République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université20 Août 1955 Skikda
Faculté des Sciences
Département de l'Informatique

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

De master académique-Option : **Système d'Information(SI)**

Thème :

Un système de détection d'intrusion

Présenté Par :

- GUIRA Toufik
- BOULAHIA Abdelhafid

Encadré Par :

Mr.BENOUDINA Lazher

Session : Juin 2023

Remerciement

En premier lieu, je remercie le bon Dieu de m'avoir donné la force et la patience nécessaire pour achever ce travail.

Je tiens à remercier très sincèrement toutes les personnes qui, par leurs conseils et leurs encouragements ont contribué à l'aboutissement de cette mémoire pour l'obtention du diplôme de master:

En premier lieu, je tiens à exprimer ma profonde reconnaissance à notre encadreur ***Mr.BENOUIDNA Lazher,*** *pour ses précieux conseils et son orientation tout au long de notre recherche.*

Nos remerciements aux membres de jury qui ont accepté de juger notre travail.

Enfin nous exprimons notre profonde reconnaissance à tous responsables et enseignants de l'université de Skikda qui ont contribuent à notre formation.

Dédicace

Tout d'abord, je voudrais remercier Dieu Tout-Puissant, ***mes parents****, mon frère* ***Rashid****, la première personne qui m'a appris à lire et à écrire, et à tous mes frères et sœurs, et un merci spécial à ma femme,* ***Mahriya Aouatif****, qui m'a toujours accompagné à mes côtés, et à tous les membres de sa famille sans exception, et à ma tante* ***Massouda****, qui m'a toujours encouragée à poursuivre mes études. Je tiens à remercier tous les professeurs émérites, en particulier les encadrés du stade* ***BenouDina Lazhar****, et merci de tout cœur d'appréciation et de respect à l'enseignante d'anglais* ***Fatima Al-Zahra Khoja****.*

Toufik

Table des matières

Table des Figures

Liste des Tableaux

Résumé

Assurer la sécurité des réseaux d'entreprises contre les attaques, le vol d'informations et les intrusions est devenu plus que nécessaire de nos jours. Un employé au sein de la même entreprise peut fournir un service aux pirates en les utilisant de manière abusive ou intentionnelle pour causer des dommages matériels considérables. Afin de rendre le système de protection des entreprises efficace, il est essentiel de mettre en place un système qui fonctionne automatiquement, traite les différentes anomalies, et empêche toutes les intrusions et les attaques électroniques malveillantes. Malgré les multiples systèmes de protection, ils restent limités face au développement impressionnant et important du piratage électronique. Parmi ces systèmes, le système de détection d'intrusion (IDS) basé sur multi-agents reste l'un des meilleurs, car il agit comme le système immunitaire de l'homme. Il effectue une lecture préliminaire des paquets, puis les reconnaît pour prendre les mesures appropriées dès la première fois avec l'aide des développeurs, puis par lui-même, ce qui en fait un système très efficace et évolutif jour après jour.

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

Abstract

Securing corporate networks connected to the Internet against attacks, information theft and hacking has become more than necessary to day.An employee belonging to the same organization can provide a service to hackers by misusing it or intentionally to cause property damage, often to the same organization. To make the system of protection of institutions, a special system must be developed that works automatically, corrects various imbalances, and prevents all harmful intrusions and cyberattacks. There are several regulations that remain limited to the terrible and large development of electronic hacking, and perhaps a multi-agent based intrusion detection system (IDS) is one of the best of these regulations, because it works like a human immune system, it does a preliminary reading of the rays and The then recognizes to take the appropriate measures the first time with the help of developers that alone, making it a very effective system, must be developed day by day.

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

ملخص:

تأمين شبكات المؤسسات المربوطة من الهجمات ومن سرقة المعلومات والاختراقات أصبحت أكثر من ضرورية في الوقت الراهن. يمكن للموظف المنتمي لنفس المؤسسة أن يقدم خدمة للمخترقين بسوء استعماله أو عن قصد لإلحاق ضرر مادي على الغالب بها. ولجعل نظام الحماية الخاص بالمؤسسات فعال وجب وضع نظام يعمل بصفة آلية ويعالج مختلف الاختلالات ويمنع جميع الاختراقات والهجمات الإلكترونية الضارة. هناك عدة أنظمة حماية تبقى محدودة أمام التطور الرهيب والكبير للقرصنة الإلكترونية، ولعل نظام كاشف الاختراقات (IDS) متعدد الوكلاء يبقى من أحسن هذه الأنظمة، لأنه يعمل كجهاز المناعة عند الإنسان، يقوم بقراءة أولية للحزم ومن بعدها يتعرف عليها ليتخذ الإجراء المناسب في المرة الأولى بمساعدة المطورين ومن بعد ذلك وحده وهو ما يجعله نظام فعال جدا قابل للتطور يوما بعد يوم.

الكلمات المفتاحية: الأمن، الشبكة، IDS، أنظمة كشف التسلل، أنظمة المناعة الاصطناعية، أنظمة متعددة العوامل.

Introduction générale :

1. Contexte de la recherche :

Pendant les dix dernières années le monde a connus une très grande accélération de croissance et de diversité de données, avec l'apparition des réseaux sociaux dont la notion de big data à vue le jour et l'apparition aussi du notion d'IOT (internet of things), cette énorme et large capacité et surtout la vaste diversité de données et l'accès très facile à internet à rendue la tache de filtrer ou de détecter une attaque ou intrusion à un système très difficile, par ailleurs dans l'autre côté une nouvelle génération de piraterie et hakersse propage suite au développement de nouveaux matériels et logiciels plus puissants et plus performants ce qui a permis est rendu facile au pirates ou hakers de s'infiltrer dans un système, ils trouvent des différentes failles (parfois très faciles) par lesquels ils réussissent à accéder à n'importe quel système et reste cacher sans se faire détecter(aujourd'hui c'est comme ce cacher dans un océan avec sa grande capacité et diversité des espèces contrairement au paravent ce cacher dans une petite rivière limité).

Devant cette situation et comme la plupart des entreprises ainsi que les institutions officielles ou gouvernementales aujourd'hui ont un accès à internet ce qui veux dire qu'elles sont au premier front face aux menaces et cyber attaques 24/24 ce qui rond l'obligation et la nécessité de faire de nouvelles stratégies et plusieurs améliorations au système de protection pour augmenter la capacité de détecter ces attaques ou infiltrations avant même qu'elles arrivent au système et aussi contrer tout genre d'attaque ou possibilité d'intrusions.

Dans ce mémoire en va mettre en œuvre une des solutions parmi autres qui va détecter les possibilités d'intrusions ou attaques dans un système, c'est en lui-même un système de détection d'intrusion basé sur les systèmes immunitaires artificiels (AIS).

Ce travail est divisé en quatre chapitres :

Chapitre I : Sécurité informatique et Les systèmes de détection d'intrusions IDS

Dans ce chapitre en va donner une définition générale de la sécurité informatique et le rôle le plus important de ces taches pour la sécurité de l'information dans les sociétés.

Chapitre II : Les systèmes immunitaires artificiels (AIS)

Dans ce chapitre en va définir les systèmes immunitaires artificiels et voir comment sont inspiré du système immunitaire biologique.

Les différents types de ces AIS et voir quelques exemples d'algorithmes immunitaires artificiels.

Chapitre III : Les systèmes multi_agents

Dans ce chapitre en va défini l'agent dans tous les environnements et la relation entre eux, et la stratégie de défense pour protéger le SI (détecter l'anomalie puis les actions de défense)

Chapitre IV : conception et implémentation.

Dans ce dernier chapitre on parle

2. Problématique

Les systèmes de détection d'intrusion basés sur des systèmes multi_agents ont suscité un intérêt croissant en raison de leur capacité à améliorer la détection des intrusions informatiques. Cependant, plusieurs problématiques peuvent se poser lors de la mise en œuvre de tels systèmes. Voici quelques-unes des problématiques courantes :

Coordination des agents : Les systèmes multi_agents nécessitent une coordination efficace entre les différents agents pour détecter et répondre aux intrusions. La coordination peut devenir complexe, en particulier lorsque les agents ont des connaissances et des capacités différentes. La question de la coordination efficace des agents pour une détection optimale des intrusions se pose donc.

Gestion des ressources : Les systèmes multi_agents peuvent nécessiter des ressources importantes, telles que la puissance de calcul et la bande passante du réseau, pour effectuer leurs tâches de détection. La gestion efficace de ces ressources devient une problématique importante pour assurer des performances optimales du système.

Sélection des caractéristiques : La détection des intrusions repose sur l'identification de caractéristiques ou de comportements suspects. La sélection efficace des caractéristiques pertinentes à surveiller peut être un défi, car il est essentiel d'identifier les caractéristiques discriminantes tout en minimisant les fausses alertes.

Adaptabilité : Les environnements informatiques évoluent rapidement, ce qui nécessite une adaptabilité des systèmes de détection d'intrusion. Les systèmes multi_agents doivent être capables de s'adapter aux nouvelles menaces et aux nouvelles tactiques utilisées par les attaquants. La question de l'adaptabilité du système devient donc cruciale.

Évolutivité : La détection d'intrusion doit être réalisée en temps réel dans des environnements à grande échelle. Assurer l'évolutivité du système pour gérer efficacement un grand volume de données

et de trafic réseau est une problématique importante pour les systèmes basés sur des systèmes multi_agents.

Sécurité : Les systèmes de détection d'intrusion eux-mêmes peuvent être sujets à des attaques. Assurer la sécurité et l'intégrité des agents et des communications entre eux devient une préoccupation majeure pour garantir l'efficacité du système.

Ces problématiques nécessitent une attention particulière lors de la conception et de la mise en œuvre de systèmes de détection d'intrusion basés sur des systèmes multi_agents. Des recherches et des efforts continus sont nécessaires pour relever ces défis et améliorer l'efficacité de ces systèmes dans la détection des intrusions informatiques.

Chapitre I

Sécurité informatique & système de détection d'intrusions IDS

I) Sécurité informatique et système de détection d'intrusion :

Introduction :

Dans ce chapitre on va commencer par la sécurité des systèmes informatiques, les risques informatiques et leur gestion, par la suite on va définir aussi les attaques informatiques et le danger qu'elles représentent sur les entreprises et institutions précisément sur leurs systèmes informatiques ; et enfin on va arriver sur les systèmes de détection d'intrusions qui sont l'une des solutions possibles et efficaces pour contrer les attaques sur le système informatique.

On va voir en détail leurs définition ; les diffèrent types et leurs rôles, comment ils agissent pour filtrer le trafic arrivant et sortant du système informatique.

I-1) La sécurité informatique :

C'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. [1]

I-1-1)Les domaines de sécurité :

La sécurité informatique s'intéresse à la protection contre les risques liés à l'informatique ; elle doit prendre en compte :

- les éléments à protéger : matériels, données, utilisateurs ;
- leur vulnérabilité ;
- leur sensibilité : quantité de travail impliqué, confidentialité…
- les menaces qui pèsent sur eux
- les moyens d'y faire face (préventifs et curatifs) : complexité de mise en œuvre, coût… [1]

Sécurité physique :

Aspects liés aux systèmes matériels Aspects liés à l'environnement : locaux, alimentation électrique, climatisation,… ; nécessitante la prises des différents mesures de sécurité : Respect de normes de sécurité, Protections diverses, Traçabilité des entrées, Gestion des accès, Redondance physique, Marquage de matériels.

Sécurité logique :

Admettant plusieurs prises de mesures dans :

- Mécanismes logiciels de sécurité

- Contrôle d'accès logique : identification, authentification, autorisation
- Protection des données : cryptage, anti-virus, sauvegarde

Sécurité applicative :

L'objectif est d'éviter les « bugs » : Méthodologie de développement par la Mise en place des :

- Plans de Contrôles et tests
- Plans de migration des applications

Sécurité de l'exploitation :

Elle vise le bon fonctionnement des systèmes

- Procédures de maintenance, de test, de diagnostic, de mise à jour
- Plan de sauvegarde Plan de secours

Sécurité des télécommunications :

Nécessité d'une infrastructure réseau sécurisée

- au niveau des accès
- au niveau des protocoles
- Au niveau des systèmes d'exploitation

Au niveau des équipements

I-1-2)Les exigences fondamentales en sécurité informatique [2] :

Il convient d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité :

La confidentialité - Seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.

L'intégrité - Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.

La disponibilité - Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- **La non-répudiation -** Une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificatsnumériques grâce à une clé privée.

- **L'authentification -** Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

Bref, on mesure la sécurité d'un système entier à la sécurité du maillon le plus faible. Ainsi, si tout un système est sécurisé techniquement mais que le facteur humain, souvent mis en cause, est défaillant, c'est toute la sécurité du système qui est remise en cause.

I-1-3)Les risques informatiques :

C'est l'ensemble des facteurs et actions qui menaces la sécurité et le bon fonctionnement d'un système informatique.

"C'est un élément incontournable de l'outil de production et de gestion des établissements de crédits. Ces derniers se sont donc penchés sur la sécurité et la qualité de leur système d'information. (Henri J., 2001, p. 34)". [3]

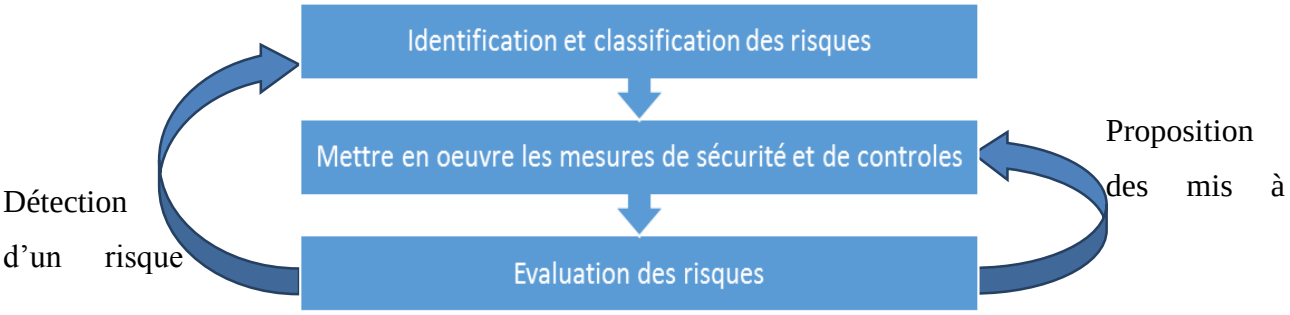
Pour mieux maitriser la sécurité et risques informatiques on doit adapter une stratégie de gestion des risques informatiques.

"Inutile de se préoccuper de sécurité sans avoir défini ce qui était à protéger : en d'autres termes, toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son périmètre de sécurité…

Il est également important de définir contre qui et quoi l'entreprise doit se prémunir. En effet les mesures à appliquer pour se prémunir d'un même risque, par exemple de fuite d'informations, ne seront pas les mêmes si l'attaquant est un pirate peu expérimenté ou une agence de renseignement. Cette définition du périmètre et du niveau souhaités est parfois appelée cible de sécurité". [4]

- **La gestion des risques informatiques :**

  C'est l'identification et la classification des risques pour mieux décider sur la sécurisation du système. [5]



I-1 Gestion des risques informatiques

I-1-4)Les attaques informatiques :

A-Définition :

C'est tout ensemble d'actions qui essaye d'exploiter une ou plusieurs failles du système informatique afin de compromettre :

- La confidentialité : ex. le vol des données, fuite d'informations par canal caché.
- L'intégrité : ex. modifications des fichiers.
- La disponibilité : ex. occupation illégitime des ressources.
- L'authenticité : ex. vol de brevet scientifique des inventions.

Un cyber attaque peut être le fait d'une personne seule (hacker), d'un groupe de pirates, d'une organisation criminelle ou même d'un État. Ces attaques informatiques sont facilitées par la quantité croissante d'informations mises en ligne et par des failles de sécurité dans les systèmes.

Sur internet des attaques ont lieu en permanence. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

B-Différentes causes d'attaques :

Il y a plusieurs raisons qui poussent un pirate à s'infiltrer ou attaquer un système informatique :

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Collecter des informations personnelles sur un utilisateur.
- Récupérer des données bancaires.
- S'informer sur une organisation.
- Troubler le bon fonctionnement d'un service.

- Utiliser le système de n'importe quel utilisateur comme rebond (faire des utilisateurs simples avec leurs matériels comme source d'attaque).
- Exploiter les ressources d'un système comme pirater un système ayan une bande passante très élever. [5]

C-Etapes d'une attaque :

Généralement Il y a une méthodologie retenue par les pirates pour s'introduire dans un système informatique :

- **Reconnaissance :** la collecte d'un maximum d'informations sur la victime ou le système.
- **Compromis initial :** exécuter des codes malicieux sur le système cible qui permet de lancer l'attaque.
- **Implémentation :** Installations des outils d'attaques sur le système.
- **Contrôle des privilèges :** augmentation des privilèges d'admiration et modification du contrôle d'accès…
- **Reconnaissance interne :** exploitation de l'environnement interne du système pour avoir plus de détail qui guide l'attaque.
- **Déplacement latéral :** propager l'attaque ; plus d'exploitation des failles afin de se déplacer dans l'environnement du système (passer d'un utilisateur à d'autres ou à un serveur ou d'autre serveur…).
- **Maintenir la présence :** installation de plusieurs portes dérobées ou des canaux cachés permettant des futurs accès.
- **Effacer la trace :** après l'atteint de son objectif l'attaquant supprime ses traces d'exécution des différents programmes et commandes dans le système tout en gardant toujours un accès.

D-Les différentes classes d'attaques informatiques :

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

D-1.Classification selon l'effet de l'attaque

Selon les effets résultant de l'attaque on peut classifier les attaques en deux groupes principaux, les attaques passives et les attaques actives.

- **Les attaques passives :** consistent à accéder, utiliser ou à observer le système cibles ans modifier les données ou dysfonctionner les ressources de ce dernier, elles sont généralement

indétectables (ex. : capture de contenu, analyse de trafic).

- **Les attaques actives :** consistent à effectuer des changements non autorisés sur les données des systèmes, à s'introduire dans des équipements réseau ou à perturber leurs fonctionnements, les attaques de ce type sont bien évidemment plus dangereuses.(ex.: mascarade et déni de service).

D-2.Classification selon la source de l'attaque :

En termes de relation intrusion-victime, les attaques sont classées comme suit :

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

D-3.Classification selon la cible de l'attaque :

- **Les attaques réseaux :** Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à leur implémentation.
- **Les attaques applicatives :** Les attaques applicatives s'appuient principalement sur des vulnérabilités spécifiques aux applications utilisées.

E-Exemples d'attaques :

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

Voici des exemples d'attaques les plus connues aujourd'hui ciblant les réseaux informatiques.

E-1.Attaques de Dénis de Services (Denial Of Service[DOS])

Est une attaque informatique ayant pour but de rend rein disponible un service, d'empêcher les utilisateurs légitimes d'un service offert. Il peut s'agir de :

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

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise. Les principales attaques

qu'on peut trouver sont Apache2, Back, Land, Mail bomb, SYNFlood, Ping of death, Process table, Smurf, Syslogd, Teardrop, Udpstorm.

E-2.Probing (Sondage)

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

E-3.Attaques User to Root

L'objectifdecetteclassed'attaquesestd'obtenirlamaindel'administrateursystème(Root) à partir d'un simple compte utilisateur par l'exploitation des vulnérabilités, Les exploits les plus connus sont les débordements réguliers des Buffers (buffer over flows) du saux erreurs de programmation, Les principales attaques de ce type sont : Eject, Ffbconfig, Fdformat, Load module, Perl, Ps, Xterm.

E-4.Attaque Remote to User

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

E-5.L'usurpation d'adresse IP (IP Spoofing)

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

E-6.Les analyseurs réseau (sniffer)

Est un dispositif permettant d'écouter le trafic d'un réseau, c'est à-dire de capturer les informations qui y circulent, vu que les données dans un réseau non commuté sont envoyées à toutes les machines du réseau et dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Le sniffer peut également servir cette propriété à une personne malveillante ayant un accès physique au réseau pour collecter des informations (ex : les mots de passes), mais un sniffer

peut aussi être utilisé comme un outil positif pour le but d'étudier et de capturer le trafic d'un réseau par les administrateurs réseaux et les détecteurs d'intrusion (IDS).

E-7.Balayage des ports (port scanning)

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

E-8.TCP Session Hijacking

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

E-9.Les trappes (backdoor)

C'est une fonction ou un programme permettant à un pirate de prendre le contrôle d'un ordinateur à distance. Il peut être placé dans un cheval de Troie ou un virus.

E-10.Attaque par virus

Il s'agit d'un programme autoreproductible et généralement de structure qui contamine le disque dur ainsi que tous autres supports de stockage utilisés et qui peut faire exécuter à l'ordinateur des actions non désirées. Le virus informatique peut donc se propager à l'intérieur même de l'ordinateur, en infectant petit à petit tous les fichiers. Il est donc destiné à modifier à notre insu le fonctionnement de l'ordinateur, certains virus peuvent simplement faire «beeper» le PC, d'autres peuvent détruire les données (formater, effacer le secteur de démarrage, voir détruire le matériel).

I-1-5)Mécanismes de défense contre les attaques réseaux :

C'est l'ensemble de procédures ou dispositifs qui sont conçu pour détecter, prévenir ou contrer les attaques qui menacent la sécurité informatique, il existe plusieurs outils de prévention contre ces attaques réseaux, Nous allons citer ci-dessous quelques mécanismes :

- **Chiffrement :** Algorithmes généralement basés sur des clefs en transformant les données. Son efficacité est dépendante du niveau de sécurité des clefs.
- **Signature numérique :** Données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic :** Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- **Notarisation :** Utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès :** Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.
- **Antivirus :** Logiciel censé à protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- **Le pare-feu :** Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le travers. Ila pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quelles sont les communications autorisées ou interdites. Le pare-feu n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système, ainsi ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- **Journalisation ("logs") :** Enregistrement des activités de chaque acteur. Permet de constater que des attaques ont eu lieu (audit), de les analyser et potentiellement de faire en sorte qu'elles sensée ne produisent pas.
- **Analyse des vulnérabilités ("Security audit") :** Identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles sauront lieu. **[6]**
- **Système de détection d'intrusion :** Repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects autorisés par un utilisateur légitime. Son inconvénient est la mauvaise détection : taux de faux positifs, faux négatifs.

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

I-2) Les systèmes de détection d'intrusions (IDS) :

I-2-1)Définition :

La détection d'intrusions est un terme général qui désigne des méthodes automatiques qui, basées sur l'analyse de séquences d'événements temps réel et/ou enregistrés, peuvent alerter l'administrateur de sécurité de possibles violations de sécurité. [6]

La détection d'intrusions fait référence à la capacité d'un système informatique de déterminer automatiquement, à partir d'événements relevant de la sécurité, qu'une violation de sécurité se produit ou s'est produite dans le passé. [6]

I-2-2)Modèle de base d'un IDS

L'objectif d'une IDS est d'abord la détection d'intrusion, et ensuite informer l'opérateur ou le personnel informatique de la possibilité d'une intrusion dans le réseau. La Figure ci-dessus montre les différents composants de ce système. Il est à noter que les IDSs peuvent ne pas avoir tous ces composants séparés. Certains IDS combinent ces composants en un seul module alors que d'autres ont plusieurs instances de ces modules. [7]

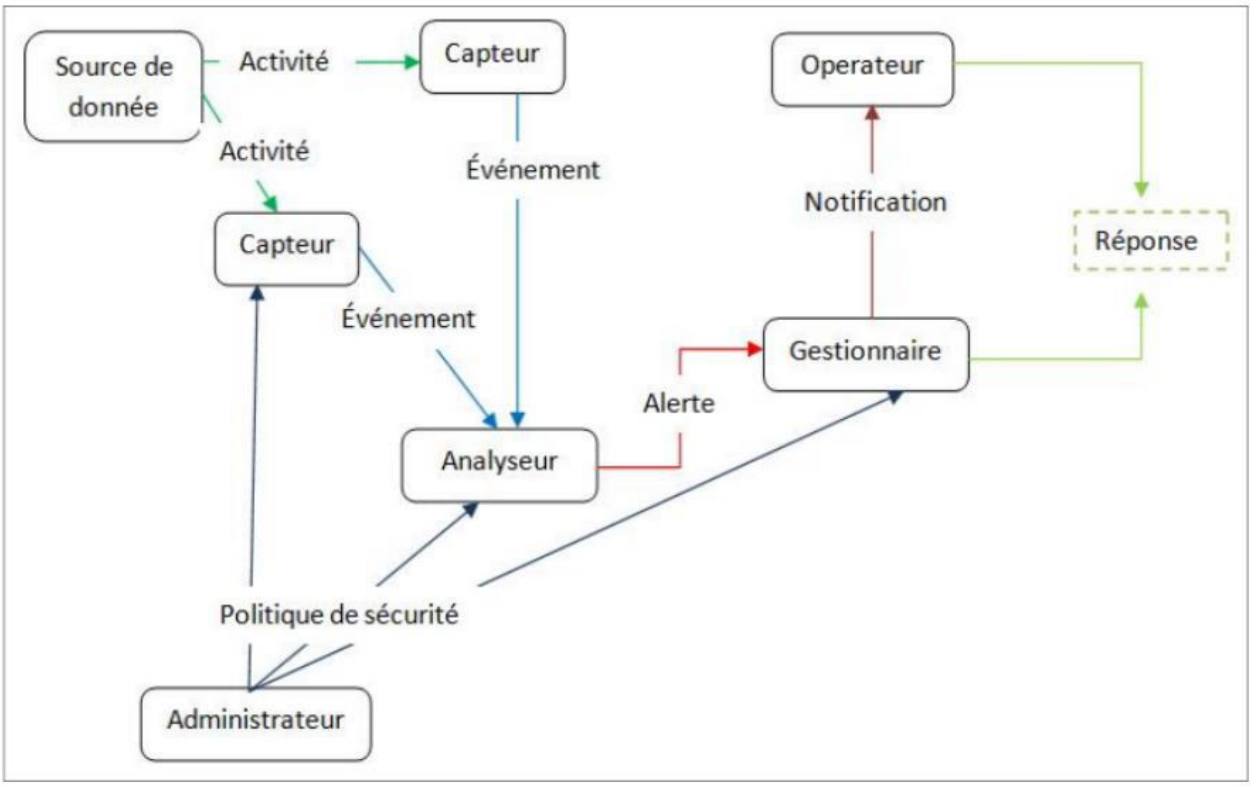


Figure I-2: Modèle fonctionnel du Système de détection d'intrusion [7]

- **L'administrateur :**

Établit la politique de sécurité de l'organisation qui déploie et configure les différents composants d'IDS. Il prend en charge *la déclaration* prédéfinie *des activités autorisées* à se dérouler sur le réseau ou sur des hôtes particuliers pour répondre aux besoins d'un système d'information.

- **La source de données :**

Le Système IDS utilise des capteurs appropriés pour analyser les données survenant de sources différentes pour détecter les activités non autorisées.

- **Le capteur :**

Le capteur collecte toutes les informations des activités survenant et les transfère à l'analyseur comme des avènements (i.e. séquence d'activités).

- **L'analyseur :**

Analyse les événements captés pour signaler les activités indésirables.

- **Le gestionnaire :**

Permet à l'opérateur de gérer les différents composants du système et s'occupe de la configuration du capteur, la configuration de l'analyseur, la gestion de la notification d'événements, etc.

- **La réponse :**

C'est les mesures prises comme réponse à un événement. [8]

I-2-3)L'évolution des IDS :

Le but de la détection d'intrusion est de surveiller les activités du réseau pour détecter les comportements anormaux et les abus dans le réseau. Le concept de détection d'intrusion a été introduit au début des années 1980 après l'évolution d'Internet. [9]

Le tableau ci-dessous présente les jalons de l'histoire de l'évolution des IDS :

Date	Evènement
1980	James Anderson a publié une étude décrivant les moyens d'amélioration d'audit de sécurité desordinateurs et la surveillance des sites du client. L'idée originale derrière l'automatisation de ladétection d'intrusions est souvent inspirée de son papier *« How to use accounting audit files todetect unauthorized access ».* L'étude de James Anderson a précisé que les fichiers d'auditdu SI contiennent des informations vitales pour la compréhension et l'étude des comportements des utilisateurs et la détection de comportements déviants.
1984-1986	Dorothy Denning et Peter Neumann ont recherché et développé le premier modèle d'un IDS entemps réel. Ce prototype a été nommé : Système Expert de Détection d'Intrusions (IDES). Cet IDES était initialement un système expert basé sur des règles formé pour détecter une activité malveillante connue. Ce même système a été affiné et amélioré pour former ce que l'on appelle aujourd'hui le système expert de détection d'intrusions de nouvelle génération (NIDES) .
1988	Des membres du projet Haystack ont formé Haystack Labs en tant qu'entreprise commerciale dans le développement de la détection d'intrusions basée sur l'hôte .
1989	L'apparition des premières notions de Système de Détection d'Intrusions Distribuée (Distributed Intrusion Detection System DIDS). Les DIDS améliorent les principes de détection précédant en analysant des informations contenues sur plusieurs machines. L'analysedes informations a été étendue à l'ensemble des postes clients et ne se restreint plus à l'analyse d'un seul serveur (Haystack Lab).
1990	La notion Système de Détection d'Intrusions Réseau a été abordée. Heberlien, qui a égalementcontribué à l'évolution du projet DIDS, est le premier à avoir introduit la notion de système dedétection d'intrusions hybride, utilisant à la fois comme source de données les informations provenant de l'activité réseau et celle de l'activité du système.
1993	L'US Air Force a mis en place des systèmes automatisés de mesure des incidents de sécurité (ASIM), et l'équipe qui a développé cette solution a formé le Wheel Group en 1994 .

1994	La commercialisation des Systèmes de détection d'intrusions a débuté dans les années 1990 avec l'apparition du premier Système de Détection d'Intrusions Réseau en 1994 (NetRanger deWheel Group) [15], Cisco a acheté le Wheel Group en 1998; cette acquisition a constitué le cœur des services IDS et de sécurité .
1996	ISS « Internet Security Systems » a annoncé la sortie d'un outil pour augmenter la sécurité du réseau avec la reconnaissance d'attaque en temps réel appelée RealSecure.
1997	ISS annonce la première sortie commerciale de leur IDS appelée RealSecure 1.0 pour Windows NT 4.0.
Aujourd'hui	Les fournisseurs font de plus en plus de la publicité qu'ils peuvent traiter à la vitesse du gigabit. (tels que : Les systèmes de sécurité Internet (ISS), NetworkICE et Intrusion.com) annoncent qu'ils peuvent analyser et alerter sur le trafic gigabit. Au fur et à mesure que les réseaux se développent et deviennent plus rapides, les IDS peuvent perdre leur popularité. Pour résoudre ce problème, les fournisseurs se sont tournés vers l'hôte. Dans le but est de fournir des donnéeslorsqu'il est directement sondé pour obtenir des informations et profiter de ses avantages (analyse de l'audit ou des données journal, traitement en temps réel et distribué). Il existe de nombreuses formes telles que l'IDS basé sur l'hôte:TCP Wrappers, Tripwire et un outil gratuit tel que Snort.

Tableau I-1 : Les jalons de l'histoire des IDS [10]

La figure suivante présente l'évolution des IDS :

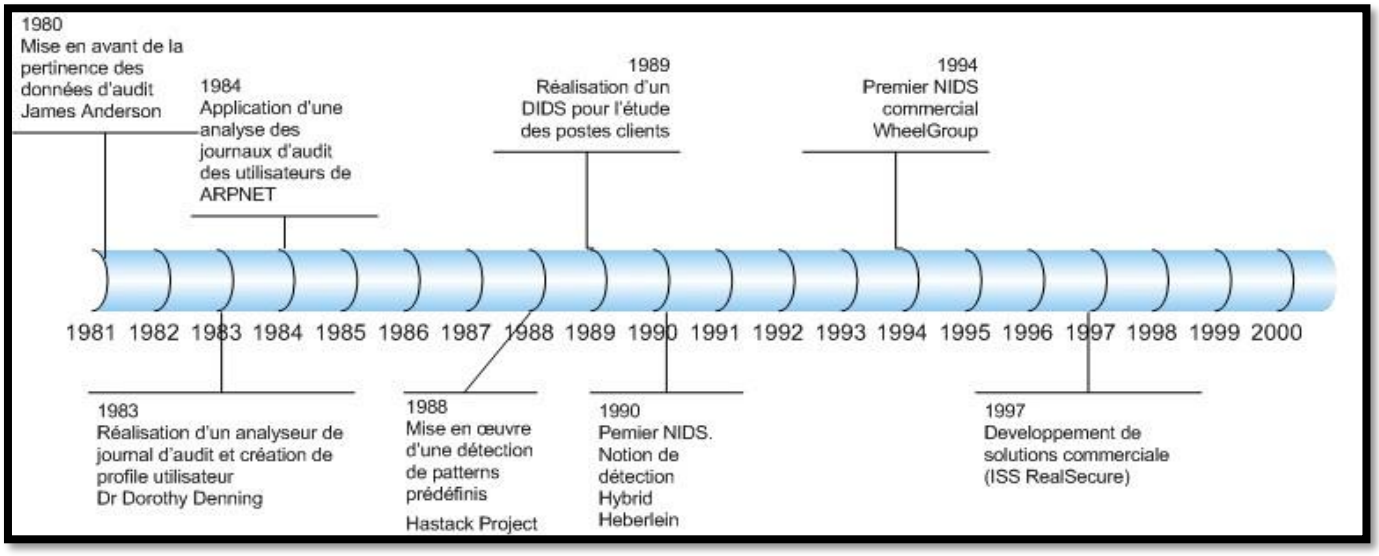


Figure I-3: L'évolution des IDS [11]

I-2-4)Les caractéristiques des IDS :

Le rôle d'un système de détection d'intrusions est de détecter aussi bien un intrus essayant de causer des dommages au système qu'un utilisateur légitime abusant des ressources. Le système de détection d'intrusions doit s'exécuter constamment sur le système, en travaillant en arrière - plan, et ne notifiant l'administrateur de sécurité que lorsqu'il détecte quelque chose qu'il considère comme suspicieux ou illégal [12]. Les systèmes de détection d'intrusions offrent une défense lorsque les vulnérabilités systèmes sont exploitées et cela sans qu'il y ait nécessité de remplacer des équipements très coûteux. [13]

Parmi les systèmes existants, nous pouvons citer DIDS (Distributed Intrusion Detection System) [14] et CSM (Cooperating Security Manger) [15]. DIDS a été conçu pour surveiller un réseau local LAN. Sa nature centralisée représente un désavantage majeur dans le cas de réseaux WAN où les communications avec l'entité gestionnaire peuvent congestionner le réseau. CSM a été développé pour un environnement distribué. Cependant, il ne peut pas être facilement portable vers un autre environnement. En règle générale, les systèmes de détection d'intrusions existants sont mal adaptés à la complexité croissante des réseaux et des attaques auxquels ils sont sujets. Traditionnellement, ils utilisent des méthodes basées sur des modèles de système expert, des modèles statistiques, réseaux de neurones, etc. Ces systèmes sont généralement développés pour des réseaux et systèmes bien définis et ne sont pas adaptés à des environnements dynamiques. En effet, les paramètres des modèles utilisés sont prédéfinis. Ainsi, si une nouvelle attaque doit être détectée, il est très difficile de modifier le système de détection d'intrusions. Globalement, l'architecture des systèmes existants est monolithique. [13]

Dans cette architecture, l'analyse des données collectées par une ou plusieurs entités distribuées n'est effectuée que par un seul module (DIDS). Cette approche présente deux inconvénients majeurs. D'une part, elle présente un point de rupture, dans le cas où l'entité centrale serait attaquée et d'autres parts le déploiement de ce type de systèmes à grande échelle est limité. Dans d'autres systèmes, tel que CSM, l'analyse des données est effectuée sans l'utilisation d'une entité centralisée ce qui résout les problèmes engendrés par l'approche monolithique. Cependant, il existe encore certains inconvénients tel que : 1) la difficulté de s'adapter aux changements qui peuvent se produire dans le réseau et aux comportements des utilisateurs qui varient considérablement ; 2) la difficulté de mise à jour de ces systèmes, lorsque l'on veut améliorer ou rajouter de nouvelles méthodes de détection. [13]

Pour une détection d'intrusions efficace, il est très important de considérer certaines caractéristiques :

A-La distribution :

Un grand nombre d'attaques réseaux se caractérisent par des comportements anormaux à différents éléments du réseau (serveur, routeur,…). Il est donc très important de distribuer les fonctions de détection à plusieurs entités qui surveillent différents points du réseau.

B-L'autonomie :

Des échanges excessifs d'informations entre les entités distribuées peuvent congestionner le réseau. Il serait donc plus judicieux de laisser l'entité, surveillant un élément réseau, effectuer une analyse locale et détecter les comportements intrusifs locaux. Ainsi, les entités distribuées doivent être autonomes.

C-La délégation :

La dynamicité des réseaux nécessite de pouvoir modifier, à n'importe quel moment, les fonctions de détection d'intrusions pour les adapter aux changements se produisant dans le réseau surveillé. Cela est possible grâce au modèle de délégation. Les tâches déléguées sont envoyées aux entités autonomes. Chaque entité aura à exécuter sa propre tâche. Lorsque de nouvelles tâches doivent être ajoutées, ceci est fait dynamiquement.

D-La communication et coopération :

La complexité des attaques coordonnées ne facilite pas leur détection par une seule entité. En effet, chaque entité n'ayant qu'une vue locale restreinte du réseau, il lui est très difficile de détecter ce type d'attaques. La détection de ce genre d'attaques, nécessite une corrélation des différentes analyses effectuées à différents points du réseau. Les différentes entités doivent alors se communiquer leurs analyses et coopérer afin de détecter efficacement les attaques coordonnées.

E-La réactivité :

L'objectif majeur de la détection d'intrusions est de réagir rapidement lorsqu'une attaque se produit afin de limiter les dommages qui peuvent être causés.

F-L'adaptabilité :

Les politiques de sécurité d'une entreprise peuvent changer. Dans ce cas l'administrateur doit changer et/ou rajouter de nouvelles politiques afin de modifier et réadapter les tâches de détection d'intrusions. Le système de détection d'intrusions doit alors s'adapter à ces changements.

En considérant ces six caractéristiques, il apparaît très clairement qu'un SMA est très approprié au problème de détection d'intrusions. L'approche adoptée pour la conception de ce SMA est basée sur deux niveaux : 1) un niveau ***macro*** qui décrit la structure organisationnelle et fonctionnelle du

SMA et 2) un niveau ***micro*** qui décrit l'architecture de l'agent de sécurité. Les deux paragraphes suivants décrivent ces deux niveaux. [13]

I-2-5)Classification des IDS :

Il existe de nombreux systèmes de détection d'intrusion, ces IDS peuvent être classifiés d'après plusieurs critères. Nous avons opté pour le modèle apparu dans la Figure au-dessus :

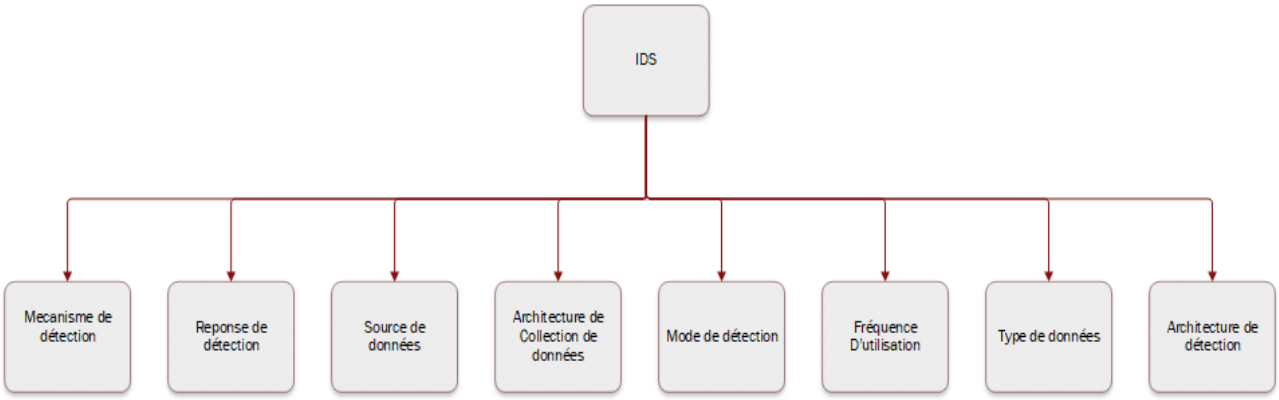


Figure I-4: Taxonomie des systèmes de détection d'intrusion [16]

A-Selon la méthode de détection :

Ces IDS utilisent généralement deux techniques de détection : la détection par anomalie et la détection basée sur les signatures.

A.1. Détection basée sur les signatures

Elle se base sur les connaissances accumulées sur des attaques spécifiques et les vulnérabilités du système. L'inconvénient de cette approche est que seules les attaques connues peuvent être détectées, tandis que les nouvelles attaques passeront inaperçues. Cependant, son principal avantage reste sa grande précision face aux cas d'attaques connues. En effet, elle génère beaucoup moins de faux positifs (fausses alarmes) que celle basée sur l'analyse des anomalies. [17]

A.2.Détection par anomalie

Cette approche de détection suppose que l'intrusion peut être détectée par l'observation de la déviation par rapport au comportement normal ou prévu du système ou des utilisateurs. Le point fort de cette approche est qu'elle arrive à détecter les nouvelles formes d'attaques qui exploitent les nouvelles formes de vulnérabilités non connues auparavant. Cette approche est moins dépendante du système d'exploitation par rapport à l'approche par scénario. Elle peut aussi détecter les attaques d'abus de privilège qui n'exploitent aucune vulnérabilité. Malgré cet énorme avantage, il est à noter certaines insuffisances. Le principal inconvénient de cette technique est le taux de fausses alarmes

très élevé parce que l'ensemble du périmètre du comportement d'un système d'information ne peut pas être complètement couvert pendant la phase d'apprentissage. En outre, le comportement peut changer au fil du temps. Ce qui nous oblige à refaire l'apprentissage du comportement normal, ce qui cause soit l'indisponibilité temporaire du système de détection d'intrusion ou des fausses alarmes supplémentaires. [18]

B-Selon l'emplacement :

B.1.Les systèmes de détection d'intrusion basés hôte (HIDS) :

Comme son nom l'indique, HIDS est installé sur un hôte ou un système et est chargé de surveiller et de prévenir les menaces sur cet hôte uniquement. De telles menaces peuvent affecter un système de plusieurs manières, notamment l'accès au système, la modification des fichiers système, l'occupation inutile de la mémoire du système et l'occupation permanente du processeur. Toutes ces activités sont destinées à rendre le système indisponible pour les tâches assignées. HIDS observe en permanence les fichiers journaux sur l'hôte pour prévenir de telles menaces. Une autre méthode pour protéger l'hôte consiste à surveiller l'utilisation du système en temps réel. Un tel système de détection d'intrusion bénéficie d'une stratégie de protection élevée. Il est très difficile pour un attaquant d'envahir directement le système. [16]

L'inconvénient du HIDS est le coût d'installation élevé, en particulier dans le cas de réseaux plus importants. C'est un fait que HIDS utilise les ressources de chaque hôte. Par conséquent, il n'est pas attrayant pour les réseaux ad hoc à ressources limitées. [16]

B.2.Les systèmes de détection d'intrusion basés réseaux (NIDS) :

Le système de détection d'intrusion réseau est destiné à détecter l'intrusion dans les donnéestransmises par le réseau ou le sous-réseau aux utilisateurs rattachés. NIDS écoute passivement le traffic réseau et essaie de détecter les intrusions en comparant les données d'audit avec les menaces déjà connues stockées dans sa base de données. Si à n'importe quel moment une correspondance se produit, il génère une alarme et avertit l'administrateur concerné. La session d'analyse comprend l'analyse des paquets, de leurs charges utiles et de l'adresse IP et des ports. Un tel système de détection d'intrusion est moins cher en termes de coût d'installation par rapport au HIDS. Cependant, la surveillance du trafic sortant et entrant de l'ensemble du réseau entraîne un goulot d'étranglement des performances. De plus, ils provoquent également des retards de communication. Le NIDS souffre du problème du point de défaillance unique. [16]

B.3.Les systèmes de détection d'intrusion hybrides (NIDS+HIDS) :

Pour surmonter les inconvénients mentionnés ci-dessus du HIDS et du NIDS, un autre système d'intrusion, à savoir le système de détection d'intrusion hybride, est développé, qui combine les fonctionnalités des deux IDS. Les IDS hybrides contiennent des agents qui jouent le rôle de communication entre HIDS et NIDS. Les agents mobiles visitent chaque hôte et effectuent le processus de détection en vérifiant les fichiers journaux du système. A côté des agents mobiles, il existe d'autres agents, à savoir des agents centraux qui parcourent l'ensemble du réseau pour détecter les anomalies de trafic. [16]

B.4.Les systèmes de détection d'intrusion de nœud réseau (NNIDS) :

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

Une autre différence entre NNIDS et NIDS vient de ce que le NIDS fonctionne en mode "promiscuité ", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à destination d'une adresse ou d'une plage d'adresse. Puisque tous les paquets ne sont pas analysés, les performances de l'ensemble sont améliorées. Ce type d'IDS n'est pas encore très répandu, mais ilest de plus en plus utilisé pour étudier le comportement de nœuds sensibles d'un réseau. [16]

C-Selon le type de réponse :

Les IDS peuvent également être classés en deux classes, à savoir les IDS actifs et les IDS passifs :

C-1. IDS actif

Un IDS actif détecte les menaces dans un système ou un réseau et répond activement en bloquant ou en prévenant les menaces détectées. Étant donné que l'IDS actif lui-même empêche la menace après sa détection sans aide extérieure, il est donc également appelé système de détection et de prévention des intrusions (IDPS). Les systèmes IDSP sont réputés pour leur protection automatisée et sont largement utilisés pour protéger les systèmes en temps réel. Ils ont certaines limitations en raison des exigences d'énormes ressources de mémoire et de calcul. [16]

C-2.IDS passif

Passive IDS, comme son nom l'indique, est un IDS qui surveille uniquement le réseau ou un système en silence et ne joue aucun rôle direct dans la prévention de la menace. Au lieu de cela, informez un administrateur ou toute autre entité responsable de bloquer la menace. [16]

D-IDS basé sur la source de données :

Les systèmes de détection d'intrusion sont classés en trois types en fonction de la source des données. Ces types sont décrits un par un.

D-1.Système de détection d'intrusion basé sur l'hôte (HIDS) :

Comme son nom l'indique, HIDS est installé sur un hôte ou un système et est chargé de surveiller et de prévenir les menaces sur cet hôte uniquement. De telles menaces peuvent affecter un système de plusieurs manières, notamment l'accès au système, la modification des fichiers système, l'occupation inutile de la mémoire du système et l'occupation permanente du processeur (L. Vokorokos al, 2010). Toutes ces activités sont destinées à rendre le système indisponible pour les tâches assignées. HIDS observe en permanence les fichiers journaux sur l'hôte pour prévenir de telles menaces. Une autre méthode pour protéger l'hôte consiste à surveiller l'utilisation du système en temps réel. Un tel système de détection d'intrusion bénéficie d'une stratégie de protection élevée. Il est très difficile pour un attaquant d'envahir directement le système. L'inconvénient du HIDS est le coût d'installation élevé, en particulier dans le cas de réseaux plus importants. C'est un fait que HIDS utilise les ressources de chaque hôte. Par conséquent, il n'est pas attrayant pour les réseaux ad hoc à ressources limitées. [16]

D-2.Système de détection d'intrusion basé sur le réseau (NIDS) :

Le système de détection d'intrusion réseau est destiné à détecter l'intrusion dans les donnéestransmises par le réseau ou le sous-réseau aux utilisateurs rattachés. NIDS écoute passivement le trafic réseau et essaie de détecter les intrusions en comparant les données d'audit avec les menaces déjà connues stockées dans sa base de données. Si à n'importe quel moment une correspondance se produit, il génère une alarme et avertit l'administrateur concerné. La session d'analyse comprend l'analyse des paquets, de leurs charges utiles et de l'adresse IP et des ports. Un tel système de détection d'intrusion est moins cher en termes de coût d'installation par rapport au HIDS. Cependant, la surveillance du trafic sortant et entrant de l'ensemble du réseau entraîne un goulot d'étranglement des performances. De plus, ils provoquent également des retards de communication. Le NIDS souffre du problème du point de défaillance unique. [16]

D-3.Système de détection d'intrusion hybride :

Pour surmonter les inconvénients mentionnés ci-dessus du HIDS et du NIDS, un autre système d'intrusion, à savoir le système de détection d'intrusion hybride, est développé, qui combine les fonctionnalités des deux IDS. Les IDS hybrides contiennent des agents qui jouent le rôle de communication entre HIDS et NIDS. Les agents mobiles visitent chaque hôte et effectuent

le processus de détection en vérifiant les fichiers journaux du système. A côté des agents mobiles, il existe d'autres agents, à savoir des agents centraux qui parcourent l'ensemble du réseau pour détecter les anomalies de trafic. [16]

E-IDS basé sur le mode de détection

E-1.IDS en ligne :

Online IDS est une classe de taxonomie IDS dans laquelle le trafic réseau (entrant et sortant) est surveillé en permanence pour détecter les intrusions. Si une intrusion est détectée dans le trafic entrant ou sortant, elle est bloquée dès que possible par le module d'atténuation de l'IDS. Il s'agit de la classe IDS la plus largement utilisée et est également appelée IDS en temps réel. L'importance d'un tel IDS est davantage due au réseau accessible à tous, à tout moment et de partout. [16]

E-2.IDS hors ligne :

D'autre part, l'IDS hors ligne détecte de temps à autre les intrusions dans les référentiels de données autonomes des grands systèmes centraux. Les IDS hors ligne sont relativement utilisésà plus petite échelle en raison de l'utilisation d'activités basées sur le réseau partout et dans toutes sortes d'applications sur ce globe. [16]

F-IDS basé sur l'architecture de détection

L'architecture fait référence à la structure opérationnelle du système de détection d'intrusion.L'IDS peut être classé en quatre groupes différents en fonction de l'architecture de détection telle que l'architecture d'agent autonome, distribuée et coopérative, hiérarchique et mobile. [16]

F-1.Architecture autonome :

Il ressort clairement du nom que chaque nœud d'une telle architecture possède son propre moteur de détection d'intrusion qui détecte les intrusions pour ce nœud spécifique uniquement. Les données collectées par ce nœud spécifique sont utilisées pour comparer avec l'activité malveillante pour la prise de décision. Cette architecture est robuste grâce au fonctionnement indépendant de chaque IDS. Un tel IDS nécessite moins de ressources et peut être déployé facilement. Two Stage IDS est un schéma basé sur une architecture autonome. Les limites courantes de cette architecture sont :

- Les attaques coordonnées ne sont pas détectées dans ces IDS.
- Peut provoquer une collision en raison d'un IDS indépendant à chaque nœud.

- La précision de détection est faible par rapport aux IDS distribués.

F-2.Architecture coopérative distribuée :

Identique à l'architecture autonome, IDS est également installé sur chaque nœud de l'architecture distribuée. Leur fonction est de détecter les intrusions en surveillant les données d'audit locales. Un point qui différencie cette architecture de la précédente est que les données ou résultats d'audit sont partagés avec les nœuds voisins. Cela aide à fournir un mécanisme de détection distribué et coopératif pour la résolution des attaques qui étaient difficiles dansune architecture autonome (C.V. Zhou al, 2010). Cette architecture a amélioré la précision de détection et est capable de détecter les attaques coordonnées. Cette architecture est robuste aux modifications des réseaux. Architecture IDS coopérative basée sur l'analyse des réseaux sociaux et l'IDS assisté par amis (S.A. Razak al, 2008) présentent des schémas baséssur l'architecture coopérative distribuée. Certaines limitations de cette architecture sont :

- Le maintien d'un mécanisme de détection local et global génère une architecture complexe.
- Augmentation des frais généraux de communication en raison de la coopération.
- Sujet aux attaques telles que les attaques de chantage.

F-3.Architecture hiérarchique :

Cette architecture IDS divise le réseau en clusters multicouches où chaque cluster a peu de membres avec un chef de cluster. Chaque chef de cluster joue un rôle de premier plan eta plus de responsabilités que les nœuds ordinaires. Un IDS plus sophistiqué est installé sur le cluster head. Des IDS ordinaires et légers sont installés sur les nœuds restants du cluster. Cette architecture a réduit le risque d'attaques passives telles que les écoutes clandestines. Contrairement à l'architecture distribuée, cette architecture ne nécessite pas de coopération et le surcoût de communication est réduit. Il est également robuste aux modifications du réseau. L'IDS hiérarchique utilisant le modèle de la théorie des jeux (H. Otrok al, 2008), l'IDS hiérarchique optimal (K. Manousakis al, 2008) et la détection d'anomalies de cluster (H. Deng al, 2006) sont quelques-unes des approches basées sur l'architecture hiérarchique. Certaines limitations bien connues sont :

- Signaler des retards.
- Les dommages à la tête du cluster peuvent affecter l'ensemble du cluster.
- Communication supplémentaire en raison du changement répété du chef de cluster.

F-4.Architecture basée sur les agents mobiles :

Cette architecture dispose d'agents avec des logiciels spécialisés et peuvent se déplacer librement ici et là pour visiter chaque nœud du réseau. Tous les nœuds sont censés installer un logiciel agent. Ils ont la capacité de corréler les activités suspectes trouvées dans les nœuds surveillés. Cette architecture prend en charge l'ajout de nouvelles capacités sans redémarrer le système de détection (S.A. Onashoga al, 2009). Des charges et des latences réseau plus faibles sont les avantages de cette architecture, ainsi que l'opulence de la tolérance aux pannes. Cette architecture montre également une évolutivité dans un environnement hétérogène.

G-IDS basé sur la fréquence d'utilisation :

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

G-1.IDS continu :

Les IDS analysent le flux d'informations en continu. Ce mode est communément utilisé dans les IDS réseau, le trafic réseau est analysé directement après la capture. L'analyse en continue permet de prendre des actions immédiates contre toute activité malveillante détectée. Ce mode est efficace dans le cas où la vitesse de traitement des IDS est supérieure à la vitesse de transfert dans le réseau, sinon il est impossible de faire l'analyse en temps réel [25]. Cela est nécessaire dans des contextes sensibles (confidentialité) et/ou commerciaux (confidentialité, disponibilité). C'est toutefois un processus coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système [26].

G-2.IDS périodiques :

Certains systèmes de détection d'intrusions analysent périodiquement les fichiers d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans descontextes peu sensibles (une analyse journalière, par exemple) [26].

I-2-6)Architecture des IDS: [10]

A-Architecture de base :

Plusieurs architectures ont été proposées pour décrire les différents éléments intervenants dans unsystème de détection d'intrusions. L'architecture la plus simple est composée de trois modules : la source de données, l'analyseur des données et le module de réponses.

B-Les modules d'IDS :

B-1.Source de données :

Appelée aussi sonde de capture ou senseur, elle s'occupe de la récupérationdes informations et des événements liés à la détection, pour les envoyer au module d'analyse. Laposition de la sonde de capture joue un rôle très important dans la qualité de la détection. Plusieurs sondes peuvent être utilisées dans le même IDS. Ces sondes seront positionnées dans despoints stratégiques du système.

Les sources possibles de données à analyser sont une caractéristique essentielle des systèmes de détection d'intrusions. Les données proviennent, soit de fichiers générés par le système d'exploitation, soit des fichiers générés par des applications, soit encore d'informations obtenues en écoutant le trafic sur le réseau.

Sources d'information ***système***

Un système d'exploitation propose plusieurs sources d'information :

- **Historique des commandes systèmes** : Tous les systèmes d'exploitation fournissent des commandes pour avoir un « instantané » de ce qui se passe. Ainsi, sous UNIX, des commandes telles que « *ps* », « *pstat* » ou « *vmstat* » fournissent des informations précises sur les événements système.
- **Accounting** : L'accounting fournit des informations sur l'usage des ressources partagées par les utilisateurs (temps processeur, mémoire, espace disque, débit réseau, applications lancées)
- **Système d'audit de sécurité** : Tous les systèmes d'exploitation proposent ce service pour définir des événements, les associer à des utilisateurs et assurer leur collecte dans un fichier d'audit. On peut donc potentiellement disposer d'informations sur tout ce que font lesutilisateurs : accès en lecture à un fichier, exécution d'une application, etc.

Les outils utilisant ces sources de données sont appelés **Host Based Intrusion Detection System**,« **HIDS** ».

Sources d'information applicatives

Les grandes catégories d'applications savent toutes générer des informations sur l'utilisation qui en est faite. C'est le cas des fichiers de logs générés par les serveurs ftp et les serveurs web. Peu de systèmes de détection d'intrusions les utilisent. On peut toutefois citer l'outil WebStalker.

Sources d'information ***réseau***

Des dispositifs matériels ou logiciels (sniffers) permettent de capturer le trafic réseau. Cette sourced'information est intéressante car elle permet de rechercher les attaques en déni de service qui

se passent au niveau réseau et les tentatives de pénétration à distance. Néanmoins, il est difficile de savoir qui est à l'origine de l'attaque car il est facile de masquer son identité en modifiant les paquets réseau. Presque tous les outils (commerciaux) récents utilisent cette source d'information

Les outils utilisant ces sources de données sont appelés **Network Based Intrusion Detection System, « NIDS »**

B-2.L'analyseur des données :

C'est le cœur de l'IDS, ce module permet d'analyser les informations collectées par les sondes de capture. Il utilise une base de connaissances liée aux attaques et pour la recherche des traces des activités malveillantes il applique des différents modèles d'analyse.

B-3.Le module de réponses :

C'est le module qui assure les réponses des IDS aux activités malveillantes détectées. Les réponses peuvent être actives ou passives, c'est les contre-mesures nécessaires pour contrer les intrusions. Ça peut être un simple message d'alerte, une sauvegarde dans un fichier log ou bien interrompre une connexion.

La figure suivante présente un schéma récapitulatif de l'architecture de base d'IDS :

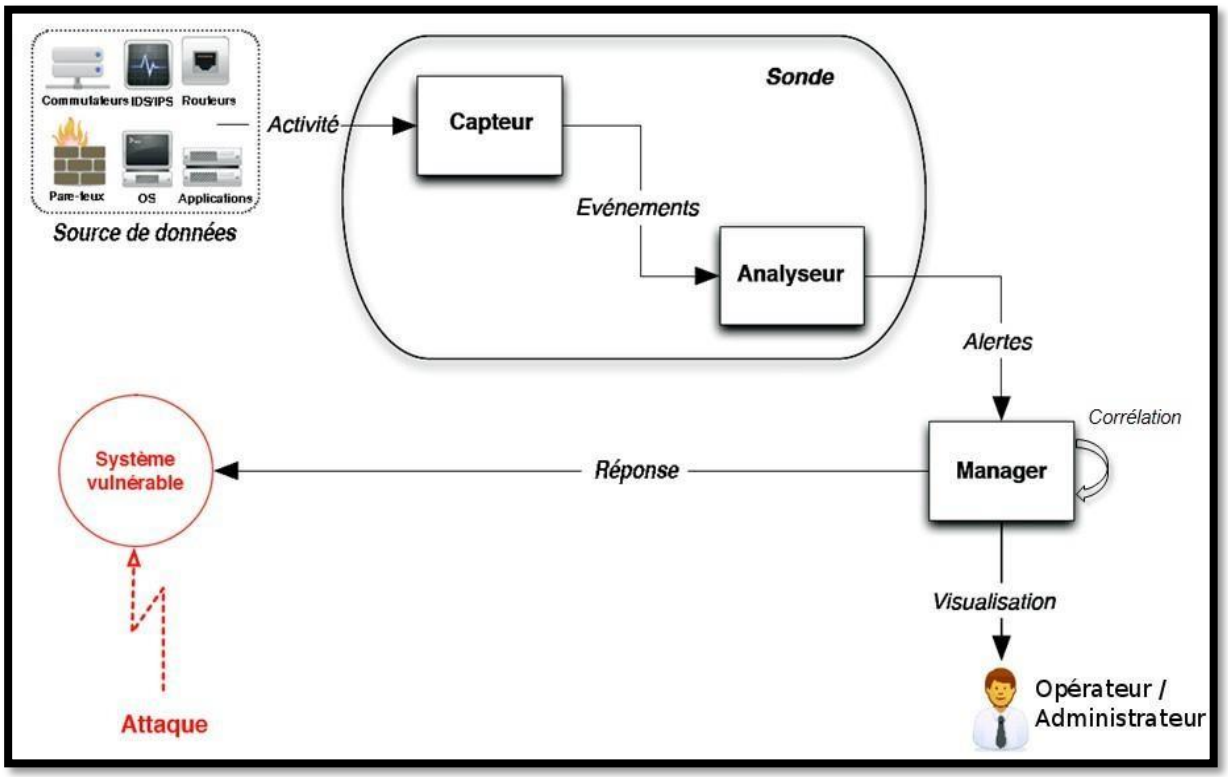


Figure I-5 Architecture de base d'IDS [10]

I-2-7)Le déploiement des IDS : [8]

De nombreux types de technologies d'IDSs selon l'endroit et l'environnement où ils sont déployés pour inspecter les activités suspectes ainsi que les types d'événements qu'ils peuvent reconnaître.

A-Architecture de réseaux :

Liés au nombre de systèmes IDSs et à la corrélation des données entre eux, il existe trois (03) Architectures :

A-1.Systèmes centralisés :

Un seul système qui prend la charge de collecter les données et identifier les intrusions

A-2.Systèmes Distribué :

Les données sont collectées par plusieurs IDSs permettant la corrélation des données entre eux pour identifier les attaques distribuées

A-3.Systèmes hybrides

B-Type de réseaux :

Dépend de l'interconnexion de l'IDS avec les systèmes de surveillance. Il peut être une connexion filière, sans fils, hybride.

C-Type de technologie :

L'adoption de plusieurs types de technologies IDS peut atteindre l'objectif d'une détection plus complète et plus précise.

C-1.IDS basé sur l'hôte :

Surveille et collecte les caractéristiques des hôtes contenant des informations sensibles, des serveurs exécutant des services publics et des activités suspectes.

C-2. IDS basé sur réseaux :

Capture le trafic réseau sur des segments de réseau spécifique via des capteurs, puis analyse les activités des applications et des protocoles pour reconnaître les incidents suspects.

C-3.IDS Sans fil :

Similaire à l'IDS basé sur réseaux, mais il capture le trafic réseau sans fil, comme les réseaux Ad-hoc, les réseaux de capteurs sans fil et les réseaux maillés sans fil.

C-4.Système basé sur l'analyse du comportement du réseau :

Cette classe des systèmes se diffère à la classe précédente (IDS basé sur des réseaux), ce système inspecte le comportement du trafic réseau pour reconnaître les attaques avec des flux de trafic inattendus, comme DDos Attaques, malware et des services AP inattendus.

C-5.Système Hybride :

Adoptée Les technologies précédentes pour atteindre l'objectif d'une détection plus complète et plus précise.

I-2-8)Critères de tests d'un IDS :

A-Avantage des IDS :

Les systèmes de détection d'intrusion offrent beaucoup d'avantages comme :

- une efficacité plus grande que celle de la détection manuelle des intrusions ;
- l'utilisation d'une base de connaissance plus grande pour prédire les intrusions ;
- la surveillance et l'analyse des événements système et des comportements des utilisateurs ;
- la reconnaissance des modèles d'activité qui diffèrent de l'activité normale ;
- la capacité de traiter un large volume de données ;
- la production d'alertes presque en temps réel, ce qui réduit le dommage potentiel des attaques ;
- des mesures de contre-attaque automatique comme la fermeture des sessions, désactivation des comptes utilisateur, lancement des scripts automatiques ;
- l'ajout d'une valeur préventive forte ;
- la création automatique des rapports.

B- Limite des IDS :

Les IDS sont confrontés aux défis suivants :

- détecter les attaques récemment publiées ou variantes d'attaques existantes ;
- répondre efficacement aux attaques lancées par des attaquants sophistiqués ; enquêter automatiquement les attaques sans intervention humaine ;
- résister à des attaques qui sont destinées à les vaincre ou les contourner ;
- l'utilisation de messages cryptés pour transporter des informations malveillantes ;
- des niveaux inacceptables de faux positifs et de faux négatifs rendant difficile la détermination de vrais positifs ;
- une visibilité limitée du trafic sur le réseau résultant des réseaux locaux commutés (des réseaux plus rapides empêchent l'analyse efficace en temps réel de
- tout le trafic).

Conclusion :

Ce chapitre a été consacré à la présentation des attaques et des risques qui menacent la sécurité informatique au niveau personnelle ou au niveau des entreprises ainsi que la proposition des IDS comme étant un moyen de renforcement de la politique sécurité qui sert non seulement à diminuerles risques mais aussi réagir face aux tentatives d'outrepasser les mécanismes de sécurité.

A travers ce chapitre on a pu présenter l'évolution des IDS au cours du temps avec ses différents types et les avantages tirés de chaque type, Ce qui rend les IDS un élément indispensable dans la sécurité des hôtes et des réseaux car ils sont très efficaces dans la détection des activitésmalveillantes grâce aux nouvelles approches et techniques de détection appliquées.

A la fin du chapitre, on a terminé avec des perspectives d'avenir des prochains IDS afin de surpasser les limites des IDS actuels d'une part et d'une autre part pour améliorer les performanceset les méthodes de détection.

Chapitre II

Les systèmes immunitaires

II) Les systèmes immunitaires :

Introduction :

L'immunité biologique est un système naturel capable de réagir et de s'adapter aux menaces biologiques qui guettent l'organisme hôte. Ce système a suscité l'intérêt d'une communauté croissante de chercheurs. Leurs travaux ont contribué à l'émergence de systèmes immunitaires artificiels (SIA) comme un nouveau paradigme de l'intelligence artificielle. L'objectif de ce chapitre est d'identifier les principes immunitaires biologiques les plus pertinents, et de présenter les applications qui s'en sont inspirées dans les systèmes de production. Ce chapitre va nous permettre de constater qu'il n'existe pas d'approche immunitaire consensuelle, et de remarquer que les SIA ont été appliqués à plusieurs domaines, sauf le pilotage de systèmes de production soumis à des perturbations. Nous déduisons que l'immunité biologique peut apporter plusieurs réponses intéressantes aux lacunes des approches de pilotage existantes en matière de prise en compte et traitement des perturbations. Toutes ces constatations nous permettent de définir notre problématique de recherche. Cette dernière consiste à envisager l'immunité biologique comme un support pouvant inspirer un cadre conceptuel intégré pour la prise en compte des perturbations dans les systèmes de production. [19]

II-1) Le système immunitaire :

Le système immunitaire est une collection de cellules, des molécules et des organes. Il représente un mécanisme d'identification capable de percevoir et de combattre le dysfonctionnement de ses propres cellules et les micro-organismes exogènes infectieux qui envahissent le corps [18].

II-2) Les systèmes immunitaires naturels :

Introduction :

L'immunité biologique est un système naturellement doté de mécanismes lui permettant de justifier d'un haut degré de réactivité et d'adaptabilité contre les menaces biologiques qui guettent l'organisme hôte. Les caractéristiques de ce système ont intéressé les chercheurs et les ont incités à les étudier pour en dériver des applications artificielles. Leurs efforts ont contribué à l'émergence de plusieurs systèmes immunitaires artificiels (SIA). [19]

II-2-1)Historique :

Année	Evènement
1798	**Edward Jenner** lance la vaccination contre la variole.

1879	**Louis Pasteur** met au point un vaccin atténué contre le choléra du poulet.
1885	**Louis Pasteur** met au point un vaccin contre la rage.
1891	**Robert Koch** explore l'hypersensibilité de type retardé.
1900	**Paul Erlich** théorise la formation d'anticorps spécifiques.
1906	**Clemens Von Pirquet** a inventé le mot allergie.
1938	**John Marrack** formule une hypothèse de liaison antigène-anticorps
1959	**Niels Jerne, David Talmage, et Macfarlane Burnet** développent la théorie dela **sélection** clonale
1957	**Alick Isaacs** et **Jean Lindemann** découvrent l'interféron (cytokine).
1962	**Rodney Porter** et son équipe découvrent la structure des anticorps.
1962	**Jaques Miller** et son équipe découvrent l'implication du thymus dans l'immunité cellulaire.
1962	**Noel Warner** et son équipe distinguent les réponses immunitaires cellulaires et humorales.
1968	**Anthony Davis** et son équipe découvrent la coopération entre **les cellules T** et les **cellules B** dans la réponse immunitaire.
1974	**Rolf Zinkernagel** et **Peter Doherty** explorent la restriction du **complexe majeur d'histocompatibilité « CMH »** .
1985	**SusumuTonegawa** , **Leroy Hood** et l'équipe identifient les gènesd'immunoglobulines.
1987	**Leroy Hood** et son équipe identifient les gènes du récepteur des lymphocytes T
1985	Les scientifiques commencent l'identification rapide des gènes des cellules immunitairesqui se poursuit jusqu'à présent.

Tableau II-1:Les jalons de l'histoire de l'immunologie [20]

II-2-2)Système Immunitaire Naturel « SIN » :

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'. On distingue deux types principaux d'immunité naturelle : une innée et une acquise. [21]

II-2-3) Architecture du système immunitaire :

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

A-L'immunité innée :

L'immunité innée est une immunité élémentaire qui est adaptée seulement à un certain nombre très réduit d'antigènes. On trouve ce type d'immunité chez les nouveaux nés qui ne sont pas encore vaccinés. Une immunité non adaptative pour longtemps peut conduire à des infections et à la mort car le corps n'est pas encore bien protégé contre les antigènes de l'environnement. [21]

B-L'immunité acquise

L'immunité acquise est une immunité à mémoire (réponse secondaire), qui se développe lors de l'apparition du même antigène dans le même système immunitaire pour la deuxième fois ou plus, et qui engendre le développement et la génération des cellules B mémoire pour ce type d'antigène déjà rencontré (mémorisé) dans le système. Cette réponse est plus rapide que celle innée. Une réponse immunitaire engendre une augmentation de la température du corps, ce qui explique que les cellules B développées sont en train de lutter contre les antigènes introduits dans l'organe humain. La réponse immunitaire primaire est plus lente mais elle garde les informations du passage des antigènes dans le système. Il paraît intéressant de s'inspirer de ce phénomène de mémorisation pour une reconnaissance artificielle des formes. [21]

II-2-4)Propriétés du système immunitaire

Le système immunitaire biologique est un système robuste, complexe et adaptatif qui défend le corps contre les agents pathogènes étrangers. Il est capable de catégoriser toutes les cellules(ou Molécules) dans le corps. [24]

Citons quelques propriétés les plus importantes du système immunitaire [24]

- ***Multicouche :***

Le système immunitaire possède une architecture multicouche composé de deux sous-systèmes inter-liés qui sont : le système immunitaire inné et le système immunitaire adaptatif. Ces deux systèmes combinent leurs tâches et responsabilités pour assurer la protection et la sécurité globale

- ***Unicité :***

Chaque élément dans le système immunitaire assume ces responsabilités particulières.

- ***Autonomie :***

Le système immunitaire humain ne dispose d'aucun contrôle central. Il possède une autonomie globale dans la détection et l'élimination des intrus.

- ***Distribution :***

Les cellules immunitaires et les molécules sont distribuées dans le corps humain pour assurer la protection. Il n'existe pas un point de contrôle centralisé.

- ***Parallélisme :***

Le système immunitaire est capable de produire plusieurs réponses immunitaires en même temps à des endroits dispersés.

- ***Tolérance au soi :***

Le système immunitaire humain peut différencier entre les cellules de soi et les cellules de non-soi.

- ***Apprentissage :***

Le système immunitaire augmente la capacité d'identification des anticorps à un antigène sélectif (les réponses primaire et secondaire). Il apprend continuellement les structures de pathogènes.

- ***Adaptabilité :***

Le système immunitaire humain permet la production des cellules de plus en plus spécialisées pour l'identification des antigènes. Cela est garanti par la théorie de la sélection clonale suivie par le mécanisme de l'hyper mutation somatique.

- ***Dynamique :***

Le système immunitaire est dynamique il crée de nouvelles cellules et molécules, et élimine les cellules vieilles ou endommagées. Un bon exemple de la dynamique du système immunitaire est la théorie du réseau idiotypique

- ***Mémorisation :***

Suite à une réponse immunitaire donnée, les cellules intervenantes se transforment en cellules mémoires avec une durée de vie longue afin de répondre plus rapidement à une nouvelle intrusion du même type d'antigène.

- ***Coopération :***

Les cellules immunitaires coopèrent afin de défendre le système, ainsi assurent une meilleure détection

- ***Détection :***

Le système immunitaire est capable d'identifier et de détecter tout type d'intrusion sans aucune connaissance préalable de l'antigène.

- ***Discrimination entre soi et non-soi:***

La plus importante propriété qui est à la base des réactions immunitaires est l'aptitude du système immunitaire à distinguer entre les cellules du Soi et les cellules du non-Soi (étrangères) ainsi que la possibilité de reconnaitre le type exact de chaque cellule étrangère.

II-2-5)Mécanismes biologiques de détection : [19]

Les cellules du système immunitaire présentent à leur surface des récepteurs dits « PRR » (pour « Pattern Recognition Receptors »). Ces récepteurs sont capables d'identifier des portions (ou « PAMP », pour « Pathogen Associated Molecular Pattern ») présentes à lasurface des pathogènes, des fragments (ou « antigènes ») de ces pathogènes ou des « toxines », qui sont des substances sécrétées par ces pathogènes. LesPAMP, les antigènes ou les toxines représentent des empreintes permettant de détecter la présence d'un pathogène.

Plusieurs théories ont été proposées afin d'expliquer comment est-ce que le système immunitaire distingue les éléments (cellules,tissus, substances, molécules) qui appartiennent à l'organisme – le Soi – de ceux qui sont nuisibles à l'organisme – le Non Soi.

Selon la théorie de la discrimination Soi/Non Soi, la surface des cellules immunitaires est munie de récepteurs, dits « PRR » (pour « Pattern Recognition Receptors »), capables de détecter exclusivement le Non Soi, de se lier avec ses empreintes et de déclencher les mécanismes permettant de l'éliminer. Ainsi, la décisiond'élimination du pathogène, ainsi que celle sur la manière avec laquelle ce dernier est éliminé reviennent aux cellules immunitaires. Par exemple, la Figure ci-dessus illustre ce mécanisme par lequel une cellule immunitaire (lymphocyte B) est capable de détecter la présence d'un antigène.

La théorie du danger fournit une autre vision, selon laquelle la prise de décision revient non pas aux cellules immunitaires, mais plutôt aux cellules de l'organisme que le système immunitaire est sensé protéger. Selon cette théorie, les SIB sont capables de détecter et de réagir au danger, plutôt que de détecter ou de réagir au Non Soi. Les cellules agressées sont capables de guider la réponse immunitaire par la production de signaux de danger qu'elles émettent lorsqu'elles périssent de manière anormale.

Ces signaux établissent un périmètre de danger autour de la cellule agressée, au sein duquel les cellules immunitaires qui réussissent à identifier le pathogènesont activées pour le capturer.

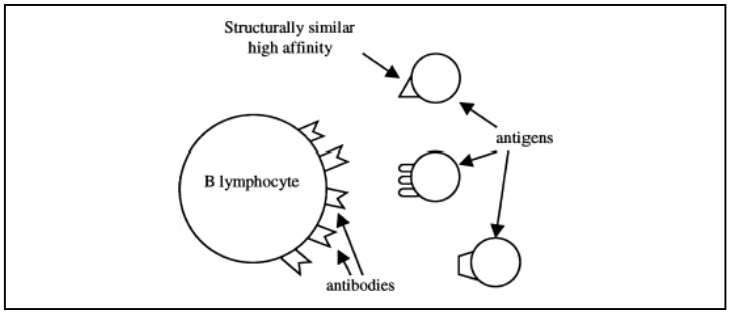


Figure II-1: Mécanisme de détection structurale.

Par ailleurs, certains virus sont capables d'échapper à la détection par leurs empreintes (PAMP, antigènes ou toxines) et ne se manifestent qu'après avoir infecté des cellules hôtes. Lorsqu'un tel virus envahit une cellule de l'organisme, il dérègle son fonctionnement. Les cellules infectées manifestent alors à leur surface des récepteurs

Différents de ceux habituellement affichés, ou ne manifestent plus du tout de récepteurs. Certaines cellules spécialisées (cellules NK et Tk) du système immunitaire sont capables de détecter ce changement dans le comportement des cellules infectées. Elles sont alors activées et procèdent à l'élimination des cellules infectées.

II-2-6)Les réponses immunitaires : [19]

Les principales caractéristiques d'une réponse immunitaire adaptative en présence d'un antigène sont décrites par le principe de sélection clonage.

Cette théorie stipule que seuls les lymphocytes B qui détectent l'antigène sont sélectionnés, prolifèrent, se différencient, et sécrètent des anticorps, molécules très spécifiques à l'antigène capables de le neutraliser et de faciliter son élimination par d'autres cellules immunitaires. Lorsqu'un lymphocyte B détecte un antigène, plus précisément, lorsquel'intensité de la liaison chimique entre les récepteurs à la surface du lymphocyte B et l'antigène excèdent un seuil d'activation ou seuil d'affinité, il est stimulé pour reproduire des clones (copies) de lui-même. En se formant, ces clones subissent un mécanisme de maturationde l'affinité destiné à améliorer la capacité des lymphocytes B à détecter l'antigène. Ce mécanisme est mis en œuvre grâce à des mutations à la fois rapides, pour accélérer la réponse à l'antigène, et de haute fréquence pour améliorer la qualité de la liaison chimique avec l'antigène.

Une réponse immunitaire réussie conduit à la formation de cellules mémoires ayant une haute affinité avec l'antigène à l'origine de la réponse. Si des cellules mémoires issues d'une première réponse immunitaire sont confrontées de nouveau à un antigène connu, ou ayant unestructure voisine de celle d'un antigène connu (principe d'immunisation), elles sont immédiatement activées et déclenchent une deuxième réponse immunitaire plus rapide et plus virulente que la première.

II-2-7)Les théories immunitaires :

Le choix d'un algorithme immunitaire traduit la décision du concepteur d'adopter tel ou tel mécanisme impliqué dans l'immunité naturelle pour le traduire en outil de résolution d'un problème donné. Il existe plusieurs algorithmes immunitaires différents qui s'appliquent à une variété de domaines divers mais qui traduisent tous l'un des mécanismes naturels déjà explicités. Dans la suite, on donne la version standard de ces algorithmes, plus particulièrement l'algorithme de sélection négative (« Negative Selection Algorithm »), l'algorithme de sélection clonage (« Clonal Selection Algorithm ») et l'algorithme du réseau immunitaire (« Immune Network Algorithm »). [19]

A-La sélection positive :

Pour acquérir la tolérance au soi, le thymus met tout d'abord en place une **sélection vis-à- vis du CMH** dite « **sélection positive** ». Seuls les lymphocytes qui expriment un TCR capable de reconnaitre une molécule HLA (c'est le CMH chez l'être humain) survivent et se multiplient.Les lymphocytes avec un TCR ne reconnaissant pas la protéine HLA sont éliminés car elles sont non fonctionnelles. Plus de 90% des cellules passant dans le thymus meurent lors de cette 1ère étapede sélection. [10]

Cette sélection permet de conserver seulement les lymphocytes T capables de reconnaitre des antigènes dans un contexte restreint au CMH du Soi (les antigènes sont alors présentés par le CMHdes cellules présentatrices comme les cellules dendritiques). [10]

B-La sélection négative :

B-1.Pour les lymphocytes T

Les thymocytes simples positifs reconnaissent alors encore les molécules du soi comme les molécules du non-soi. Ils vont donc ensuite migrer vers la médulla au niveau de laquelle ils continueront leurs maturations et subiront la **sélection vis-à-vis du peptide** dite « **sélection négative** ». Cette dernière utilisera la caractéristique des **cellules dendritiques** à exprimer un facteur de transcription appelé **AIRE** (pour *Auto-Immune-Regulator-Element*) qui lui-même permet

l'expression de peptides du soi de tissus n'ayant aucun rapport avec le thymus, eux-mêmesprésentés par des molécules du CMH du soi ; ces cellules sont dites **auto-réactives**.

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

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

B-2.Pour les lymphocytes B

La sélection négative est appliquée aussi sur les cellules B dans la moelle osseuse, quand les cellules B immatures identifient les cellules du soi, elles seront éliminées. Ce mécanisme est appliqué seulement sur les cellules B immatures dans la moelle osseuse. La tolérance au soi des cellules nouvellement générées après le processus de la sélection clonale et l'hypermutationsomatique, sera assurée par l'assistance des cellules T d'aide [1].

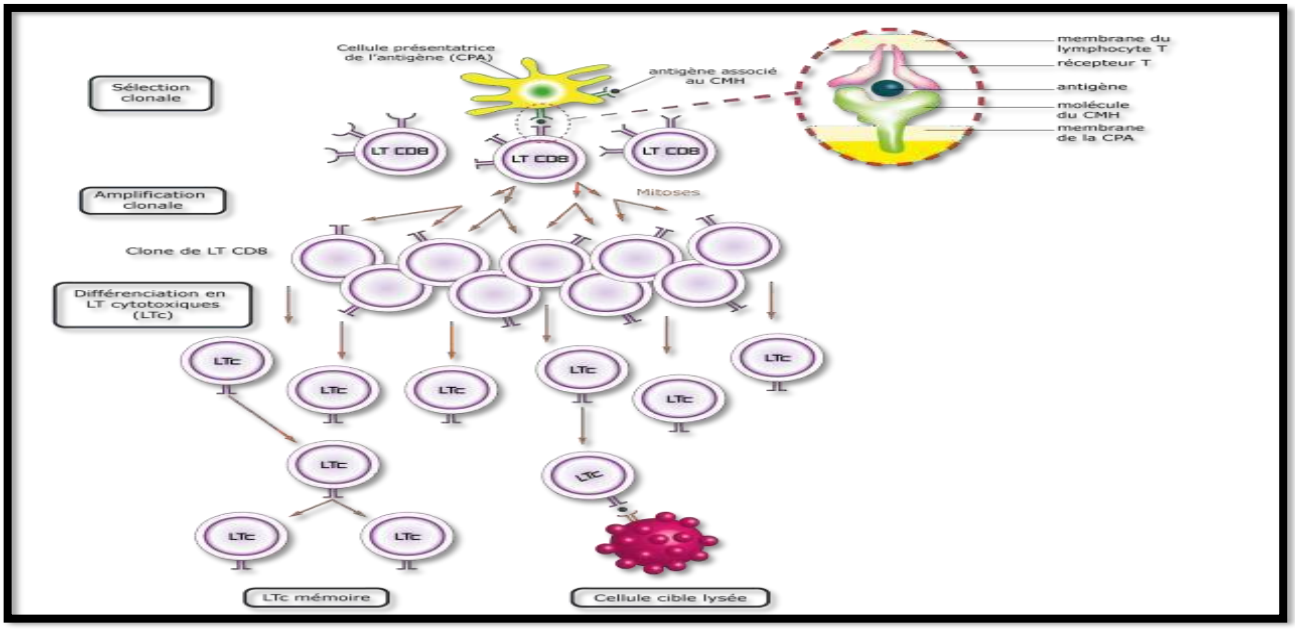
C-La sélection clonale

C-1.Pour les lymphocytes T

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

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

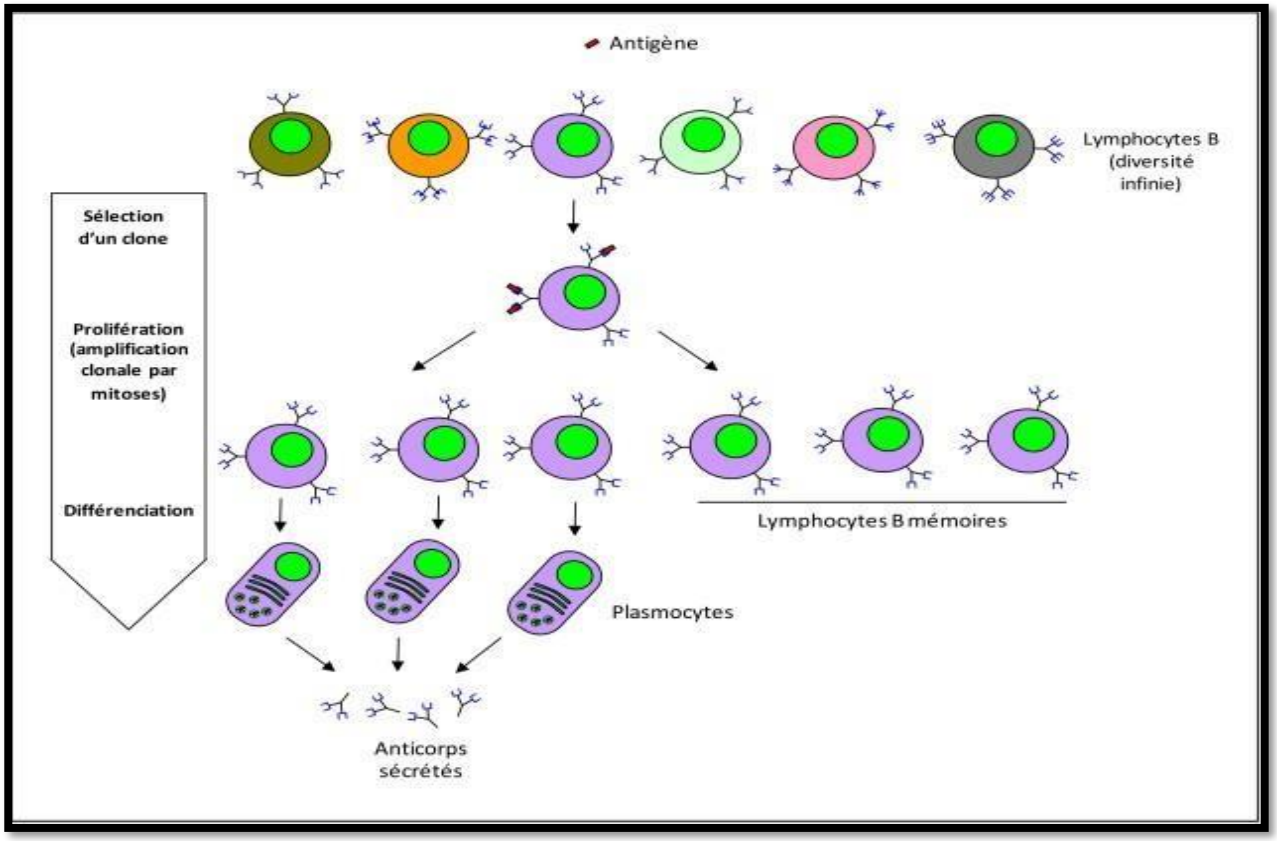
Lorsque la reconnaissance s'effectue entre les antigènes / CMH (des CPA) et les récepteurs T (des lymphocytes T CD8), les LT CD8 sont activés et deviennent sensibles aux interleukines (facteurs stimulants) ; ils prolifèrent (par mitoses) et se transforment en cellules tueuses, les lymphocytes cytotoxiques (LTc), capables de détruire par contact une cellule infectée par un virusdont l'antigène a été reconnu. [10]



II-2: Reconnaissance entre les LT CD8 et les cellules infectées

C-2.Pour les lymphocytes B

La sélection clonale c'est les séquelles de la réponse immunitaire suite à un stimulus antigénique subissant des proliférations et différentiations. Quand un antigène s'infiltre dans le corps, les cellules immunitaires reconnaissent cet antigène avec des degrés d'affinité différents. L'appariement fort entre les récepteurs des anticorps et l'antigène, produit la stimulation des cellules B, c'est-à-dire la prolifération (clone) et la maturation des cellules de plasma. Le taux de prolifération d'une cellule est proportionnel par rapport à son affinité. La réponse des cellules B est la production d'un seul type d'anticorps qui est relativement spécifique à l'antigène. Les cellules qui ont les plus grandes affinités seront les plus proliférées et réciproquement. Puis, les lymphocytes qui ont une forte affinité peuvent se différencier en des cellules mémoires. [10]



*II-3: **De la détection de l'antigène à la production massive d'anticorps adaptés à cet antigène***

C-3.L'hypermutation somatique

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

L'hypermutation somatique est inversement proportionnelle à l'affinité d'une cellule c'est-à-dire les cellules qui ont les plus hautes affinités seront les moins mutées et réciproquement. Le mécanisme de l'hypermutation somatique permet au système immunitaire d'augmenter la capacité d'identification des anticorps par rapport à un antigène sélectif. [10]

II-3) Les systèmes immunitaires artificiels :

Introduction :

L'immunité biologique représente une source riche d'inspiration pour les chercheurs de différents domaines. Ces chercheurs n'ont pas hésité à puiser dans cette source pour développer des applications artificielles destinées à résoudre des problèmes. Leurs travaux ontconduit à l'émergence d'une nouvelle discipline, celle des systèmes immunitaires artificiels.

La multitude d'applications et la diversité des approches artificielles inspirées de l'immunité biologique rend toute tentative pour définir ce que pourrait être « un » système immunitaire artificiel une tâche compliquée. Par exemple ne recensent pas moins de trois définitions de la discipline des systèmes immunitaires artificiels.

II-3-1)Définition :

Un système immunitaire artificiel est un système informatique basé sur les métaphores du système immunitaire naturel. [32]

II-3-2)Historique :

Les travaux sur les AIS ont dans le milieu des années 80 avec l'article de Farmer, Packard et Perelson sur les réseaux immunitaires (1986). Cependant, c'est seulement dans le milieu des années 90 que les SIA devinrent un sujet à part entière. Les travaux de Forrest sur la sélection négative commencèrent en 1994, tandis que Dasgupta menait des études sur les algorithmes de sélection négative. Hunt et Cooke commencèrent leurs travaux sur les modèles de réseaux immunitaires en 1995. Timmis et Neal continuèrent ces travaux en y apportant des améliorations. Le premier livre sur les Systèmes Immunitaires Artificiels a été écrit par Dasgupta en 1999. Les travaux de De Castro & Von Zuben et Nicosia & Cutello sur la sélection clonale (CLONALG) furent remarqués en 2002. De nouvelles voies, comme la théorie du danger et des algorithmes inspirés par le système immunitaire inné ont également été explorées. Le fait qu'elles apportent quelque chose de nouveau au-delà des algorithmes existants est actuellement le sujet de débats qui animent le développement des AIS. Au départ, les travaux sur les AIS visaient à trouver des abstractions efficientes des phénomènes découverts dans le système immunitaire. Plus récemment, les praticiens des SIA se sont aussi intéressés à la modélisation du système immunitaire et à l'application des résultats issus des AIS aux problèmes d'immunologie (ce qui entre dans le cadre de l'immuno-informatique).

II-3-3)Les algorithmes immunitaires de base :

A leurs débuts les systèmes immunitaires artificiels étaient composés typiquement de trois algorithmes intelligents, nommés : le modèle du réseau immunitaire, l'algorithme de la sélection clonale et l'algorithme de la sélection négative. Cette section présente les différents algorithmes et modèles définis dans la littérature, pour chaque algorithme cité en haut, on présentera son inspiration biologique, le principe de l'algorithme et enfin quelques domaines d'applications :

A-Algorithme de sélection négative

Cet algorithme est la traduction de la capacité des systèmes immunitaires naturels à différencier le « Soi » du « Non Soi » (« Self/Non self discrimination »). Il sert à détecter des changements ou des variations dans un ensemble initialement défini.

A supposer que l'ensemble des éléments du « Soi » soit connu, l'algorithme standard de sélection négative a pour rôle de générer un ensemble de cellules immunitaires, appelées « Détecteurs », capables de reconnaître toute autre cellule sauf celles appartenant à l'ensemble du « Soi ». Cet algorithme est résumé [19].

1. initialisation : Générer aléatoirement un ensemble de détecteurs candidats
2. Censure : Tant que le nombre de détecteurs est insuffisant,

Faire

- Evaluation d'affinité : calculer l'affinité entre chaque élément du « soi » et un détecteur candidat
- Sélection : éliminer tout détecteur qui reconnaît un élément du « soi ».Autrement, incrémenter le nombre de détecteurs valides.

Fin Faire

3. Pilotage : piloter un nouvel ensemble de « soi » pour détecter des variations : Si un détecteur de l'ensemble des détecteurs ainsi générés identifie un élément parmi le nouvel ensemble de « soi », alors cela signifie qu'une variation a été détectée.

Figure II-4: 3 : Algorithme Sélection Négative [19]

B-Algorithme de sélection clonage :

Cet algorithme est la traduction de la capacité des systèmes immunitaires naturels à monter une réponse immunitaire capable d'éliminer les pathogènes. Etant donnée une représentation des antigènes, et une représentation des cellules immunitaires, cet algorithme sert à optimiser l'affinité des cellules immunitaires aux antigènes.

L'algorithme standard de sélection clonage génère et reproduit un ensemble de cellules immunitaires, appelées anticorps (ou lymphocytes), capables de reconnaître les éléments de l'ensemble des antigènes. Les cellules capables de reconnaître des antigènes se reproduisent asexuellement (clonage) et proportionnellement à leur degré d'affinité avec les antigènes. Durant la phase de clonage, les cellules immunitaires subissent une mutation leur permettant d'augmenter leur affinité avec les antigènes (processus de maturation d'affinité). Le taux de mutation est inversement proportionnel à l'affinité de la cellule immunitaire avec l'antigène reconnu. Cet algorithme est résumé. [19]

1. initialisation : Générer aléatoirement un répertoire de cellules immunitaires
2. Sélection clonage : Pour chaque antigène,

Faire

- Mesure d'affinité : calculer l'affinité entre chaque cellule immunitaire etl'antigène
- Sélection : sélectionner les cellules de plus grande affinité
- Reproduction et mutation : cloner les cellules immunitaires sélectionnées proportionnellement à leur affinité avec l'antigène. Muter chaque clone avec un taux de mutation inversement proportionnel à leur degré d'affinité

Fin Faire

3. Cycle

Répéter

Sélection Clonage

jusqu'à critère de convergence (d'arrêt)

Figure II-5 : Algorithme Sélection Clonage [19]

C-Algorithme du réseau immunitaire

D'après la théorie du réseau immunitaire, les cellules immunitaires peuvent identifier et être identifiées par d'autres cellules immunitaires. Lorsqu'une cellule immunitaire identifie un antigène ou une autre cellule immunitaire, elle est stimulée. Par ailleurs, lorsqu'une cellule immunitaire est identifiée par une autre cellule immunitaire, elle est supprimée.

L'algorithme du réseau immunitaire reflète cette dynamique des cellules immunitaires biologiques. Il peut être utilisé pour optimiser l'affinité des cellules immunitaires aux antigènes, et/ou pour des fins de classification.

Soient :

N_{st} : taux de stimulation par le réseau N_{sup} : taux de suppression par le réseauA_{st} : taux de stimulation par l'antigène

Alors l'équation (II-2.C.1) décrit le niveau de stimulation S d'une cellule du réseau immunitaire.

$$S = N_{st} – N_{sup} + A_{st} \qquad \text{(II-2.C.1)}$$

Le niveau de stimulation d'une cellule immunitaire détermine ses probabilités de reproduction et de mutation. La Figure II-6 fournit le schéma général d'un algorithme standard du réseau immunitaire.

1. initialisation : Initialiser un réseau de cellules immunitaires
2. Sélection clonage : Pour chaque antigène,

Faire

Méta dynamique : introduire de nouvelles cellules dans le réseau etéliminer les cellules inutiles (selon un certain critère)

Identification antigénique : confronter les cellules immunitaires àl'antigène

Interactions du réseau : confronter les cellules immunitaires entre elles

Niveau de stimulation : calculer le niveau de stimulation de chaque celluleimmunitaire (équation (II-2.C.1))

Dynamique : mettre à jour la structure du réseau en fonction des niveauxde stimulation : propager les cellules qui ont les plus grandes affinités et éliminer les cellules qui ont les plus faibles affinités.

Fin Faire

3. Cycle

Répéter

Etape 2

jusqu'à critère de convergence (d'arrêt)

Figure II-6: Algorithme du réseau immunitaire [19]

Conclusion :

Dans ce chapitre, on a présenté quelques définitions, concepts et motivations du développement des systèmes multi_agents. Ces derniers proposent une vision renouvelée de l'informatique, vécuecomme un prolongement théorique aux techniques à objet, Ces systèmes sont

performants et flexibles, permettant la modélisation distribuée des traitements et des connaissances grâce aux leurs caractéristiques notamment l'autonomie, les interactions entre entités et la décentralisation des calculs. En effet les SMA représentent actuellement un champ de recherche très actif afin grâce aux leurs avantages.

Chapitre III

Les systèmes multi-agent

III) Les systèmes multi-agent :

Introduction :

IDS est une solution de gestion de la sécurité intégrée à de nombreuses approches d'intelligence artificielle [22], mais la plupart d'entre elles ont été complexes, aussi la distribution des hôtes rendre la détection d'intrusion difficiles, Ce qu'il faut, une solution de sécurité flexible et adaptable offrant une plus grande autonomie. Il est donc nécessaire de revoir la manière dont la détection d'intrusion standard est conçue et implémenter pour identifier et atténuer sa vulnérabilité. Dans ce contexte, les systèmes multi_agents offrent un équilibre entre les exigences de sécurité, la flexibilité du système et l'adaptabilité. En fait, la technologie des systèmes multi_agents (SMA) est l'un des domaines de l'intelligence artificielle distribuée (DAI) qui consiste en un ensemble de facteurs individuels appelés environnements distribués. Chaque agent coopère et communique avec d'autres agents. Dans ce chapitre, on parle sur l'approche de SMA intégrer avec la détection d'intrusion premièrement on définir l'agent avec ces caractéristiques et leurs types, et on a également étudié le système multi_agents. Enfin, on cite quelques systèmes de détection d'intrusion basé sur le système multi-agent.

III-1) Agents et systèmes multi-agent :

Les systèmes multi-agents, en tant que sous-domaines de DAI, sont considérés comme des systèmes informatiques dans lesquels plusieurs agents autonomes et intelligents interagissent et travaillent en collaboration pour effectuer un ensemble de tâches et atteindre un ensemble d'objectifs.

III-1-1) Définition d'agent :

Définition 1 : « Un agent est une entité autonome, capable d'agir sur elle-même et sur son environnement, et dont ces actions sont les conséquences de ces observations, ces connaissances, son interaction et communication avec d'autres agents » [23].

Définition 2 : « Un agent est un système informatique, situé dans un environnement, et qui agit d'une façon autonome et flexible pour atteindre les objectifs pour lesquels il a été conçu » [24].

III-1-2) Les caractéristiques des agents :

A partir des définitions précédentes nous pouvons décrire plusieurs propriétés qui caractérisent le comportement des agents [25]

- **Intelligence :** le terme « intelligence » signifie que l'agent est en mesure d'afficher un niveau de priorité de renseignement différent, allant d'actions prédéfinies (planification) à l'auto-apprentissage (définition de nouvelles actions).

- **Autonomie:** est la capacité d'un agent de fonctionner sans intervention directe d'être shumains ou d'autres agents et d'avoir un contrôle quelconque sur son état interne et son environnement externe ;
- **Situer :** l'agent est capable d'agir sur son environnement à partir des entrées sensorielles qu'il reçoit de ce même environnement. Exemples : systèmes de contrôle de processus, systèmes embarqués.
- **Communication :** Pour que les agents puissent collaborer et coordonner leurs actions à effectuer, ils doivent échanger des messages entre eux.
- **Adaptabilité :** Les agent peuvent s'adapter au changement de leur environnement et ont la capacité d'acquérir un comportement intelligent par l'apprentissage.
- **Sociabilité :** est la capacité d'un agent à s'intégrer dans un vaste environnement peuplé d'une société d'agents avec laquelle l'agent doit échanger des messages pour réaliser des actions utiles. Cette propriété est satisfaite même lorsque les systèmes doivent partager leurs connaissances et leurs attitudes mentales (croyances, objectifs, désirs, etc.).
- **Proactivité :** est la capacité d'un agent d'anticiper les situations et de changer de ligne de conduite. C'est une propriété pertinente qui apparaît dans la gestion du réseau et du système afin d'éviter des effets désastreux sur les performances globales. En effet, les agents proactifs sont capables de manifester des comportements axés sur les objectifs en prenant certaines initiatives.
- **Réactivité :** est la capacité d'un agent de modifier son comportement au fil du temps pour atteindre ses objectifs en matière de résolution de problèmes.

III-1-3) Le type des agents :

Les actions des agents sont prises en fonction de perceptions retenues par les situations externes. Dans intelligence artificielle distribué (DAI) on distingue trois types d'agents en fonction de leur niveau d'intelligence réactif, cognitif :

A-Agents réactifs :

Un agent réactif réagit rapidement pour résoudre un problème simple qui ne nécessite pas de raisonnement complexe. Ainsi, l'intelligence du système émerge des interactions entre un grand nombre de ce type d'agents

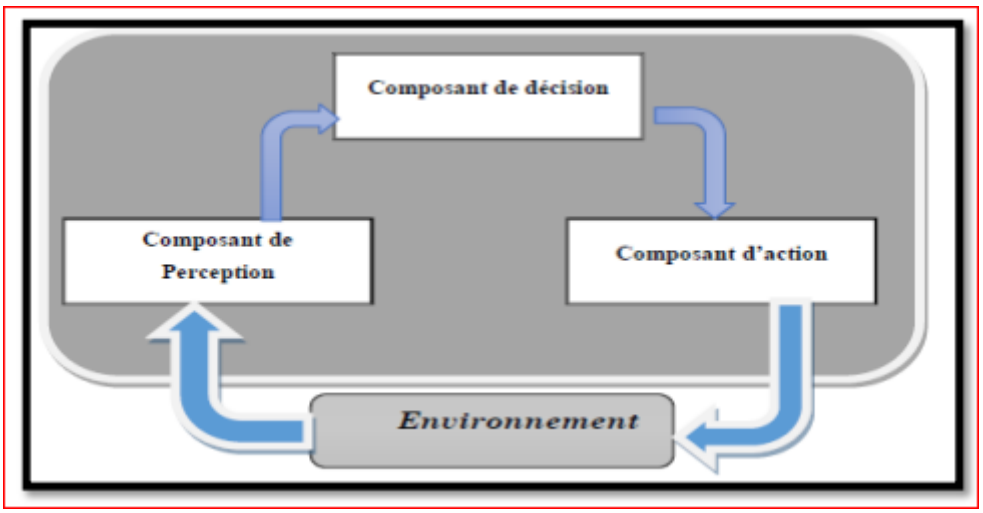


Figure III-1 : Structure d'un agent réactif [26]

B-Agents cognitifs :

Un agent cognitif est capable de trouver une solution à un problème complexe tout en communiquant avec d'autres agents et en interagissant avec sa base de connaissances. Ses principales caractéristiques comprennent une grande capacité de raisonnement, le traitement de données, la perception, l'apprentissage, le contrôle, la communication et le domaine de la réactivité de l'expertise. [27]

C-Agents hybrides :

Est un mélange d'agent réactif et cognitif, possède un réflexe (évolution réactive) pour résoudre des problèmes répétés et réfléchit (une attitude cognitive) à des situations système complexes. [26]

III-2) Systèmes Multi Agents :

III-2-1) Définition d'un SMA

Un système multi-agents est un ensemble organisé d'agents.

Il est constitué d'une ou plusieurs organisations qui structurent les règles de cohabitation et de travail collectif entre agents.

Dans un même système, un agent peut appartenir à plusieurs organisations.

III-2-2)Réalisation et implémentation d'un système multi-agent

Les questions qui se posent ici portent sur la manière de réaliser des systèmes multi-agents.

Cet aspect prend en compte des techniques de systèmes distribués et de langages concurrents, tels que les langages d'acteurs.

Architecture en couche

Un système multi-agent conçu autour d'agents communicants possède une architecture caractéristique qui est illustrée figure 2.

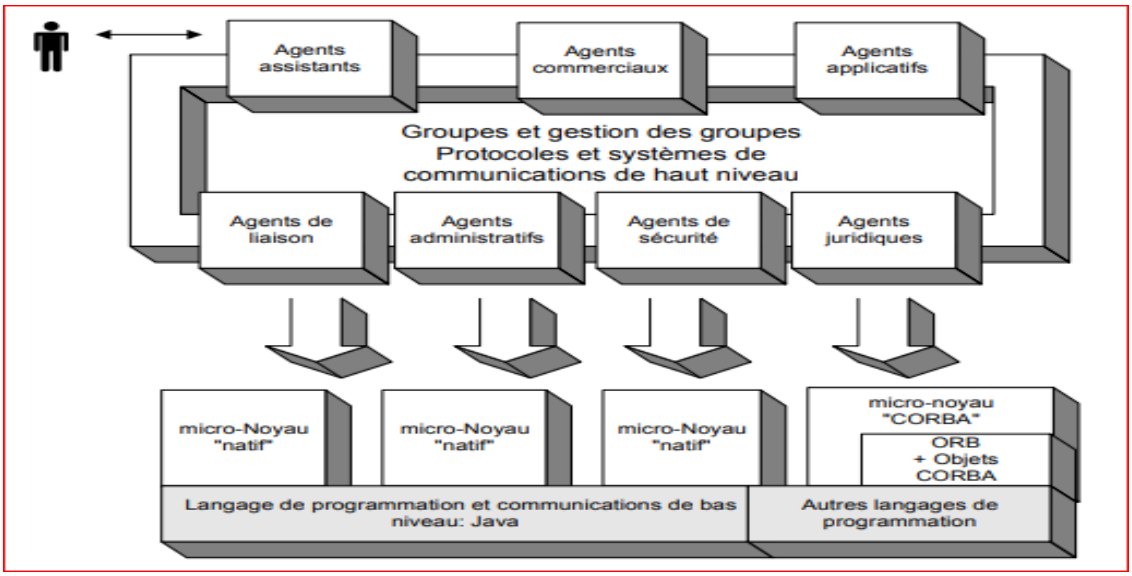


Figure III-2: L'architecture d'un système multi-agent fonctionnant sur réseau.

Le niveau 0 correspond à l'ensemble des ressources disponibles telles que les mécanismes de communication de bas niveau (sockets Unix, protocoles TCP/IP ou http, etc.) ainsi que les mécanismes d'exécution parallèles tels que les « threads ». C'est au-dessus de cette couche, qui est utilisée comme un existant, que vient s'intégrer un système multi-agent proprement dit. Le niveau 1 décrit les couches de bas niveau d'un système multi-agent : les primitives de communication entre agents distants (primitives de type KQML), les serveurs de noms permettant à des agents d'entrer et de sortir du système (procédures de check-in check-out), ainsi que les moteurs qui implémentent le cycle de base de fonctionnement d'un agent. Ce cycle est lié à un processus en boucle de type perception/délibération/action. Le niveau 2 correspond à l'ensemble des mécanismes génériques qui sont mis en œuvre dans un système multi-agent. Il s'agit du niveau fondamental sur lequel porte la plupart des recherches décrites dans la section précédente : définition de protocoles génériques de coopération, description d'agents administratifs et de liaison tels que les « courtiers » (ou brokers) qui mettent en rapport les agents qui demandent et ceux qui offrent des services, description de langage de contenu généraux, comportements génériques d'agents, etc. Le niveau 3 enfin traite des applications spécifiques et des domaines particuliers auxquels on dédie un système multi-agent particulier.

III-2-3)Architecture d'un système multi-agent :

A-Les architectures d'agents à base de tableaux noirs

L'architecture de tableau noir a été l'une des plus utilisée dans les systèmes multi-agents cognitifs symboliques et elle a donné lieu à une abondante littérature. Originellement développée dans le cadre de l'intelligence artificielle traditionnelle (c'est-à-dire, du point de vue de l'IAD, pour réaliser des systèmes mono-agents), l'architecture de tableau noir s'est rapidement imposée en IAD comme une architecture suffisamment souple et puissante pour pouvoir implémenter les mécanismes de raisonnement et de calculs intervenant à l'intérieur des agents, notamment avec le système DVMT. [28]

Le modèle de tableau noir est fondé sur un découpage en modules indépendants qui ne communiquent directement aucune information, mais qui interagissent indirectement en partageant des informations. Ces modules, appelés sources de connaissance ou KS (pour Knowledge Sources), travaillent sur un espace qui comprend tous les éléments nécessaires à la résolution d'un problème. L'architecture d'un système à base de tableau noir comprend trois sous-systèmes : 1) Les sources de connaissance. 2) La base partagée (le «tableau» proprement dit) qui comprend les états partiels d'un problème en cours de résolution, les hypothèses et les résultats intermédiaires et toutes les informations que s'échangent les KS. 3) Un dispositif de contrôle qui gère les conflits d'accès entre les KS, ces derniers intervenant de manière «opportuniste» c'est-à-dire sans être déclenchés effectivement par un système centralisé de contrôle. C'est cette partie qui a connu le plus de modifications au cours de l'évolution de ces architectures. On pourra se reporter à [29]pour un panorama général sur les architectures à base de tableaux noirs.

Si dans un premier temps, les systèmes à base de tableau noirs furent considérés comme des systèmes d'IAD, chaque KS pouvant être perçu comme un agent qui interagit avec les autres KS, il n'en est plus de même aujourd'hui. Du fait de leur mécanisme de contrôle très centralisé et de leur manque de mémoire locale et donc de localité des informations, ces systèmes sont maintenant envisagés comme des architectures pratiques pour la réalisation de systèmes «intelligents» et, en particulier, pour implémenter la structure interne d'agents cognitifs symboliques. Nombre de systèmes multi_agents ont été implémentés de cette manière aux Etats Unis [28]et en France.

L'architecture de tableau noir présente de nombreux avantages dont, en tout premier lieu, une remarquable souplesse pour décrire des modules et articuler leur fonctionnement. Son principal inconvénient provient de sa relative inefficacité, due à la très grande expressivité de son contrôle. De ce fait, ce type d'architecture s'avère particulièrement utile lors de la phase de prototypage de la réalisation de systèmes ou lorsque les temps de réponses ne sont pas trop contraints. Néanmoins, des versions de BB1 **Source spécifiée non valide.**ont montré que même dans des cas où il était nécessaire

d'avoir des temps de réponses en temps réel, la gestion fine du contrôle pouvait accélérer de manière drastique son comportement en prenant les bonnes décisions et en choisissant les tâches importantes et urgentes au bon moment [30].

B- Architectures multi_agents et acteurs

Dans son article initial [31], Hewitt développait l'idée qu'il était possible de repenser la notion de structure de contrôle des langages traditionnels en les reconsidérant comme des schémas (patterns) de communications entre entités autonomes appelées acteurs. Depuis, les langages d'acteurs, en particulier sous l'influence de Agha [32], de Tokyo [33] et de Yonezawa [34] ont surtout été étudiés comme des modèles d'exécution pour la programmation par objets concurrents. Mais quelques travaux ont voulu rester dans les idées initiales que prônaient Hewitt et qu'il confirma avec ses notions de «sémantique des systèmes ouverts» [35] P. Carle [36], S. Giroux [37] et J. Ferber [38], tout en estimant que les langages d'acteurs sont effectivement de très bons outils pour l'implémentation de calculs parallèles, considèrent néanmoins qu'ils présentent des caractéristiques tellement originales qu'ils modifient par leur présence la notion même d'architecture multi-agents en envisageant les agents et les systèmes multi-agents comme des extensions naturelles de la notion d'acteur.

La communication entre acteurs s'effectue par envois de messages asynchrones, les réponses étant renvoyées à un acteur, appelé «Customer» chez Hewitt, qui se charge de traiter la réponse et qui représente la continuation locale du calcul. De nombreux langages d'acteurs ont été proposés. Les plus célèbres et actuellement opérationnels sont ABCL [39], MERING IV [40] et ACTALK [41]. Ce dernier, qui est conçu comme une extension de SMALLTALK, est à la base d'un grand nombre de plates-formes multi-agents, le premier en date ayant été MAGES III [41], l'un des plus récents étant DINA [42].

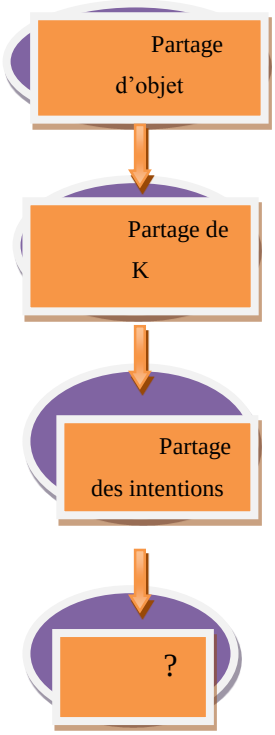
Autre exemple, celui de L. Gasser dont le système MACE [38], fortement influencé par les idées de Hewitt, a lui-même inspiré la plupart des plates-formes de développement ultérieures. Le rapport entre acteurs et agents est ainsi des plus féconds et nul doute que l'avenir verra d'autres travaux tendant à montrer les liens très étroits qui unissent ces deux concepts.

III-2-4)Communication entre agents [38]

La communication inter-agent est fondamentale à la réalisation du paradigme agent, tout comme le développement du langage humain était la clé du développement de l'intelligence humaine et des sociétés.

Pour échanger les informations et les connaissances, les agents utilisent des **ACL (Agent Communication Language).**

A- Évolution ACL :



-> Partage des objets, des appels de procédure et de SDD (CORBA, RPC, …)

-> Partage des connaissances (faits, règles, contraintes, procédures, …) KIF, KQML, FIPA, ….

-> Partage des intentions (croyances, buts, intentions) => Niveau intentionnel Théorie BDI

-> Que peut-on partager d'autre ? Expériences, Stratégies…

Figure III-3 : Évolution ACL

B-Le modèle BDI et la communication

Communication

Révéler à l'autre l'état de nos croyances, désires et intentions.

Essayer d'influencer l'état des croyances, désires et intentions de l'autre.

Un agent a des croyances sur le monde (son environnement), sur les croyances des autres agents et sur les croyances qu'ont les autres agents sur lui …

C- Langages de communications entre agents

Tout langage multi agent est représenté par une structure de donnée comprenant les champs :

- ✓ **Emetteur**
- ✓ **Récepteur**
- ✓ **Langage utilisé :** langage dans lequel le vrai message est rédigé
- ✓ **Contenu du message :** le vrai message qui fait l'objet de la communication
- ✓ **L'ontologie :** le vocabulaire dans un domaine donné pour que les agents puissent se comprendre Ensemble de définitions concernant le message

De nombreux langages de communications entre agents (ACL) se sont développés.

1. ***KQML*** (93, 97)
2. ***FIPA***-ACL (97, 99, 2000)

C-1. KQML (Knowledge Query and Manipulation Language)

KQML a été conçu comme étant à la fois un format de message et un protocole de transfert de messages venant aider les agents intelligent au partage et échange de données de haut niveau tout en étant indépendant des machines.

KQML est un langage qui se présente sur 3 couches :

La couche contenu
La couche communication
La couche message

- ***a- La couche « Contenu »***

Il s'agit du contenu réel du message, il peut être écrit dans le langage de représentation du programme de l'agent.

KQML peut transporter des messages écrits dans n'importe quel langage de représentation (ex : PROLOG, KIF, LISP, C, KQML (lui-même), XML ...)

- ***b- La couche « Communication »***

Dans cette couche on retrouve des informations d'un niveau un peu plus bas permettant le bon fonctionnement de la communication telles que l'identité de l'émetteur ou celle du récepteur du message, ainsi qu'un identificateur unique pour le message.

- ***c- La couche « Message » :***

Cette couche constitue le cœur du langage.

Elle incorpore des arguments décrivant le contenu des messages tels que le langage utilisé, l'ontologie…

Ces arguments permettent à KQML d'analyser, acheminer et délivrer les messages même si leur contenu lui est opaque et inaccessible.

KQML : la syntaxe

(KQML-performative

Niveau message

:language<text>

:ontology< text>

Niveau communication

:sender<text>

:receiver<text>

Niveau contenu

:content<expression>

KQML les performatives :

36 performatives répartis en 3 catégories :

- Les 18 performatives de discours : servent à échanger des connaissances et des informations présentes dans la base de connaissance de l'agent (ask-if, ask-one, tell, describe, stream-all …)
- Les 11 performatives d'interconnexion : aide à la mise en relation des agents entre eux (register, unregister, broadcast …)
- Les 7 performatives d'exception : servent à changer le déroulement normal des échanges (error, sorry, standby …)

Quelques performatives

E : l'agent émetteur

R : l'agent récepteur

C : le contenu du message

BVC : la base virtuelle de connaissances (connaissances attribuées par chaque agent aux autres agents)

- **ask-one :** E veut que seulement **R** réponde à sa question **C**

- **ask-if : E** veut savoir si la réponse à la question précisée en C se trouve dans la **BVC** de **R**

- **tell : E** affirme au R que C'est dans la **BVC** de **E**

- **broadcast : E** veut que R transmette à son tour la performative à toutes ses connexions

- **error : E** considère le message précédent de **R** comme mal formé

- **sorry : R** ne peut pas fournir plus d'information

http://www.exso.com/courses/cs101c/kqml/node6.html

Exemple de KQML

l' agent A veut connaître toutes les personnes définies comme étant des hommes.

```
(ask-all
   :sender A
   :receiver B
  :language PROLOG
   :ontology phylosophie
   :content homme (=x)
   :reply_with question1
)
```

Plates-formes des systèmes multi_agents && KQML

Une plate-forme de développement des systèmes multi_agents est une infrastructure de logiciels utilisée comme environnement pour le déploiement et l'exécution d'un ensemble d'agents.

1 - AgentBuilder

- http://www.agentbuilder.com
- AgentBuilder est entièrement programmé en Java.
- Les agents construits en utilisant AgentBuilder communiquent en utilisant KQML.
- Disponible pour Windows 98/ME/NT/2000/XP, Solaris et Linux

2 - JAT : Java(tm) Agent Template

- http://www-cdr.stanford.edu/ABE/JavaAgent.html
- La communication est basée sur KQML.

- Java Intelligent Agent Library

- http://www.bitpix.com/business/main/bitpix.htm
- La communication est basée sur KQML.
- La librairie supporte aussi les agents mobiles.

C-2.La norme FIPA :

La FIPA (Foundation for Intelligent Physical Agents) est une organisation à but non lucratif fondée en 1996 dont l'objectif est de produire des standards pour l'interopération d'agents logiciels hétérogènes.

FIPA ACL : Syntaxe similaire à celle de KQML.

- **FIPA-ACL**

sender : l'émetteur du message

receiver : le destinataire du message

reply-to : participant à l'acte de communication

content : le contenu du message (l'information transportée par la performative)

language : le langage dans lequel le contenu est représenté

ontology : le nom de l'ontologie utilisé pour donner un sens aux termes utilisés dans le content conversation-id : identificateur de la conversation

reply-with : identificateur unique du message, en vue d'une référence ultérieure

in-reply-to : référence à un message auquel l'agent est entrain de répondre (précisé par l'attribut reply-with de l'émetteur)

reply-by : impose un délai pour la réponse

- **Catégorie de performatives FIPA**

Information

query_if, query_ref, sunscribe, inform, inform_if, inform_ref, confirm, disconfirm, not_understood Gestion des erreurs

not-understood, failure

Négociation

cfp (Call for proposal), propose, accept_proposal, reject_proposal

……

……

http://jmvidal.cse.sc.edu/talks/agentcommunication/performative s.xml

- **Exemple de FIPA**

L'agent A veut informer l'agent B du temps qu'il fera demain, selon ses prévisions :

(inform

:sender A

:receiver B

:content temps (demain, pleuvoir)

:language Prolog

)

- **Les protocoles d'interaction FIPA**

Sémantique : une description de protocole représente un schéma d'interaction, ensemble de messages échangés entre différents agents

Protocoles :

fipa-request: le récepteur est demandé d'exécuter une action

fipa-query : le récepteur est demandé d'exécuter un acte informatif

FIPA-Request

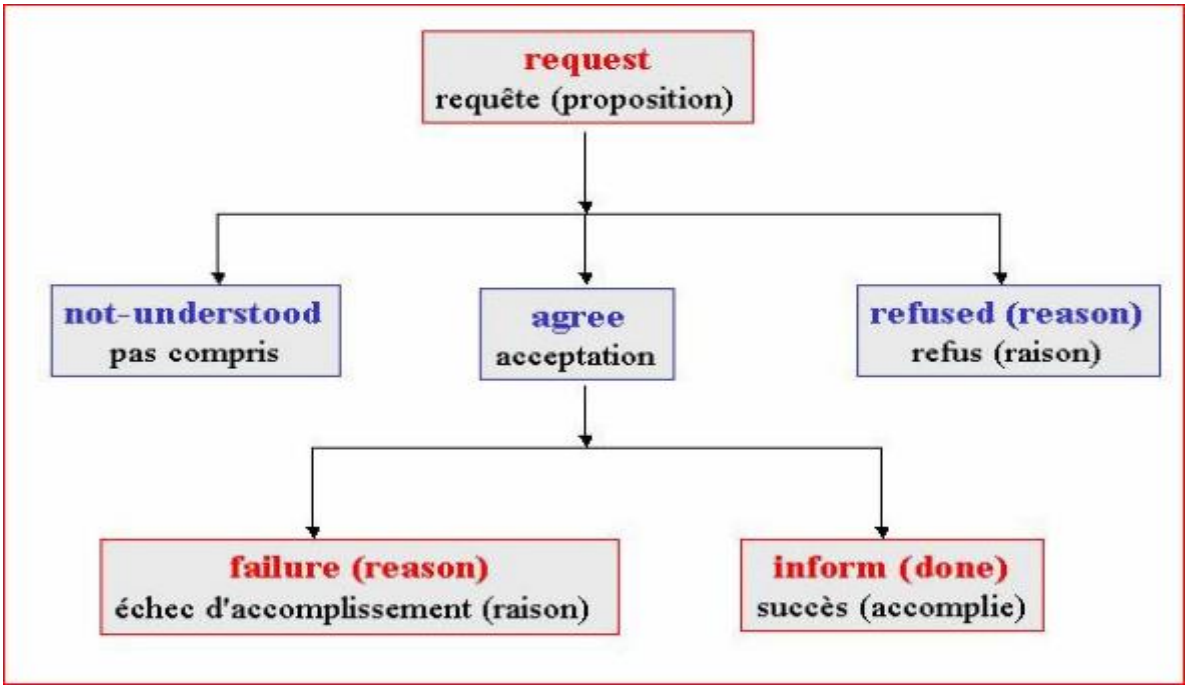


Figure III-4 : fipa Request

Avec FIPA-request, un agent sollicite un autre agent pour exécuter des actions et l'agent récepteur retourne soit une réponse favorable à l'exécution d'actions, soit une réponse défavorable expliquée par telle ou telle raison. Supposons que l'agent i aie besoin de l'agent j pour exécuter l'action « action ».

- L'agent i envoie « request » à l'agent j.
- Si l'agent j'accepte la requête, il retourne « agree ». Ensuite, quand j'a fini d'exécuter « action », il en informe i en utilisant « inform ».
- Si l'agent j'accepte mais rencontre un problème durant le traitement de « action », il retourne « failure » et les raisons de l'échec.
- Si l'agent j n'accepte pas la requête de l'agent i, j retourne « refuse » et les raisons de ce refus.

FIPA-Query

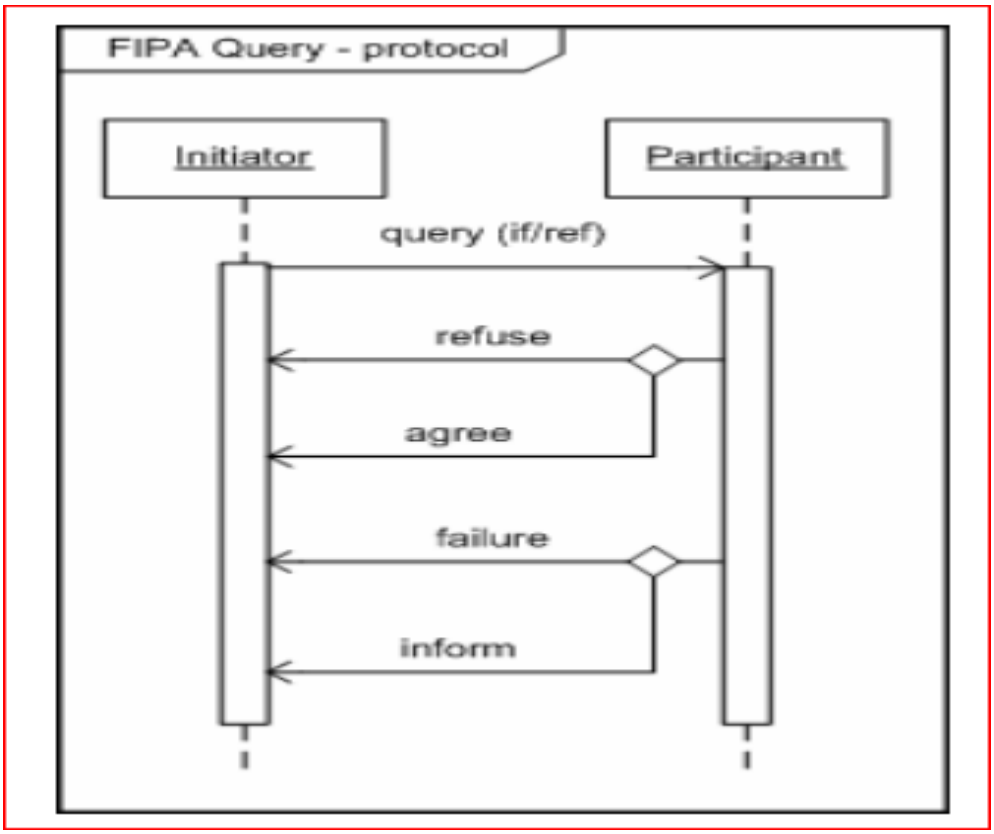


Figure III-5 : fipa Query

FIPA-Query signifie que l'agent émetteur sollicite l'agent récepteur pour exécuter un des types d'un performatif «inform», c'est-à-dire pour répondre à la demande.

Supposons que l'agent i fasse une demande à l'agent j.

- L'agent i envoie un performatif «query» à l'agent j.
- Si l'agent j peut répondre à la demande, il l'informe en utilisant le performatif « inform ».

- Si l'agent j a essayé de répondre à la demande mais qu'il ne le peut pas, il retourne «failure» et les raisons de cette impossibilité.
- Si l'agent j refuse de répondre à la demande, il retourne «refuse» et les raisons de ce refus.

  - **Plates-formes des systèmes multi_agents && FIPA**

  JADE : http://jade.tilab.com/

- Langage utilisé : Java.
- FIPA ACL pour la communication.

III-2-5) Collaboration et coordination d'actions :

Les différentes formes d'interaction sont la collaboration et la coordination d'actions. La première s'intéresse à la manière de répartir le travail entre plusieurs agents, qu'il s'agisse de techniques centralisées ou distribuées, et la seconde analyse la manière dont les actions des différents agents doivent être organisées dans le temps et l'espace de manière à réaliser les objectifs. Enfin, lorsque des conflits apparaissent, il est important de pouvoir en limiter leurs effets. Les techniques de négociation servent ainsi à satisfaire les parties impliquées en établissant des compromis ou en dépassant la nature du conflit.

La coopération est la forme générale d'interaction la plus étudiée dans les systèmes multi-agents1. De manière simplifiée, le problème de la coopération peut se ramener à déterminer qui fait quoi, quand, où, avec quels moyens, de quelle manière et avec qui, c'est-à-dire en fait à résoudre les différents sous-problèmes que constituent la collaboration par répartition de tâches, la coordination d'actions et la résolution de conflits. La réalisation de systèmes de répartition de services et de coordinations, tels que la médiation (usage de médiateurs ou courtiers pour la répartition des services en fonction des offres et des demandes (Figure 6) ou le réseau contractuel, fondé sur la notion de marché [43] passent par l'établissement de protocoles de conversations, qui peuvent faire l'objet d'une représentation et d'une validation par réseaux de Pétri.

Présentation et d'une validation par réseaux de Pétri. L'analyse des systèmes d'interaction passe aussi par la planification distribuée et la coordination d'actions. Des techniques tant cognitives que réactives ont été développées. Les premières ont été initiées par Lesser, Durfee et Decker avec le modèle PGP (Partial Global Planning) [44] [45]. Depuis, d'autres modèles ont été présentés. En France signalons les recherches portant sur la technique d'insertion incrémentale de plans [48]et sur l'usage de réseaux de Petri récursifs pour la définition de protocoles de planification distribuée [47].

En ce qui concerne les techniques réactives, celles-ci ont été surtout appliquées à la coordination de mouvements dans des groupes de robots (cf. section 4.4) [50].

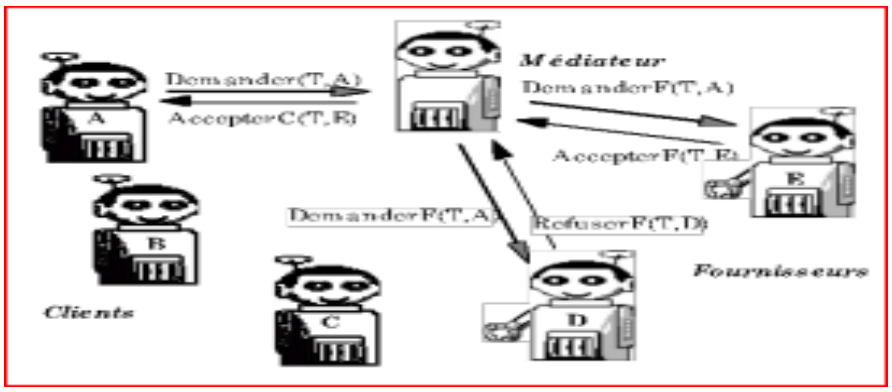


Figure III-6: La répartition de taches par médiation

III-2-6) Les Plateformes SMA :

Afin de réaliser une opérationnalisation plus accessible des systèmes multi-agents, des travaux ont tenté de réutiliser des architectures et des langages existants pour construire des environnements de développement de ces systèmes. Parmi les plateformes les plus connues, on peut citer :

- ✓ **AnyLogic :** Logiciel de simulation multi_agents et multi-méthode.
- ✓ **CORMAS :** (COmmon Ressources Multi-Agent System) est un Framework de développement de systèmes multi_agents, open-source et basé sur le langage de programmation orientée objet SmallTalk. Il est centré sur les problématiques de recherche en sciences du développement et de négociation entre acteurs.
- ✓ **DoMIS :** Est un outil permettant la conception de Systèmes Multi_agents (orientés « pilotage opérationnel de systèmes complexes »). Utilisé pour l'analyse désionnelle des systèmes complexes.
- ✓ **JACK :** Est un langage de programmation et un environnement de développement pour agents cognitifs, développé par la société Agent Oriented Software comme une extension orientée agent du langage Java.
- ✓ **Jadex :** Est une plate-forme agent développée en JAVA par l'université de Hambourg qui se veut modulaire, compatible avec de nombreux standards et capable de développer des agents.
- ✓ **Jagent :** Est un Framework open-source réalisé en Java dont l'objectif est de faciliter le développement et le test de systèmes multi_agents. MAGIQUE : Est une plate-forme pour agents physiquement distribués écrite en Java et fournissant un modèle de communication original d'appel à la cantonade. Dans MAGIQUE, les compétences sont dissociées des agents. L'architecture des agents et les différentes compétences sont développées séparément. Les compétences sont ensuite greffées comme plugin dans les agents au gré du concepteur. Cette plate-forme est développée au sein du LIFL.
- ✓ **MadKit :** La plate-forme MadKit (acronyme de Multi_agents Développement Kit) a été conçue en 1996 par Jacques Ferber, Olivier Gut Knecht et Fabien Michel au laboratoire LIRMM de l'université de Montpellier, c'est un ensemble de packages écrits en java qui implémente le micro noyau agent. La plate-forme MadKit est développée pour exploiter les avantages de programmation multi-agents qui se basent sur le modèle organisationnel Aalaadin.

- ✓ **SWARM :** SWARM (Minar, 1996) est une plate-forme multi_agents avec agents réactifs. L'inspiration du modèle d'agent utilisé vient de la vie artificielle. SWARM est l'outil privilégie de la communauté américaine et de chercheurs en vie artificielle. L'environnement offre un ensemble de bibliothèque qui permet l'implémentation des systèmes multi-agents avec un grand nombre d'agents simples qui interagissent dans le même environnement.
- ✓ **ZEUS :** ZEUS (Nwama ; 1999) est une plate-forme de développement de SMA générique, personnalisable et pourrait être augmentée par l'adjonction de nouveau composants. Elle est présentée sous forme d'un ensemble de classes implémentées dans le langage Java. En cela, elle est complètement portable et peut être utilisée sur tous systèmes disposant d'une machine virtuelle Java. [38]
- ✓ **Jade :** JADE (Java Agent DEveloppement), est un Framework de développement de systèmes multi_agents, open-source et basé sur le langage Java. Il offre en particulier un support avancé de la norme FIPA-ACL, ainsi que des outils de validation syntaxiques des messages entre agents basés sur les ontologies.

- Est une plate-forme multi-agent créé par le laboratoire TILAB.
- C'est un Framework qui permet le développement de systèmes multi-agent et d'applications conformes aux normes FIPA (Foundation for Intelligent Physical Agents).
- La FIPA est une organisation en 1996 dont l'objectif est de produire des standards pour l'interopération d'agents logiciels hétérogènes.
- Jade possède trois modules principaux (nécessaire aux normes FIPA). DF « Directory Facilitator » fournit un service de « pages jaunes » a la plateforme ;
  - ACC « Agent Communication Channel » gère la communication entre les
  - agents ; AMS « Agent Management System » supervise l'enregistrement des agents,
  - leur authentification, leur accès et l'utilisation du système (RMA).
- Ces trois modules sont activés à chaque démarrage de la plate-forme.

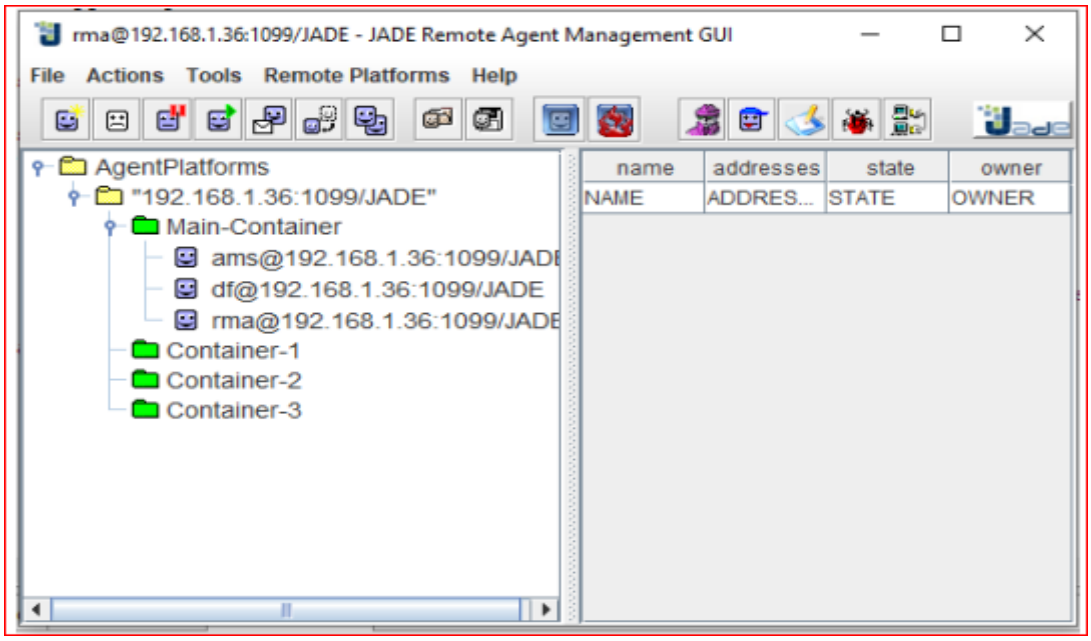


Figure III-7: Structure de la plateforme Jade

Chapitre IV

Conception & implémentation

IV) Conception et Implémentation

Introduction

Suite au succès de l'application des systèmes immunitaires artificiels dans le domaine de sécurité,plus précisément la détection d'intrusions et les caractéristiques des systèmes multi_agents telles que l'adaptabilité, la distribution et la coopération. On a proposé un système de détection d'intrusion qui combine les avantages des deux systèmes les SIA et les SMA. En effet le système proposé implémente l'approche par scénario appliquée sur un NIDS (IDS réseau) en s'appuyant sur l'algorithme de sélection négative dans un univers multi agents qui supporte la distributivité etla coopération pour fournir une meilleure surveillance du réseau.

IV-1) Formatage et extraction d'attributs

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

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

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

IV-1-1)Attaques par « Déni de Service » (Denial Of *Service* DOS) :

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

IV-1-2)Attaques par « Utilisateur vers Administrateur » (User to Root U2R) :

L'attaquant commence à avoir un accès à un compte utilisateur normal sur le système, ensuite il essaie d'exploiter la vulnérabilité sur ce système pour obtenir un accès administrateur.

IV-1-3)Attaques par « Distant vers local » (Remote to Local R2L):

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

IV-1-4)Attaques par « Sonde » (Probing) :

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

Le tableau suivant présente les 41 attributs de chaque enregistrement :

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

Tableau 2: les attributs de chaque ligne de connexion [38]

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

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

Tableau 3: les attaques de chaque classe [38]

IV-2) La sélection d'attributs pertinents :

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

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

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

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

Tableau 4: les attributs pertinents de chaque classe d'attaque. [38]

IV-3) Conception du système proposé

IV-3-1)Les composants immunitaires

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

A-Antigène (AG) :

Dans notre approche, nous considérons une intrusion tout paquet IP de typeantigène, ce dernier peut être

A-1.Un élément de soi :

si le paquet est considéré comme étant une connexion normale et qui n'aaucun risque sur le réseau.

A-2.Un élément de non soi :

Si le paquet est considérer comme une attaque sur le réseau (uneconnexion anormale).

B-Anticorps :

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

C-Mesure d'affinité :

a. Dans le but de mesurer l'affinité entre le couple Antigène /Anticorps, notresystème s'appuie sur la distance de Hamming (DH). Dont :

- Un antigène est représenté par un vecteur Ag=<Ag1, Ag2,..., AgL>,
- Un anticorps est à son tour représenté par un vecteur Ab=<Ab1,Ab2,…,AbL>.

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

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

Affinité :

1 si Distance_Haming(Ag,Ab)>δ

0 sinon

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

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

D-Les algorithmes immunitaires :

Dans le cadre de notre étude on a choisi l'algorithme de la sélection négative car il a prouvé à travers plusieurs travaux précédents son efficacité en ce qui concerne la discrimination entre le soi et le non soi citant comme exemple le travail de **S.Hofmeyr**,qui a conçu un IDS nommé LYSIS basé sur l'algorithme de la sélection négative. Qui se déroule comme suit : Les agents du système :

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

Agent	Fonction
Agent Routeur	Assure la connectivité, en recevant les paquets de l'extérieur et les retransmettre vers les hôtes cibles sices paquets ne présentent aucun risque sur le réseau. Il agit comme un capteur de paquets pour l'IDS.

Agent PaquetGenerator	Permet la génération des paquets du trafic réseau(générer des onnexions normales)
Agent Host 1	Cet agent simule l'hôte numéro1 du réseau surveillé
Agent Host 2	Cet agent simule l'hôte numéro 2 du réseau surveillé
Agent Host 3	Cet agent simule l'hôte numéro3 du réseau surveillé
Agent HistoryAgent	Permet l'IDS de vérifier si une connexion est anormale toute en consultant l'historique desattaques sur ce réseau.
Agent Detector 1	Permet la détection d'intrusion pour les paquets ciblant l'hôte 1 du réseau en s'appuyant sur la base d'attaques du système.la discrimination du soi et noi-soi ici est basée sur l'algorithme de la sélection négative Cette agent représente l'analyseur des données d'IDS
Agent Detector 2	Même principe de fonctionnement du Agent Dector1sauf qu'il s'occupe de la détection d'intrusion pour l'hôte 2
Agent Detector 3	Même principe de fonctionnement du Agent Dector1sauf qu'il s'occupe de la détection d'intrusion pour l'hôte 3
Agent Hacker	C'est le responsable du lancement des différents attaques vers les hôtes cibles (générer des connexions malveillantes)
Agent Alert	C'est l'agent responsable de déclanchement d'alertesi une attaque est détectée

Tableau 5: Les agents du système proposé

IV-3-2)Le processus de déroulement :

A-La construction de la base d'attaque

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

1. Extraction des attributs pertinents de chaque attaque à partir de la base KDD cup 99.
2. Elimination des détecteurs redondants.
3. Vérification de correspondance avec les modèles de soi avec élimination des détecteurs qui reconnaissent le soi.

Vérification de correspondance avec les modèles de non soi. L'organigramme ci-dessous résume le processus de construction de la base d'attaques :

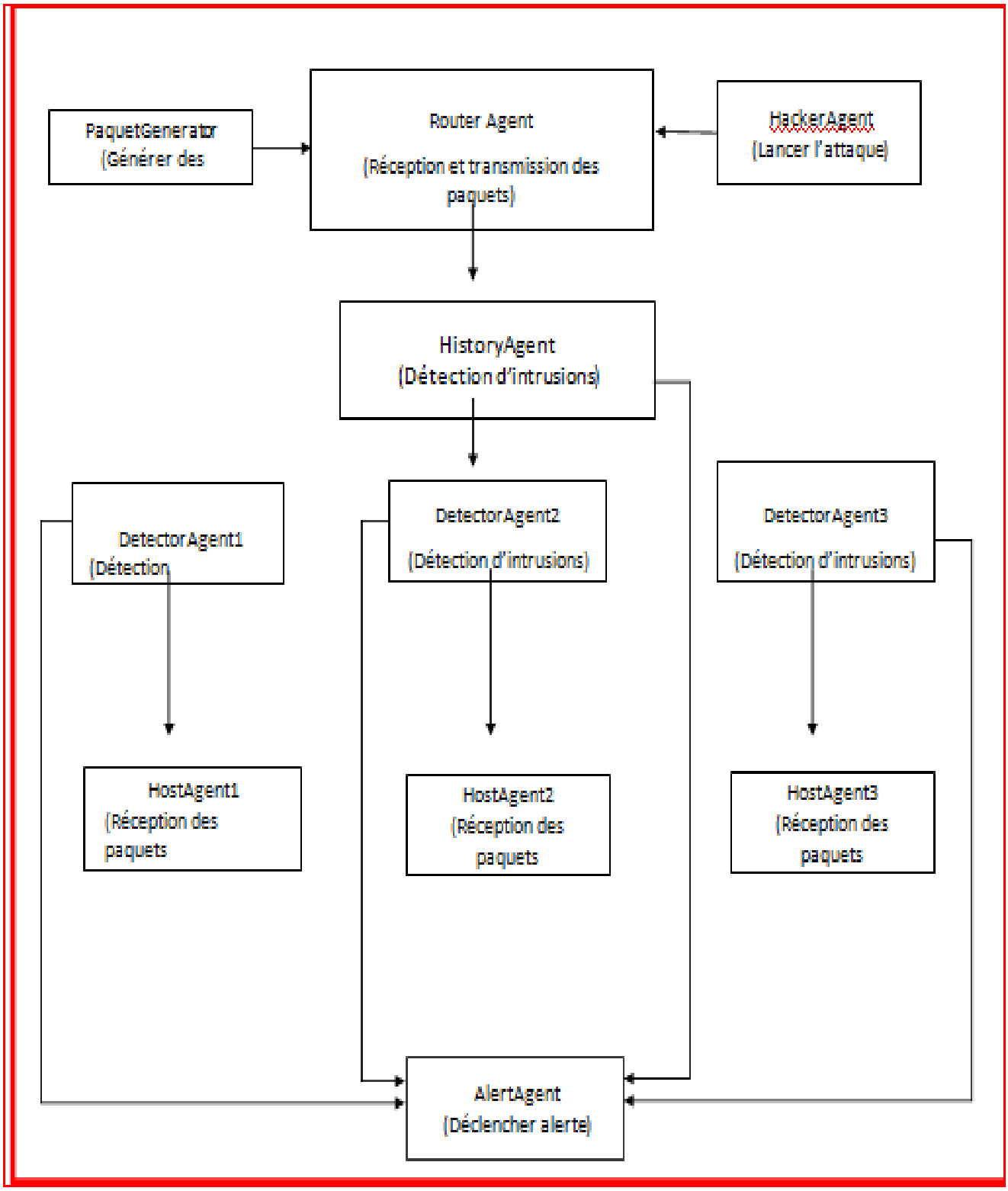


Figure IV-1: processus de génération de détecteur.

B-Le processus de détection

Afin de générer un trafic réseau, l'agent Paquet Generator génère des paquets et envoie ces derniers vers l'Agent routeur comme un trafic normal. Pour lancer une attaque, l'agent Hackerprend place et envoie à son tour un paquet malveillant vers le routeur.

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

- **La première phase :**

la vérification est réalisée par rapport à la base d'historique d'attaques subies par le réseau surveillé dans le but de minimiser le temps et accélérer la génération de réponse tout en cherchant dans une base d'historique réduite en terme de taille par rapport à labase d'attaques .si le paquet existe dans la base d'historique, l'Agent HistoryAgent va envoyerla réponse vers le routeur qui va à son tour bloquer ce paquet ainsi qu'une alerte va être déclenchée par l'agent AlertAgent . Sinon il lance la deuxième phase de détection.

- **La** deuxième **phase :**

L'agent DetectorAgent va vérifier le paquet entrant par rapport à la base d'attaques construite précédemment.si il existe une corrélation entre le paquet entrant et le détecteur, la réponse va être envoyé vers le routeur, si une attaque est détectée le routeur va bloquer ce paquet ainsi qu'une alerte va être déclenchée par l'agent AlertAgent de plus l'agentDetectorAgent va ajouter la nouvelle attaque détectée dans l'historique des attaques. Si aucuneattaque n'a été reconnue alors le routeur est autorisé à transmettre le paquet vers la cible.

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

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

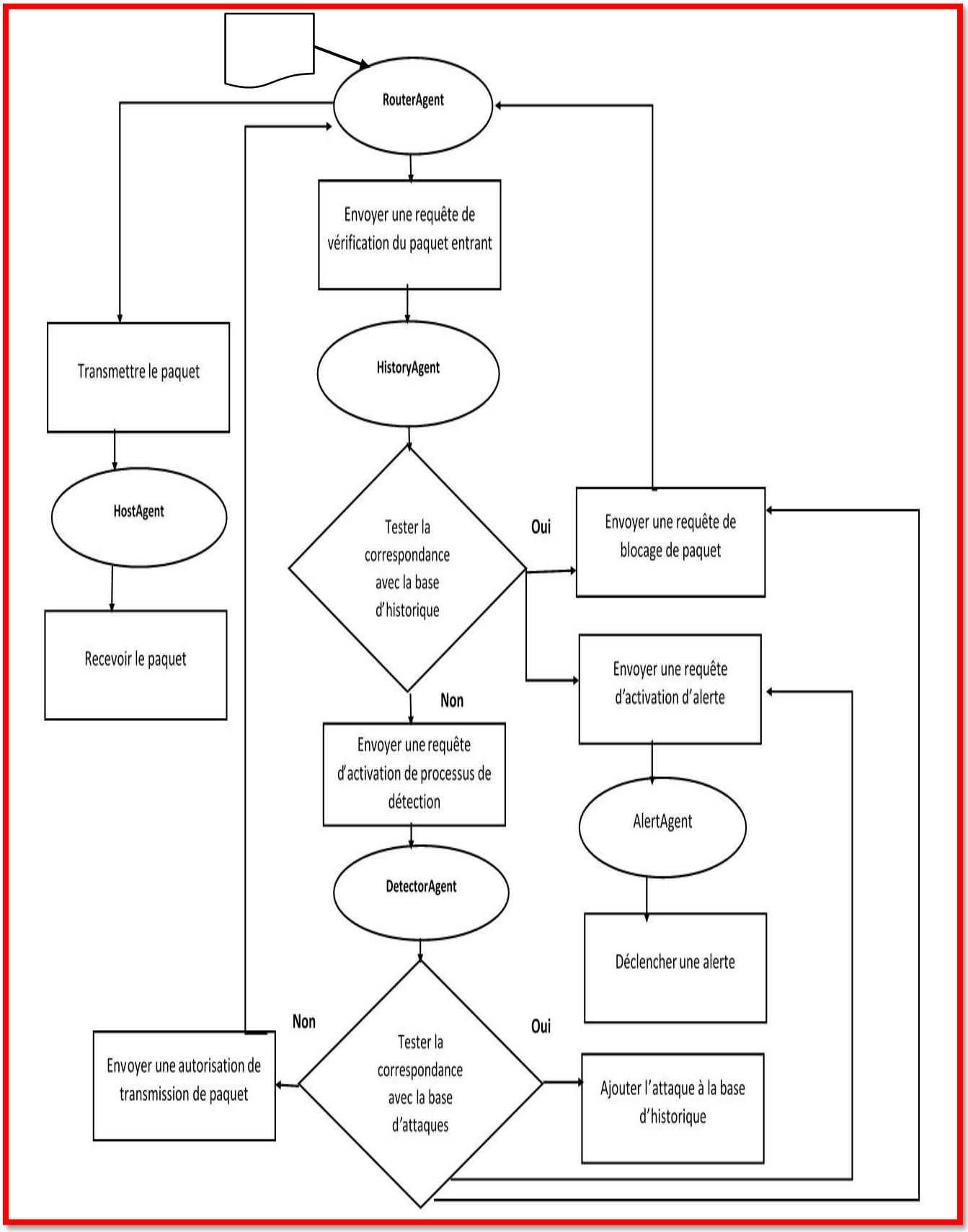

RouterAgent
Envoyer une requête de vérification du paquet entrant
HistoryAgent
Tester la correspondance avec la base d'historique
Oui
Envoyer une requête de blocage de paquet
Envoyer une requête d'activation d'alerte
AlertAgent
Déclencher une alerte
Non
Envoyer une requête d'activation de processus de détection
DetectorAgent
Tester la correspondance avec la base d'attaques
Oui
Ajouter l'attaque à la base d'historique
Non
Envoyer une autorisation de transmission de paquet
Transmettre le paquet
HostAgent
Recevoir le paquet

Figure IV-2 : Le processus de détection

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

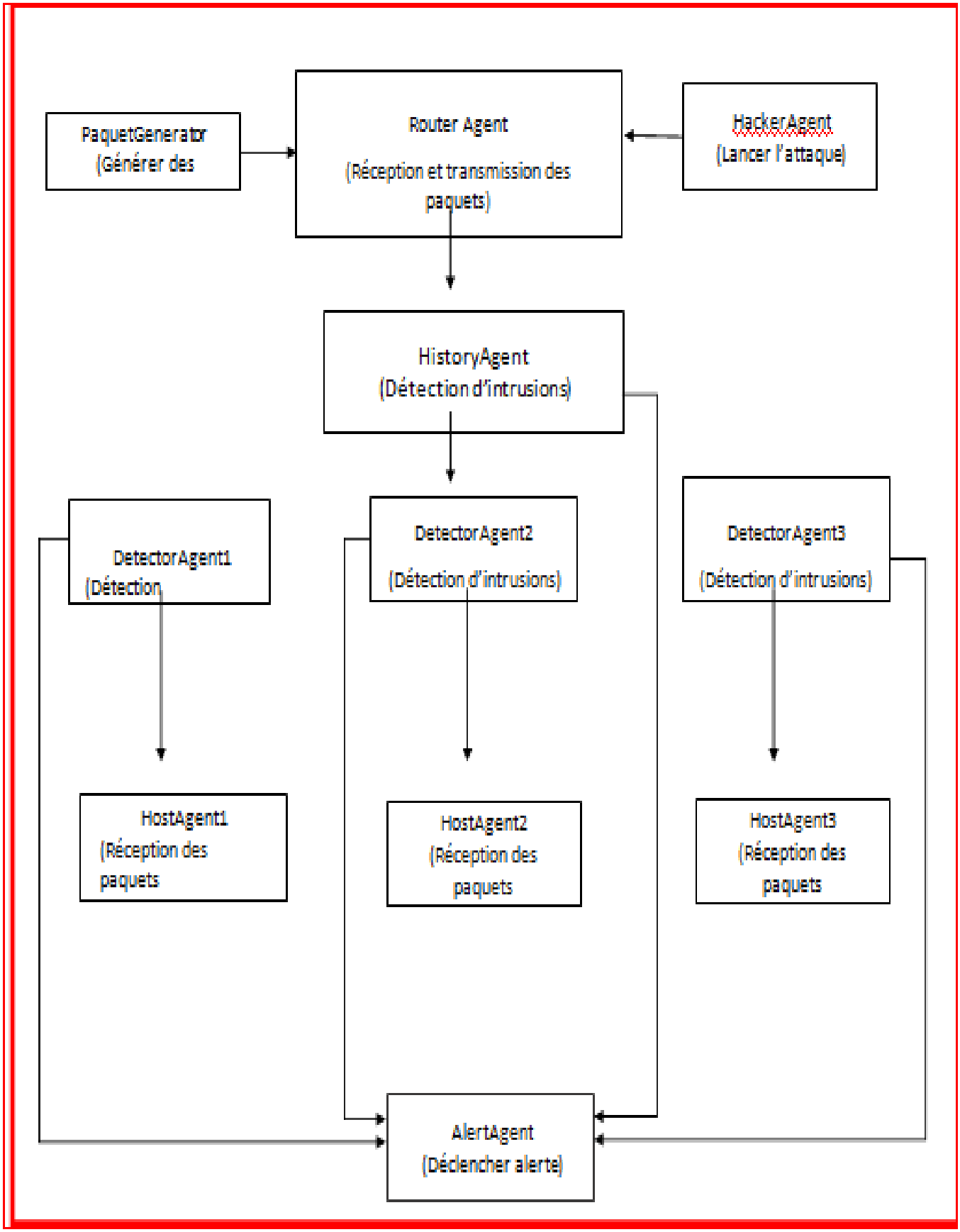


Figure IV-3: Architecture générale du système proposé

La figure suivante présente le diagramme de séquence :

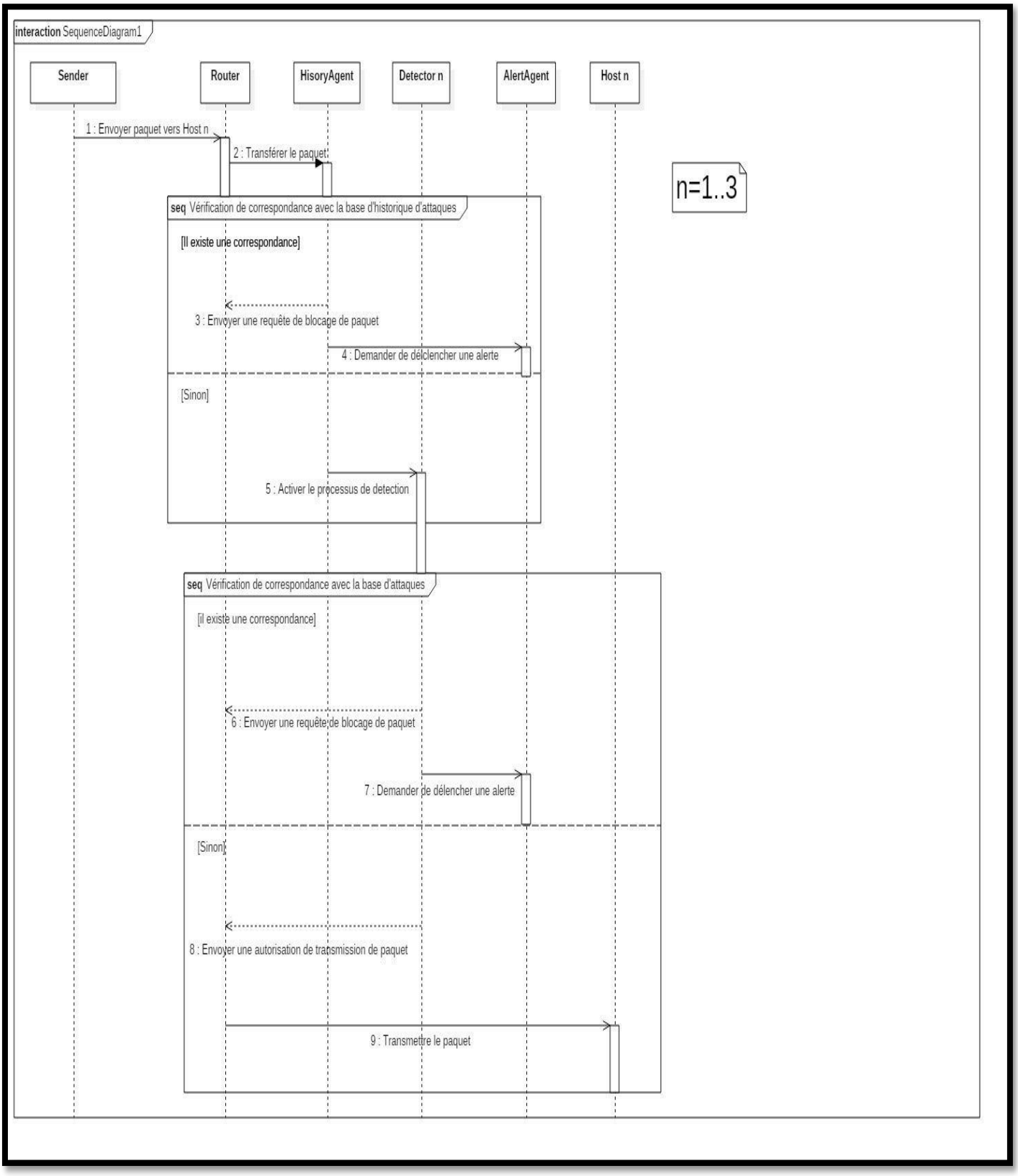


Figure IV-4: Diagramme de séquence

Remarque :

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

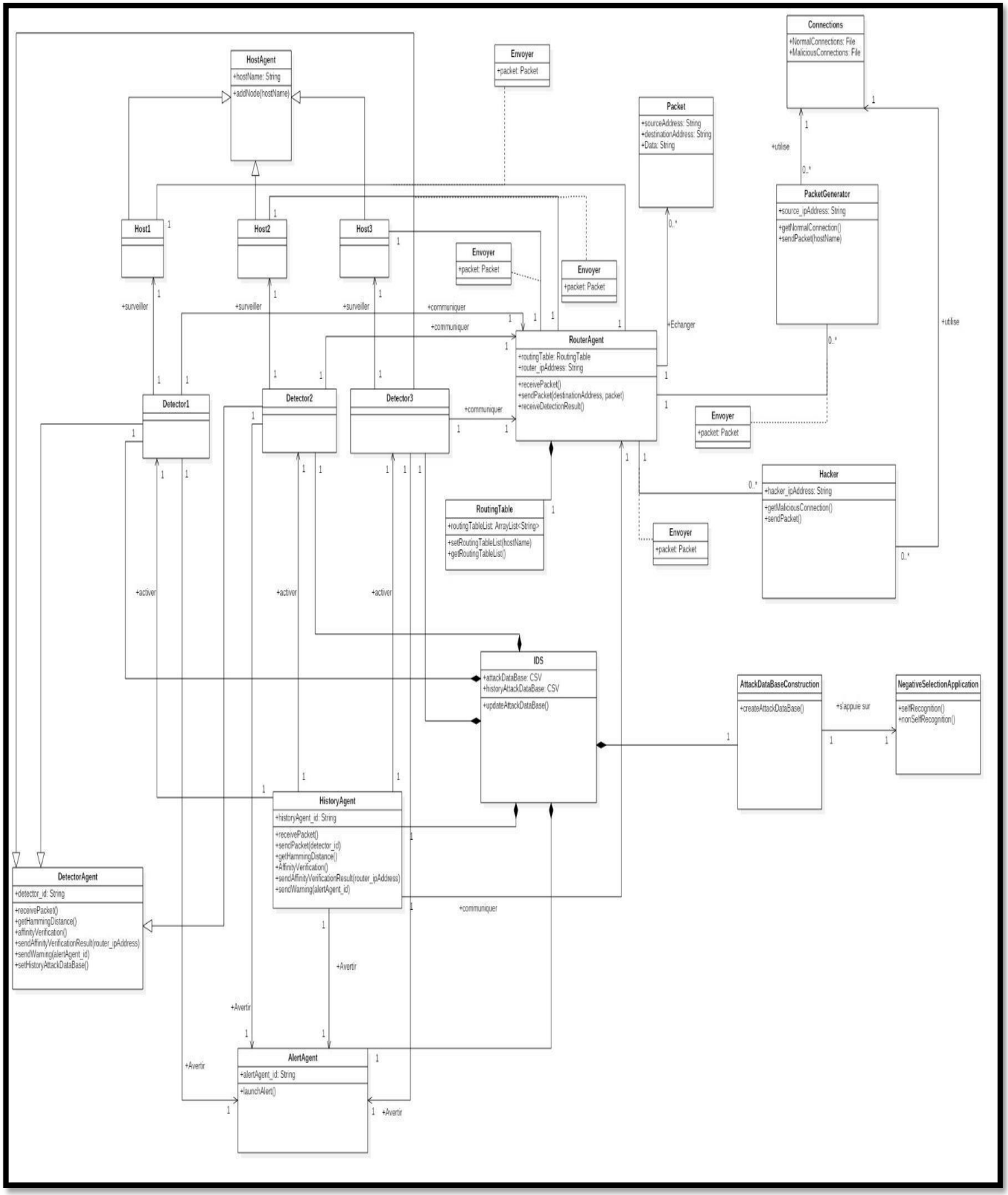


Figure IV-5: Diagramme de classe

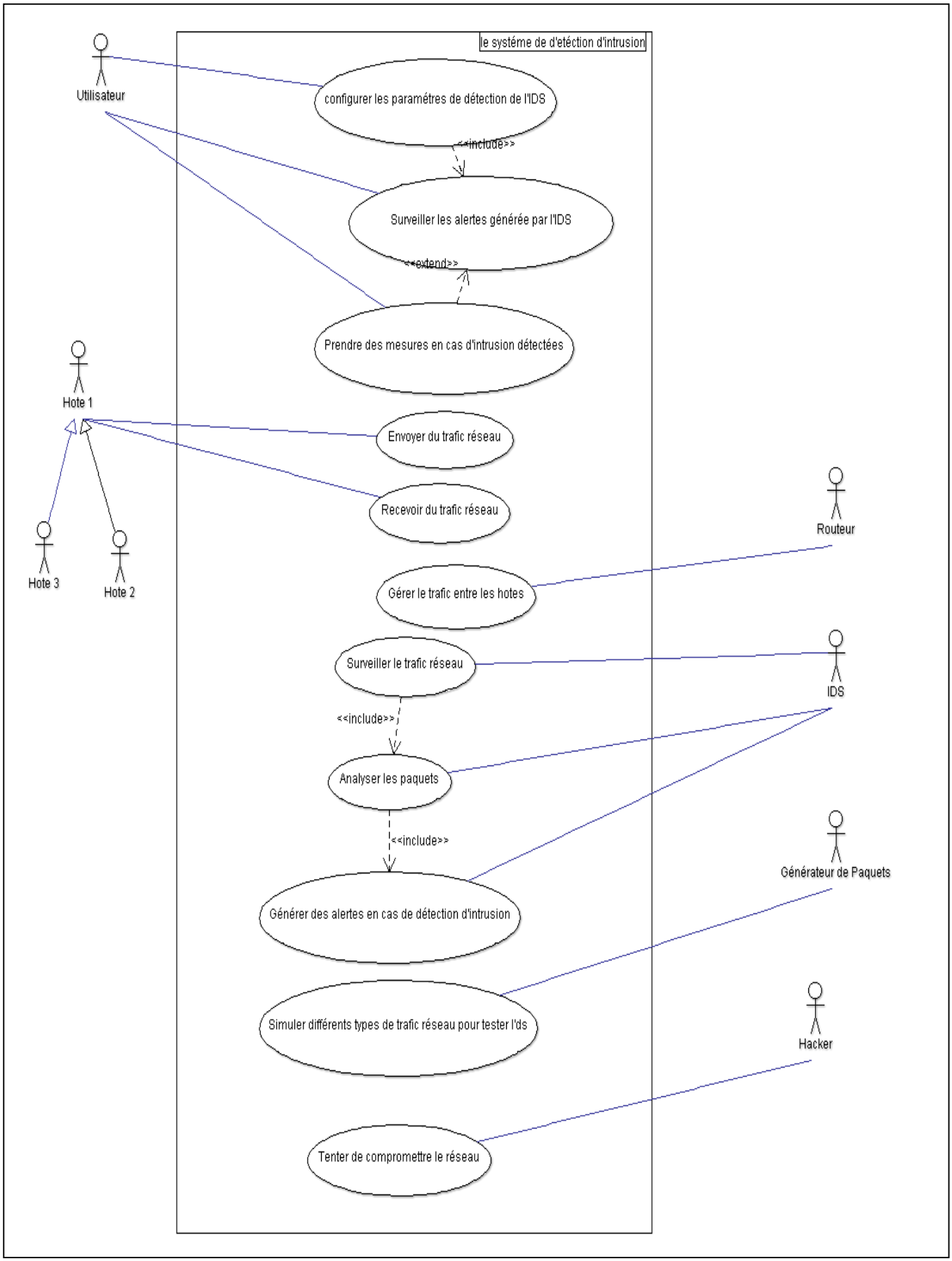


Figure IV-6:diagramme de cas d'utilisation

IV-4) Etude expérimentale et résultat

Pour évaluer le système proposé on a calculé le taux de détection et le taux de fausse alerte avec :

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

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

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

FN: False Negative (Faux Négatif) événement intrusif identifié comme normal

Taux dedétection= TP/TP+FN

Taux de fausse Alerte= FP/FP+TN

Tester sur les quatre types d'attaques : DOS, PROBE, L2R et U2R

On a obtenu les résultats suivants :

	TP	FP
Normale	**98.97%**	**1,03%**
DOS	**98.88%**	**1.12%**
Probe	**92.85%**	**7,15%**
R2L	**83.38%**	**16,62%**
U2L	**81.09%**	**18,91%**

Tableau 6: Les résultats du système

IV-5) Les environnements de développement :Delphi

IV-5-1)Introduction au Delphi

Le Delphi utilise le langage Pascal Objet qui est une amélioration apportée par Borland du langage Pascal. Pour simplifier on pourrait dire que le Pascal Objet est au Pascal ce que le C++ est au C.

IV-5-2)Présentation

Delphi est à la fois un langage de programmation orienté objet (POO) et un environnement de développement intégré. Édité par la société Embarcadero(anciennement Borland puis CodeGear), il se pose en alternative au langage Visual Basic en proposant un développement a la fois très rapide et de grande qualité.

IV-5-3)Installation

Tout ce dont vous avez besoin pour programmer en Delphi/Pascal Objet est le logiciel Delphi ou un environnement de développement d'intégré (IDE) associé. Pour acheter Delphi, allez sur http://www.embarcadero.com. Pour une version de Delphi gratuite (mais moins performante), allez sur http://www.turboexplorer.com. Pour un IDE open source associé à Delphi, allez sur http://www.lazarus.freepascal.org mais vous devez savoir qu'il y a des différences entre Delphi et Lazarus.

Attention, le langage Delphi ne tourne que sur Windows. L'alternative au langage Delphi pour Linux s'appelle Kylix.

Choisissez un de ces liens et installez l'IDE. Le meilleur compromis est sans doute Turbo Delphi Explorer.


ArgoUML:

IV-5-4)Introduction

Ce logiciel est un outil de modélisation UML qui est Open Source. Il a été créé en 1999 par Toby Baier pour Tigris en partenariat avec l'université de Californie. La dernière version date du 13 octobre 2000 et c'est la version v0.8.1a. C'est un logiciel entièrement écrit en Java qui est basé sur UML 1.3. Il nécessite l'installation de JDK 1.2 ou plus.
Son installation se fait facilement en mode graphique.

IV-5-5)But de ce logiciel

Ce logiciel permet de créer des diagrammes UML et le code source correspondant. Il ne supporte que la notation UML. Par contre, il ne fait pas d'analyse inverse.
Il ne peut générer qu'un seul langage : le Java.

IV-5-6)Diagrammes UML

ArgoUML permet de créer :

- des diagrammes de classes
- des use-case
- des diagrammes d'états
- des diagrammes d'activité
- des diagrammes de collaboration
- des diagrammes de déploiement

IV-5-7)Plateforme Jade

Jade est un Intergiciel pour le développement d'applications pair à pair d'agents intelligents sur desplateformes fixes, téléphones mobiles, ... etc. Elle satisfait les spécifications de la FIPA-ACL. JADE fonctionne sous tous les systèmes d'exploitation, inclut tous les composants Obligatoires qui contrôlent un SMA C'est un projet Open Source, LGPL License contrôlée par Telecom Italia Lab(TILAB), qui reste propriétaire du projet **Source spécifiée non valide.**.

IV-5-8)Matériel

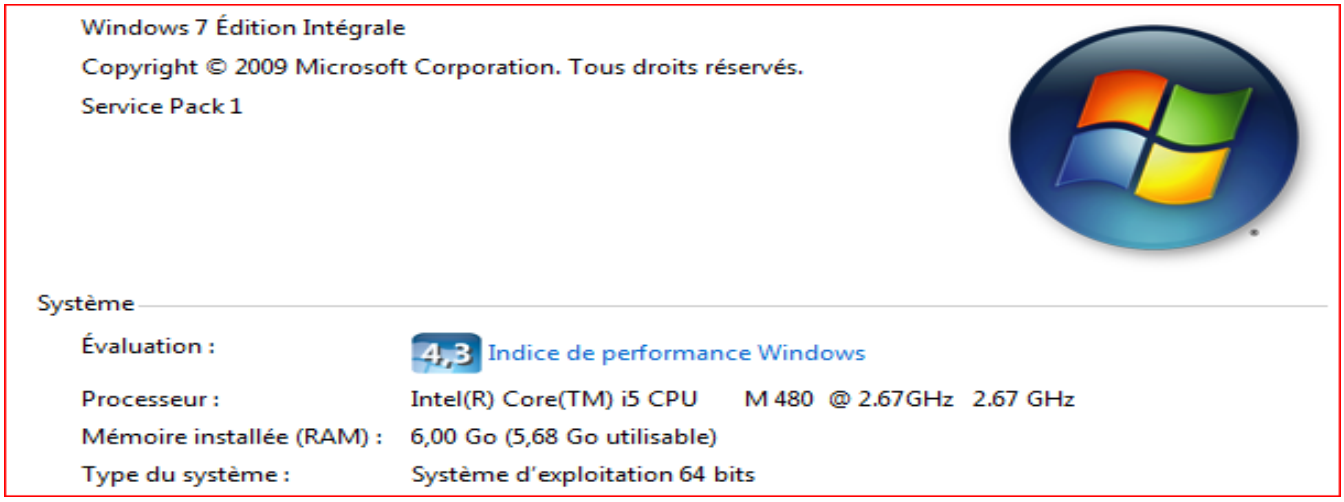
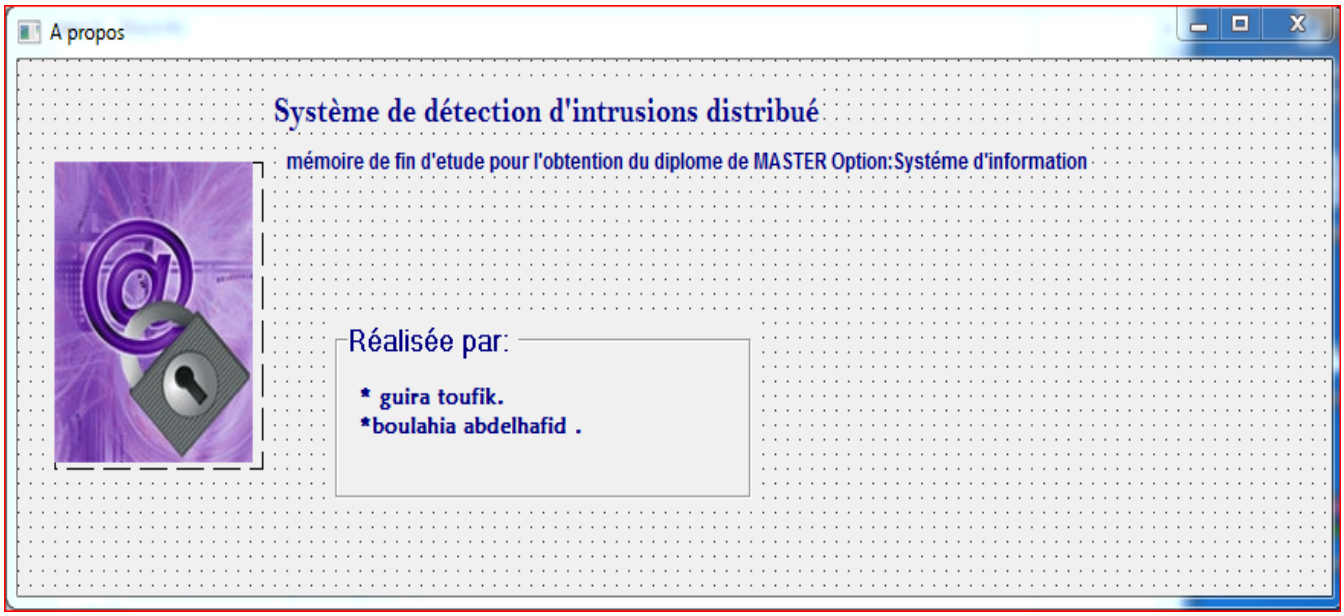
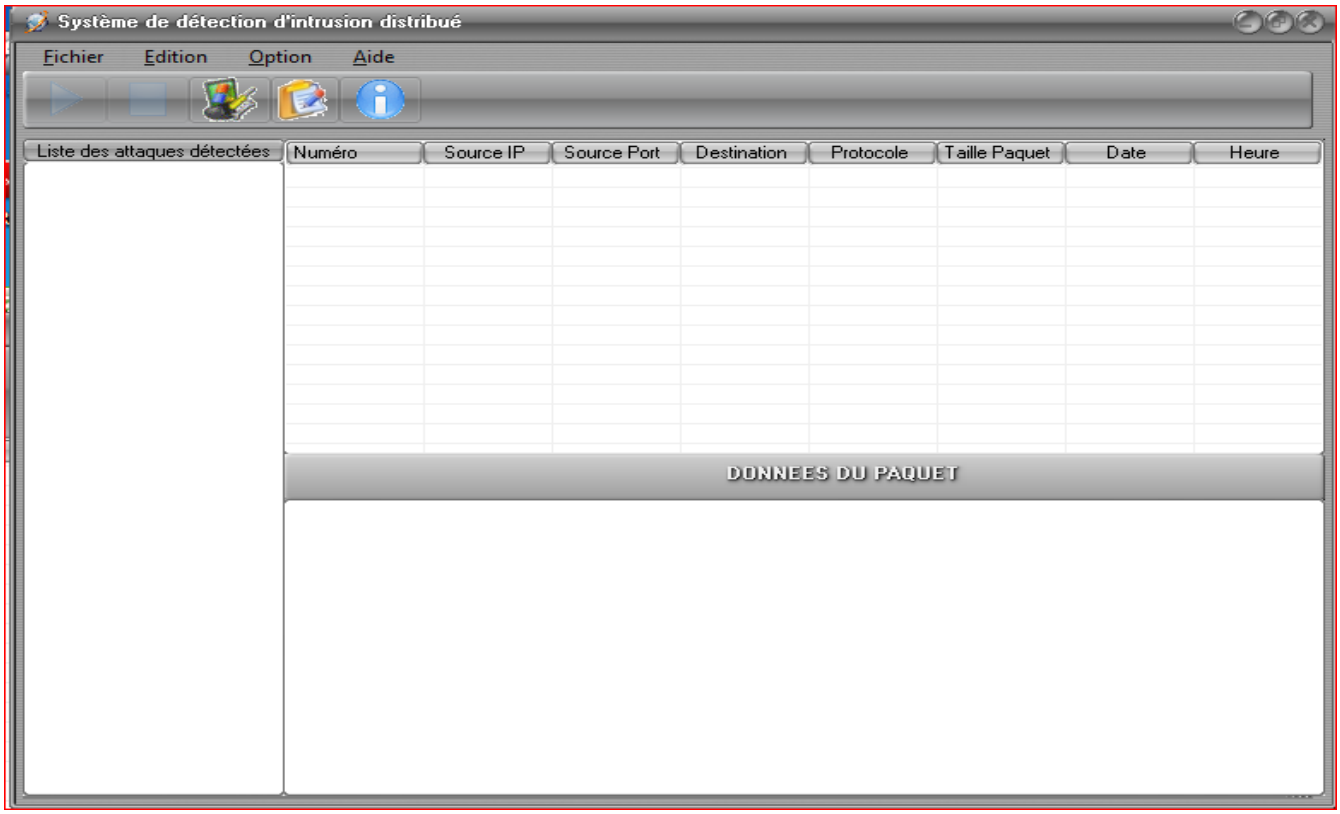
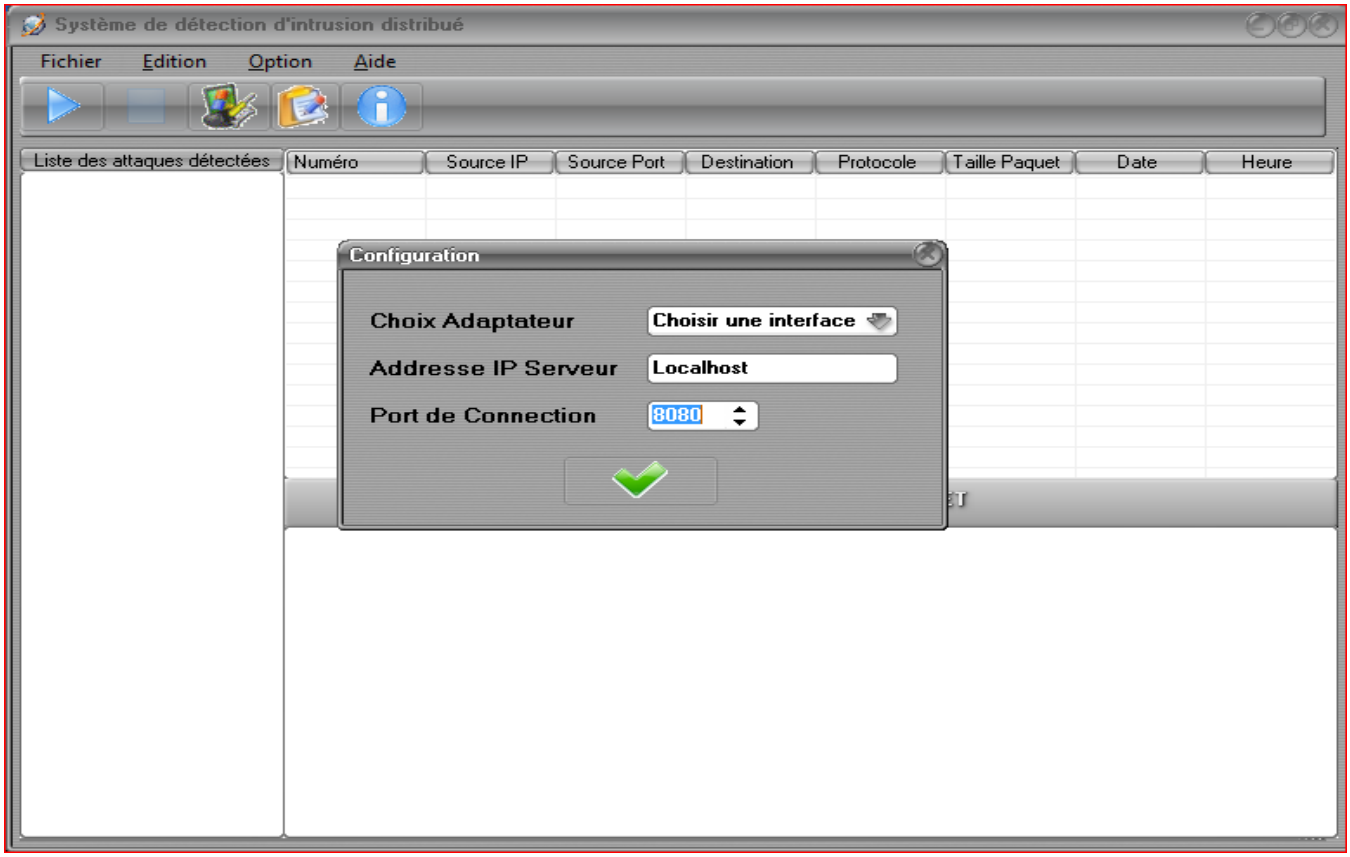


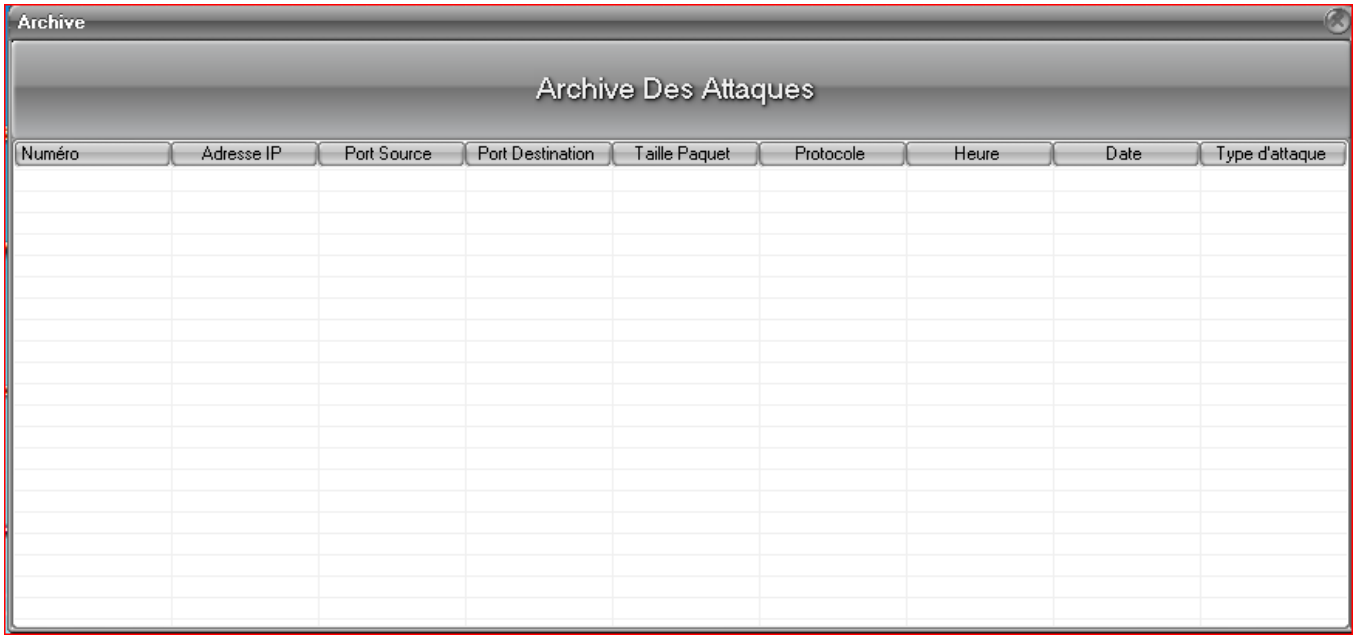
Figure IV-7:le système de réalisation de notre application

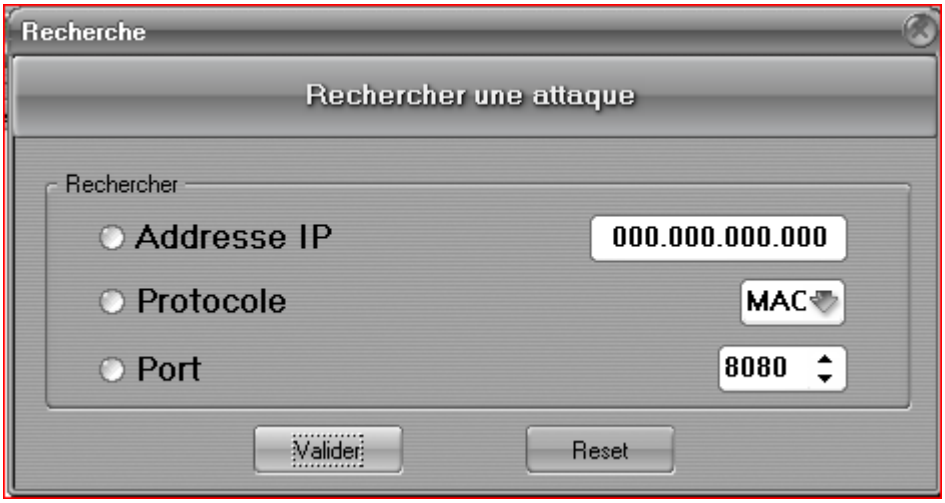
IV-6) Interface du système



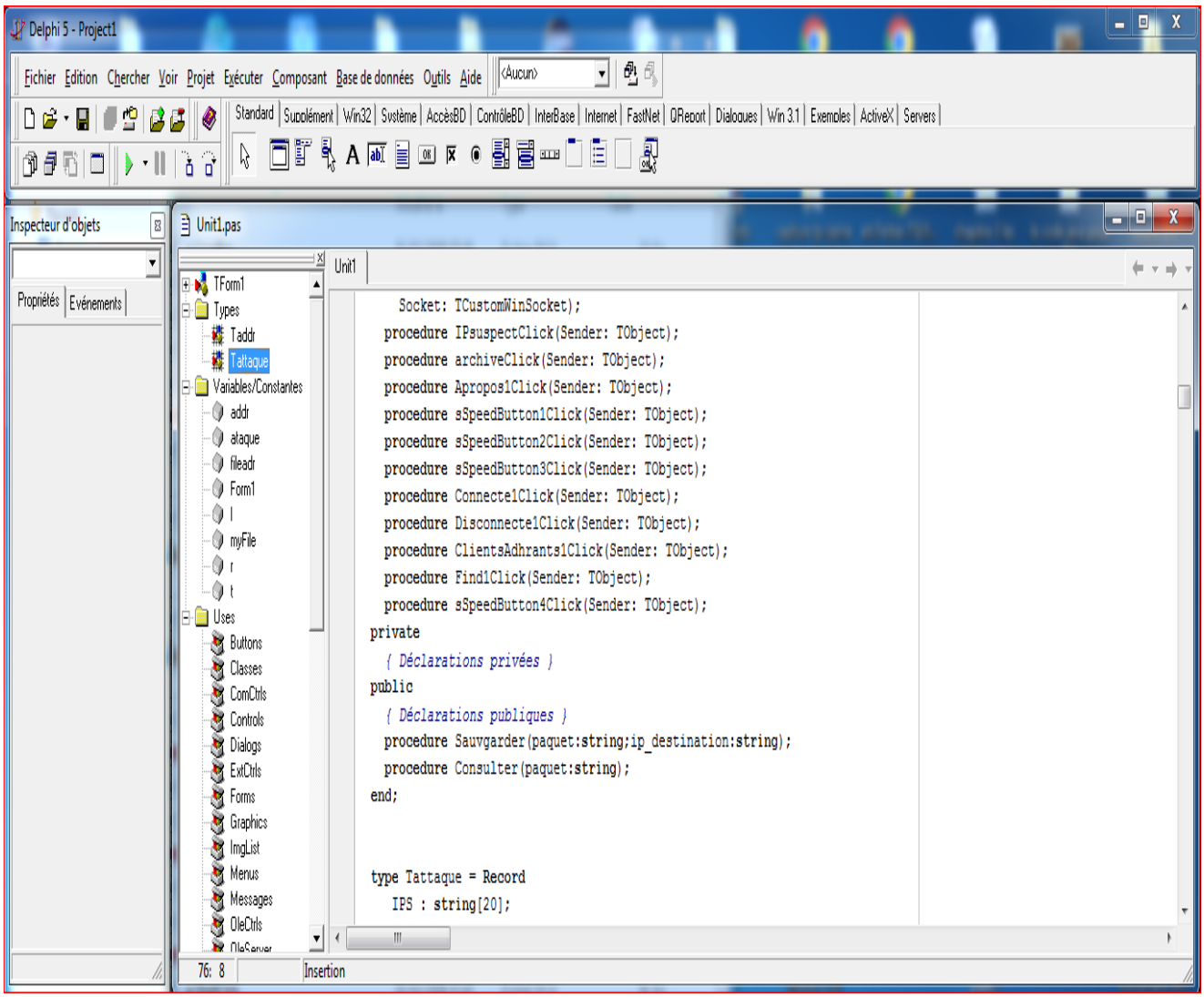

Système de détection d'intrusion distribué
Fichier
Edition
Option
Aide
Liste des attaques détectées
Numéro
Source IP
Source Port
Destination
Protocole
Taille Paquet
Date
Heure
DONNEES DU PAQUET

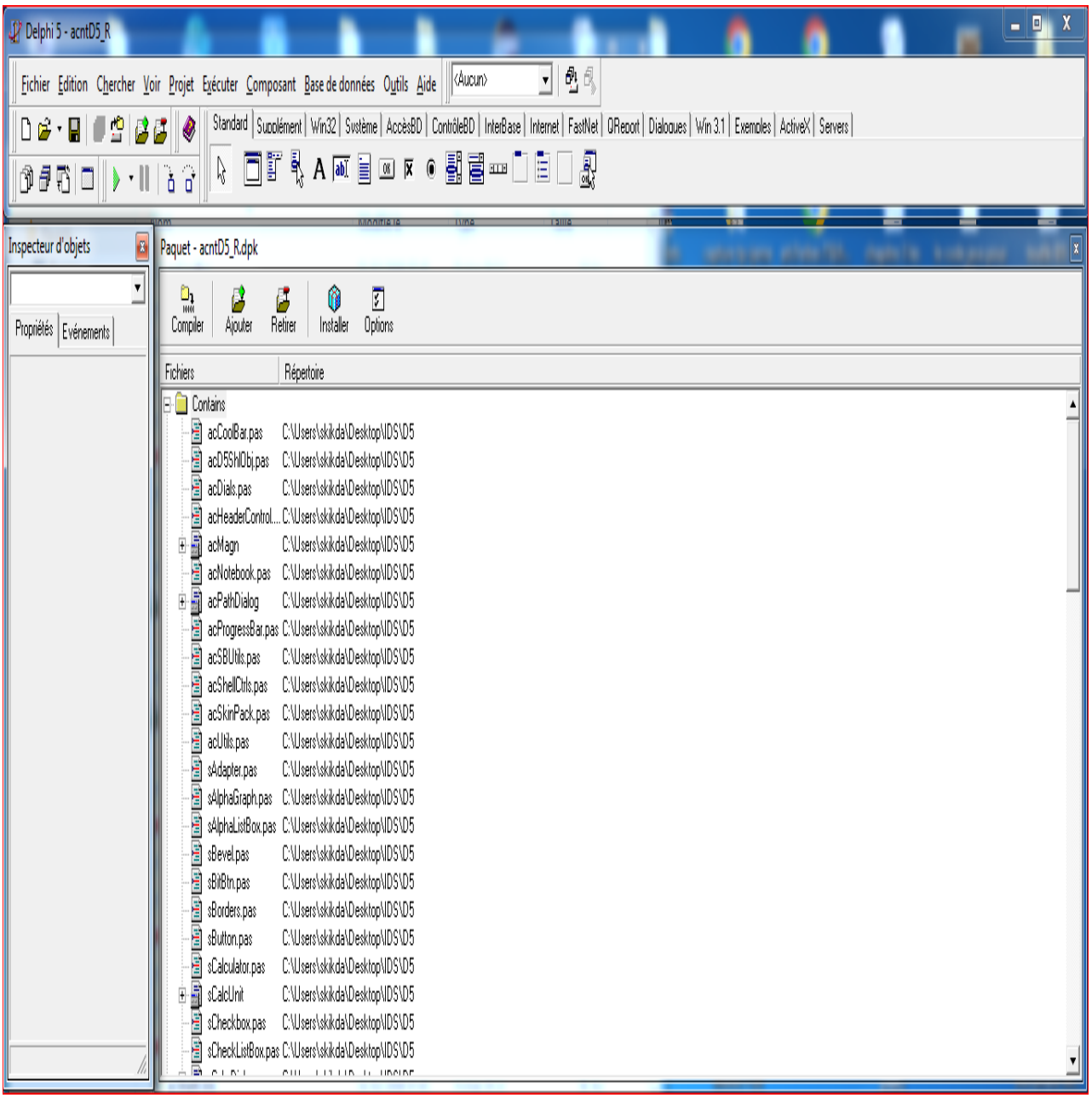

Système de détection d'intrusion distribué
Fichier
Edition
Option
Aide
Liste des attaques détectées
Numéro
Source IP
Source Port
Destination
Protocole
Taille Paquet
Date
Heure
Configuration
Choix Adaptateur
Choisir une interface
Addresse IP Serveur
Localhost
Port de Connection
8080

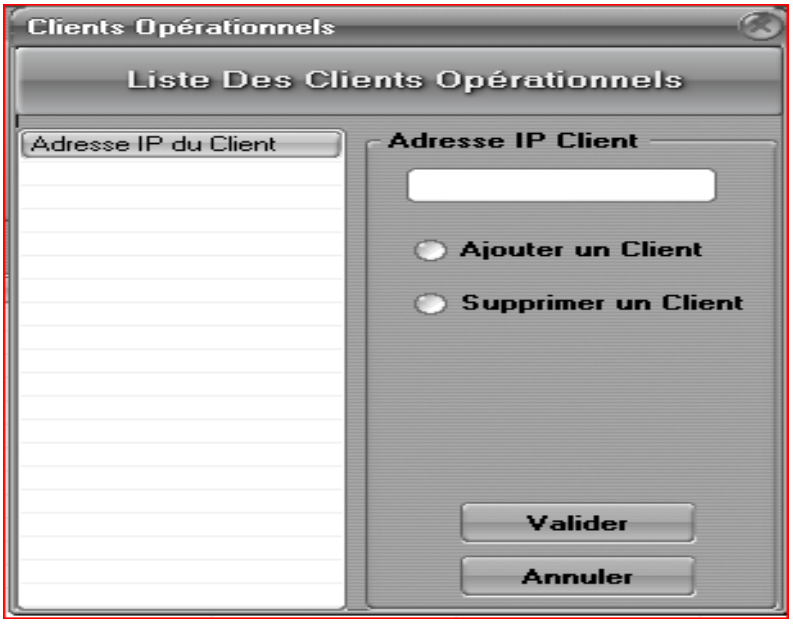

Archive
Archive Des Attaques
Numéro
Adresse IP
Port Source
Port Destination
Taille Paquet
Protocole
Heure
Date
Type d'attaque

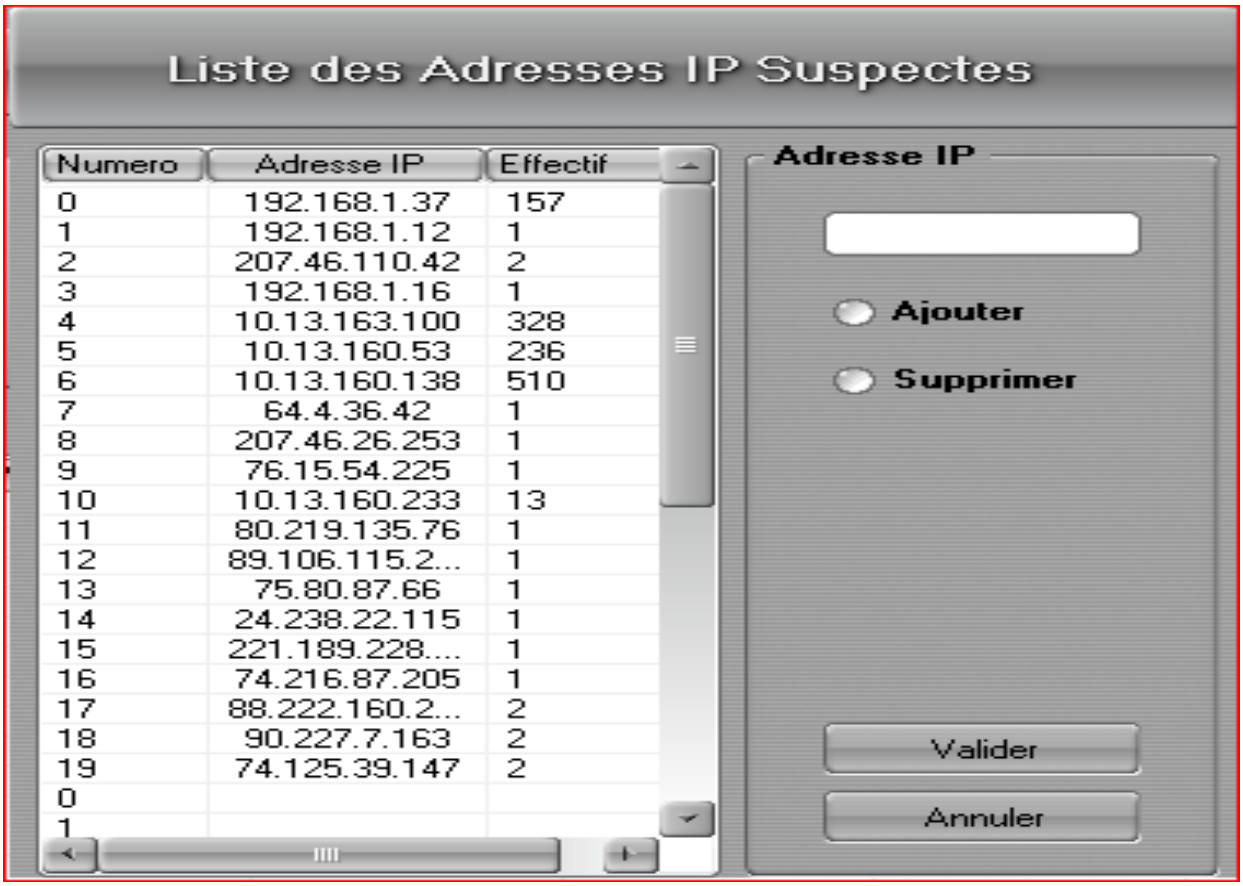

Recherche
Rechercher une attaque
Rechercher
Addresse IP
000.000.000.000
Protocole
MAC
Port
8080
Valider
Reset

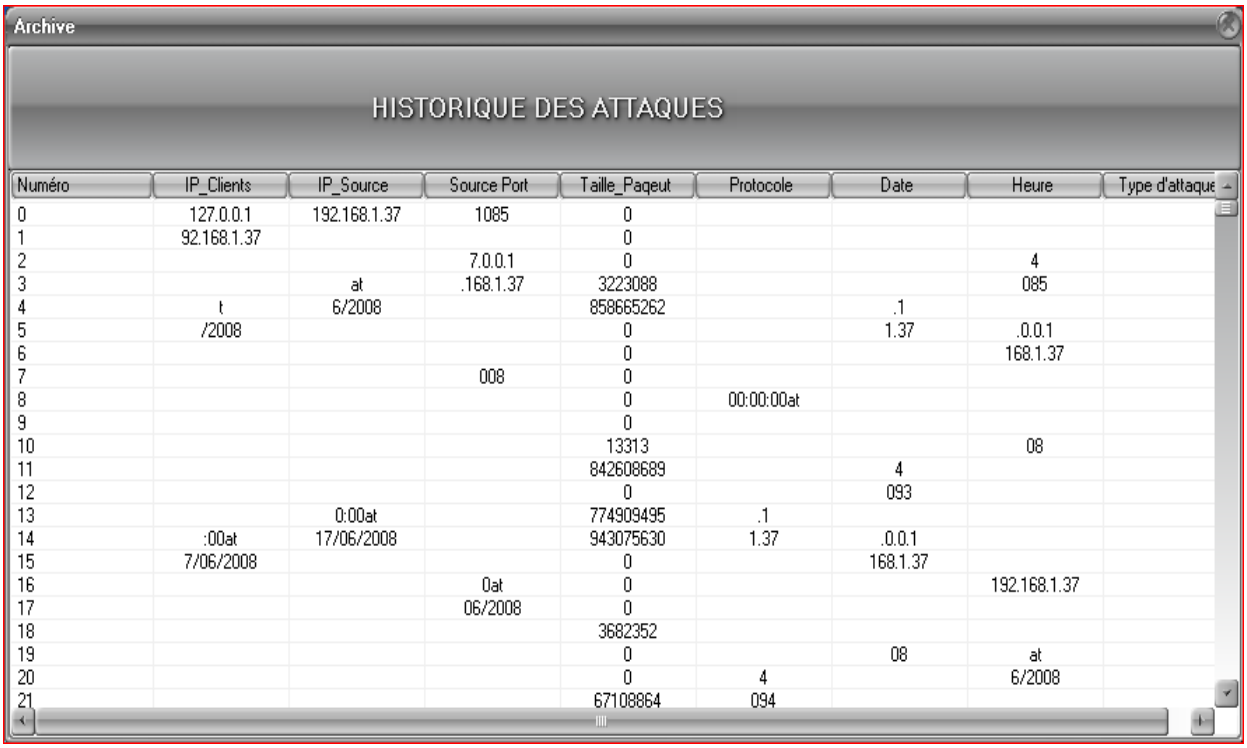

Client IDS
Invalid network adapter.
OK


Delphi 5 - Project1
Fichier Edition Chercher Voir Projet Exécuter Composant Base de données Outils Aide
Standard Supplément Win32 Système AccèsBD ContrôleBD InterBase Internet FastNet QReport Dialogues Win 3.1 Exemples ActiveX Servers
Inspecteur d'objets
Propriétés Evénements
Unit1.pas
Unit1
TForm1
Types
Taddr
Tattaque
Variables/Constantes
addr
alaque
fileadr
Form1
I
myFile
r
t
Uses
Buttons
Classes
ComCtrls
Controls
Dialogs
ExtCtrls
Forms
Graphics
ImgList
Menus
Messages
OleCtrls
Socket: TCustomWinSocket);
procedure IPsuspectClick(Sender: TObject);
procedure archiveClick(Sender: TObject);
procedure Apropos1Click(Sender: TObject);
procedure sSpeedButton1Click(Sender: TObject);
procedure sSpeedButton2Click(Sender: TObject);
procedure sSpeedButton3Click(Sender: TObject);
procedure Connecte1Click(Sender: TObject);
procedure Disconnecte1Click(Sender: TObject);
procedure ClientsAdhrants1Click(Sender: TObject);
procedure Find1Click(Sender: TObject);
procedure sSpeedButton4Click(Sender: TObject);
private
{ Déclarations privées }
public
{ Déclarations publiques }
procedure Sauvgarder(paquet:string;ip_destination:string);
procedure Consulter(paquet:string);
end;
type Tattaque = Record
IPS : string[20];
76: 8
Insertion

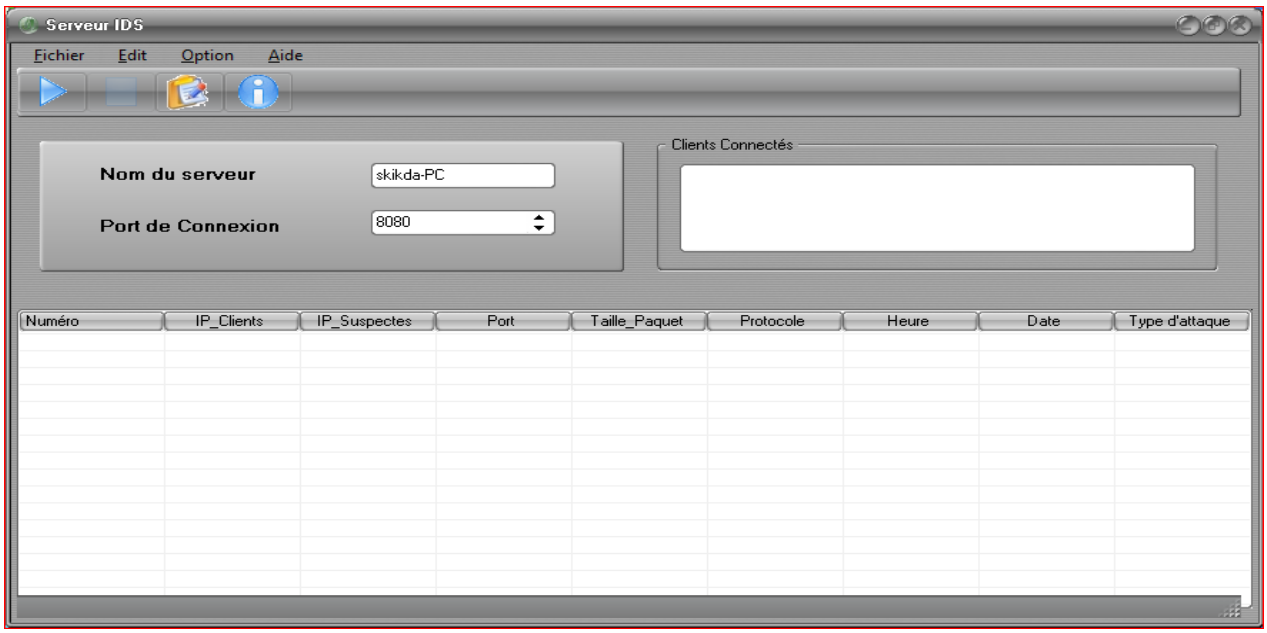

Delphi 5 - acntD5_R
Fichier Edition Chercher Voir Projet Exécuter Composant Base de données Outils Aide
Standard Supplément Win32 Système AccèsBD ContrôleBD InterBase Internet FastNet QReport Dialogues Win 3.1 Exemples ActiveX Servers
Inspecteur d'objets
Propriétés Evénements
Paquet - acntD5_R.dpk
Compiler Ajouter Retirer Installer Options
Fichiers Répertoire
Contains
acCoolBar.pas C:\Users\skikda\Desktop\IDS\D5
acD5ShlObj.pas C:\Users\skikda\Desktop\IDS\D5
acDials.pas C:\Users\skikda\Desktop\IDS\D5
acHeaderControl... C:\Users\skikda\Desktop\IDS\D5
acMagn C:\Users\skikda\Desktop\IDS\D5
acNotebook.pas C:\Users\skikda\Desktop\IDS\D5
acPathDialog C:\Users\skikda\Desktop\IDS\D5
acProgressBar.pas C:\Users\skikda\Desktop\IDS\D5
acSBUtils.pas C:\Users\skikda\Desktop\IDS\D5
acShellCtrls.pas C:\Users\skikda\Desktop\IDS\D5
acSkinPack.pas C:\Users\skikda\Desktop\IDS\D5
acUtils.pas C:\Users\skikda\Desktop\IDS\D5
sAdapter.pas C:\Users\skikda\Desktop\IDS\D5
sAlphaGraph.pas C:\Users\skikda\Desktop\IDS\D5
sAlphaListBox.pas C:\Users\skikda\Desktop\IDS\D5
sBevel.pas C:\Users\skikda\Desktop\IDS\D5
sBitBtn.pas C:\Users\skikda\Desktop\IDS\D5
sBorders.pas C:\Users\skikda\Desktop\IDS\D5
sButton.pas C:\Users\skikda\Desktop\IDS\D5
sCalculator.pas C:\Users\skikda\Desktop\IDS\D5
sCalcUnit C:\Users\skikda\Desktop\IDS\D5
sCheckbox.pas C:\Users\skikda\Desktop\IDS\D5
sCheckListBox.pas C:\Users\skikda\Desktop\IDS\D5


Clients Opérationnels
Liste Des Clients Opérationnels
Adresse IP du Client
Adresse IP Client
Ajouter un Client
Supprimer un Client
Valider
Annuler


Liste des Adresses IP Suspectes
Numero
Adresse IP
Effectif
0 192.168.1.37 157
1 192.168.1.12 1
2 207.46.110.42 2
3 192.168.1.16 1
4 10.13.163.100 328
5 10.13.160.53 236
6 10.13.160.138 510
7 64.4.36.42 1
8 207.46.26.253 1
9 76.15.54.225 1
10 10.13.160.233 13
11 80.219.135.76 1
12 89.106.115.2... 1
13 75.80.87.66 1
14 24.238.22.115 1
15 221.189.228.... 1
16 74.216.87.205 1
17 88.222.160.2... 2
18 90.227.7.163 2
19 74.125.39.147 2
0
1
Adresse IP
Ajouter
Supprimer
Valider
Annuler



Numéro	IP_Clients	IP_Source	Source Port	Taille_Paqeut	Protocole	Date	Heure	Type d'attaque
0	127.0.0.1	192.168.1.37	1085	0				
1	92.168.1.37			0				
2			7.0.0.1	0			4	
3		at	.168.1.37	3223088			085	
4	t	6/2008		858665262		.1		
5	/2008			0		1.37	.0.0.1	
6				0			168.1.37	
7			008	0				
8				0	00:00:00at			
9				0				
10				13313			08	
11				842608689		4		
12				0		093		
13		0:00at		774909495	.1			
14	:00at	17/06/2008		943075630	1.37	.0.0.1		
15	7/06/2008			0		168.1.37		
16			0at	0			192.168.1.37	
17			06/2008	0				
18				3682352				
19				0		08	at	
20				0	4		6/2008	
21				67108864	094			



IV-7) Conclusion

Dans ce chapitre, on a présenté le système proposé qui est un système de détection d'intrusions basé sur l'algorithme de sélection négative dans un univers multi agents. Ensuite, on a détaillé les différentes étapes nécessaires à la mise en œuvre. Par la suite nous avons présenté les résultats obtenus après les expérimentations qui ont été réalisées. Ces résultats sont satisfaisants et qui ont prouvé l'efficacité de combinaison des deux approches les systèmes immunitaires artificiels et les systèmes multi agents pour obtenir un taux de détection d'attaques élevé.

Conclusion Générale

V) Conclusion générale

Les systèmes de détection d'intrusion informatique basés sur les systèmes multi_agents (SMA) offrent une approche prometteuse pour renforcer la sécurité des systèmes d'information. Ces systèmes distribués, composés d'agents autonomes, permettent une surveillance efficace des réseaux informatiques, une détection rapide des activités malveillantes et une adaptation aux changements de l'environnement.

L'utilisation des SMA dans les IDS présente plusieurs avantages. Tout d'abord, la répartition des tâches entre les agents permet une surveillance plus efficace du réseau, en se concentrant sur des parties spécifiques ou des ensembles de ressources. De plus, la coopération entre les agents permet une détection plus précise des intrusions, en combinant les informations et les analyses de différentes sources. Les IDS basés sur les SMA sont également plus résilients, car la défaillance d'un agent n'entraîne pas nécessairement l'échec de tout le système.

Cependant, l'adoption des IDS basés sur les SMA n'est pas sans défis. La coordination et la communication entre les agents nécessitent des mécanismes sophistiqués pour garantir la cohérence des informations et la prise de décision distribuée. De plus, la conception et la configuration de tels systèmes peuvent être plus complexes que celles des IDS traditionnels, nécessitant une expertise et des ressources supplémentaires.

Malgré ces défis, les IDS basés sur les SMA ont montré leur potentiel dans la détection d'intrusion informatique. Leur capacité à gérer des environnements complexes et dynamiques, à s'adapter aux changements et à détecter les attaques de manière distribuée les rendent adaptés à une variété de domaines d'application. Par exemple, ils peuvent être utilisés dans les réseaux d'entreprise, les infrastructures critiques, les systèmes de Cloud computing, etc.

Dans l'avenir, il est essentiel de continuer à améliorer les techniques et les mécanismes utilisés dans les IDS basés sur les SMA. Des recherches supplémentaires sont nécessaires pour développer des modèles de coordination et de communication efficaces, ainsi que des méthodes de détection plus avancées. De plus, il est important de prendre en compte les aspects de sécurité et de confidentialité dans la conception de ces systèmes, afin de prévenir les attaques visant les agents ou les mécanismes de communication.

En conclusion, les systèmes de détection d'intrusion informatique basés sur les systèmes multi_agents offrent une approche prometteuse pour renforcer la sécurité des systèmes d'information. Leur capacité à surveiller, détecter et répondre aux activités malveillantes de manière distribuée en fait une option intéressante pour les environnements informatiques complexes. Cependant, des

recherches continues et des développements technologiques sont nécessaires pour exploiter pleinement leur potentiel et faire face aux défis liés à leur mise en œuvre.

VI) Bibliographie

[1] D. R. Grevisse.phd, «Cours de sécurité informatique & crypto,» Congo, 2019.

[2] D. Abderrahim, «Cours Sécurité des systèmes informatique,» Université , SAVOIE-France, 2020.

[3] A. S. A MAHBOUB, «Gestion du risque opérationnel état d'avancement des Banques Algérienne cas de la BADR Laghouat,Recherches économiques managériales,» Université de Biskra, Biskra, 2019.

[4] C. W. C. Q. L Bloch, «Sécurité informatique : , Edition,» 2007.

[5] D. d. l'informatique, «Cours de sécurité des systèmes d'information : analyse des risques,» université Alger Benyoucef Benkhada, Alger, 2019.

[6] B. H. Rahmani Amine, «La détection d'intrusion (Optimisation par classification)».

[7] Wood Mark, ErlingerMichael, «Intrusion detection message exchange requirements.,» 01 01 2002. [En ligne]. Available: https://tools.ietf.org/html/rfc4766. [Accès le 22 05 2023].

[8] H. Djallel, «Un système de détection d'intrusion pour la cybersécurité.,» Université de 08 mai 1945, Guelma, 2020.

[9] M. Vijayarani, «Intrusion Detection System,» 2015.

[10] G. S. Hadef Houda, «Réalisation d'un système de detection d'intrusion basé sur les systèmes immunitaires artificiels par système multi agents,» Departement de l'informatique Université 20 Aout 1955 , Skikda, 2020.

[11] G. Bruneau, «The History and Evolution of Intrusion Detection,» en ligne http://www.sans.org/reading-room/whitepapers/detection/paper/344, 2001.

[12] K. Price, «Intrusion Detection Pages,» Université de Purdue, Purdue, 1998.

[13] K. Boudaoud, «Un système multi-agents pour la détection d'intrusions,» Institut EURECOM, Sophia-Antipolis France.

[14] B. e. K. L.T. Heberlein, «Network Intrusion Detection,» IEEE Network Journal, 1994.

[15] E. A. F. e. U. W. P. Maj.Gregory B. White, «Cooperating Security Managers: A Peer Based Intrusion Detection System,» IEEE Network journal, 1996.

[16] K. Rachid, «Développement d'un système de detection d'intrusion dans les réseaux mobiles,» departement d'informatique, Faculté des sciences exactes, Université Mustapha Stambouli , Mascara, 2022.

[17] P. N. DOKO, «Sécurité des systèmes d'information : Cas de l'EPAC,» ÉCOLE POLYTECHNIQUE ,UNIVERSITÉ D'ABOMEY-CALAVI, 2016.

[18] H. A. R. Dacier M. Wespi A Debar, «Taxonomy for Intrusion-Detection Systems.,» 2000.

[19] S. Darmoul, «Etude de la contribution des systèmes immunitaires artificiels au pilotage de systèmes de production en environnement perturbé,» Université Blaise Pascal - Clermont-, Clermont, 2010.

[20] «Encyclopedia,» [En ligne]. Available: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/history-immunology. [Accès le 17 05 2023].

[21] A. B. Hiba Khelila, «Application du système immunitaire artificiel ordinaire et amélioré pour la reconnaissance des caractères artificiels,» aLaboratoire Signal Image Parole –SIMPA-, Université des Sciences et Technologie d'Oran, BP 1505El M'naouer, Oran ,Algérie, 2010.

[22] M. L. M. N. R. a. C. E. S. J. McCarthy, «A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence,(1956),» *AI Magazine,* vol. 27, n° %14, 2006.

[23] C. P. Laurent Deveaux, «Le rôle des agents intelligents sur l'Internet,» *Revue française de gestion,* vol. 05, n° %1152, 2004.

[24] I. J. e. B. M. B. Chaib-draa, «Systèmes multiagents : Principes généraux et applications,» *Département d'Informatique, Pavillon Pouliot,* p. 41, 2001.

[25] A. BELAZOUI, «Modélisation d'un comportement coopératif d'un agent,» UNIVERSITE MOHAMED KHIDER DE BISKRA, BISKRA, 2016.

[26] C. S.-B. C. HANACHI, «Introduction aux Systèmes Multi-Agents,» Université Toulouse I & IRIT., Toulouse , 2001.

[27] A. GROULS, «AGENTS ET SYSTÈMES MULTI-AGENTS VERS UNE SYNTHÈSE DE CES CONCEPTS,» UNIVERSITÉ DU QUÉBEC À MONTRÉAL, MONTRÉAL, 2013.

[28] Y. T. W. Sha Liu, «Interaction Model of the Cabin of Combined Sugarcane Harvesters,» College of Engineering, China Agricultural University, Beijing 100083, China, Beijing , 2021.

[29] B. Tawfik, «Conception d'une plateforme multi agent pour la collecte de données dans une base de données distribuée,» UNIVERSITE MOHAMED KHIDER , BISKRA, 2015.

[30] C. A. HAYES-ROTH B., *A Satisficing Cycle for Real-Time Reasoning in,* 1993.

[31] [. 7. H. C. V. C. S. a. P. o. M. P. Artificial.

[32] [. 8. A. G. A. A. M. o. C. C. f. D. Systems..

[33] T. M., *The Society of Objects. Proc.,* of the OOPSLA'93 Conference, 1993.

[34] YONEZAWA A., *An Object-Oriented Concurrent System. Computer,* (ed.) ABCL:, 1990.

[35] [. 9. H. C. O. I. S. S. f. D. Artificial.

[36] [. 9. C. P. U. L. d. p. l. a. d. intégrant.

[37] G. S., *Agents et systèmes, une nécessaire unité. Thèse de Doctorat,* 1993.

[38] F. J, «Les systèmes multi-agents: un aperçu général. Technique et Science Informatiques,» vol.16 n°8, pp. 979-1012, 1997.

[39] Y. A., *An Object-Oriented Concurrent System. Computer,* (ed.) ABCL: , 1990.

[40] [. 8. B. J.-P. A. a. T. f. C. a. D. A. L. i. the.

[41] F. J. S. F. M. :. BOURON T., *a Multi-Agent Testbed for.*

[42] D. M. GUESSOUM Z., *A Real-Time Agent Model in an Asynchronous-Object,* 1996.

[43] [. 7. S. R. G., *A Framework for Distrib. Problem Solving. Proc.,* 1979.

[44] C. P. FERBER J., *Actors and Agents as Reflective Concurrent Objects: a Mering.*

[45] D. E. DECKER K., *Generalizing the Partial Global Planning Algorithm.,* 1992.

[46] R. F. I. F. e. S. S. ALAMI R., *A paradigm for plan-merging and its.*

[47] H. S. SEGHROUCHNI A. E. F., *A Recursive Model for Distributed Planning.,* 1996.

[48] [. 9. R. F. C. m.-r. p. i. i. d. p. Doctorat.

[49] S. G. T. G. Wei Wang, «owards fast detecting intrusions: using key attribute of network traffic,» Third International Conference on Internet Monitoring and Protection, Bucharest, Romania, 2008.