reconnaitre un grand membre de défirent modèles et de répondre accordement .En outre le système immun peut distinguer entre une matière (substance) étrangère et si propres cellule du système immunitaire, ainsi que maintenir peut de sens de soi.

- **Extraction de caractéristiques**: Grâce à l'utilisation de cellules présentatrices d'antigène (APC), le système immunitaire est capable d'extraire des caractéristiques de l'antigène en filtrant le bruit moléculaire de l'antigène avant d'être présenté aux lymphocytes

- **Diversité :** pendant le processus del'hyper mutation somatique, un sang divers d'anticorps est crée dans la réponse à un antigène .en assurant que pas seulement les antigènes envahissants ont été détruits, mais ainsi le système immunitaire est prêt par attaquer avec une variation le gère du même antigène.

- **Apprentissage :** pendant interaction dans le réseau immun, le système immun pourrait témoigner un mécanisme d'apprentissage, s'adaptant aux antigènes tel qu'ils sont présentés par la création d'anticorps et les éliminer du système en fin. Le mécanisme de l'hyper mutation somatique permet aussi un système immun d'affiner sa réponse à un pathogène envahissant.

- **Détection distribuée :** il y a une distribution inhérente à l'intérieure de système immun, il y a aucun point de contrôle assemblé, chaque lymphocyte est simulé spécifiquement et répond aux nouveaux antigènes.

- **Auto régulation :** les dynamiques des systèmes immuns sont le fait que la population du système immun est contrôlés par des interactions locales et non par un point de contrôle local.

- **Distributé:** Les lymphocytes du système immunitaire biologique sont capables de détecter l'anomalie indépendamment, avec le contrôle d'un centre, ce qui signifie qu'ils constituent un système hautement distribué. Lors de la conception du système immunitaire artificiel, cette fonctionnalité est très utile pour l'auto-protection et la robustesse de l'AIS. L'architecture

basée sur des agents a été proposée pour simuler la distribution du système immunitaire **[Jon Timmis ,Thomas Knight,2002].**

- **Multi-couches:** Le système immunitaire biologique a une structure multicouche. Une seule couche du système immunitaire biologique ne peut pas protéger l'organisme de toutes les invasions, mais la coopération de plusieurs couches est en mesure d'atteindre la protection de sécurité du système. Bien que cette caractéristique ne soit pas unique au système immunitaire biologique, c'est une caractéristique très importante du système immunitaire biologique. Les études et les implémentations de la fonction multi-couches dans le système immunitaire artificiel pour les systèmes informatiques peuvent grandement améliorer la sécurité des systèmes informatiques.

- **Disposabilité:** Aucune cellule immunitaire dans le système immunitaire biologique n'est indispensable. Chaque cellule immunitaire a un cycle de vie. Dans l'étude des systèmes immunitaires artificiels, nous pouvons emprunter le mécanisme pour atteindre le cycle de vie des anticorps immunitaires.

- **Autonomie:** Le système immunitaire biologique n'exige pas de nœud de contrôle central. Ils peuvent automatiquement reconnaître et détruire les antigènes envahissants et la mort des cellules immunitaires à jour eux-mêmes, la réalisation de la fonction immunologique sur leurs propres.

- **Pas de couche sécurisée:** Dans le système immunitaire biologique, toute cellule peut être envahie par des pathogènes, y compris des lymphocytes. Mais d'autres lymphocytes peuvent tuer l'agent pathogène envahissant. L'aide mutuelle entre les lymphocytes forme la base de la sécurité du système immunitaire biologique.

- **Changement dynamique de la couverture:** Le système immunitaire biologique peut maintenir un bon équilibre entre l'espace et le temps du jeu de détecteurs. Le système immunitaire biologique ne peut pas former un grand ensemble de détecteurs pour contenir toutes les informations d'invasion. À tout moment, le jeu de détecteurs introduit dans le corps n'est qu'une petite partie de l'ensemble du détecteur. Le jeu de détecteurs coulés se mettra à jour avec le temps et le cycle de vie. Un tel mécanisme présente de grands avantages pour améliorer la portabilité et la couverture du système immunitaire biologique.

- **Identité via le comportement**: Dans le domaine du cryptage, l'algorithme de cryptage est utilisé pour l'identification. Cependant, le système immunitaire biologique utilise les représentations de l'anticorps et de l'antigène pour l'identification. Dans le domaine des systèmes informatiques, toute représentation est basée sur "0" et "1" en bas. Trouver une représentation raisonnable donnera un bon effet de reconnaissance.

- **Détection incomplète**: Toute correspondance entre anticorps et antigènes n'est pas une correspondance complète. Cette caractéristique peut améliorer la diversité et la généralisation des détecteurs. Juste quelques anticorps sont capables de détecter un grand nombre d'antigènes

- **Jeu de chiffres:** Le jeu de chiffres se réfère principalement au temps de l'invasion et la réponse de protection. La réponse immunitaire doit être plus rapide que la vitesse d'invasion, sinon la protection immunitaire sera submergée par l'invasion. Les chercheurs de système immunitaire artificiel indiquent que plus d'attention devrait être payée au poids-léger du système

- **Mémoire**: Après une réponse immunitaire à un antigène donné, certains ensembles de cellules et de molécules sont dotés d'une durée de vie accrue afin de fournir des réponses immunitaires plus rapides et plus puissantes aux infections futures par les antigènes identiques ou similaires. Ce processus, connu sous le nom de maturation de la réponse immunitaire, permet le maintien de ces cellules et molécules réussies à reconnaître les antigènes**[Ying Tan,2016].**

4. Fonctionnement du système immunitaire naturel

Le système immunitaire protège l'organisme contre l'invasion de corps étrangers. Il est constitué decellules différentes réparties dans tout l'organisme. Chaque catégorie de cellules a une fonction spécifique etse déplace dans l'organisme selon les besoins **[J.R. Al-Enezi et al,2010].**

La réponse immunitaire fait intervenir deux types de mécanismes qui sont d'apparitions successives au coursde l'évolution des espèces et sont intimement connectés : **[D. Dasgupta, Z. Ji, F. Gnnzalez, 2003].**

- **L'immunité naturelle non spécifique**, encore appelée innée ou naïve, repose sur une distinction globale du soi et du non-soi. C'est une réponse immédiate, non spécifique de l'agresseur et non adaptative.

- **L'immunité acquise spécifique**, également appelée immunité saisie ou adaptative, représente la partie du système immunitaire qui peut identifier spécifiquement et éliminer sélectivement le microorganisme et les molécules étrangères elle se caractérise par une spécificité antigénique, diversité, et mémoire immunologique.

5. Système immunitaire artificiel (SIA)

5.1. Historique des AIS

Lessystèmes immunitaires artificiels (AIS) sont des systèmes informatiques inspirés par les principes etles processus du système immunitaire naturel des vertébrés.

Les algorithmes exploitent typiquement les caractéristiques du système immunitaire d'étude et de mémoirepour résoudre un problème. Ils sont couplés à l'intelligence artificielle et quelques algorithmes d'AIS sont étroitement liés à algorithmes génétiques **[Jon Timmis et al,2000]**.

Le système immunitaireartificielle a commencé au milieu des années 80 par Farmer, Packard et Perelson's (1986) et papiers de Bersini et de Varela sur les réseaux immunisés (1990). Cependant, c'était seulement au milieu des années 90 que l'AIS est devenu un domaine à son propre chef. Forrest et autres (sur choix négatif) a commencé en 1994; et Dasgupta a entrepris des études étendues sur des algorithmes négatifs de choix. La chasse et le Cooke ont commencé les travaux sur les modèles immunisés de réseau en 1995; Timmis et Neal ont continué ce travail et ont apporté quelques améliorations. De Castro et Von Zuben's et travail de Nicosia et de Cutello (sur choix clonal) est devenu notable en 2002. Le premier livre sur les systèmes immunitaires artificiels a été édité par Dasgupta en 1999.

Nouvelles idées, telles que la théorie de danger et les algorithmes inspirés par système immunitaire inné, sont maintenant explorés également. Bien qu'un certain doute qu'ils offrent encore à quelque chose au-delà des algorithmes existants d'AIS, ceci soit discuté avec chaleur, et la discussion fournit un les forces d'entraînement principales pour le développement d'AIS à l'heure actuelle.

À l'origine l'AIS s'est mis à trouver des abstractions efficaces des processus trouvés dans système immunitaire mais, plus récemment, il devient a intéressé en modelant les processus biologiques et en s'appliquant des algorithmes immunisés aux problèmes de bioinformatiques **[Dipankar Dasgupta,1999].**

5.2. Définitiond'un système immunitaire artificiel

Le système immunitaire artificiel est un système de renseignement informatique inspiré du mécanisme de fonctionnement et des principes du système immunitaire biologique. Basé sur le concept et l'idée de «obtenir la sagesse de la nature», et en simulant le mécanisme de fonctionnement des systèmes immunitaires biologiques, les systèmes immunitaires artificiels réussir à obtenir de nombreux avantages des systèmes immunitaires biologiques, y compris la patience de bruit pour apprendre sans un enseignant, Organisé, pas de contrôle centrale, et le renforcement de la mémoire, et d'autres fonctionnalités. Les systèmes immunitaires artificiels se sont développés dans un domaine de recherche de l'intelligence de calcul, et ont attiré beaucoup de chercheurs intéressés**[Ying Tan,2016].**

5.2.1. Définition 1

Selon Timmis **[Jon Timmis,Thomas Knight ,2002**] : « Un système immunitaire artificiel est un système informatique basé surles métaphores du système immunitaire naturel ».

5.2.2. Définition 2

Dasgupta a défini le système immunitaire artificiel comme suit **[Vasile Parvan, 2009]** : « Le systèmeimmunitaire artificiel est la composition de méthodologies intelligentes inspirées par lesystème immunitaire naturel afin de résoudre des problèmes du monde réel ».

5.2.3. Définition 3

Tandis que Timmis et De Castro **[J.Timmis & De Castro.L.N,2003]** ont donné la définition suivante : « Les systèmesimmunitaires artificiels sont des systèmes adaptatifs inspirés par des

théoriesimmunologiques et des observations de fonctions immunitaires, des principes et des modèles, qui seront appliqués à la résolution des problèmes ».

5.3. Le processus de conception d'un AIS

- Un schéma pour concevoir un algorithme de point de vue quantitatif exige au moins les éléments de base suivants **:**
- Une représentation pour les composants du système.

- Un ensemble de mécanismes pour évaluer l'interaction des individus avec l'environnement. Les environnements sont simules par un ensemble de stimulus d'entrée, une ou plusieurs fonctions d'évaluation.
- La procédure d'adaptation qui dirige la dynamique du système, c'est-a-dire comment son comportement varie dans le temps.
- Ce schema est adopte par Timmis & de Castro qui ont propose un processus de conception d'un AIS et leur principe est :
- Une représentation pour créer les modèles abstraits des cellules et d'organes immunitaires.
- Un ensemble de fonction nommée fonction d'affinité pour évaluer les interactions entre ces éléments artificiels d'une manière quantitative.
- Un ensemble d'algorithmes pour diriger la dynamique du système immunitaire artificiel.**[J.Timmis & De Castro.L.N,2003][J. Timmis et al,2004].**

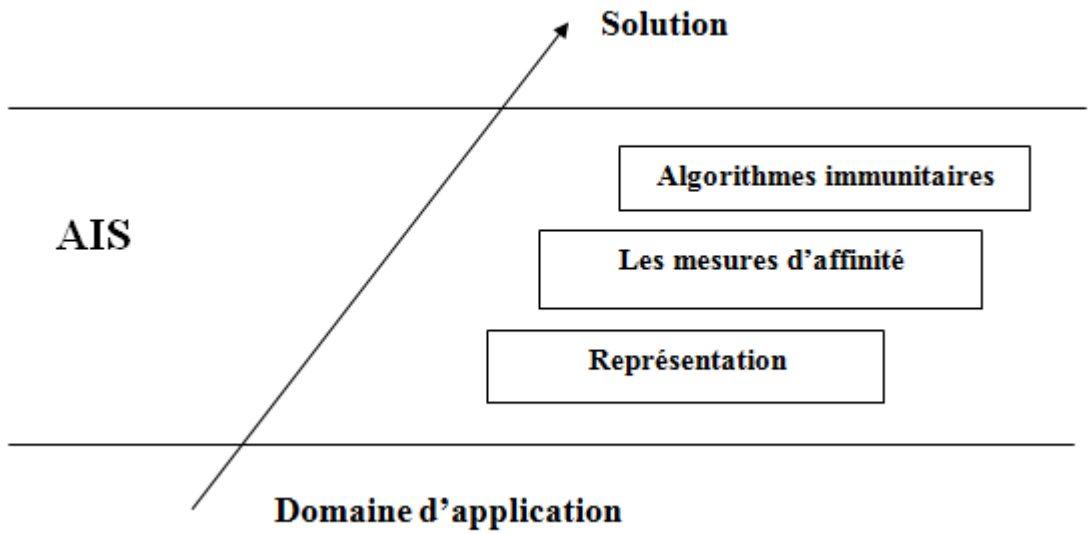

Figure 2.3 : La structure de conception d'un AIS[J.Timmis & De Castro.L.N,2003]

5.3.1. La représentation

Il a été noté qu'ils présentaient des molécules réceptrices de surface dont les formes sont complémentaires des formes d'antigènes, leur permettant de reconnaître les agents pathogènes et ensuite d'effectuer une fonction effectrice. Les cellules immunitaires et les molécules sont donc les éléments qui doivent être modélisés et utilisés pour créer SIA**[De Castro L. N , J. I. Timmis,2003].**

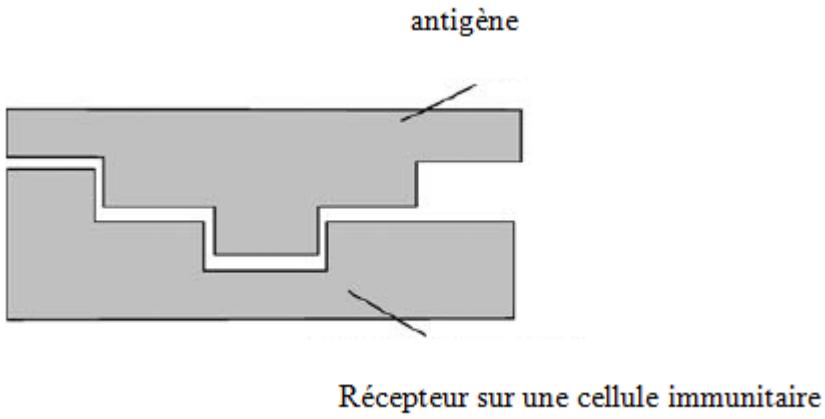

Figure 2.4 : Reconnaissance par régions de complémentarité[De Castro L. N , J. I. Timmis,2003]

5.3.1.1. Le modèle Shape – Space

Perelson et Oster (1979) ont d'abord proposé le concept d'espace-forme (S). Compte tenu du fait que la reconnaissance des antigènes est réalisée par les récepteurs cellulaires, les espaces de forme permettent une description quantitative des interactions des molécules et antigènes récepteurs. Comme dans le système immunitaire biologique, dans un espace de forme S, le degré de liaison (degré de concordance ou affinité) entre un récepteur antigénique (Ab ou TCR) et un antigène (Ag) est mesuré via des régions de complémentarité.

5.3.1.2 Les concepts de base du modèle

- **Formegénéralisée**

L'ensemble des caractéristiques qui caractérisent une molécule est appelé sa forme généralisée. La représentation Ag-Ab (binaire ou valeur réelle) détermine une mesure de distance à utiliser pour calculer le degré d'interaction entre ces molécules. Mathématiquement, la forme généralisée d'une molécule (m), un anticorps (Ab) ou un antigène (Ag), peut être représentée comme l'ensemble de coordonnées $m = <m_1, m_2, ..., m_L>, m \in S^L c\ R^L$ tel que m est un point dans un espace L- dimensionnel, où S représente le modèle Shape-Space**[De Castro L. N , Fernando J. Von Zuben,2002].**

- **L'identification via les régions de complémentarité**

Une population (répertoire) de N individus (récepteurs cellulaires) correspond à un espace de forme avec un volume fini V contenant N points. Comme les interactions antigène-anticorps sont mesurées par des régions de complémentarité, les déterminants antigéniques sont également caractérisés par des formes généralisées dont les compléments se situent dans le même volume V. Cette liaison entre l'antigène et l'anticorps peut être considérée, en termes simples, comme une serrure et une clé.

- **Le seuild'affinité**

Il est supposé que chaque anticorps interagit de manière spécifique Avec tous les antigènes dont les compléments existent dans une petite région environnante. Cette région est caractérisée par un paramètre ε, appelé seuil d'affinité.

- **La régiond'identification**

Le volume V_ε résultant de la définition du seuil d'affinité est appelé région de reconnaissance. Il est possible qu'un antigène puisse présenter des formes différentes, c'est-à-dire une légère variation du même antigène.

5.3.2. Mesures d'affinité

Comme l'affinité Ag–Ab est rattachée à leur distance, elle peut être estimée via toute mesure de distance entre deux chaînes ou vecteurs, tel que l'Euclidien, le Manhattan ou la distance de Hamming. Dorénavant, Si on considère un anticorps $Ab=<Ab_1,Ab_2,..Ab_L>$ et un antigène $Ag=<Ag_1,Ag_2,..Ag_L>$ alors la distance D entre eux peut être définie comme :

Où Eq. (1) est la distance Euclidienne, Eq. (2) la distance de Manhattan et Eq. (3) la distance de Hamming. Étant donné une représentation pour les molécules, le formalisme d'espace de forme définit un espace S avec la volume finie V dans lequel toutes les molécules sont représentées. Si nous supposons qu'un antigène donné est reconnu, il est possible d'introduire le concept d'affinité comme une représentation de l'espace de toutes les affinités possibles des sites attachant l'antigène (les anticorps ou TCRs) par rapport à cet antigène**[De Castro L. N, J. I. Timmis,2003].**

$D=\sqrt{\sum_{i=1}^{L}(Ab_i - Ag_i)^2}$ la distance Euclidienne (1)

$D=\sum_{i=1}^{L}|Ab_i - Ag_i|$ la distance de Manhattan (2)

$D=\sum_{i=1}^{L} \delta i$ où $\delta i=\begin{cases} 1 \text{ si Abi} \neq \text{Ag} \\ 0 \text{ sin on} \end{cases}$ la distance de Hamming (3)

5.4. Les algorithmes du système immunitaire artificiel

5.4.1. L'algorithme de la sélection négative

La sélection négativeInspiré par le processus de génération des cellules T dans les systèmes immunitaires, Forrest et al (1994) ont proposé un algorithme de sélection négative, qui est devenu l'un des plus célèbres algorithmes AIS**.[Ying Tan,2016]** La sélection négative de T-cellules élimine ces cellules dont les récepteurs sont capables de reconnaître les antigènes du soi. de cette façon, toutes les cellules T qui survivent à la sélection négative sont Supposé ne reconnaître que des antigènes non-soi. C'est une idée très intéressante pour le développement d'algorithmes qui contrôlent un système contre une anomalie ou un comportement inhabituel.

La sélection négative est le processus qui permet de distinguer le soi du non soi, elle a été appliquée à des problèmes de détections d'anomalies, son algorithme a la forme suivante :

- **Générer** le *Soi* comme étant un ensemble *S* d'éléments dans un espace *U* qui doivent être surveillés. *S* peutreprésenter le sous-ensemble des états considérés comme normaux pour le système.
- **Générer** un ensemble *F* de détecteurs (motifs) s'appariant avec certains éléments de *S*. Pour copier lefonctionnement du système immunitaire générer des détecteurs aléatoires et supprimer ceux qui sont tropgénéraux. Une approche efficace essaye de réduire au minimum le nombre de détecteurs produits tout enmaximisant la zone couverte de l'espace du *non soi*.
- **Surveillez** *S* à l'aide de *F*. Si l'un quelconque des détecteurs ne s'apparie pas alors un changement s'estproduit.

Domaine d'application : Cet algorithme est utilisé dans la sécurité informatique et la détection des spam

5.4.2. Algorithme de sélection clonale

Le principe de sélection clonale est l'ensemble du processus de reconnaissance des antigènes, de prolifération cellulaire et de différenciation en cellules de mémoire (Burnet, 1959), Castro et Zuben (2002) ont proposé un algorithme de sélection clonale appelé CLONALG pour

l'apprentissage et l'optimisation**[De Castro L. N et al, 2002]** Cet algorithme a été initialement proposé pour effectuer la reconnaissance des motifs et ensuite adapté pour résoudre les tâches d'optimisation multimodale. Compte tenu d'un ensemble de motifs à reconnaître (P), les étapes de base de l'algorithme CLONALG sont les suivantes: **[R. Al-Enezi et al, 2010].**

- Produire un ensemble de solutions (répertoire d'anticorps) de *N* candidat qui sont défini par le problème àétudier ;
- Choisir les *n1* cellules qui ont la plus grande affinité à l'antigène ;
- Copier (produire des copies identiques de) ces cellules choisies. Le nombre de copies est proportionnelaux affinités : plus l'affinité est haute, plus le nombre de clone est grand;
- Changer la structure des cellules choisies (hyper mutation). Le taux de changement est proportionnelle àleurs affinités : plus l'affinité est haute, plus le taux de Changement est petit;
- Sélectionner les *n2* cellules (du résultat de l'étape 4) qui ont la plus grande affinité à l'antigène pourcomposer le nouveau répertoire ;
- Remplacer quelques cellules qui possèdent des valeurs d'affinité faible par les nouvelles cellules ;
- Répéter les étapes 2 à 6 jusqu'à ce qu'un critère d'arrêt donné soit rencontré.

Domaine d'application : Ce genre d'algorithme peut être utilisé pour des problèmes d'optimisations, deClustering, ou de reconnaissance des formes.

5.4.3. Algorithme du réseau immunitaire

La sélection clonale artificielle est une abstraction des mécanismes de mémorisation des systèmesimmunitaires, les algorithmes développés sont généralement dédiés à l'optimisation ou à larecherche. Unanticorps est une abstraction de la cellule S et des anticorps qu'elle produit, et les antigènes représentent eux-mêmes.

La théorie du réseau immunitaire propose que le système immunitaire ait un comportement dynamique même en l'absence de stimuli externes. Il est suggéré que les cellules et les molécules immunitaires sont capables de se reconnaître, ce qui confère au système un comportement propre qui n'est pas dépendant de la stimulation étrangère**[De castro L.N,Von Zuben .F.J ,2000]**.

L'algorithme qui représente ce mécanisme est l'AINET "Artificial Immune NETwork" inspiré de la théorie du réseau immunitaire postulé par Jerne, a été développé par de Castro et Zuben dans le but de trouver un ensemble réduit de points qui représente de près l'ensemble des points d'entrée, Une représentation d'entrée compressée avec moins de redondance. Le processus au sein d'aiNet qui évolue une population vers un ensemble de détecteurs efficaces est de nature très semblable à une approche de sélection clonale: la principale différence étant qu'il existe des interactions entre les membres de la population via un mécanisme de suppression qui supprime les membres dont la correspondance entre eux et Une donnée de formation est inférieure à un certain seuil. Une version simplifiée d'aiNet peut être décrite comme suit: **[J. Timmis et al, 2008].**

Entrée: G = modèle à reconnaître, N un ensemble de détecteurs aléatoires, n nombre de meilleurs anticorps
Sortie: M = ensemble de détecteurs générés capables de reconnaître le modèle d'entrée
1. Créer une population aléatoire initiale B
2. Pour chaque modèle à apprendre
  2.1 Déterminer la distance inverse pour le motif dans B à chaque membre de N
  2.2 Sélectionnez n membres de B qui correspondent le mieux à chaque motif
  2.3 Cloner et muter chaque n en proportion de la qualité de la correspondance avec le motif
  2.4 Conserver l'appariement le plus élevé de n et placer dans un ensemble M
  2.5 Effectuer la dynamique de réseau dans M pour enlever les membres faibles de M
  2.6 Générer b éléments aléatoires et placer dans B
3 répéter

6. Les domaines d'application des AIS

- **Détection du virus**

Selon la capacité de distinguer le soi et non-soi du système immunitaire, Forrest propose des principes et des lois de SIB dont SIA peut prendre l'inspiration et il a fait beaucoup de travail de recherche pour le soutenir. En prenant l'inspiration du mécanisme de BIS la

résistance et l'anéantissement du virus biologique inconnu, T.Okamolo a proposé un système antiviral basé sur l'agent distribué. Il se compose de deux parties : le système immunitaire et le système de récupération. La fonction du système immunitaire est identifient les renseignements de non-soi (le virus informatique) en empoignant les renseignements de soi ; Le système de récupération copie des dossiers de l'ordinateur non-infecté à l'ordinateur qui a été infecté par le réseau pour y couvrir les dossiers. Basé sur les mêmes principes, SIA est aussi utilisé anti-piratage, la maintenance de sécurité de réseau et la maintenance de système.

- **Filtrage du courrierindésirable**

La filtration de Spam est un problème de reconnaissance des formes important et typique parce que spam provoque beaucoup de problèmes à notre vie de communication quotidienne. Dans la solution du problème, tant les méthodes statistiques classiques que les méthodes SIA ont été présentées et la plupart d'entre eux se concentrent à étudier des méthodes d'extraction de trait et un design de la conception des classificateurs. La fonction principale de l'extraction de caractéristiques est d'extraire des informations discriminantes à partir de messages et de transformer des messages en vecteurs de caractéristiques. Les méthodes d'extraction de trait statistiques essaient de recueillir et analyser des caractéristiques numériques de messages, telles que les fréquences de terme et la relation entre les termes et les catégories e-mail. Quelquesrépandussont Bag-of-Words (BoW), Sparse Binary Polynomial Hashing (SBPH) et Orthogonal Sparse Bigrams (OSB).

- **L'analyse des données**

AIS a la capacité de l'analyse des données et la classification en combinant les avantages des classificateurs, réseaux de neurones et inférence machine . Par conséquent, il a été utilisé dans les champs de datamining et le traitement de l'information. Timmis a expliqué comment mettre en œuvre un SIA non supervisé et d'auto-apprentissage spécifiquement**[Ying Tan,2016].**

7. Extension du système immunitaire artificiel

7.1. Le modèle de soi / non soi

Le système immunitaire adaptatif et en particulier les cellules B secrètent des anticorps spécifiques pour reconnaître et réagir au stimulus. La correspondance entre l'antigène et l'anticorps est l'élément de base dans la plupart des implémentations des AIS. La caractéristique principale du système immunitaire est sa capacité à répondre aux envahisseurs étrangers sans réagir aux

molécules de soi. Afin d'assurer ce rôle, le système immunitaire a besoin de différencier entre les cellules de soi et entre les cellules étrangères ou les pathogènes.

Cette discrimination est apprise tôt dans la vie grâce aux différents processus immunitaires qui jouent un rôle important pour réaliser la tolérance au soi . Le modèle de soi / non soi se base sur ce principe de telle sorte que la réponse immunitaire soit déclenchée quand le corps rencontre quelque chose de non soi ou étrangère**[Uwe Aickelin , Steve Cayzer,2002].**

7.1. 1.Critique du modèle de soi / non soi

La théorie de danger défie le point de vue du modèle de soi / non soi, elle souligne qu'il existe des exemples de discrimination apparaissant après la distinction de soi / non soi . Par exemple :

- Il n'y a pas de réaction immunitaire contre les bactéries étrangères dans l'intestin ou l'alimentation que nous mangeons bien que les deux soient des entités étrangères.
- Certains processus auto réactifs sont utiles, par exemple contre les molécules soi exprimées par des cellules stressées.

La définition de soi est limitée au sous-ensemble réellement vu par les lymphocytes pendant la maturation.

- Le corps humain change pendant sa durée de vie et par conséquence le soi change aussi. Donc, les défenses contre le non soi au début de la vie pourraient être auto réactives plus tard.
- D'autres aspects qui semblent être en contradiction avec le point de vue traditionnel sont les maladies auto-immunes et certains types de tumeurs qui sont combattues par le système immunitaire. Ainsi, le cas où il n'existe aucune attaque contre le non soi dans le cas des greffes.

7.2. Le modèle de théorie de danger

Cette théorie est proposée par Matzinger et qui propose des nouvelles conditions pour le déclenchement de la réponse immunitaire. Elle propose que la réponse immunitaire soit déclenchée suite à l'existence de danger et non suite à l'existence d'un élément étranger **[Matzinger. P, 1994]**

7.2.1. Le principe de base de la théorie de danger

L'idée de la théorie du danger est que le système immunitaire ne répond pas aux éléments de « non soi » mais aux éléments qui déclenchent le « danger » dans le corps.Cette théorie est confirmée

par l'observation qu'il n'y a pas besoin d'attaquer tout ce qui est étranger, ce qui semble être pris en charge par les exemples ci-dessus. Dans cette théorie, le danger est mesuré par les dommages aux cellules indiqués par les signaux de détresse qui sont envoyés lorsque les cellules meurent d'une façon inhabituelle (nécrose) par opposition à la mort de cellule programmée (apoptose) . Ces signaux de danger sont reconnus par les cellules de présentation d'antigène (APC) qui sont des cellules critiques pour l'initialisation de la réponse immunitaire

La figure 2.5 illustre comment on peut imaginer une réponse immunitaire selon la théorie du danger. Une cellule en détresse envoie un signal d'alarme, après quoi les antigènes dans le voisinage sont capturés par des cellules présentatrices d'antigène (APC) telles que les macrophages, qui déplacent au nœud de lymphe local et présentent les antigènes aux lymphocytes. Essentiellement, le signal de danger établit une zone de danger autour de lui-même. Ainsi, les cellules B produisant des anticorps qui correspondent aux antigènes dans la zone dangereuse sont stimulées et subissent ainsi le processus d'expansion clonale, par contre celles qui ne correspondent pas ou sont trop loin ne seront pas stimulées **[Aickelin. U et al, 2003].**

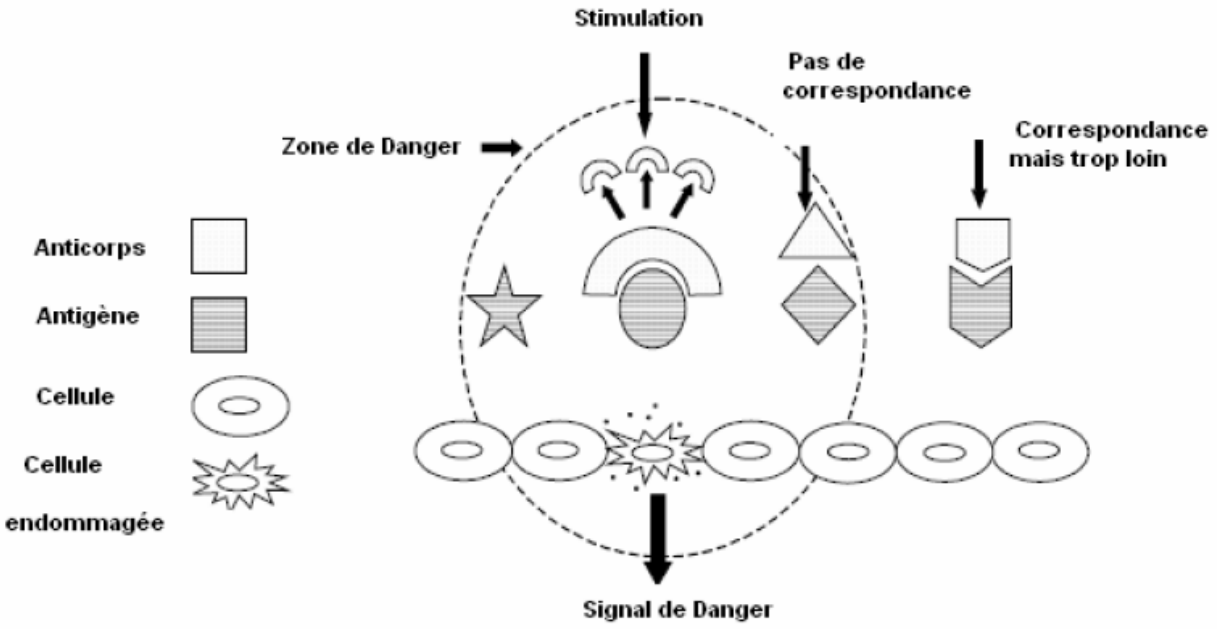

Figure 2.5 : Principe de la théorie de danger [Aickelin. U et al, 2003].

8. Conclusion

Nous avons vu que les systèmes immunitaires possèdent un grand nombre de caractéristiques cognitives comme la mémoire, la reconnaissance des nouvelles formes, l'adaptabilité et le traitement distribué de l'information donc on peut dire que les systèmes immunitaires forment un excellent outil pour la création des contrôleurs adaptatifs, l'apprentissage et la détection des fautes.

Sans système immunitaire, l'organisme ne serait plus protégé contre les microbes, les virus, les substances toxiques... Comment s'organisent les défenses immunitaires ? Quel est le rôle des lymphocytes ? Quelles sont les conséquences lorsque ce système est déréglé ? Telles sont les principales questions trouvant leurs réponses au cours de ce chapitre.

CHAPITRE 3 : LES SYSTÈMES DE DÉTECTION D'INTRUSION BASÉ SUR LE SYSTÈME IMMUNITAIRE ARTIFICIEL

1. Introduction

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 des agents étrangers.

Les caractéristiques saillantes qui peuvent contribuer à la conception d'IDS compétents en réseau sont analysées. L'analyse montre que les actions coordonnées de plusieurs mécanismes sophistiqués du système immunitaire humain satisfont tous les objectifs de conception identifiés. Par conséquent, conclut que la conception d'un IDS basé sur le réseau basé sur le système immunitaire humain est prometteuse pour les futurs IDS basés sur le réseau.

Ce chapitre sera consacré à l'exposition des différents travaux exploitant les systèmes immunitaires artificiels dans le domaine de détection d’intrusions. Une discussion sera établie sur ces différents travaux afin de montrer certains problèmes existants dont le but est la présentation des motivations de l’approche proposée.

2. Un système immunitaire pour la sécurité des systèmes informatiques

Le problème de système immunitaire est semblable à celui de système de sécurité des systèmes informatiques: le système immunitaire protège le corps contre les agents pathogènes et analogiquement le système de sécurité informatique devrait protéger les ordinateurs contre les intrusions. Cette analogie peut être plus concrète en comprenant les problèmes rencontrés par les systèmes de sécurité informatique. Il existe plusieurs aspects de la sécurité informatique:

- **Confidentialité:** l'accès à des données restreintes ou confidentielles ne devrait être autorisé qu'aux l'utilisateur est autorisés, par exemple, il est impératif que les institutions militaires limitent la connaissance des informations classifiées
- **Intégrité:** les données doivent être protégées contre les opérations non autorisées, il est essentiel préserver l'intégrité des informations critiques.
- **Disponibilité:** Les informations et les ressources informatiques devraient être disponibles si nécessaire par des utilisateurs légitimes. En particulier, ceci est essentiel dans les cas où ces informations sont nécessaires pour prendre des décisions critiques dans un délai limité.
- **Responsabilité:** dans le cas où le compromis d'un système informatique a été détecté, le système de sécurité informatique devrait conserver suffisamment d'informations pour identifier ces intrus.
- **Justesse :** Les fausses alarmes de classification incorrecte des événements doivent être réduites au minimum pour que le système soit utilisable. Les faibles niveaux de correction peuvent interférer avec d'autres aspects de la sécurité.

La similitude entre le problème de la sécurité informatique et problème de système immunitaire peut être montrée en traduisant la langue de l'immunologie en termes de sécurité informatique: on peut dire que le système immunitaire détecte les abus d'une politique spécifiquement implicite et répond à ces abus par contre- Attaquant la source de l'abus. La politique est implicitement spécifiée par la sélection naturelle et ne souligne que certains aspects de la sécurité: La disponibilité et l'exactitude sont d'une importance primordiale, et dans une moindre mesure, l'intégrité et la responsabilité.

La disponibilité permet au corps de continuer son fonctionnement même dans le cas d'existence des attaques de pathogènes. La justesse signifie empêcher le système immunitaire d'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 ou restreintes dans le corps qui doivent être protégées à tout prix par des étrangers. **[Steven Andrew Hofmeyr, 1999]**

3. Exigences des IDS à base de réseau

Les fonctions nécessaires à la conception d'un IDS basé sur le réseau compétent sont les points suivants :

- **Robustesse:**

Le système de détection d'intrusions doit être doté par des points de détection multiples pour qu'il soit assez robustes contre l'attaque et tout défaut du système . Le point faible d'un IDS est son échec et sa subversion par des intrus. Si les intrus connaissent déjà l'existence d'un IDS et peuvent le subvertir, alors l'effort de développer l'IDS était inutile.

- **Configurabilité:**

La configuration d'un IDS doit être facile aux exigences locales de chaque hôte ou de chaque composant de réseau. Les hôtes individuels dans un environnement de réseau sont hétérogènes. Ils peuvent avoir des exigences de sécurité différentes. En plus des hôtes, les différents composants du réseau tels que les routeurs, les filtres, les DNS, les pare-feux ou les différents services réseau peuvent avoir différentes exigences de sécurité.

- **Extension:**

La facilité d'étendre la portée de la surveillance IDS par l'ajout de nouveaux hôtes facilement et simplement indépendamment des systèmes d'exploitation. Lorsqu'un nouvel hôte est ajouté à un environnement de réseau existant et surtout lorsque ce nouvel hôte exécute un système d'exploitation différent doté d'un format différent des données d'audit, il n'est pas simple de le surveiller de manière cohérente avec les IDS existants.

- **Scalabilité:**

Il est nécessaire d'obtenir une évolutivité fiable pour rassembler et analyser correctement le volume élevé des données d'audit des hôtes distribués. Dans le cas des IDS monolithiques, la procédure de collecte des pistes d'audit est distribuée et son analyse est centralisée. Cependant, il est très difficile de transmettre toutes les données d'audit à un seul IDS pour analyse sans perdre les données. Même si cela évolue correctement pour toutes les données d'audit, cela peut entraîner une grave dégradation des performances du réseau.

- **Adaptabilité:**

il doit être ajusté dynamiquement afin de détecter les intrusions de réseau dynamiquement changeantes. 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.

- **Analyse globale:**

pour détecter les intrusions de réseau, elle devrait surveiller collectivement plusieurs événements générés sur différents hôtes pour intégrer des preuves suffisantes et identifier la corrélation entre plusieurs événements. De nombreuses intrusions de réseau exploitent souvent les multiples points d'un réseau. car l'analyse établie par un seul hôte peut donner juste une erreur normale. Mais si elles sont contrôlées collectivement à partir de points multiples, elles peuvent clairement être identifiées comme une tentative d'attaque.

- **Efficacité**:

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. Un seul IDS devrait effectuer le suivi, la collecte de données, la manipulation des données et la prise de décision. Il peut imposer un gros frais généraux sur un système et pourrait imposer un fardeau particulièrement sur la CPU et les E / S, entraînant une dégradation sévère des performances du système et du réseau.

4. les objectifs de conception des IDS à base de réseau

4.1. Distribué :

Le premier objectif de conception est d'être La distribution. Un système de détection d'intrusions basé réseau distribué délègue ses responsabilités à un certain nombre de composants distribués. Un certain nombre de processus de détection d'intrusion indépendants surveillent seulement un petit aspect du système global. Ils fonctionnent simultanément et coopèrent les uns avec les autres. Si un IDS basé sur le réseau est distribué, il répondra aux exigences suivantes.

4.2. Robustesse :

Le système de détection d'intrusions doit être doté par des points de détection multiples pour qu'il soit assez robustes contre l'attaque et tout défaut du système. Le point faible d'un IDS est son échec et sa subversion par des intrus. Si les intrus connaissent déjà l'existence d'un IDS et peuvent le subvertir, alors l'effort de développer l'IDS était inutile.

4.3. Configurabilité :

La configuration d'un IDS doit être facile aux exigences locales de chaque hôte ou de chaque composant de réseau. Les hôtes individuels dans un environnement de réseau sont hétérogènes. Ils peuvent avoir des exigences de sécurité différentes. En plus des hôtes, les différents composants du réseau tels que les routeurs, les filtres, les DNS, les pare-feux ou les différents services réseau peuvent avoir différentes exigences de sécurité.

4.4. Extension

La facilité d'étendre la portée de la surveillance IDS par l'ajout de nouveaux hôtes facilement et simplement indépendamment des systèmes d'exploitation. Lorsqu'un nouvel hôte est ajouté à un environnement de réseau existant et surtout lorsque ce nouvel hôte exécute un système d'exploitation différent doté d'un format différent des données d'audit, il n'est pas simple de le surveiller de manière cohérente avec les IDS existants.

4.5. Scalabilité

Il est nécessaire d'obtenir une évolutivité fiable pour rassembler et analyser correctement le volume élevé des données d'audit des hôtes distribués. Dans le cas des IDS monolithiques, la procédure de collecte des pistes d'audit est distribuée et son analyse est centralisée. Cependant, il est très difficile de transmettre toutes les données d'audit à un seul IDS pour analyse sans perdre les données. Même si cela évolue correctement pour toutes les données d'audit, cela peut entraîner une grave dégradation des performances du réseau.

4.6. Adaptabilité

Il doit être ajusté dynamiquement afin de détecter les intrusions de réseau dynamiquement changeantes. 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.

4.7. Analyse globale

Pour détecter les intrusions de réseau, elle devrait surveiller collectivement plusieurs événements générés sur différents hôtes pour intégrer des preuves suffisantes et identifier la corrélation entre plusieurs événements. De nombreuses intrusions de réseau exploitent souvent les multiples points d'un réseau, car l'analyse établie par un seul hôte peut donner juste une erreur normale. Mais si elles sont contrôlées collectivement à ne partir de points multiples, elles peuvent clairement être identifiées comme une tentative d'attaque.

4.8. Efficacité

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. Un seul IDS devrait effectuer le suivi, la collecte de données, la manipulation des données et la prise de décision. Il peut imposer un gros frais général sur un système et pourrait imposer un fardeau particulièrement sur la CPU et les E / S, entraînant une dégradation sévère des performances du système et du réseau.

Même si diverses approches ont été développées et proposées jusqu'à maintenant, aucun modèle existant basé sur le réseau ne satisfait complètement ces exigences.

5. Une analyse des capacités des systèmes immunitaires humains

En effectuant une analyse prudente des capacités complexes des systèmes immunitaires humains, il est possible d'identifier plusieurs caractéristiques importantes pour la détection d'intrusion en réseau. Ces caractéristiques spécifiques peuvent agir ensemble afin de satisfaire chacun des trois objectifs de conception des IDS compétents: distribution, auto-organisation et la souplesse.

5.1. Un modèle distribué

Le système immunitaire humain est distribué. Les mécanismes suivants permettent au système immunitaire humain de détecter les antigènes d'une manière véritablement répartie.

5.1.1. Réseau immunitaire

Le système immunitaire humain est implémenté par les interactions entre un grand nombre de différents types de cellules. Au lieu d'utiliser un coordonnateur central, les systèmes immunitaires humains supportent le niveau approprié de réponses immunitaires en maintenant le statut d'équilibre entre la suppression par anticorps et l'activation par antigène.

5.1.2. Ensembles d'anticorps uniques

Le système immunitaire humain génère différents groupes d'anticorps pour détecter différents antigènes. Son mécanisme d'évolution grâce à la sélection naturelle des bibliothèques de gènes et à la sélection clonale maintient un certain nombre d'ensembles d'anticorps différents. Par conséquent, chaque ensemble d'anticorps est unique et indépendant.

Ces propriétés ne requièrent aucun coordonnateur central et permettent au système immunitaire humain de détecter des antigènes au niveau local d'un anticorps.

5.2. Auto-organisation

La réponse immunitaire est composée de trois étapes évolutionnaires qui sont: l'évolution de la bibliothèque de gènes générant un anticorps efficace, une sélection négative éliminant les anticorps inappropriés et la sélection clonale d'un anticorps performant. Ces trois

étapes sont autoorganisées plutôt que a direction par un organe central ou obtenir une information prédéfinies.

5.2.1. L'évolution de la bibliothèque de gènes

La production des anticorps compétents nécessite une certaine connaissance de propriétés antigéniques. Le système immunitaire apprend ces connaissances par l'évolution de la bibliothèque de gènes. Puisque ce processus d'évolution est auto organisée, il permet aux bibliothèques de gènes d'agir comme une archive d'information afin de détecter les antigènes observés.

5.2.2. Sélection négative

En tant que deuxième étape, cela élimine les anticorps immatures avec les cellules du soi. Le système ne possède aucune information globale sur les cellules de soi, la satisfaction de cette contrainte est assurée dans le thymus et la moelle osseuse en présentant des cellules individuelles et en éliminant les anticorps qui attaquent ces cellules.

5.2.3. Sélection clonale

En tant que troisième étape, Ce processus permet la prolifération des meilleurs anticorps alors que les anticorps de faible affinité meurent après une durée de vie. Ainsi, selon les antigènes existants seulement les anticorps les plus convenables survivent. De la même façon au lieu de l'obtention de l'information prédéterminée sur les antigènes spécifiques, le système immunitaire est capable de sélectionner d'une manière autonome les anticorps les plus convenables en agissant avec les antigènes existants.

5.2.4. La souplesse

Le système immunitaire humain est souple. Les mécanismes suivants lui permettent au système immunitaire d'être souple et sont concentrés sur trois idées:

1. **Comment** un grand nombre d'antigènes peuvent être détectés avec un nombre plus petit ou des anticorps.
2. **Comment** les informations connues d'antigène peuvent être réutilisées de manière efficace .
3. **Combien** d'anticorps peut être généré avec un nombre limité de gènes.

La liaison approximative, les cellules de mémoire et l'expression des gènes fournissent respectivement les réponses à ces questions.

5.2.5. La liaison approximative

La réponse immunitaire est déclenchée lorsque l'affinité de l'anticorps et de la liaison de l'antigène est supérieure à un certain seuil. En d'autres termes, un seul anticorps peut détecter n'importe quel nombre d'antigènes tant que leur affinité est supérieure au seuil. Cette liaison approximative contribue à augmenter la généralité des systèmes immunitaires.

5.2.6. Cellules de mémoire

Les cellules de mémoire stockent l'information génétique des antigènes précédemment détectés et répondent efficacement et rapidement lorsqu'ils rencontrent les mêmes antigènes à l'avenir. Les cellules de mémoire ont une durée de vie plus longue que les anticorps ordinaires, elles conservent l'immunité sans avoir à créer les mêmes anticorps à nouveau.

5.2.7. Expression génique

Le système immunitaire maintient la diversité des anticorps afin d'assurer la détection efficace d'une large gamme d'antigènes. Dans un processus de développement d'anticorps, connu sous le nom d'expression génique, plusieurs mécanismes génétiques sont utilisés pour générer divers anticorps à partir des bibliothèques de gènes. L'idée principale de ces mécanismes est qu'un grand nombre de nouveaux anticorps peuvent être générés à partir de nouvelles combinaisons de segments de gènes dans les bibliothèques de gènes.**[Jungwon Kim,Peter Bentley]**

6. Modélisation d'un système de détection d'intrusion basé système immunitaire artificiel

Le but de l'IDS est non seulement d'empêcher l'attaque, mais également de signaler tous les comportements anormaux du système. Pour concevoir un IDS basé sur AIS réussi, la première chose à considérer est la présentation du problème du système dans le domaine ID, puis la combinaison de méthodes AIS avec IDS.

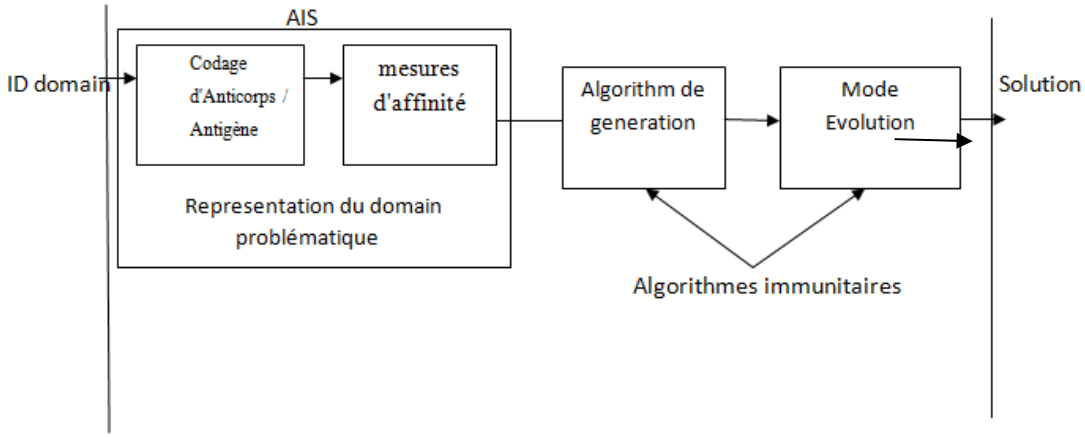

Figure 3.1: Cadre pour la conception IDS basée sur AIS **[Hua Yang et al, 2014].**

Pour appliquer AIS dans IDS, trois étapes sont suivies:

1. Représenter les éléments du système et l'interaction des individus sous une forme immunitaire. L'objectif de cette étape est de représenter les éléments ID d'une manière immunologique (par exemple, de créer des modèles abstraits de cellules immunitaires, de molécules, etc.) et de quantifier l'interaction de ces éléments par des mesures d'affinité. Par exemple, le comportement anormal dans IDS est présenté comme l'antigène (non-soi) dans AIS. Dans le domaine ID, affinité signifie la similitude entre les détecteurs et les données. Différentes représentations peuvent adopter des mesures d'affinité.

2. Générer les répertoires initiaux (algorithme de génération),

3. Optimiser l'algorithme (mode d'évolution) **[Hua Yang et al, 2014].**

7. Travaux antérieurs pour systèmes de détections d'intrusion basée sur un système immunitaire artificiel

Au cours des dernières années, l'utilisation du système immunitaire artificiel a été favorisée par les chercheurs pour construire des systèmes de détection d'intrusion basés sur celui-ci. Bien que cette idée n'ait pas été Complètement appliqué aux IDS de l'actualité, mais beaucoup d'efforts ont été faits pour développer cette idée **[Fanelli, R. L, 2009].**

1. Le travail de **Somayaji et al** en **1996** est la première tentative qui intègre l'immunologie dans un système de détection d'intrusions dont le but était la conception et la vérification d'un système de détection d'intrusions basé sur la notion de soi. Ce travail s'inspire principalement du travail de **[Forrest et al1994].**

Le système proposé est basé hôte, il contrôle principalement les processus privilégiés. Le système collecte les informations pour définir le soi pendant la période d'apprentissage, ces informations sont sous la forme des séquences de commande desendmail (un agent de transport des emails dans le système UNIX) dont le résultat est une base de données de séquences de commandes. Ensuite, pendant la phase de test, le système vérifie l'occurrence des nouvelles séquences qui n'existent pas dans la base de données du programme en exécution. Chaque séquence qui n'existe pas dans la base de données est considérée comme une erreur. Une anomalie est déclenchée si le nombre d'erreurs atteint un seuil prédéfini **[Somayaji et al,1996].**

2. Le travail proposé par **Hofmeyr et al** en **1998**espère améliorer les systèmes de détection d'intrusions basés sur la détection d'anomalies. Le principe de ce travail est semblable au travail précédent de **Somayaji et al** en **1996 [Somayaji et al, 1996]** mais avec quelques améliorations. Les séquences d'appels système sont représentées dans des fenêtres d'appels système qui seront confrontées à la base de données de comportements normaux. L'évaluation de la similarité entre deux séquences est établie via la distance de Hamming. Une erreur est déclenchée s'il y'a une déviation du comportement normal et si le nombre d'erreurs dépasse un certain seuil, une alerte est générée.

Le point intéressant de ces travaux c'est la démonstration que les séquences d'appels système des processus privilégiés sont appropriées pour définir l'ensemble de soi dans un hôte contrôlé. Cependant, ces travaux pour la détection d'intrusions inspirés d'immunologie n'ont pas incorporé les différentes propriétés du système immunitaire, ils ont essayé seulement d'utiliser le concept de base du système immunitaire humain qui est la détection des entités du non soi. **[Hofmeyr et al ,1998].**

3. Afin de construire un système robuste, distribué, tolérant aux erreurs et adaptatif et qui intègre les différentes propriétés du système immunitaire, **Hofmeyr[Steven Hofmeyr,1999] et Forrest et Hofmeyr[S. Hofmeyr ,S. Forrest,2000]**ont développé un système de détection d'intrusions basé AIS nommé **LYSIS « Lightweight Intrusion detection SYStem »**, qui est désigné à protéger un réseau local (LAN) contre les attaques arrivantes du réseau par l'exploitation de plusieurs mécanismes inspirés du système immunitaire humain.

Le système de détection d'intrusions proposé est basé réseau et il examine les connexions TCP dont les connexions normales définissent l'ensemble de soi. Ces connexions TCP sont sous la forme des triplets de chemin de données qui contient les attributs suivants : l'adresse IP source, l'adresse IP destination, le port ou le service.

Les détecteurs sont représentés par des chaînes binaires, générés par l'algorithme de la sélection négative. La règle de correspondance utilisée entre un détecteur et un élément de soi ou de non soi est une règle de correspondance partielle qui est la règle de r bits contigus qui indique l'existence d'une correspondance entre un détecteur et une chaîne quelconque s'il sont au moins r bits contigus en commun.

4. **Dasgupta et al** en **1999** propose une structure générale pour un système de détection d'intrusions basé AIS. Cette structure utilise une architecture multi agent pour supporter le modèle du système immunitaire pour la détection d'intrusions. Cette structure du système de détection d'intrusions basé AIS suit simplement la caractéristique de détection multi niveau du système immunitaire humain plutôt que l'emploi des propriétés de système immunitaire humain, comme la détection distribuée, la sélection clonale et la sélection négative, etc. **[Dasgupta et al,1999].**

5. **Kim & Bentley** en **2001** ont évalué les **performances** de l'utilisation de l'algorithme de la sélection négative comme un détecteur d'anomalies pour la détection d'intrusions de réseau. le travail se base sur le système LISYS avec la définition d'un ensemble large de soi afin de tester les performances de cet algorithme dans un environnement du réseau réel. Deux changements principaux ont été faits pour s'adapter à des ensembles de soi plus compliqués à savoir : l'adoption de plus grande cardinalité de génotypes et l'application d'une fonction de correspondance sur phénotypes plutôt que génotypes.

Les résultats de ce travail ont montré une performance pauvre de l'algorithme de la sélection négative lorsqu'il est appliqué aux problèmes du monde réel. Comme le système à protéger devient de plus en plus large, il est difficile de trouver un ensemble de détecteur adéquat pour fournir la couverture nécessaire. **[Kim, Bentley, 2001].**

Kim [J. Kim, P. Bentley ,2001] a proposé un nouvel algorithme **Dynami CS** qui intègre les principaux concepts utilisés dans le système LISYS proposé par **Hofmeyr [Steven Hofmeyr,1999]**comme par exemple : la mémoire immunitaire, la période de tolérance des détecteurs, le seuil d'activation, la costimulation, etc.

Ce travail tente de traiter le comportement dynamique de l'environnement contrôlé par un système de détection d'intrusions qui change d'une manière constante dans lequel le comportement normal à un moment peut devenir anormal plus tard, **Kim** a essayé de vérifier les deux propriétés suivantes :

- L'apprentissage progressif du comportement normal du système en se basant sur un petit sous-ensemble de soi à la fois.
- Les détecteurs doivent être remplacés si les comportements normaux déjà appris ne représentent plus des comportements normaux puisqu'ils sont soudainement altérés par une opération de changement de soi légale.

6. Aickelin et al en **2005** propose l'incorporation de la théorie de danger dans les techniques de détection d'intrusions pour construire un système de détection d'intrusions capable de répondre d'une manière efficace aux menaces connues ainsi qu'aux nouvelles attaques avec des taux réduits de faux positif. Ils souhaitent la construction d'un modèle de calcul pour la théorie de danger avec l'intégration des signaux d'alarme.

Cette théorie qui montre la capacité du système immunitaire humain à repérer les signaux de danger pour répondre aux menaces en se basant sur la corrélation de ces signaux. **Aickelin et al** propose d'utiliser le même concept pour construire un IDS basé théorie de danger pour traiter le problème de corrélation d'alerte dont les signaux seront rassemblés à partir des hôtes et de réseaux. Ces signaux sont corrélés avec des alertes qui peuvent être de

deux types: apoptose ou nécrose qui sont définies en parallèle de la mort cellulaire de type apoptose et nécrose respectivement. **[Aickelin et al, 2005]**

7. Greensmith et al en **2005** ont proposé un nouvel algorithme inspiré d'immunologie pour la détection d'intrusions qui se base sur l'abstraction du fonctionnement des cellules dendritiques. Ce travail est apparu après le projet souligné par **Aickelin et al** en **2005 [Aickelin et al ,2005]**qui propose l'application de la théorie de danger aux systèmes de détection d'intrusions. Ce travail utilise les cellules dendritiques qui sont des cellules de présentation d'antigène qui ont la capacité d'agir comme un détecteur d'anomalies.

L'algorithme proposé est une abstraction de fonctionnement de base et des chemins de différenciation des cellules dendritiques qui sont responsables de la traduction de l'information sur la santé du tissu au système immunitaire adaptatif. Cela est réalisé par la combinaison des différents signaux qui apparaissent dans le système. Initialement, les cellules dendritiques se trouvent dans un état immature dont le rôle principal est la collection des antigènes, puis selon la combinaison des différents signaux de danger présents dans le système, ces cellules deviennent soient des cellules matures ou bien des cellules semi matures. Par exemple, en présence de signaux d'alarme dus aux dommages de l'hôte, les cellules dendritiques changent leur état en des cellules prétendues matures et présentent les protéines rassemblées du tissu endommagé avec une information de contexte indiquant que le tissu est endommagé**.**

Comme nous avons vu précédemment, les différents travaux dans le domaine de la détection d'intrusions ont exploité les différents modèles du système immunitaire artificiel, le tableau ci-dessous (Tableau 3.1) récapitule les différents travaux avec les différents modèles immunitaires utilisés qui sont :

- **La bibliothèque de gènes** signifie que le système implémenté utilise une méthode évolutionnaire pour initialiser les génotypes des détecteurs et non pas d'une façon aléatoire.
- **La sélection clonale** qui correspond au processus de prolifération et différenciation d'hypermutation. cellules B pour incrémenter la généralité et la couverture des détecteurs par le processus.
- **La mémoire immunitaire** permet l'apparition de la réponse secondaire afin d'obtenir une réponse plus rapide et plus efficace à une attaque déjà connue.

- **Le réseau idiotypique** correspond à l'implémentation de la théorie du réseau idiotypique qui propose qu'il existe une interaction entre les différents composants immunitaires.
- **Le modèle de soi et non soi** qui permet au système de reconnaître ce qui est normal ou ce qui lui appartient afin de détecter le non soi.

Modèles / Travaux	Soi / Non soi	Bibliothèque de gènes	Sélection négative	Sélection clonale	Mémoire immunitaire	Réseau idiotypique	Multi agent	Théorie de danger
[Forrest et al 1994]	**X**							
[Somayaji et al,1996]	**X**							
[Hofmeyr et al ,1998]	**X**							
[Dasgupta et al,1999].	**X**		**X**	**X**			**X**	
[S. Hofmeyr,S.Forrest ,2000]	**X**		**X**		**X**			
[Kim, Bentley,2001].			**X**		**X**			
Greensmith et al ,2005								**X**
[Aickelin et al,2005]								**X**

Tableau 3.1 : Un résumé des différents travaux dans le domaine des IDS [Kim et al, 2007]

8. Conclusion

Dans ce chapitre, nous avons exposé le lien entre l'objectif d'un système de détection d'intrusions et celui du système immunitaire. Le système immunitaire possède une architecture multicouche comme nous l'avons décrit dans le chapitre précédent qui est composée principalement de deux couches qui sont le système immunitaire inné et le système immunitaire adaptatif. Le système immunitaire inné est semblable aux détecteurs basés signature d'un IDS car les deux systèmes ont les connaissances antérieures des attaques. De la même façon le système immunitaire adaptatif est semblable au détecteur d'anomalies d'un IDS parce que les deux systèmes produisent de nouveaux détecteurs d'une manière adaptative afin de détecter les attaques inconnues.

Nous pouvons conclure que le système immunitaire est la meilleure solution qui pourrait être utilisée pour concevoir un système de détection d'intrusions compétent et efficace.

PARTIE II CONTRIBUTION

CHAPITRE 4 : IMPLÉMENTATION ET RÉSULTAT

1. 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 la 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 .

L'algorithme proposé intègre plusieurs modèles du système immunitaire artificiel:l'algorithme de la sélection négative, la sélection clonale, la mémoire immunitaire, le modèle des cellules dendritiques.

2. Ressources matériels et logiciel

Pour la mise en œuvre des applications, nous avons utilisé un micro portable ayant les caractéristique suivantes : Micro processeur Intel i3 à 2.3 GHZ, avec une RAM 2 Go, un Disque dur 250 Go, le système d'exploitation Windows 7.0 Edition Intégrale et comme langage de programmation nous avons utilisé le langage C#, nous avons choisi la méthode de l'approche de base de signature.

3. Notre contribution

Un tour minutieux sur ces travaux nous a permis d'enregistrer les observations suivantes :

- Le modèle de soi / non soi est le modèle le plus adapté dans les différents travaux cités ci-dessus.
- Les travaux cités n'ont pas encore exploité le modèle de la bibliothèque de gènes.
- L'utilisation de l'algorithme de la sélection négative défini par Stéphanie Forrest etson groupe comme un algorithme de base pour générer les détecteurs de non soi.
- La proposition d'un nouveau modèle immunitaire qui se base sur la théorie de danger par **[Greensmith et al,2005]** se basant sur l'abstraction du fonctionnement des cellules dendritiques et qui intègre la notion de danger.

Cette étude prudente nous a permis de constater que les systèmes de détection d'intrusionsbasés sur les systèmes immunitaires artificiels ont encore des points à explorer. Ils peuventadopter des concepts et des aspects plus larges inspirés d'immunologie comme : la théorie de danger et la bibliothèque de gènes.

4. Approche proposée :

Pour la mise en évidence de notre proposition , on s'est basé sur la notion qui dit que : ce n'est plus le caractère étranger d'un élément qui déclenchera une réponseimmunitaire mais c'est le caractère dangereux de l'élément. Cette théorie qui permet de contrôler les envahisseurs dans lesystème qui peuvent être de « non soi mais inoffensifs » et de « soi mais nuisibles ». Nous essayons dans notre travail d'intégrer des idées inspirées de cette nouvelle théorie afin desurmonter les problèmes liés au modèle de soi / non soi.

Nous voulons, à travers cette proposition, exploiter ce fonctionnement de base du système immunitairenaturel pour la détection d'intrusions en ajoutant quelques améliorations sur l'algorithme de la sélectionnégative qui se base sur le modèle de soi et de non soi. Cette amélioration se base principalement sur l'intégration de la notion de danger pour permettre la détection des intrusions réelles causées par desutilisateurs internes ou externes qui endommagent le système.

D'une manière générale,l'approche proposée tente de combiner entre deux éléments de base dans la détection desintrus qui sont les cellules T et les cellules dendritiques. Cette combinaison est tirée à partirdu modèle de la théorie de danger proposé par **Matzinger[Matzinger. P, 1994]**et qui décrit l'interactionentre les cellules dendritiques et les cellules T.

L'approche proposée peut être résumée comme suit :

1. Nous supposons que les signaux de danger apparaissent après une attaque.
2. Le traitement de ces signaux est effectué par les cellules dendritiques.
3. Ces cellules présentent les éléments détectés aux cellules T avec l'information de contexte qui indique la nature de l'élément détecté qui peut être dangereux ou non dangereux dont le but est la détection puis l'élimination des éléments nuisibles

4.1. Fonctionnement

Comme nous avons présenté dans le chapitre relatif au système immunitaire artificiel, le système immunitaire humain contient plusieurs éléments qui travaillent en collaboration pourassurer la protection du corps humain. Un élément principal est les cellules dendritiques quisont des cellules de présentation d'antigènes, spécialisées dans la présentation des protéinesrassemblées pendant leurs phases d'immaturation.

Leur mode de fonctionnement peut être résumé comme suit :

- Chaque élément rassemblé sera présenté avec une information de contexte qui indique s'il est collecté dans un environnement sain ou dangereux.
- Quand les cellules dendritiques achèvent l'étape de maturation, elles peuvent présenter ces éléments au système immunitaire adaptatif et en particulier aux cellules T avec des signaux de contexte dont le but principal est l'activation des cellules T naïves.

- Les cellules T qui ont un récepteur complémentaire à l'antigène seront activées si le contexte de présentation est dangereux ou nécrotique.
- Cependant, si le contexte de présentation est apoptose, alors cela engendre la tolérance des cellules T qui peuvent détecter l'antigène.

L'algorithme, qu'on a proposé, se base principalement sur l'incorporation des interactions existantes entre les deux types systèmes immunitaires inné et adaptatif. Ces interactions peuvent engendrer.

- Soit une activation des détecteurs si l'élément présenté par les cellules dendritiques est un élément dangereux ou bien
- Soit la tolérance des détecteurs dans le cas contraire.

En plus, ces interactions génèrent des changements considérables au niveau des éléments mémoires dont le but est l'obtention d'une mémoire immunitaire qui permet uniquement la détection des éléments dangereux.

Les étapes de l'algorithme proposé peuvent être résumées comme suit :

1. A chaque étape de génération, les cellules dendritiques vont présentent un ensemble d'élément de taille prédéfinie choisi aléatoirement à partir de l'ensemble d'antigènes.
2. Suivant le contexte de l'élément présenté, un nombre d'opération sera établi afin de permettre à la population des détecteurs mémoires la détection des éléments intrusifs.
3. S'il s'agit d'un élément ayant un contexte dangereux, alors l'algorithme vérifie si cet élément est détectable par la population des détecteurs mémoires ce qui conduit à la suppression de cette protéinede l'ensemble d'éléments présenté.
4. Mais, si l'élément dangereux n'est pas détectable par la population des détecteurs mémoires alors l'algorithme vérifie s'il y'a un détecteur qui peut détecter cet élément dans la population des détecteurs matures.
5. Si un tel détecteur existe alors il sera ajouté à la population des détecteurs mémoires et la protéine correspondante sera supprimée de l'ensemble des éléments présentés.
6. Cependant, s'il n'existe aucun détecteur mature qui permet l'identification de cette protéine alors elle sera sauvegardée pour une nouvelle recherche dans les générations suivantes.

7. Dans le cas où l'élément présenté est un élément non dangereux alors l'algorithme vérifie s'il est détectable par la population des détecteurs mémoires afin de supprimer le détecteur correspondant.
8. Pendant la phase de contrôle effectuée par la population des détecteurs mémoires, chaque élément détecté est considéré comme une intrusion. Deux vérifications sur la nature de détection seront utilisées par la suite pour vérifier la fiabilité de l'algorithme:
    - Vérifier si l'élément détecté est un élément dangereux afin de compter le taux de détection des éléments dangereux pour définir **le taux de détection vrai positif.**
    - Vérifier si l'élément détecté est un élément non dangereux afin de compter le taux d'erreurs effectué par l'algorithme pour définir **le taux de détection vrai négatif.**

4.2. Acteurs et composants

L'algorithme présenté intègre plusieurs modèles du système immunitaire artificiel, qui sont :

- L'algorithme de la sélection négative qui est utilisé afin de générer des détecteurstolérants au soi.
- La sélection clonale qui est intégrée pendant le processus de génération des détecteursinitiaux de telle sorte que les détecteurs qui assurent le plus grand nombre dedétections seront choisis pour produire des nouveaux détecteurs.
- La mémoire immunitaire qui permet d'avoir une réponse secondaire rapide.
- Le modèle des cellules dendritiques qui permet de présenter les protéines rassembléesavec une information de contexte afin de générer des changements constants sur lapopulation des détecteurs mémoires selon le contexte de ces éléments.

❖ Les remarques

- Les éléments de l'ensemble d'antigènes restant qui ne sont pas détectés par la population desdétecteurs mémoires seront utilisés dans la phase de contrôle effectuée par la population desdétecteurs matures dont le but principal est la génération de nouveaux détecteurs mémoirescapables de détecter ces éléments dans le futur.
- Les éléments de l'ensemble de soiseront exploités pour générer des nouveaux détecteurs immatures.

4.3. Discussion

1. Le programme utilisé pour la démonstration commence par la création d'un ensemble de six modèles normaux qui ne font pas partie d'une cyber-attaque, représentant des paquets de réseau TCP / IP sous forme binaire. C'est ce qu'on appelle l'auto-set dans la terminologie AIS. Bien sûr, dans un système AIS réel, un jeu de paquets contiendrait vraisemblablement des dizaines ou des centaines de milliers de paquets, et chaque paquet aura une taille plus grande que celle de 12 bits utilisés dans la démonstration (généralement 48-256 bits).

2. Ensuite, le programme de démonstration crée trois lymphocytes artificiels. Chaque lymphocyte a un anticorps simulé composé de quatre bits (encore, artificiellement petit), un âge et un champ de stimulation. Le champ anticorps simulé est essentiellement un détecteur. Comme vous le verrez à bref délai, les lymphocytes sont créés de sorte qu'aucun d'entre eux ne détecte aucun des motifs dans l'auto-jeu.

Nous observons tout d'abord que :

- Une fois le système initialisé, le programme de démonstration commence la simulation avec six modèles d'entrée :
- La première entrée est détectée par le lymphocyte 1, mais parce que chaque lymphocyte a un seuil d'activation, le lymphocyte ne déclenche pas d'alarme.
- À l'instant t = 3, le lymphocyte 1 détecte une autre entrée suspecte mais, encore une fois, le seuil n'est pas encore dépassé.

Mais à l'instant t = 5, le lymphocyte 1 détecte un troisième paquet d'entrée suspecte et une alerte simulée est déclenchée

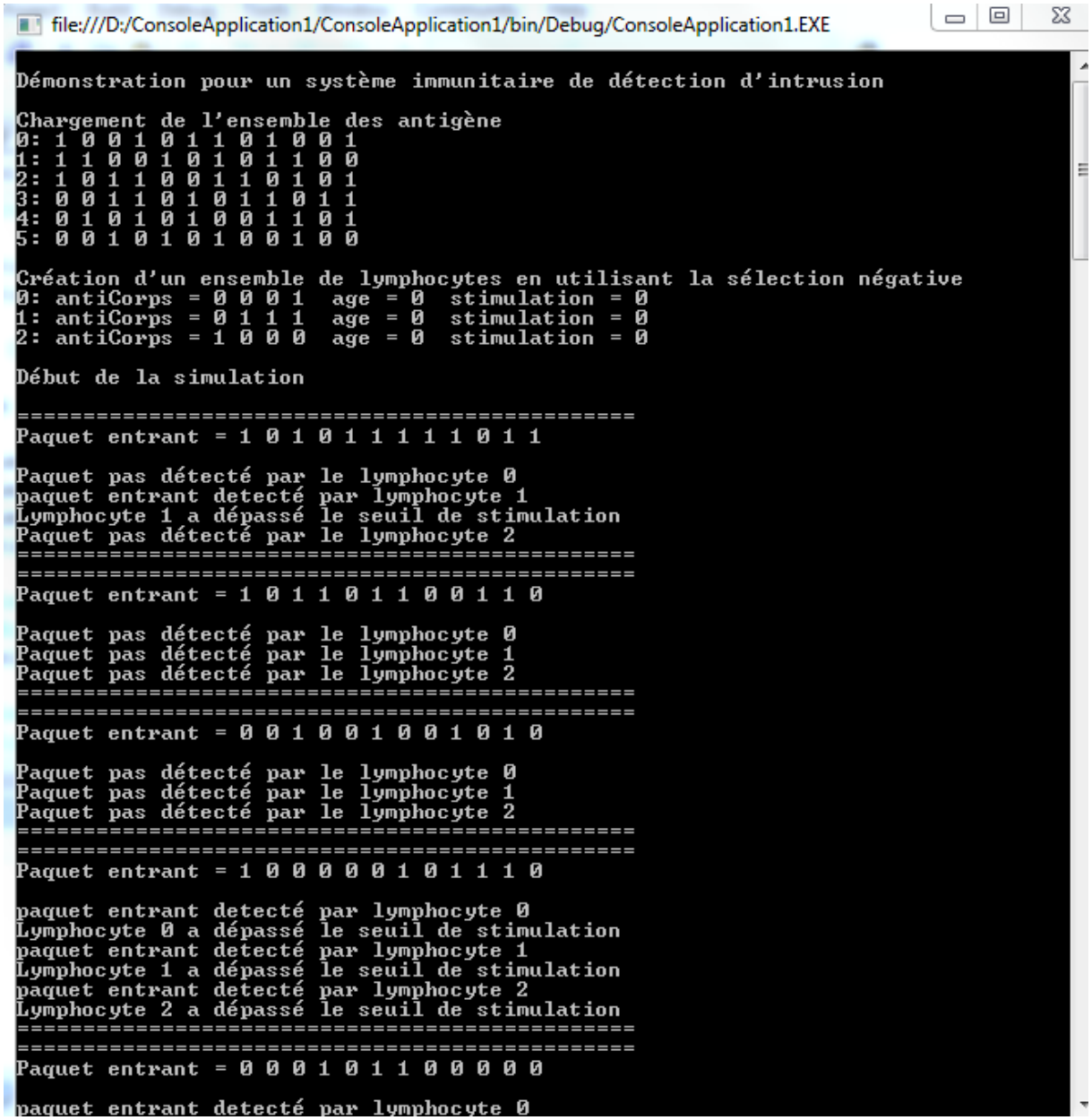

Figure 4.1 : le résultat d'algorithme proposé.

5.conclusion

Le modèle distinction entre le soi et non soi présente quelques problèmes. Avec l'apparition de la théorie de danger qui défie ce modèle et qui présente des nouvelles idées intéressantes, nous avons exploité quelques concepts proposés par cette nouvelle théorie dans la détection d'intrusions afin de surmonter les problèmes liés au modèle de soi et de non soi.

L'algorithme proposé dans ce travail essaye de surmonter les problèmes liés au modèle de soi et de non soi par l'amélioration de l'algorithme de la sélection négative qui se base principalement sur la discrimination entre le soi et le non soi, et qui ne permet pas la détection des éléments dangereux qui constituent réellement des intrusions, ces éléments qui peuvent être des éléments de soi ou de non soi, dont le but est de réaliser les taux de détection .

Cette solution intègre plusieurs concepts du système de détection d'intrusions basé AIS, elle intègre aussi quelques concepts de base de la théorie de danger par l'exploitation de la notion de danger.

Dans cet algorithme, la détection des intrus est liée aux dommages qui peuvent apparaître dans le système, impliqués par des éléments internes ou bien par des éléments extérieurs.

.

CONCLUSION GÉNÉRALE

Conclusion générale

À en juger par les évolutions actuelles, les systèmes informatiques vont vrai semblablement continuer à s'immiscer davantage dans notre quotidien. Le développement de ces systèmes de plus en plus ubiquitaires s'accompagne naturellement de nombreux défis technologiques tels que la mobilité, l'évolutivité et l'autonomie, la réactivité, etc. Parmi ces défis, la question cruciale de la sécurité reste un enjeu majeur en raison de la dématérialisation croissante de l'information et des risques de plus en plus importants liés à la complexité de ces systèmes.

Avec la complexité croissante des réseaux et les systèmes informatiques, les solutions inspirées de la biologie constituent une source d'inspiration intéressante. Ces approches inspirées de la biologie restent intéressantes par rapport à d'autres approches pour deux raisons principales. D'une part, les systèmes informatiques et les espèces biologiques sont souvent attaqués, et d'autre part, 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 assurent la protection du corps contre les intrus d'une manière très puissante.

A travers ce mémoire, nous nous sommes focalisés sur l'utilisation des systèmes immunitaires artificiels dans la sécurité des systèmes informatiques et plus précisément les systèmes de détection d'intrusions. Pour cette raison, nous avons exposé les systèmes de détection d'intrusions, puis nous avons étudié les systèmes immunitaires artificiels afin de pouvoir établir l'analogie entre les systèmes de détection d'intrusions et les systèmes immunitaires artificiels.

Vu l'émergence de la théorie de danger dans l'immunologie et qui défie l'immunologie classique qui se focalise sur la discrimination entre le soi et le non soi. Nous avons essayé d'exploiter la notion de danger stipulée par cette théorie afin de surmonter les problèmes liés au modèle de soi et de non soi qui est le modèle le plus populaire puisqu'il est adopté dans les différents travaux proposés dans ce domaine, dont l'objectif principal est de pouvoir détecter les éléments dangereux qui ont initié des dommages dans le système.

Nous avons utilisé la notion de danger et les interactions immunitaires existantes entre le système immunitaire inné et le système immunitaire adaptatif pour améliorer l'algorithme de la sélection négative qui est fondé sur le modèle de soi et de non soi afin d'obtenir la possibilité de détecter les éléments dangereux dans le système, ces intrus qui peuvent être soient des éléments internes ou externes du système. Nous espérons dans l'avenir d'intégrer d'autres concepts inspirés du système immunitaire humain et en particulier les fonctionnalités proposées par la théorie de

danger comme par exemple la zone de danger qui est établie au tour de signaux d’alarme déclenchés, cette zone qui peut être intégrée dans le système immunitaire artificiel en terme temporelle.

BIBLIOGRAPHIE

[Aickelin. U et al, 2003]	**Aickelin. U, Bentley . P , Cayzer. S ,Kim . J , McLeod. J** « Danger Theory: The Link between AIS and IDS? », in Proceedings ICARIS 2003, 2nd International Conference on Artificial Immune Systems, 147-155, 2003.
[B. White et al,1996]	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.
[Bruce Schneier,2007]	Bruce Schneier, « Security Industry et De la pertinence de l'industrie de la sécurité informatique» ,3 mai 2007.
[De castro L.N ,Von Zuben .F.J,1999]	De Castro .L.N ,Von Zuben .F.J «Artificial Immune Systems: Part I - Basic theory and applications », Technical report, TR-DCA-01/99, December 1999.
[De castro L.N.,Von Zuben .F.J, 2000]	De castro L.N.,Von Zuben .F.J «the clonal selection algorithm with engineering application» proc of GECCO00 ,worksho proceeding,36-37,2000
[De castroL.N,2001]	Leandro Nunes de Castro «An Introduction to the Artificial Immune Systems» Prague, 22-25th April, 2001.
[**De Castro L. N et al,2002]**	Leandro N. de Castro, Fernando J. Von Zuben « Learning and Optimization Using the Clonal Selection Principle » 2002.
[Dado et Guillaume,2003]	Dado konate, Guillaume Lehmann, **«** RAPPORT DE TER SUR PRELUDE-IDS»,13-04-2003.
[De Castro L. N , J. I. Timmis,2003]	De Castro L. N,J. I. Timmis «Artificial immune systems as a novel soft computing paradigm » 14 juillet 2003.
[D. Dasgupta, Z. Ji, F. Gnnzalez,2003]	D. Dasgupta, Z. Ji, F. Gnnzalez, « Artificial Immune System (AIS) Research in the Last Five Years»2003

[Dipankar Dasgupta,1999]	Dipankar Dasgupta «Artificial Immune Systems and Their Applications» University of Memphis, Springer-Verlag Berlin Heidelberg 1999.
[Didier Marcant et Cédric, 2005]	Didier Marcant & Cédric DE BOCK - TTN/FA 2006 - Décembre 2005
[Dorothy E ,Denning,1987]	Dorothy E et Denning« An intrusion detection model »IEE transaction of software ingineering ,VOL .SE -13,NO,2 February 1987
[F.Sabahi, A.Movaghar,2008]	F.Sabahi, A.Movaghar IEEE Member, « Intrusion Detection: A Survey », 2008.
[Fanelli, R. L, 2009]	Fanelli, R. L ,«A Hybrid Model for Immune Inspired Network Intrusion Detection. In: Artificial Immune Systems», Phuket, Thailand. 107-119. 2009.
[Frédéric Majorczyk ,2008]	Frédéric Majorczyk. «Détection d'intrusions comportementale par diversification de COTS : application au cas des serveurs web». Informatique [cs]. Université Rennes 1, 2008
[Goodman D et al,2002]	Goodman D, Boggess L, Watkins A « Artificial immune system classification of multiple class problems »,2002
[Greensmith et al,2005]	Greensmith. J &Aickelin. U &Cayzer. S «Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection», To appear in the Proceeding of the fourth International Conference on Artificial Immune Systems (ICARIS-05), 2005.
[Ghorbani et al,2010]	Ghorbani et al **«**network intrusion detection and prevention»,2010
[H. Debar et al, 1999]	H. Debar, M. Dacier , A. Wespi « A revised taxonomy for Intrusion Detection Systems », Computer science, 1999
[**H. Debar et al,2000]**	H. Debar, M. Dacier , A. Wespi. « A revised taxonomy for intrusion detection systems. Annales des télécommunications ». July–August 2000
[Hiba Khelil, A. Benyettou ,2010]	Hiba Khelil, Abdelkader Benyettou, « Application du système immunitaire artificiel ordinaire et amélioré pour la reconnaissance des caractères artificiels » ,2010
[Hung-Jen et	Hung-Jen Liao a , Chun-Hung Richard Lin a,n , Ying-Chih Lin a,b ,

al,2012]	Kuang-Yuan Tung, « Intrusion detection system: A comprehensive review »,2012
[Hussain Ahmad et al,2014]	Hussain Ahmad Madni Uppal , Memoona Javed and M.J. Arshad, «An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications »,February 2014.
[James P,Anderson,1980]	James P. Anderson« Computer security threat monitoring and surveillance. Rapport technique » 26 février 1980.
[Jungwon Kim,Peter Bentley]	Jungwon Kim and Peter Bentley « The Human Immune System and Network Intrusion Detection »
[jean olivier et al,2000]	Jean-Olivier Gerphagnon , Marcelo Portes de Albuquerque , Marcio Portes de Albuquerque , « Attaques Informatique» 2000.
[Jon Timmis et al,2000]	Jon Timmis , Mark Neal , John Hunt«An artificial immune system for data analysis»,2000
[Jon Timmis ,Thomas Knight ,2002]	Jon Timmis and Thomas Knight «Artificial Immune Systems: Using the Immune System as Inspiration for Data Mining» University of Kent at Canterbury, UK ,2002
[J. Kim,2002]	J. Kim « Integrating Artificial Immune Algorithms for Intrusion Detection », PhD Thesis, University College London, 2002.
[J.Timmis,De Castro.L.N,2003]	J.Timmis & De Castro.L.N « Artificial Immune System as a novel Soft ComputingParadigm ». To appear in the Soft Computing Journal, vol7, Issue 7, July 2003.
[J. Timmis et al,2004]	J. Timmis & T. Knight & L.N. De Castro & E.Hart, «An overview of Artificial immune Systems », Natural computation series, pages 51-86, Springer, 2004.
[Jonathan Krier ,2006]	Jonathan Krier Publié le 21 juillet 2006 «Les systèmes de détection d'intrusions »
[J. Timmis et al,2008]	J. Timmis, A. Honec, T. Stibord, E. Clark « Theoretical advances in artificial immune systems» 21 janvier 2008
[J.R. Al-En et al,2010]	J.R. Al-Enezi,M.F. Abbod ,S. Alsharhan« artificial immune systems – models, algorithms and applications»

	School of Engineering and Design, Brunel University, UK. May 201
[Kim et al, 2007]	Kim, Jungwon ,Bentley, Peter ,Aickelin, Uwe , Greensmith, Julie , Tedesco, Gianni, Twycross, Jamie «Immune System Approaches to Intrusion Detection » A Review. Natural Computing, 6 (4). pp. 413-466. ISSN 1567-7818. (2007) .Access from the University of Nottingham repository
[Karen Scarfone, Peter Mell,2007]	Karen Scarfone, Peter Mell « Guide to Intrusion Detection and Prevention Systems (IDPS) », February 2007
[Labed Ines,2006]	Labed Ines «Proposition d'un système immunitaire artificiel pour la détection d'intrusions » thèse de magister informatique université mentouri de Constantine 2006.
[Landwehr et al. 1994]	Carl E. Landwehr, Alan R. Bull, John P. McDermott, et William S. Choi. « A Taxonomy of Computer Program Security Flaws», septembre 1994
[Mykerjee et al,1994]	Mykerjee. B, Heberlein. L.T , Levitt .K.N « Network Intrusion Detection », IEEE Network, Vol 8, No 3, pp .26-41, 1994.
[Matzinger. P, 1994]	Matzinger. P « Tolerance, danger and the extended family », Annual reviews inImmunology, 12: 991- 1045, 1994
[NIST,2001]	« Intrusion detection Systems ». NIST Computer Science Special reports SP 800- 31, November 2001
[OSI – Basic ,2000]	International Standards Organization. Information Processing Systems - OSI – Basic Reference Model - Part 2: Security Architecture. ISO 7498-2, February 2000.
[**P.Kazienko, P. Dorosz, 2004**].	« Intrusion Detection Systems (IDS) Part I - (network intrusion; attack symptoms; IDS tasks; and IDS architecture) », 2004
[philippe Biondi,2001]	Philippe Biondi, « Architecture expérimentale pour la détection d'intrusions dans un système informatique », Avril-Septembre 2001
[Reachard heady,1990]	Reachard heady «the architecture of network level intrusion detection system»,1990
[Rebecca Bace ,Peter Mell,2001]	Rebecca Bace , Peter Mell ; « NIST Special Publication on Intrusion Detection Systems»,2001

[R. Al-Enezi et al, 2010]	R. Al-Enezi, M.F. Abbod , S. Alsharhan « artificial immune systems – models, algorithms and applications» May 2010.
[Steven Andrew Hofmeyr, 1999]	Steven Andrew Hofmeyr «An Immunological Model of Distributed Detection and Its Application to Computer Security »May 1999.
[Seth Fogie, Cyrus Peikari, 2002]	Seth Fogie, Cyrus Peikari « Intrusion-Detection Systems».2002
[S. Staniford-Chen,1997]	S. Staniford-Chen **«** GrIDS Outline Design Document ». GrIDS Project Home Page at UC Davis's Computer Science Department, 1997.
[Uwe Aickelin , Steve Cayzer,2002]	Uwe Aickelin , Steve Cayzer « The Danger Theory and Its Application to Artificial Immune Systems».2002
[Vasile Parvan ,2009]	Vasile Parvan «Main Types of Attacks in Wireless Sensor Networks» University "Politehnica" of Timisoara, Faculty of Automatics and Computers.2009
[W. Jansen et al,2000]	W. Jansen , P. Mell, T.Karygiannis , D.Marks «Mobile Agents in Intrusion Detection And Response », 2000
[Ying Tan,2016]	Ying Tan, «Artificial Immune System Applications in Computer Security», Copyright 2016 by the IEEE Computer Society, University of Postsand Telecommunications.
Web 01	JamesP,Anderson « computer security threat monitoring and surveillance». Cohttp://csrc.nist.gov/publications/history/ande80.pdf.1980
Web 02	Jonathan krier « Les systemes de detection d'intrusion». http://dbprog.developpez.com/securite/ids/ .2006
Web 03	Carl E. landwehr, Alan R. Bull, John p. Mcdermott, william s. choi« A Taxonomy of Computer Program Security Flaws» . http://dx.doi.org/10.1145/185403.185412. 1994
Web 04	Kim, Jungwon ,Bentley, Peter ,Aickelin, Uwe , Greensmith, Julie , Tedesco, Gianni, Twycross, Jamie «Immune System Approaches to Intrusion Detection »

	http://eprints.nottingham.ac.uk/571/1/07naco_ais_ids_review.pdf. 2007
Web 05	Jungwon Kim and Peter Bentley « The Human Immune System and Network Intrusion Detection » https://pdfs.semanticscholar.org/e56b/2ad41edd08ba3a269be8d6207d2bc43ed323.pdf
Web 06	Leandro Nunes de Castro «An Introduction to the Artificial Immune Systems» Prague, 22-25th https://pdfs.semanticscholar.org/4ece/d9255c82f034133c449ace389092edffe18c.pdf. April2001.