République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITE IBNKHALDOUN-TIARET

Faculté des Mathématiques et de l'Informatique
Département Informatique

Mémoire en vue de l'obtention du diplôme de Master

Domaine : Informatique

Filière: Informatique

Spécialité: Génie Informatique

Option: Systèmes d'information et technologies web

Présentée par :

Samia BENYAHIA

Thème

Vers un nouveau Système de détection d'intrusion hybride et hiérarchique basé sur les réseaux bayésiens

Membres de Jury:

Mr. Abdelkader ALEM	Encadreur
Mr. Khaled BAKAR	Président
Mr. Ahmed MOKHTARI	Examinateur

Année universitaire : 2016–2017

Remerciements

*Je remercie **ALLAH** tout puissant de m'avoir donné le courage, la volonté et la patience pour mener à terme le présent mémoire. **« Alhamdou lillah ».***

*Mon premier remerciement va à mon promoteur **Mr** **Abdelkader ALEM**, ce travail aurait été incomplet sans sa disponibilité, sa rigueur scientifique, ses précieux conseils et ses compétences.*

Merci pour ta gentillesse, le temps que vous m'avez consacré, tes orientations. À vrai dire, je ne sais pas comment vous remercier pour tout ce que vous m'avez apporté, transmis et appris tout au long de ce travail. Merci pour l'énorme contribution afin d'accomplir ce mémoire.

*Mon vif remerciement va également à **Mr** **Khaled BAKAR** pour le grand honneur qu'il m'a fait en acceptant de présider ce jury.*

*Mon tenon surtout à remercier **Mr** **Ahmed MOKHTARI** qui a accepté avec enthousiasme et bienveillance d'examiner et discuter ce travail.*

J'adresse mes sincères remerciements à tous les enseignants de la faculté pour leurs aides, leurs encouragements et leurs conseils.

Enfin, je remercie tous ceux qui ont contribué de près ou de loin, directement ou indirectement à la réalisation de ce mémoire.

Dédicaces

Je dédie ce travail à :

Mes très chers parents,

Qui tout au long mon existence m'ont couvert d'amour et d'affection et pour tout leur sacrifices et efforts de faire de moi ce que je suis.

Mon frère et mes sœurs,

Zoheir, Sara et Nassima pour leur aide et leur soutien.

A toute ma famille

Tous mes ami(e)s dont la liste est longue et que je ne peux pas tous les citer et qui occupent une place particulière dans mon cœur.

Tous mes enseignants pour m'avoir donné ce qui est inestimable, le savoir et le savoir faire.

Toutes les personnes qui ont contribué, de prés ou de loin à la réalisation de ce travail.

A ceux qui m'ont connu et aimé

Qu'Allah leur accorde santé et prospérité.

Samia Benyahia

Sommaire

Chapitre III : Les Réseaux Bayésiens et Les Arbres de Décisions

Partie II : Partie Résultats et Discussion

Chapitre IV : Contribution dans la détection d'intrusions réseaux

Chapitre V :Implémentation et réalisation

Liste des Abréviations

ACK : accusé de réception

AD : Arbres de décision

BFTree : Best First Tree

CART : Classification And Regression Trees

CPU : Central processing unit

DARPA : Defense Advanced Research Projects Agency

DDoS : Distributed Denial of Service attack

DI : Détection d'Intrusion

Dos : Denial of Service

DR : Détection Rate

DT : Decision tree

FAR : False Alarm Rate

FN : Faux Négative

FP : Faux Positive

FTP : File Transfer Protocol

GNU : General Public License.

HIDS : Host Intrusion Detection System

ICMP : Internet Control Message Protocol

IDE : Integrated Development Environment

IDS : Intrusion Détection Systems

IP : Internet Protocol

KDD: Knowledge Discovery in Databases

MIT : Massachusetts Institute of Technology

NB : Naive Bayes

NFPH-IDS : New Fast Performed Hiearchical Intrusion Detection System

NIDS : Network Intrusion Detection System

Probe : Probing

R2L : Remote to Local

RB : Réseaux bayésiens

RF : Randon Forest

RT : RandonTree

SC : Simple Cart

SI :	Systèmes d'information
SSI :	La Sécurité des Systèmes d'Information
SYN :	synchronize
TCP :	Transmission Control Protocol
U2R :	User to Root
VN :	Vrai Négative
VP :	Vrai Positive
WEKA :	Waikato Environment for Knowledge Analysis
XSS :	Cross-Site Scripting

Liste des figures

Liste des tableaux

INTRODUCTION

Introduction générale

La sécurité informatique est devenue une obligation pour toute organisation pour faire face aux attaques afin de minimiser le risque. La sécurité informatique est la protection de l'information et des systèmes d'information contre les accès, la perturbation afin de garantir la confidentialité, l'intégrité et la disponibilité.

La sécurité des systèmes doit constituer le moyen de protéger dans un sens large le SI ou de minimiser les risques encourus par l'entreprise dans l'usage de l'outil informatique.

En sécurité informatique, la détection d'intrusion est l'acte de détecter les actions qui essaient de compromettre la confidentialité, l'intégrité ou la disponibilité d'une ressource.

Les systèmes de détection d'intrusions (IDS) sont généralement considérés comme une seconde ligne de défense pour protéger contre les activités malicieuses.

La détection des tentatives d'attaques sur un réseau est une problématique très importante dans le domaine de la sécurité informatique. Les technologies classiques de protection des réseaux de type Firewall filtrant sont en effet inefficaces contre la plupart des attaques actuelles. Aussi sont apparus de nouveaux équipements réseaux pour prendre en compte ces carences, les NIDS, systèmes de détection d'intrusions réseaux, dont le but est de détecter les tentatives d'attaque qu'un firewall ne peut pas bloquer. Malheureusement, en pratique, les NIDS génèrent tellement d'alertes sur un réseau important qu'il en devient très difficile de déterminer celles générés par une attaque réelle. On distingue deux grands types d'approches pour détecter des intrusions. La première consiste à rechercher des signatures connues d'attaques tandis que la seconde consiste à définir un comportement normal du système et à rechercher ce qui ne rentre pas dans ce comportement.

Dans ce contexte, Notre travail consiste à proposer un système de détection d'intrusion efficace et performant en minimisant le nombre de fausses alertes et maximisant le taux de détection. L'idée principale est de faire coopérer et hybrider plusieurs classificateurs en intégrant les décisions d'un classificateur dans un autre classificateur bayésien naif.

Ce manuscrit est organisé en 5 chapitres

- Dans le premier chapitre on va présenté les notions de base de la sécurité informatique dans laquelle on va abordé les différents risque informatique et leurs solution.
- Le Deuxièmes chapitre aborde les Systèmes de détection d'intrusion (IDS).
- Puis Les Réseaux Bayésiens et Les Arbres de Décisions dans laquelle sont décrites avec les

différents classificateurs utilisés.

- Notre Contribution est présentée dans le chapitre 4 dans laquelle on va discuter les résultats obtenus.
- Un cinquième chapitre pour l'implémentation et réalisation. dans laquelle on va présenter un prototype illustratif de notre système.

En fin Nous allons terminer ce rapport par une conclusion et les perspectives à prospecter.

PARTIE
État de l'art

La sécurité informatique

Système de détection d'intrusion

Les Réseaux Bayésiens et Les Arbres de Décisions

CHAPITRE I

La sécurité informatique

Introduction

L'univers des systèmes d'information (SI) composé de réseaux et de système informatiques prend un rôle et une place chaque jour plus important dans les entreprises.

Cependant l'actualité présentée par les médias nous démontre que le SI est vulnérable et qu'il peut subir des piratages, des attaques (virus, hackers…), des pertes de données, il est donc indispensable pour les entreprises de savoir définir et garantir la sécurité de ses ressources informatiques.

La sécurité des systèmes doit constituer le moyen de protéger dans un sens large le SI ou de minimiser les risques encourus par l'entreprise dans l'usage de l'outil informatique [1].

Nous nous occupons, dans ce chapitre, de spécifier les failles de sécurité que peut rencontrer un utilisateur d'une part. D'autre part, nous nous intéressons à la présentation des principes de la sécurité informatique ainsi que quelque solution de sécurité qui garantit la viabilité d'un système.

1. Les risques informatiques

La prolifération du nombre d'ordinateurs et de ses applications, compte tenu du volume, de la qualité et de l'importance des informations conservées dans les systèmes informatisés, à engendré une multitude de menaces intentionnelles qui pouvant porter atteinte au caractère confidentiel, à l'authenticité et à l'accessibilité des données emmagasinées dans ces systèmes informatisés [7].

Un risque se définit comme une combinaison de menaces exploitant une vulnérabilité et pouvant avoir un impact. De manière générale, les risques sont soit des causes (attaques, pannes, ...) soit des conséquences (fraude, intrusion, divulgation ...).

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérablité}}{\text{Contre} - \text{mesures}}$$

La menace représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité appelée parfois faille représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace [9].

2. Les types des risques informatiques

Il existe différents types des risques les principaux sont :

2.1 Les risques physiques

Il s'agit de toutes les atteintes physiques directes dont peut être victime un SI au cours de son cycle de vie. Il s'agit d'événements tels que [8] :

- Incendies, explosion, effondrement.
- Dommages électriques, défaillance matérielle.
- Tempêtes, inondations, événements naturels.
- Bris de machines, vol, actes de vandalisme.

2.2 Les risques logiques

Parmi les risques logiques en peut citer [10] :

- La maladresse : comme en toute activité, les humains commettent des l'erreurs d'usage.
- sabotage qui vise la mise hors service d'un SI ou de l'un de ses composants.
- les virus et programmes malveillants.
- Le L'écoute ou espionnage de données pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects.
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.
- destruction de données.
- usage d'un système compromis pour attaquer d'autres cibles.
- L'inconscience et l'ignorance des risques qu'ils entourent les systèmes, ou une planification inefficace contre les menaces.
- L'email frauduleux qui consiste à accéder à l'information par copie illégale
- Le détournement de mot de passe et Le chantage de diffusion non autorisée de données confidentielles.
- L'interception qui snifée un accès avec modification des informations transmises sur les voies de communication avec l'intention de détruire, modifier, d'insérer des nouveaux messages.
- L'accès illégitime lorsqu'une personne se fait passer occasionnellement pour une autre en usurpant son identité.

3. La sécurité informatique

3.1 Définition

La sécurité des systèmes d'information (SSI) est une discipline de première importance car le SI est pour toute entreprise un élément absolument vital [6].

La sécurité est un ensemble de stratégies, conçu et mises en place pour détecter, prévenir et réduire la vulnérabilité d'un système et lutter contre les menaces accidentelles ou intentionnelles. [3] Selon la norme ISO/IEC 27001 : 2005, la sécurité de l'information se caractérise par [2] :

- **L'intégrité** : consistant à assure que la donnée reçue est la même que celle qui a été émise, [2] c'est-à-dire garantir que les données sont bien celles que l'on croit être et ne doit pouvoir être modifiée que par les personnes autorisées.
- **La confidentialité** : « la confidentialité est le maintien du secret des informations » (Le Petit Robert), consistant à assurer que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de la traiter [2] : c'est-à-dire L'information ne doit être diffusée qu'aux personnes autorisées.
- **La disponibilité** : consistant à assure que la donnée est présente et accessible à tout moment aux personnes autorisées [2].
- **l'authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources.
- **La non-répudiation** : permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire. Aussi qui permet de garantir qu'une transaction ne peut être niée ou rejetée par aucun des correspondants [2], à cette notion sont associées [13] :

- **L'imputabilité**: une action a eu lieu et automatiquement un enregistrement preuve de l'action est effectué.
- **La traçabilité**: mémorisation de l'origine du message.
- **L'auditabilité:** capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.

➢ chaque menace a des buts précis et vise à compromettre des services de sécurité précis, en peut citer les quatre éléments suivants :

- **Interruption d'un service** : Rendre un service ou un élément non disponible inutilisable. Par exemple : effacer un programme ,détruire ou neutraliser une composante du système.
- **Interception des données** : Rendre un accès non-autorisé à un service, à une ressource. Elle vise la confidentialité des informations. Par exemple : copie illicite, écoute, interception de données.

- **Modification des données** : vise l'intégrité des informations et le Changement de données. Par exemple : Trucage des ressources ou de logiciel.
- **Fabrication des données** : vise l'authenticité des informations. Par exemple la Création de faux usurpation d'adresse ou d'identité.

4. La politique de la sécurité informatique

Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut présenter une politique à l'égard de la sécurité.

Une politique de sécurité peut être vue comme l'ensemble des règles, des procédures et des bonnes pratiques techniques qui fixent les actions autorisées et interdites afin d'assurer la sécurité du système d'information.

En d'autres mots, c'est l'ensemble des moyens qui assurent que les ressources du SI (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. [8] et elle définit les rôles et les responsabilités de la sécurité des informations au sein de l'organisation, et exige des rapports, réponses, résolutions pour n'importe quel type d'incident de sécurité au sein de l'organisation [16].

❖ Une politique de sécurité est généralement organisée autour de 3 axes majeurs [12] :

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

❖ Une politique de sécurité tourne autour des 5 principaux concepts suivants :

- l'intégrité des données.
- la confidentialité de l'information et des échanges.
- la disponibilité des services.
- l'authentification des utilisateurs.
- la non-répudiation des transactions.

– Une seule entrave à l'un de ces principes remet toute la sécurité en cause.

4.1 Les objectifs de la sécurité informatique

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, les points principaux sont les suivant : [11]

- Empêcher la divulgation et la modification non autorisée des données.
- Définir le cadre d'utilisation des ressources du SI.
- Sensibiliser les utilisateurs à la sécurité informatique.
- La confidentialité des accès contre l'usurpation d'identité et le vol d'informations critiques.
- La disponibilité des ressources contre les arrêts de production.
- Protéger l'intégrité des données, des biens et des ressources de l'organisation.
- Prévenir les erreurs et les fraudes et anticiper les incidents et minimiser leurs impacts.
- protéger l'accès à internet et le réseau informatique.
- filtrer les courriers électroniques.

5. Les attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Vulnérabilité : Une vulnérabilité peut aussi être appelée «faille», un "défaut" elle représente une faiblesse dans un système qui pourrait être exploitée pour causer une perte, ou un dommage dans un SI.

Une attaque informatique : est une action d'exploitation d'une faille à fine de se compromet la sécurité des informations, comme elle représente toute tentative de détruire, exposer, modifier, désactiver, voler, ou d'évitement des contrôles de sécurité sur un serveur. Le succès de l'attaque dépend de la vulnérabilité du serveur attaqué, mais si elle réussit, l'attaquant aura un accès illimité au serveur et pourra faire tout ce qu'il veut (vol, destruction de données...) (ISO/IEC 27000, 2009).

Une attaque sur les réseaux consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible : comme Adressage IP, Noms de domaine, Protocoles de réseau, Services activés, Architecture des serveurs... Etc. [5].

Une intrusion : est une forme particulière d'attaque informatique à des fins autres que celles prévues, généralement dues à l'acquisition de privilèges de façon illégitime [33].

Une intrusion dans un système informatique est aussi définie par Heady et all comme « N'importe Quelle ensemble d'actions essayant de compromettre l'intégrité, la confidentialité ou l'accessibilité d'une ressource » [34]. Les intrusions sont souvent effectuées dans les contextes d'espionnage industriel ou politique.

5.1 Les classes d'attaques

De même que les risques, on peut classifier les attaques en deux classes principales : les attaques passives et les attaques actives.

L'attaque passive : les attaques passives représentent tout acte de capture d'informations d'authentification (mots de passe), surveillance des communications ou bien une écoute d'information sur le réseau sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible ce type d'attaque portent atteinte à la confidentialité des données. Et se réalise par écoute, Injection de code, usurpation d'identité, intrusion, abus de droits.

L'attaque active : les attaques actives comprennent toute tentative a pour but de contourner, arrêter ou à perturber le bon fonctionnement de protection, et parfois voler ou bien une modification illégale d'un état, d'identité des informations ou des messages, les attaques actives peuvent être exécutées sans la capacité d'écoute, ce type d'attaque portent atteinte à la confidentialité, l'intégrité, et la disponibilité des données. Et se réalise par injection de code, action physique, intrusion, abus de droits.

❖ **Les motivations des attaques peuvent être de différentes sortes : [5]**

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Glaner des informations personnelles sur un utilisateur comme des données bancaires.
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- Troubler le bon fonctionnement d'un service.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

5.2 Les types d'attaques

Il existe plusieurs attaques informatiques connues à ce jour, nous détaillons ici trois types d'attaques informatiques :

5.2.1 Les attaques réseaux

a) **L'attaque par sniffing :** cette attaque consiste à écouter une ligne de transmission par laquelle transitent des données [17], il est possible d'intercepter les trames reçues par la carte réseau

d'un système pirate et qui ne lui sont pas destinées. Le système pirate se situe donc sur le réseau local et capture tous les paquets réseau transitant sur ce réseau [23].

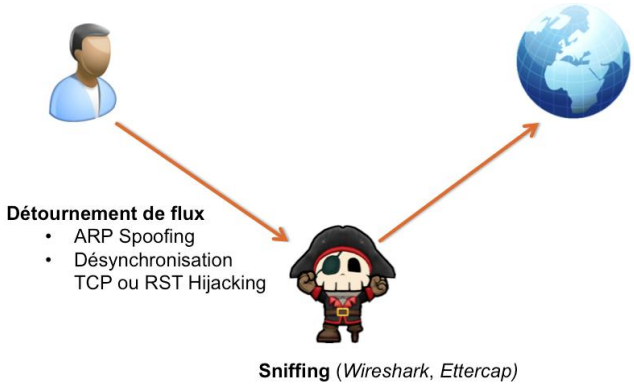

Figure 01: Attaque Sniffing.

b) L'attaque man in the middle : « L'attaque de l'homme du milieu » est une attaque qui a pour but d'observer et d'intercepter les communications entre deux victimes, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis [17].

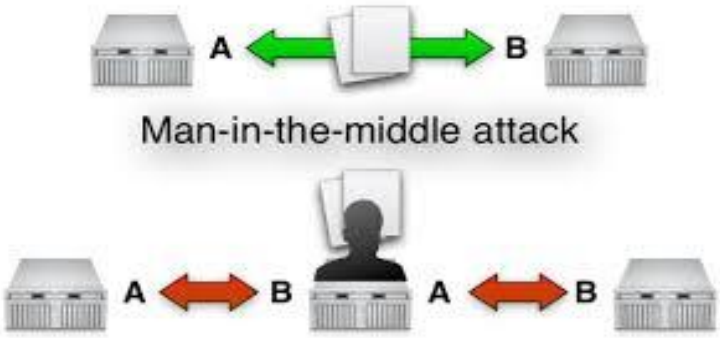

Figure 02: Attaque Man in the middle.

c) L'attaque par rebond : cette attaque est menée via un autre ordinateur qui se trouve involontairement complice et qui expédie le message d'attaque à la victime, masquant ainsi l'identité d'attaque par rebond du véritable agresseur [17].

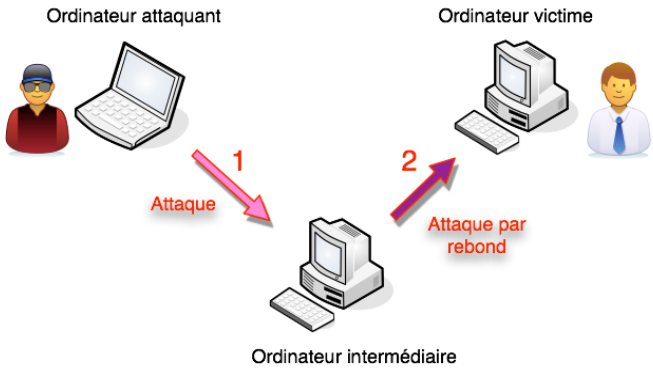

Figure 03: Attaque par rebond.

d) **Balayage de port** : le balayage de port est une technique servant à rechercher les ports ouverts sur un serveur de réseau pour tenter de trouver des failles dans des systèmes informatiques [18].

e) **L'attaque par Spoofing IP :** c'est une technique d'intrusion dans les systèmes informatiques [17], consistants à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. [19] sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu). Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès [18].

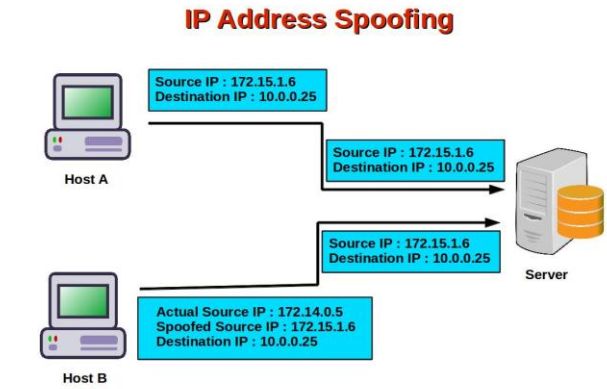

Figure 04: Attaque par Spoofing IP.

f) **Les attaques par injection :** permettent à un attaquant d'injecter du code dans un programme ou une requête, ou d'injecter des logiciels malveillants dans un ordinateur en vue d'y exécuter des commandes à distance capables de lire ou modifier une base de données ou de modifier les données sur un site Web [24].

g) **Les attaques par Cross-site Scripting** : abrégé XSS, est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page [18].

h) **L'attaque par déni de service :** en anglais « Denial of Service », abrégé en Dos c'est une attaque qui vise à crasher un programme [22], et le rendre indisponible pendant un temps indéterminé [3] en faisant déborder un tampon de taille fixe avec un trop grand nombre de données entrantes.

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « déni de service distribué » (noté DDOS pour Distributed Denial of Service).

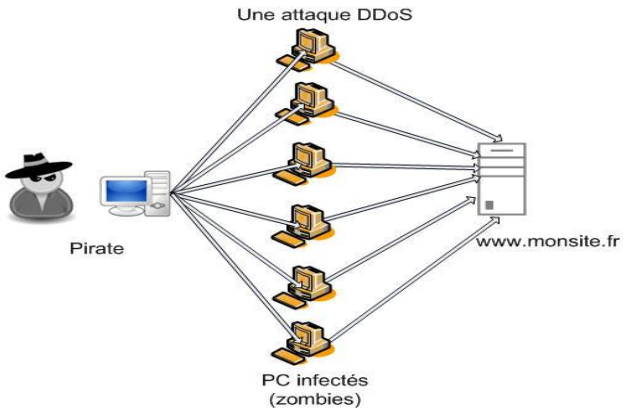

Figure 05: Attaque DDOS.

i) L'attaque du ping de la mort : en anglais « ping of death » est une des plus anciennes attaque réseau. Le principe du ping de la mort consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximale autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable [21] provoquera un crash de la machine cible.

j) L'attaque par réflexion (Smurf) : ce type est basé sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau [19].

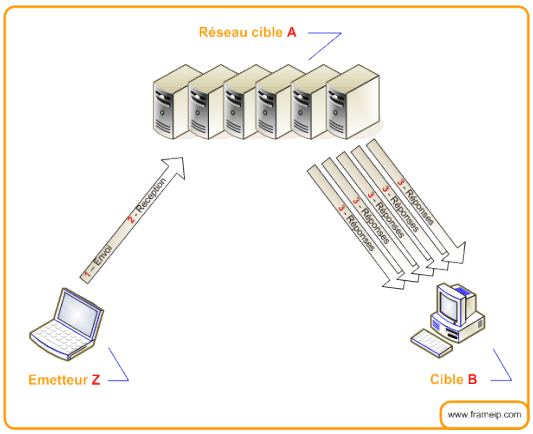

Figure 06: Attaque Smurf.

k) L'attaque SYN : est une attaque réseau par saturation [19]. Elle se fait lorsqu'un client essaie d'établir une connexion TCP sur un serveur, le client et le serveur échangent une séquence de messages, la faille vient du fait qu'au moment où le serveur a renvoyé un accusé de réception du SYN (SYN- ACK), le serveur n'a pas encore reçu d'ACK du client. On peut citer :

- SYN- Flood qui consiste à envoyer très rapidement de gros paquets d'informations à la machine routeur, ce qui risque de faire planter la machine [25].
- SYN- spamming qui consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres pour la faire saturer [25].

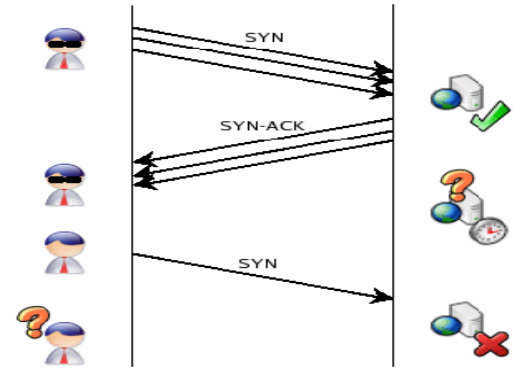

Figure 07: Attaque SYN.

l) Les attaques sur des mots de passe :

a. L'attaque par dictionnaire : est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consist à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Sinon l'attaque échouera [18].

b. L'attaque par force brute: est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé [18]. Il s'agit le cassage d'un mot de passe en testant tous les combinaisons possibles.

c. L'attaque hydride: ce type appelées « attaques hybrides », vise particulièrement les mots de passe constitués d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que « maréchal6 ») il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire [18].

5.2.2 Les attaques d'applications

a) Le dépassement de tampon (Buffer Overflow) : un dépassement de tampon se produisant lorsque le tampon (buffer) ne peut pas traiter correctement toutes les données qu'il reçoit. Lorsque le bug se produit non intentionnellement, le comportement de l'ordinateur devient imprévisible. Il en résulte souvent un blocage du programme.

b) Shellcode *:* un shellcode est une chaîne de caractères qui représente un code binaire exécutable. À l'origine destiné à lancer un « shell » (interface utilisateur d'un OS), le mot a évolué pour désigner tout code malveillant qui détourne un programme de son exécution normale. Un shellcode peut être utilisé par un hacker voulant avoir accès à la ligne de commande [18].

c) L'écran bleu de la mort : se réfère à l'écran affiché par le système d'exploitation Windows lorsqu'il ne peut plus récupérer une erreur système ou lorsqu'il est à un point critique d'erreur fatale et que l'ordinateur est devenu complètement inutilisable [18].

d) Fork Bomb : fork bomb fonctionne en créant un grand nombre de processus très rapidement

afin de saturer l'espace disponible dans la liste des processus gardée par le système d'exploitation. Si la table des processus se met à saturer, aucun nouveau programme ne peut démarrer tant qu'aucun autre ne termine [18].

5.2.3 Les attaques virales

a) **Les virus** : sont des programmes, généralement écrits en langage machine, susceptibles de s'introduire dans un ordinateur et de s'y exécuter. L'exécution peut produire de nombreux effets, allant du blocage d'une fonction à la destruction des ressources de l'ordinateur, comme l'effacement de la mémoire ou du disque dur [28] comme ils sont capable de se reproduire et de se propager.

b) **Les Vers :** ce type de Malware utilise les ressources du réseau pour se propager [20].Cette classe a été appelée vers en raison de sa particularité de «glissement» d'un ordinateur à l'autre.

c) **Les Chevaux de Troie :** sont des programmes malveillants d'apparence anodine [17].
Exécutants des tâches malignes, en une fois installé dans un ordinateur peut voler des mots de passe, supprimer des données sur les disques, provoquer un échec du système ,copier des données, ou exécuter tout autre action nuisible. Le plus connu est le backdoor.

d) **Trappes (portes dérobées)**: Permet à un utilisateur externe de prendre le contrôle d'une application par des moyens détournés [26].

6. Les solutions de la sécurité

La sécurité informatique est tout processus qui vise a garder un très bon niveau de sécurité, par des contrôles réguliers, des règles respectées (politiques de sécurité) et des solutions intelligemment déployées (Firewalls applicatifs, proxy, antivirus…etc.).
Le tout fait que la sécurité converge vers des niveaux satisfaisants mais jamais parfaits.

Il existe de nombreuses méthodes de protection des risques, certaines simples d'utilisation, avec parfois des outils logiciels en simplifiant l'utilisation. D'autres méthodes sont réservées à des grands comptes du fait de leur complexité et des ressources humaines impliquées. La sécurité informatique passe notamment par un ensemble de techniques bien identifiées :

1. **le cryptage des fichiers contenant des données sensibles :** désigne l'ensemble des techniques permettant de chiffrer des messages, les rendant ainsi inintelligibles sauf par le destinataire capable de le déchiffrer par une action spécifique. Il existe des algorithmes de cryptographie asymétrique à clé publique et à clé privée. La cryptographie permet d'assurer la confidentialité des données échangées.

2. **Les systèmes de contrôle d'accès :** permettent l'authentification des utilisateurs. Ils peuvent se faire par un mot de passe, une carte à puce, une clé, ou encore un élément biométrique.

3. **Serveur proxy :** l'utilisation d'un serveur proxy dont le but est d'isoler une ou plusieurs machines pour les protéger. De plus le proxy possède un avantage supplémentaire en termes de performance [4].

4. **Les antivirus :** Les logiciels antivirus ont pour fonction de détecter la présence de virus sur une machine et de les détruire. Certains virus sont résistants, et les logiciels antivirus peuvent avoir du mal à les détecter.

5. **Les pare-feu :** un pare-feu (Firewall) est un système physique ou logique qui inspecte les paquets entrants et sortants du réseau afin d'autoriser ou d'interdire leur passage en se basant sur un ensemble de règles appelées ACL [32]. Il existe principalement trois types de pare-feux :

- Pare-feu avec filtrage des paquets : ce pare feu filtre les paquets en utilisant des règles statiques qui testent les champs des protocoles jusqu'au niveau transport.

- Pare-feu à filtrage des paquets avec mémoire d'états : ce modèle conserve les informations des services utilisés et des connexions ouvertes dans une table d'états. Il détecte alors les situations anormales suite à des violations des standards de protocole.

- Pare-feu proxy : ce pare feu joue le rôle d'une passerelle applicative. En analysant les données jusqu'au niveau applicatif, il est capable de valider les requêtes et les réponses lors de l'exécution des services réseaux.

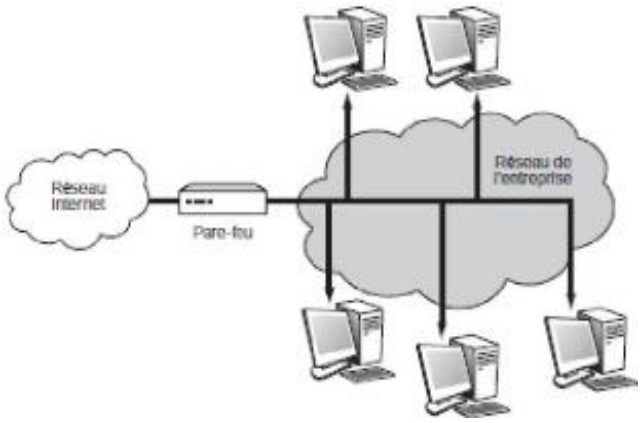

Figure 08: Placement d'un pare-feu dans un réseau.

6. **Les systèmes de détections d'intrusions (IDS) :** est simplifié par un détecteur qui analyse les informations en provenance du système surveillé [35]. Donc le rôle d'alarme .Il s'appuie sur plusieurs sources d'informations comme les fichiers d'audit, les journaux de sécurité et le trafic réseau. Les IDS constituent une bonne solution pour détecter les activités anormales qui passent inaperçues. Placés après les pare feux, les IDS constituent la dernière barrière de sécurité. Ils analysent le trafic qui passe à travers les pare feux et supervisent les activités des utilisateurs sur

le réseau local. Par ailleurs, placés avant les pare feux, les IDS découvrent les attaques à l'entrée du réseau [32].

Les IDS s'appuient généralement sur deux sources d'information : les paquets transitant sur le réseau et les informations collectées sur les machines. On parle alors de deux principes de détection l'approche comportementale et l'approche par scénario [32].

les buts des IDS sont nombreux on peut citer : [36].

- Collecter des informations sur les intrusions.
- Gestion centralisée des alertes.
- Effectuer un premier diagnostic sur la nature de l'attaque permettant une réponse rapide et efficace.
- Réagir activement à l'attaque pour la ralentir ou la stopper.

Conclusion

Dans ce chapitre nous avons vu comment un attaquant peut compromettre un système informatique en suivant une stratégie bien définie. Pour remédier à ces problèmes, des solutions de sécurité efficaces sont mises en œuvre par les administrateurs. Dans une optique d'optimisation de cette sécurisation, les systèmes de détection d'intrusions présentent un bon moyen de garantir cette sécurité des réseaux. C'est pourquoi nous entamerons dans le chapitre suivant l'étude des différents systèmes de détection d'intrusions et leur fonctionnement, ainsi que nous discutons aussi ses deux approches comportementales et par scénario.

CHAPITRE II

Système de détection d'intrusion

Introduction

L'informatique évolue, les systèmes et les réseaux informatiques deviennent de plus en plus complexes et les risques des failles augmentent donc la sécurité devienne de plus en plus difficile, car les délais laissés aux administrateurs sont souvent très courts.

Les attaques distribuées seront toujours redoutables si la plupart des machines ne sont pas protégées. Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblant suspectes. Plus communément appelé IDS, les IDS conviennent parfaitement pour réaliser cette tâche.

À travers ce chapitre, nous commençons par une présentation des principes des IDS, par la suite, nous présentons une classification des IDS selon deux approches, comportementale et par scénario.

1. Définition

Une intrusion est toute activité qui menace la politique de sécurité de l'entreprise et mène à sa violation.

La détection d'intrusion a pour but de mettre en évidence toute violation ou contournement d'un système automatique en envoyant une alerte au moment où l'intrus débute son attaque [27].

Un système de détection d'intrusions est un ensemble de composants logiciels et/ou matériels dont la fonction principale est la surveillance des événements au niveau des systèmes, des applications et des réseaux et de collecter l'information sur le comportement des utilisateurs du système et de détecter tout comportement anormales.

Les objectifs d'un IDS : [28] [32]

- Collecter des informations sur les intrusions.
- Gestion centralisée des alertes.
- Effectuer un premier diagnostic sur la nature de l'attaque permettant une réponse rapide et efficace.
- Fonctionner en permanence avec une supervision manuelle minimale.
- Utiliser un minimum de ressources du système sous surveillance.
- Etre facilement configurable pour implémenter une politique de sécurité spécifique d'un réseau.
- S'adapter au cours du temps aux changements du système surveillé et du comportement des

utilisateurs.

- Etre difficile à tromper.

2. Architecture d'un système de détection d'intrusions

Il existe plusieurs outils de détection d'intrusions , chaque outil utilise sa propre technique de détection et ses propres sources de données ce qui rend la comparaison entre ces outils très difficile [16] .Il est très intéressant de se disposer d'un modèle général qui englobe et standardise la structure d'un IDS, et qui combine : l'analyses de signatures, l'anomalies de protocoles et l'analyse de trafic. La figure 9 montre les composants d'un IDS.

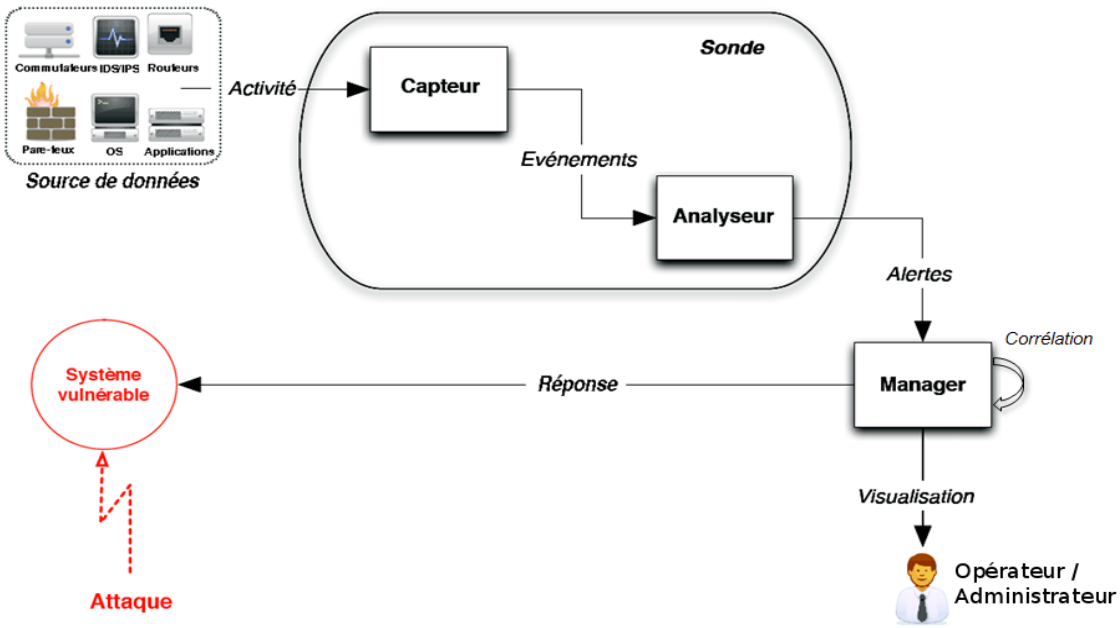

Figure 09: Architecture d'un système de détection d'intrusions.

- Les composants d'un IDS définis comme suit : [16] [27]

Source de données : c'est les informations brutes utilisées par le IDS pour détecter les activités non autorisées ou non désirées.

Capteur : un logiciel générant des événements en filtrant et en formatant les données brutes provenant d'une source de données.

Analyseur : c'est un outil matériel ou logiciel qui met en œuvre l'approche choisie pour la détection (comportementale ou par scénarios), il génère des alertes lorsqu'il détecte une intrusion.

Manager : composant d'un IDS permettant à l'opérateur de configurer les différents éléments d'une sonde et de gérer les alertes reçues et éventuellement la réaction de l'opérateur.

Événement : un message formaté et envoyé par un capteur. C'est l'unité élémentaire utilisée pour représenter un élément d'un scénario d'attaque.

Sonde : est un composant de l'architecture IDS qui collecte les informations brutes représente un ou plusieurs capteurs couplés avec un analyseur.

Alerte : est un message formaté et émis par un analyseur lorsqu'il y a des activités intrusives contre une source de données. peuvent être classées selon deux types :

- ***Faux positif :*** une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle.
- ***Faux négatif*** : une intrusion réelle qui n'a pas été détectée par l'IDS.

Activité : C'est les éléments de la source ou les occurrences au sein de la source de données qui sont identifiés par le capteur ou l'analyseur comme étant à intérêt pour l'opérateur.

3. Les familles de Système de détection d'intrusion

Depuis les années 80, divers outils des IDS ont été développés. On cite dans ce qui suit les plus importants les IDS basés sur l'hôte et les IDS basés sur le réseau et les IDS hybrides :

3.1 Les Network Intrusion Détection System (NIDS)

Les NIDS ou détections d'intrusions réseaux qui assurent la sécurité au niveau du réseau. [29] Les NIDS étant les IDS les plus intéressants et les plus utiles du fait de l'omniprésence des réseaux dans notre vie quotidienne, s'occupent d'analyser de manière passive les flux en transit sur le réseau et détecter les intrusions en temps réel. [31] surveiller le trafic réseau confrontant les paquets détectés à un ensemble de signatures ou de règle [30]. Si une signature s'applique ou si des paquets semblent dangereux.[31], il génère des alertes et enregistre l'événement comme les attaques. e.g le logiciel : Snort , patriot , Hank, Prelude, Firestorm, Bro [44] [45] [46] [47] [48] [49].

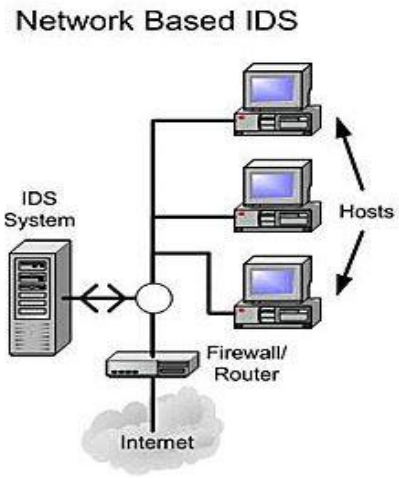

Figure 10: Détections d'intrusions réseaux NIDS.

3.2 Les Host Intrusion Detection System (HIDS)

Les HIDS sont des systèmes orientés poste qui assurent la sécurité au niveau des hôtes. [29]. Un HIDS se base sur une unique machine, n'analysant cette fois plus le trafic réseau, mais l'activité se passant sur cette machine. Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.[31] ont pour rôle de déterminer si un ordinateur donné est en train d'être attaqué ou si celui-ci a déjà été attaqué, résultant en une compromission de la sécurité et de l'intégrité du système. La surveillance après attaque se fait généralement par analyse des fichiers présents sur la machine [30] e.g. le logiciel Tripware , swatch, Dragon Squire, Tiger, Emerald. [39] [40] [41] [42] [43].

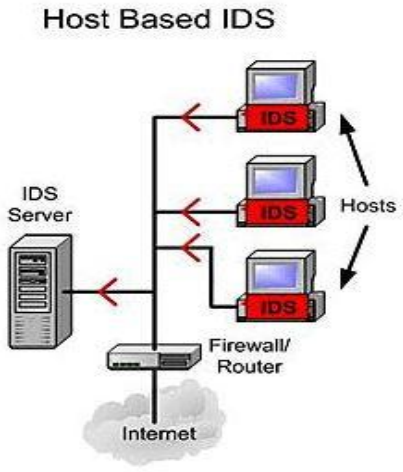

Figure 11: Détections d'intrusions hôtes HIDS.

3.3 Les IDS Hydrides (NIDS+HIDS)

Les IDS hybrides (NIDS+HIDS) est généralement utilisés dans un environnement décentralisé [31], est une sorte de tout en un, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS [31]. Ce nom peut aussi s'appliquer à une solution mêlant plusieurs IDS, ou des IDS particuliers [29].

4. Classification des systèmes de détection d'intrusions

Nous pouvons classifier les systèmes de détections d'intrusions selon quatre critères (cités ci-dessous) qui ne sont pas forcément mutuellement exclusif [26].

a) Méthode de détection et d'analyse utilisée.

b) Mode de Réponse aux attaques.

c) Emplacement de la source la d'audit.

d) Fréquence d'utilisation.

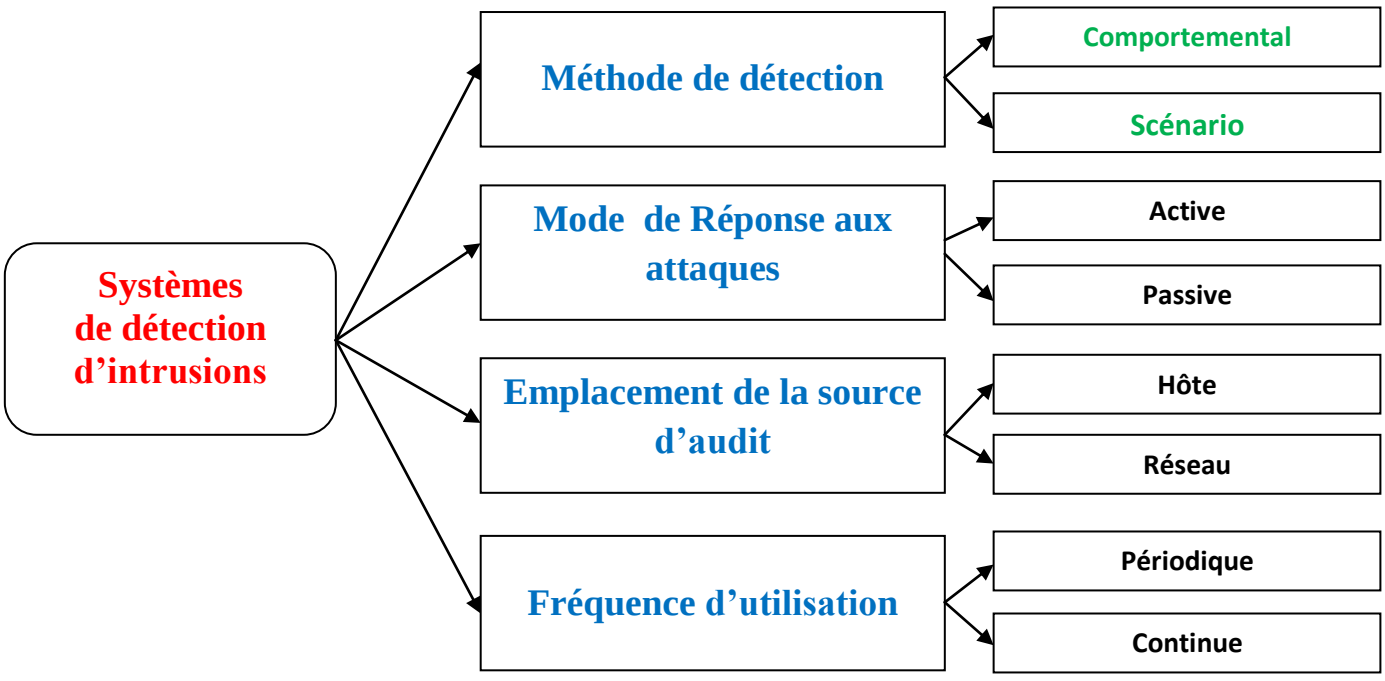

Figure 12: Taxonomie des systèmes de détection d'intrusions.

4.1 Méthode d'analyse

Les principes fondateurs des IDS ont été proposés aux Etats-Unis au début des années 1980 (Anderson 80) (Denning87), deux technique de détections d'intrusions qui se répartissant en deux grands classes : détection d'anomalies, aussi appelée approche comportementale, et détection d'attaques, dite également approche par scénario.

4.1.1 L'approche par scénario

Cette approche consiste à chercher dans les activités de l'entité surveillée les empreintes ou les signatures d'attaques connues. Chacune de ces signatures décrit une attaque bien précise et chaque attaque peut être détectée par un seul ou une séquence d'événements obtenus à partir d'une ou plusieurs sondes (collecteur d'informations). Ces derniers permettent de classifier tous les événements d'attaques qui peuvent provenir [33]. Autrement dite il s'agit de recueillir des scénarios d'attaques pour alimenter une base d'attaques. Le principe commun à toutes les techniques de cette classe consiste à utiliser une base de données, contenant des spécifications des scénarios d'attaques [31]. Le détecteur d'intrusions compare le comportement observé du système à cette base et remonte une alerte si ce comportement correspond à une signature prédéfinie.

L'avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit. Et l'inconvénient majeur de cette approche est qu'elle ne peut détecter que les attaques dont ils possèdent les signatures. Ils nécessitent également des mises à jour régulières de leur base de signatures et leur efficacité dépend du contenu de cette base. Si les signatures sont erronées ou incorrectement conçues, l'ensemble du système est par conséquent inefficace.

La figure 13 représente un modèle d'un IDS adapté pour l'approche par scénarios.

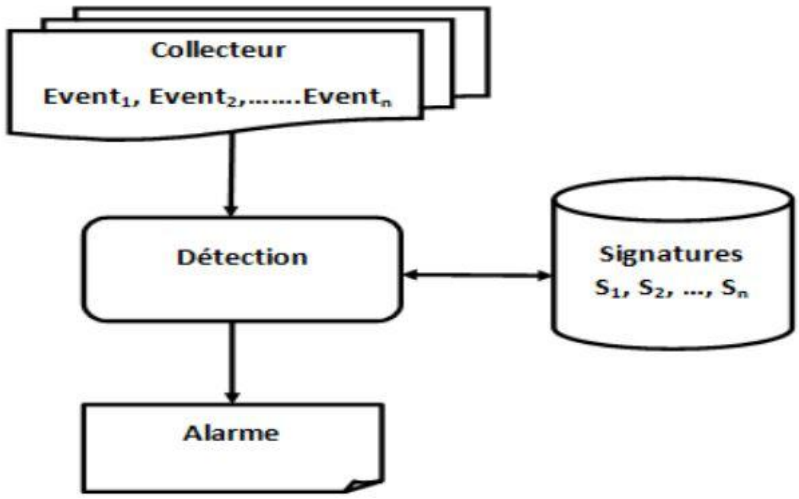

Figure 13: Modèle d'un IDS pour l'approche par scénario.

Plusieurs mécanismes ont été proposés afin de localiser les signatures d'attaques dans les traces d'audit. Parmi ces mécanismes, on peut citer : [33]

Analyse des transitions d'états : Les signatures d'attaques sont vues comme des systèmes de transitions étiquetées. En partant d'un état initial et en analysant les séquences d'actions effectuées sur le système, nous pouvons détecter des états indésirables qui reflètent des tentatives d'intrusions.

Réseaux de neurones : Les réseaux de neurones sont souvent utilisés pour répartir en différentes classes une population (un ensemble d'individus). Pour la détection d'intrusions, la population est l'ensemble d'actions effectuées sur le système et on cherche à les répartir en au moins deux classes : les actions malicieuses ou douteuses et les actions non malicieuses. Grâce à leur flexibilité et leur rapidité, les réseaux de neurones permettent de faire une analyse efficace du flux d'audit en temps réel. Il est cependant difficile de comprendre dans tous les cas les raisons qui ont amené à placer une action dans une classe ou dans une autre [33].

Reconnaissance de forme (Pattern Matching) : Il s'agit de représenter les signatures d'attaques par des séquences abstraites d'événements, de modéliser le trafic par une séquence concrète d'actions et de voir s'il est possible de les unifier [33].

4.1.2 L'approche comportementale

Cette approche (appelée aussi détection d'anomalies), à été proposée par J. Anderson dans [38] en 1980, puis révisée et étendue par D. Denning en 1987 [37]. Elle consiste à détecter si un utilisateur a fait un comportement anormal par rapport à ses habitudes. Elle utilise pour cela un modèle statistique développé par Denning dans [37] et elle se base sur un profil du comportement normal de l'utilisateur, au vu de plusieurs variables aléatoires. Lors de l'analyse, on calcule un taux de déviation entre le comportement courant et le comportement passé.

Le comportement normal des sujets est appris en observant le système pendant une période donnée appelée phase d'apprentissage (par exemple, un mois). Est enregistré dans la base de données et comparé avec le comportement présent des sujets appelé comportement à court terme.

Une alerte est générée si une déviation entre ces comportements est observée, en général, mis à jour périodiquement pour prendre en compte les évolutions possibles des comportements des sujets [31].

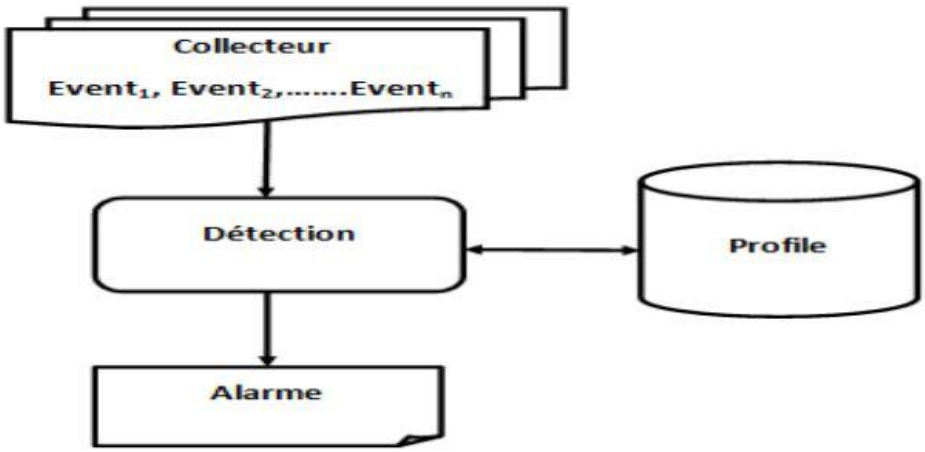

Figure 14: Modèle d'un IDS pour l'approche comportementale.

Il existe différentes techniques pour repérer les attaques : [23]

- ***Approche probabiliste*** : On prévoit quelle est la probabilité d'avoir un évènement après un autre.

Avantages de l'approche probabiliste : Construction du profil simple et dynamique et réduction de faux positifs.

Inconvénients de l'approche probabiliste: Risque de déformation progressive du profil par des attaques répétées.

- ***Approche statistique*** : Effectue des tests sur d'autres éléments concernant l'utilisateur :

- ❖ Le taux d'occupation de la mémoire.
- ❖ L'utilisation des processeurs.
- ❖ La valeur de la charge réseau.
- ❖ Le nombre d'accès à l'Intranet par jour.

Avantages de l'approche statistique : Permet de détecter des attaques inconnues et habitudes des utilisateurs apprises automatiquement.
Inconvénients de l'approche statistique : La complexité en termes de maintenance et beaucoup de faux positifs.

L'approche comportementale possède les avantages suivants : [18]

- la détection d'anomalie permet de détecter un comportement non usuel et ainsi offre la possibilité de trouver des symptômes d'une attaque sans en connaître les détails.
- peut permettre de produire de l'information qui peut être utilisée pour définir des nouvelles signatures utilisables pour les systèmes à signatures.

Cependant, l'approche comportementale possède l'inconvénient suivant :

- produit une quantité énorme de fausses alertes à cause du caractère imprévisible des utilisateurs et des réseaux.

4.2 Mode de réponse aux attaques

En fonction de leur réactivité aux attaques, les IDS se classent en deux modes de réponse :

La réponse passive: La réponse passive est disponible pour tous les IDS, elle consiste à généré simplement des alarmes en cas d'attaques et enregistrer les intrusions détectées dans un fichier de log ,envoyées par mail, par SMS, etc. qui sera analysé par le responsable sécurité. Certains IDS permettent de logger l'ensemble d'une connexion identifiée comme malveillante. Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

La réponse actifs: la réponse active est plus ou moins implémentée a pour but de stopper une attaque au moment de sa détection. Elles génèrent les alarmes, mais en plus déclenchent un processus de défense contre l'attaque. Exemple : réinitialiser la connexion, bloquer du trafic, supprimer tous les processus du système attaquant, etc.

4.3 L'emplacement des sources d'audits

Les sources d'audits sont généralement utilisées pour classifier les IDS, on cite les IDS basés sur l'hôte et les IDS basés sur le réseau et les IDS hybrides, dont on a détaillé auparavant dans la section « les familles de Système de détection d'intrusion ».

4.4 La fréquence d'utilisation (la synchronisation)

La synchronisation se rapporte au temps écoulé entre les événements qui sont surveillés et l'analyse de ces événements [37].

Périodique : les IDS basés sur une méthode de détection périodique, analysent périodiquement les fichiers d'audit à la recherche d'une éventuelle intrusion ou anomalie passée [26]. Beaucoup de HIDS utilisent une méthode de détection périodique, car ils analysent des logs issus des systèmes d'exploitation qui sont générés sous forme de fichiers.

Continue : les IDS en temps réel traitent des flux continus d'informations à partir des différentes sources d'informations [23].C'est le paradigme prédominant pour les NIDS qui analysent le trafic des réseaux. La détection exécutée par des NIDS "en temps réel" donne des

résultats assez rapidement pour permettre aux IDS de prendre des actions qui affectent le progrès de l'attaque détectée.

Conclusion

La sécurité absolue n'existe malheureusement pas, mais certaines précautions peuvent faire diminuer le risque d'avoir un système compromis. Ces mesures doivent être d'autant plus strictes quand les données ont un caractère sensible.

L'avenir des technologies de sécurité réseau est peut-être dans une intégration plus poussée des différents outils disponibles pour assurer la sécurité d'un réseau.

Cette étude nous a permis de découvrir les IDS, ces systèmes sont à présents indispensables aux entreprises afin d'assurer leur sécurité informatique.

Dans ce chapitre, nous avons commencé par définir et expliquer le fonctionnement des IDS. Ensuit, nous avons fait une étude sur la classification des IDS.

Dans le chapitre suivant on va présenter deux techniques de data mining pour la classification dans la détection d'intrusion tel que les Réseaux Bayésiens et les Arbres de Décisions.

CHAPITRE III

Les Réseaux Bayésiens et Les Arbres de Décisions

Introduction

La classification est une tâche basique en analyse de données et en apprentissage, elle consiste à attribuer une classe à un ensemble d'attributs caractérisant un objet. Cependant, construire un classificateur à partir d'un ensemble de données pré-classées (étiquetées) est un problème central en apprentissage.

Plusieurs méthodes on été proposées, tels que les arbres de décision, les réseaux bayésiens, les réseaux de neurones, les règles d'association…etc.

Les modèles graphiques probabilistes ont reçu beaucoup d'attention au cours des dernières décennies à travers un certain nombre de domaines, les réseaux Bayésiens ont réalisé un impact très important constituent une technique d'acquisition, de représentation et de manipulation de connaissance. Ils sont utilisés pour leur capacité d'effectuer des inférences dans un contexte d'incertitude.

Dans ce chapitre nous allons donner les notions de base des méthodes qui font l'objet d'une grande partie de notre contribution dans ce mémoire, plus précisément nous introduisons les concepts des arbres de décisions. Ensuite nous allons définir les réseaux bayésiens. Nous présentons les principales définitions, les notions d'indépendance conditionnelle, les principaux théorèmes et les étapes de la construction des réseaux bayésiens.

I. Les Arbres de Décisions

1. Définition des arbres de décisions

La méthode des arbres de décision AD) (Quinlan, 1986) (Quinlan, 1993) est l'une des techniques les plus intuitives et des plus populaires du data mining et la plus utilisée en classification. D'autant plus qu'elle fournit des règles explicites de classement et supporte bien les données hétérogènes, manquantes et les effets non-linéaires, cette méthode étant préférée dans la prédiction du risque en raison de sa plus grande robustesse. Ils ressortissent donc à la catégorie des classifications hiérarchiques descendantes supervisées [69]. Leur succès est notamment dû à leur aptitude à traiter des problèmes complexes de classification. En effet, ils offrent une représentation facile à comprendre et à interpréter, ainsi qu'une capacité à produire des règles logiques de classification [59].

2. Principe général des arbres de décision

La technique de l'arbre de décision est employée en classement pour détecter des critères permettant de répartir les individus d'une population en n classes. On commence par choisir la variable qui, par ses modalités, sépare le mieux les individus de chaque classe, de façon à avoir des

sous-populations, que l'on appelle nœuds, contenant chacune le plus possible d'individus d'une seule classe, puis on réitère la même opération sur chaque nouveau nœud obtenu jusqu'à ce que la séparation des individus ne soit plus possible ou plus souhaitable. Par construction, les nœuds terminaux (les feuilles) sont tous majoritairement constitués d'individus d'une seule classe avec une assez forte probabilité, quand il satisfait l'ensemble des règles permettant d'arriver à cette feuille. L'ensemble des règles de toutes les feuilles constitue le modèle de classement [69].

Un arbre de décision est composé de :

a) Nœuds de décision : contenant chacun un test sur un attribut.

b) Branches: correspondant généralement à l'une des valeurs possibles de l'attribut sélectionné.

c) Feuilles: comprenant les objets qui appartiennent à la même classe.

L'utilisation des AD dans les problèmes de classification se fait en deux étapes principales :

– la construction d'un AD à partir d'une base d'apprentissage.

– la classification ou l'inférence consistant à classer une nouvelle instance à partir de l'arbre de décision construit dans la première étape.

La construction d'un AD se base sur un ensemble d'apprentissage donné. Elle consiste à sélectionner pour un nœud de décision le test d'attribut approprié et puis de définir la classe relative à chaque feuille de l'arbre induit [59].

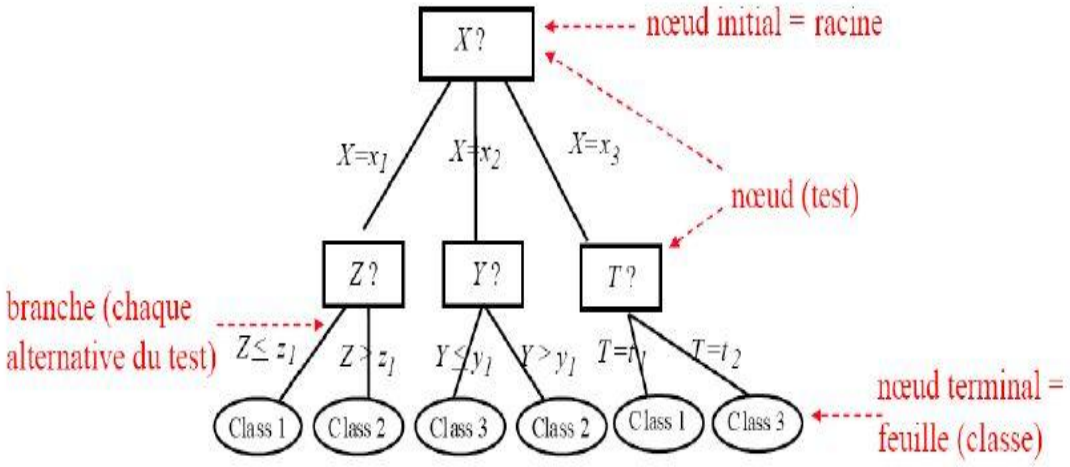

Figure 15: Exemple d'arbre de décision.

Règle de classification : aller de la racine à une feuille en effectuant les tests des nœuds.

Classe d'une feuille : classe majoritaire parmi les exemples d'apprentissage appartenant à cette feuille.

3. Construire un arbre de décision

Le schéma général pour construire un arbre est le suivant : [60]

Entrées : langage de description ; échantillon S ;
Début
Initialiser l'arbre à vide ; // la racine est le nœud courant
Répéter
Décider si le nœud courant est terminal (SI tous les points de l'arbre X sont de même classe)
Si le nœud est terminal
Alors créer une feuille associée à cette classe
Sinon choisir (selon critère !) le meilleur couple (attribut; test) pour créer un nœud
- ce test sépare X en 2 parties Xg et Xd **1)** contruire-arbre (Xg) **2)** construire-arbre (Xd)
Jusqu'à obtenir un arbre de décision ;
Fin.

Le principe consiste à diviser récursivement et le plus efficacement possible les exemples de l'ensemble d'apprentissage par des tests définis à l'aide des attributs jusqu'à ce que l'on obtienne des sous-ensembles d'exemples ne contenant (presque) que des exemples appartenant tous à une même classe. On suit ces trois opérateurs :

1. Décider si un nœud est terminal, c'est-à-dire décider si un nœud doit être étiqueté comme une feuille. Par exemple : tous les exemples sont dans la même classe, il y a moins d'un certain nombre d'erreurs.
2. Sélectionner un test à associer à un nœud. Par exemple : aléatoirement, utiliser des critères statistiques.
3. Affecter une classe à une feuille. On attribue la classe majoritaire.

4. Avantage et inconvénients des arbres de décisions [60]

1) Les Avantages :

- ✓ Facilité à manipuler des données symboliques.
- ✓ OK avec variables d'amplitudes très différentes.
- ✓ Multi-classe par nature.
- ✓ Interprétabilité de l'arbre.
- ✓ Classification très efficace en particulier sur de grande dimension.

2) Les Inconvénients :

- ✓ Sensibilité au bruit et points aberrants.
- ✓ Stratégie d'élagage delicate.

5. Les Forêts Aléatoires (Random Forests)

Une « forêt » = un ensemble d'arbre simples.

La forêt aléatoire est l'un des algorithmes d'ensemble les plus connus qui utilisent l'arbre de décision en tant que classificateur de base. La construction d'une forêt aléatoire est conforme au processus général de construire un ensemble qui se compose de trois phases principales [60].

1. L'algorithme de forêt aléatoire gagne en diversité d'ensemble en manipulant des ensembles d'apprentissage, une liste des ensembles d'apprentissage est créée à l'aide d'une Méthode d'échantillonnage.

2. La forêt aléatoire emploie le même inducteur, qui est un arbre aléatoire, sur des ensembles d'entraînement différents générés à l'étape précédente pour construire un classificateur de base. En détail, à chaque nœud, un petit groupe d'attributs d'entrée est sélectionné au hasard. La taille du groupe peut être précisée par les utilisateurs, mais généralement il est choisi comme le plus grand entier qui n'est pas supérieur à log2 M + 1, où M est le nombre de attributs d'entrée. Ensuite, le meilleur attribut ou le meilleur point de partage sera sélectionné.

3. La méthode de vote de la majorité est utilisée dans l'algorithme Random forêt de Breiman (2001),la construction d'une forêt aléatoire comprend la tâche de générer des aléas des vecteurs pour faire pousser un ensemble d'arbres et laisser ces arbres voter pour les plus populaires classe [61].

6. Avantage et inconvénients des Forêts Aléatoires [60]

Les Avantages :

- Reconnaissance très rapide.
- Multi-classes par nature.
- Efficace avec les grandes dimensions
- Robustesse aux outliers.

Les Inconvénients :

- Apprentissage souvent long.
- Valeurs extrêmes souvent mal estimées dans cas de régression.

7. Les Arbres Cart

L'acronyme CART (Classification And Regression Trees) signifie arbre de classification et de régression. Il a été développé par Leo Breiman, Jerome Friedman et plus tard rejoint par Richard Olshen et Charles Stone qui ont commencé à travailler avec des arbres de décision. [62]. CART est une technique d'apprentissage statistique, intégralement décrite par Breiman et aI. (1984). Dans cette méthode, les données des prédicteurs sont utilisées pour identifier des règles simples prévoyantes de manière fiable le type de catégorie de l'élément qui va se produire. Les règles sont toutes des règles binaires (uniquement oui ou non) et elles s'ajustent ensemble en une structure arborescente. Une fois l'arbre défini, la technique est facile à utiliser. On soumet aux règles binaires de décision de nouvelles valeurs des prédicteurs et le contrôle suit la structure de l'arbre jusqu'à un point terminal. Chaque point terminal est, associe à une catégorique donnée et il y a également un facteur de confiance (probabilité) dépendant de la facilite avec laquelle l'arbre est parvenu à classer les phénomènes de l'échantillon de développement [65].Cette procédure a l'avantage de fournir des règles d'affectation utilisable à grande échelle. Pour traiter de grandes bases de données, par convention, l'arbre est binaire pour éviter la fragmentation des données [67]. CART manipule les attributs catégoriques et continus pour construire un arbre de décision, comme il gère les valeurs manquantes et utilise l'élagage de la complexité des coûts pour supprimer des branches peu fiables de l'arbre de décision pour améliorer précision [68].

II. Les Réseaux Bayésiens

1. La notion de probabilité

Les probabilités offrent le plus ancien formalisme permettant de gérer de façon événementielle itérative l'incertitude dans les données. Dans ce cadre, la relation entre l'information des données et les différentes hypothèses envisagées est représentée par une distribution de probabilité conditionnelle. Les probabilités bénéficient de quatre siècles de travaux et reposent donc sur des fondements mathématiques et une expérience solides, ce qui explique pourquoi c'est encore la théorie la plus utilisée pour représenter l'incertain [69].

Les probabilités sont utilisées continuellement, de manière plus ou moins consciente, afin d'exprimer notre croyance sur le fait qu'un évènement se produise. L'idée d'événement est un concept générique pouvant prendre de multiples formes.

Ces probabilités sont toutes définies dans l'intervalle [0,1], quantifiant ainsi notre niveau de croyance en l'évènement [51].

Plus formellement supposons un évènement ω appartenant à l'ensemble des évènements observables possibles. On peut alors définir une fonction de probabilité tel que :

$$P: \omega \rightarrow [0,1] \; \omega \in \Omega \quad (1)$$

Où

$P(\omega) \geq 0$ représente la probabilité que ω se produise.

$P(\Omega) = 1$ dénote le caractères certain qu'au moins un des événements possibles se produise.

$P(\omega 1 \cup \omega 2) = P(\omega 1) + P(\omega 2)$ spécifie l'additivité des probabilités de deux événement disjoints $\omega 1, \omega 2$.

L'indépendance conditionnelle : Soient deux variables aléatoires X et Y. on dit que X et Y sont indépendantes conditionnellement à Z, si l'une des propriétés équivalentes suivantes est vérifiée [50].

$$p(X/Z, Y) = p(X/Z) \quad (2)$$

$$p(X/Z, Y) = p(X/Z).p(Y/Z) \quad (3)$$

2. Définition des Réseaux Bayésiens

Les réseaux bayésiens (RB), proposés par Judea Pearl [54] au début des années 1980, sont des modèles graphiques très utilisés pour représenter et manipuler des informations incertaines [55] [56]. Sur un phénomène complexe, et permettant, à partir des données, un véritable raisonnement, ainsi que de calculer des probabilités conditionnelles apportant des solutions à différentes sortes de problématiques.

L'intérêt particulier des RB est de tenir compte simultanément de connaissances a priori d'experts dans le graphe et de l'expérience contenue dans les données.

En bref, un RB est un modèle probabiliste graphique permettant d'acquérir, de capitaliser et d'exploiter des connaissances, né du besoin de créer des systèmes experts à base de probabilités [50].

Un RB est constitué de deux composantes : [53]

Une composante graphique qui consiste en un graphe orienté acyclique que nous appelons structure. Cette dernière encapsule deux connaissances principales sur le domaine. La première est les nouds qui représentent les variables d'intérêt du domaine et la deuxième est les arcs qui représentent les relations de dépendance entre ces variables dans un RB, un arc de A vers B peut être interprété par A cause B. Il s'agit de la représentation qualitative de la connaissance.

Une composante numérique qui consiste en une quantification des différents liens dans le graphe par des distributions de probabilités conditionnelles. Pour chaque nœud on dispose d'une table de probabilités P(variable|parents(variable)) qui représente la distribution locale de probabilité. L'état

de chaque nœud ne dépend que de l'état de ses parents. Il s'agit de la représentation quantitative de la connaissance.

3. Définition Formelle

La structure de ce type de réseau est simple : un graphe qui ne contient pas de boucle dans lequel les nœuds représentent des variables aléatoires, et les arcs (le graphe est donc orienté) reliant ces dernières sont rattachées à des probabilités conditionnelles.
Un RB peut être formellement défini par : [50]

- ✓ un graphe acyclique orienté G, G=G (V, E) où V est l'ensemble des nœuds de G, et E l'ensemble des arcs de G.
- ✓ un espace probabilisé fini (Ω, p).
- ✓ un ensemble de variables aléatoires associées aux nœuds du graphe et définies sur (Ω, p) tel que :

$$p(v1, v2, \dots vn) = \prod_{i=1}^{n} p(vi \mid c(vi)) \quad (4)$$

Avec C(Vi) l'ensemble des parents de Vi dans le graphe.

4. Domaines d'utilisation des réseaux bayésiens

Les domaines d'utilisation d'un RB sont multiple les principaux sont:
diagnostic médical et industriel, analyse de risques, détection de spam, datamining, détection de fraudes, exploitation du retour d'expérience, modélisation et simulation de systèmes complexes, détection d'intrusions, analyse de trajectoires de santé..etc.

5. Représentation graphique de la causalité

La représentation graphique la plus intuitive de l'influence d'un événement est de relier la cause à l'effet par une flèche orientée. S'il existe une relation causale de A vers B, toute information sur A peut modifier la connaissance sur B, et réciproquement, toute information sur B peut modifier la connaissance sur A [50].

En présence d'un graphe plus complexe, il est essentiel de conserver à l'esprit que l'information ne circule pas seulement dans le sens des flèches. Comme nous montrons dans la figure 16. La connaissance de D renforce la croyance de la cause B et la connaissance de C augmente la croyance en l'une des causes A ou B.

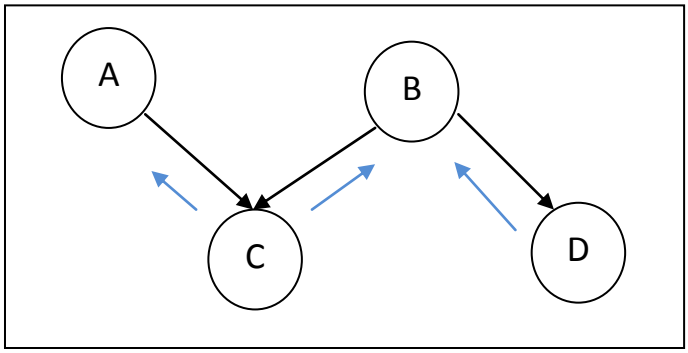

Figure 16: Représentation graphique de la causalité.

Dans un graphe on peut rencontrer plusieurs modes de connexion entre les nœuds comme le montre la figure 17 ou nous allons présenter comment l'information circule au sein d'un graphe causal.

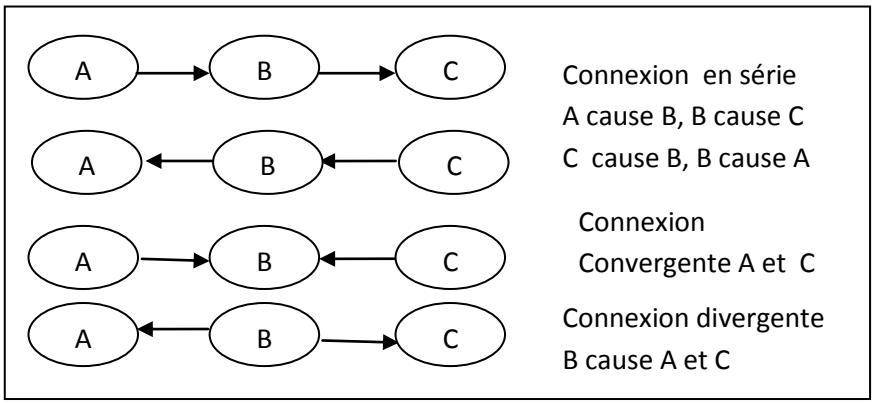

Figure 17: Circulation d'information dans d'un graphe causal.

6. D-séparation

On dit qu'un ensemble X de variables est d-séparé de Y par un ensemble Z dans G si toute chaîne reliant une variable x ∈ X à une variable y ∈ Y est bloquée par Z on note alors (X|Z|Y) [51]. Donc deux variables X, Y sont d-séparées par Z si l'une au moins des deux conditions suivantes est vérifiée :

-Le chemin converge en un nœud W, tel que W ≠ Z, et W n'est pas une cause directe de Z.

-Le chemin passe par Z, et est soit divergent, soit en série au nœud Z.

Exemple : Dans le graphe de la figure 18 A et D sont d-séparés par B car le chemin orienté allant de A vers D passe par B. Et de même le nœud D d-sépare les nœuds A B C des nœuds E F G [50].

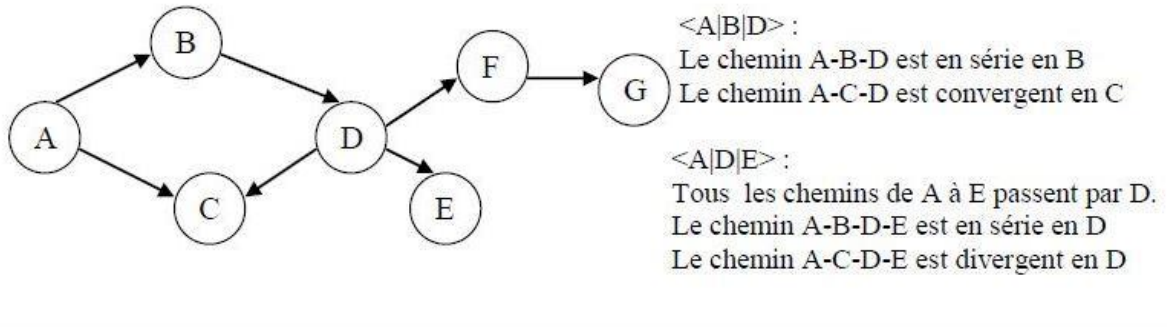

Figure 18: Exemple de D-séparation.

7. Formule de Bayes

Le calcul dans un RB s'appui sur le théorème de Bayes. Soit deux variables aléatoires X1 et X2, la probabilité conditionnelle de X2 sachant X1 est déterminée par la formule suivante si l'on connaît les probabilités de X1, X2 et X1 sachant X2 : [58]

$$p(X2/X1)=p(X1/X2)\ p(X2)\ p(X1) \quad (5)$$

- P(X1) est la probabilité a priori (ou marginale) de X1. Elle est « antérieure » au sens qu'elle précède toute information sur X2.

- P(X2/X1) est la probabilité a posteriori de X2 sachant X1. elle dépend directement de X1
- P(X1/X2) est la fonction de vraisemblance de X1 connaissant X2.

Dans le cas général, où X = {X1, X2,…, Xn}, la fonction de distribution de probabilités jointe P(X) s'écrit comme suit : [50]

$$P(X) = \prod_{i=1}^{n} P(Xi/parents(Xi)) \quad (6)$$

Pour aboutir au théorème de Bayes, on part d'une des définitions de la probabilité conditionnelle :

$$P(X2|X1)p(X1) = p(X2 \cap X1) = p(X1|X2)p(X2) \quad (7)$$

En notant $p(X1 \cap X2)$ la probabilité que X2 et X1 aient tous les deux lieux. En divisant de part et d'autre par p(X1), on obtient :

$$P(X2|X1) = \frac{p(X1|X2)p(X2)}{p(X1)} \quad (8)$$

8. Exemple d'un réseau bayésien

On va prendre un exemple pour illustrer les RB [57].

Ce matin-là, alors que le temps est clair et sec, M. Holmes sort de sa maison. Il s'aperçoit que la pelouse de son jardin est humide. Il se demande alors s'il a plu pendant la nuit, ou s'il a simplement oublie de débrancher son arroseur automatique. Il jette alors un coup d'œil a la pelouse de son voisin, M. Watson et s'aperçois qu'elle est humide. Il en déduit alors qu'il a probablement plu, et il décide de partir au travail sans vérifier son arroseur automatique.

Nous avons alors quatre variables (qui sont les événements) qui peuvent prendre chacune la valeur « vrai » ou « faux » :

A : J'ai oublie de débrancher le arroseur.

P : Il a plu pendant cette nuit.

J : L'herbe de mon jardin est humide.

W: L'herbe du jardin de mon voisin Watson est humide.

La figure 19 représente le graphe causal du modèle RB.

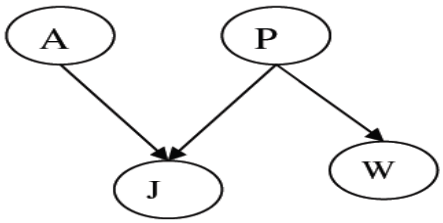

Figure 19: Graphe causal de l'exemple.

Dans ce texte, monsieur Holmes fait un raisonnement qui peut être décrit a l'aide d'un RB. L'herbe de mon jardin est mouillée (J) si et seulement si : il a plu cette nuit (P) ou j'ai oublie de débrancher mon arroseur (A). Ce qui se traduit par la liaison A-J et la liaison P-J et par les tableaux de probabilité ci-dessous.

Evénement	Probabilité
A=vrai	0.40
A=faux	0.60
P=vrai	0.40
P=faux	0.60

Tableau 01: Les probabilités à priori.

	A=vrai		A=faux	
	P=vrai	P=faux	P=vrai	P=faux
J=vrai	1	1	1	0
J=faux	0	0	0	1

Tableau 02: Les probabilités conditionnelles pour J.

L'herbe du jardin de mon voisin Watson (W) est humide si et seulement si il a plu cette nuit, ce qui se traduit par la table de probabilité associée et la liaison P-W.

	P=vrai	P=faux
W=vrai	1	0
W=faux	0	1

Tableau 03: Les probabilités conditionnelles pour W.

Calcule probabiliste analytique : M. Holmes sort de sa maison. Il s'aperçoit que la pelouse de son jardin est humide, il se pose alors une question : Il se demande alors s'il a plu pendant la nuit, ou s'il a simplement oublié de débrancher son arroseur automatique. Pour répondre à cette question cela reviens à calculer et comparer : P (A = vrai/J=vrai) et P(P= vrai/ J= vrai).

Pour cela on utilise le théorème de Bayes :

$$p(A/B) = \frac{p(A \cap B)}{p(B)} = \frac{(B/A).p(A)}{p(B)} \qquad (9)$$

Soit $$p(A = V / J = V) = \frac{p(J=V / A=V)p(A=V)}{p(J=V)} \qquad (10)$$

Et $$p(P = A / J = V) = \frac{p(J=V / P=V)p(P=V)}{p(J=V)} \qquad (11)$$

On peut aussi calculer les prévisionnelles conditionnelles, par la propriété d'inversion de Bayes : p(J=V) = p(J=V/A=V, P=V).p(A=V).p(P=V) + p(J=V/A=V, P=F).p(A=V).p(P=F) + p(J=V/A=F, P=V).p(A=F).p(P=V) + p(J=V/A=F, P=F).p(A=F).p(P=F)

Application numérique:

p(J=V) = 1* 0.40 * 0.40 + 1 * 0.40 * 0.60 + 1 * 0.60 * 0.40 + 0 * 0.60 * 0.60 = 0.16 + 0.24 + 0.24 = 0.64

$$p(P = V/J = V) = \frac{1 * 0.40}{0.64} = 0.625$$

De la même manière on retrouve p (A=V/J=V) = 0.625

Nous retrouvons ici numériquement le résultat intuitif vu plus haut, à savoir que :

- La croyance en chacune des deux causes (P) et (J) est renforcée de 0.40 à 0.625.
- Il n'est pas possible de privilégier l'une des deux causes avec cette seule information.

Dans la seconde partie (2) de son raisonnement, M. Holmes est alors amené à comparer

p (A=V/J=V,W=V) avec p (P=V/J=V,W=V)

On retrouve facilement que : p (P=V/J=V, W=V) = 1

Mr Holmes est alors certain (100%), que si la peleuse de son voisin est mouillée (W), il a plu cette nuit et va au travail sans vérifier son arroseur (A).

De même : P(A=V/J=V,W=V) = p(A=V) = 0.40 (indépendance entre W et A)

Interprétation : Mr Holmes a la certitude qu'il a plus (100%), il n'a donc aucune raison de modifier sa croyance à priori, puisque la probabilité que l'arroseur est resté branché est plus faible (40%).

9. Construction d'un réseau bayésien

Le RB peut être construit : par expertise, par analyse fonctionnelle, ou par apprentissage en exploitant une base de données.

La construction d'un RB s'effectue en trois étapes essentielles, qui sont :

La première étape dite **qualitative**: on ne considère ici que les relations d'influence pouvant exister entre les variables prises deux à deux. Ceci emmène naturellement à une représentation graphique des relations entre les variables [52].

La deuxième est l'étape **probabiliste** : introduit l'idée d'une distribution jointe définie sur les variables et fait correspondre la forme de cette distribution au graphe créé précédemment [52].

La troisième est l'étape **quantitative** elle consiste simplement à spécifier numériquement les distributions de probabilités conditionnelles [52].

La figure 20 représente les étapes de construction d'RB: [58]

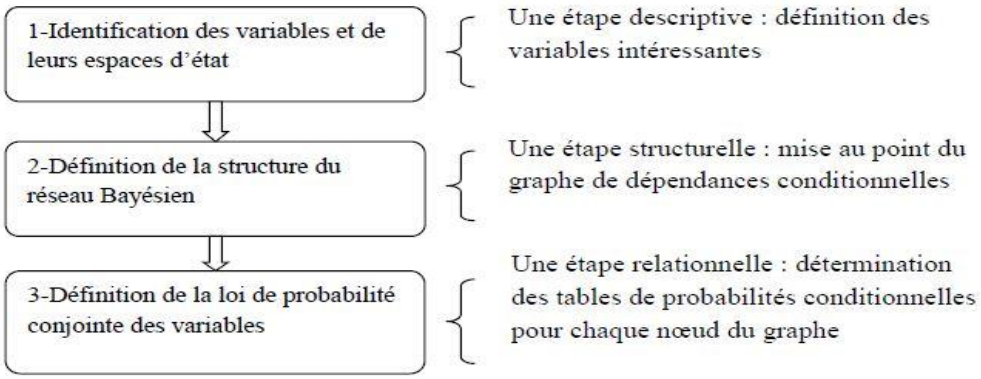

Figure 20: Les étapes de construction d'un réseau bayésien.

9.1 Identification des variables et de leurs espaces d'états

La première étape de construction du RB est la seule pour laquelle l'intervention humaine est absolument indispensable. Il s'agit de déterminer l'ensemble des variables Xi, catégorielles ou numériques, qui caractérisent le système. Lorsque les variables sont identifiées, il est ensuite

nécessaire de préciser l'espace d'états de chaque variable Xi, c'est-à-dire l'ensemble de ses valeurs possibles [50].

9.2 Définition de la structure du réseau bayésien

Une fois les variables aléatoires identifiées, il faut définir les dépendances (les influences) qui les relient chaque variable influence d'autres variables, est influencée par d'autres variables. En d'autre terme la deuxième étape consiste à identifier les liens entre variables, c'est-à- dire à répondre à la question : pour quels couples (i, j) la variable Xi influence-t-elle la variable Xj. Dans la plupart des applications, cette étape s'effectue par l'interrogation d'experts. Dans ce cas, des itérations sont souvent nécessaires pour aboutir à une description consensuelle des interactions entre les variables Xi [50].

9.3 Définition de la Loi de probabilité conjointe des variables

La dernière étape de construction du RB consiste à renseigner les tables de probabilités associées aux différentes variables. Dans un premier temps, la connaissance des experts concernant les lois de probabilité des variables est intégrée au modèle. Concrètement, deux cas se présentent selon la position d'une variable Xi dans le RB :

• La variable X_i n'a pas de variable parente: les experts doivent préciser la loi de probabilité marginale de X_i.

• La variable X_i possède des variables parentes: les experts doivent exprimer la dépendance de X_i en fonction des variables parentes, soit au moyen de probabilités conditionnelles, soit par une équation déterministe [50].

10.L'apprentissage des réseaux bayésiens

L'apprentissage d'un RB sachant un ensemble d'observations peut se décomposer en deux étapes, la première consiste à apprendre sa structure, c'est-à-dire le graphe associé au réseau, une fois sa structure connue, il est nécessaire d'estimer ses distributions de probabilités conditionnelles [51]. le problème de l'apprentissage se divise en deux parties [57] :

- L'apprentissage des paramètres, ou nous supposerons que la structure du réseau a été fixée, et où il faudra estimer les probabilités conditionnelles de chaque nœud du réseau.
- L'apprentissage de la structure, ou le but est de trouver le meilleur graphe représentant la tâche à résoudre.

10.1 Apprentissage des paramètres

L'apprentissage des paramètres d'un RB se fait à partir de données relatives au problème à modéliser. Toutefois, ces données peuvent être complètes ou incomplètes. Les algorithmes d'apprentissage des paramètres ne sont pas les mêmes dans ces deux cas.

Dans le cas où toutes les variables sont observées (critère : Apprentissage de paramètres données complètes), la méthode la plus simple et la plus utilisée est l'estimation statistique de la probabilité d'un événement par la fréquence d'apparition de l'événement dans la base de données. Cette méthode est appelée maximum de vraisemblance.

$$\widehat{\mathrm{P}}\left(\mathrm{X_i} = \mathrm{x_k}/\mathrm{Pa}(\mathrm{X_i}) = \mathrm{x_j}\right) = \hat{\theta}^{\mathrm{MV}}_{\mathrm{i,j,k}} = \frac{\mathrm{N_{i,j,k}}}{\sum_{\mathrm{k}} \mathrm{N_{i,j,k}}} \quad (12)$$

Où $N_{i,j,k}$est le nombre d'événements dans la base de données pour lesquels la variable Xi est dans l'état xk et ses parents dans la configuration xj.

Une autre méthode dite "estimation bayésienne" est aussi utilisée. Elle suit un principe différent. Elle consiste à trouver les paramètres les plus probables sachant que les données ont été observées, en utilisant des a priori sur les paramètres.

10.2 Apprentissage de structure

Lorsque la structure du RB n'est pas fournie a priori par un expert, il est possible d'apprendre cette structure à partir d'une base de données. Toutefois, dans la réalité cette base de données peut présenter un manque d'informations pour certaines mesures.

Dans le cas où notre base de données est complète (critère : Apprentissage de structure : données complètes), c'est-à-dire toutes les mesures sont complètes, deux familles à approches ont été proposées.

La première famille (algorithmes IC, PC etc.) consiste à déterminer dans un premier temps un graphe non orienté en tenant compte des différentes indépendances conditionnelles qui existent entre les variables de ce graphe, puis à orienter ce graphe pour obtenir un RB. Ces algorithmes sont peu efficaces dans le cas de problèmes de grande taille puisque la détermination de ces indépendances est exponentielle en fonction du nombre des variables.

La deuxième approche consiste à parcourir tous les graphes possibles, associer un score à chaque graphe, puis choisir le graphe ayant le score le plus élevé. Toutefois, cette méthode n'est pas simple, principalement à cause de la taille super-exponentielle de l'espace de recherche en fonction du nombre de variables. En 1977 Robinson a montré que le nombre r(n) de structures différentes des graphes possibles pour n variables est donné par la formule :

$$r(n) = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} 2^{i(n-1)} r(n-i) = n^{2^{o(n)}} \quad (13)$$

Des idées ont été proposées pour résoudre ce problème. Une première consiste à remplacer l'espace de recherche (espace des RB) par un espace plus petit, l'espace des arbres (MWST ou Maximal Weight Spanning Tree). Une deuxième idée consiste à ordonner les nœuds pour limiter la recherche des parents possibles pour chaque nœud (algorithme K2). Une troisième consiste à faire une recherche gloutonne dans l'espace des RB (algorithme GS).

11.L'inférence dans un réseau bayésien

L'inférence dans un RB est une approche déductive, l'objectif de l'inférence est de calculer n'importe quelle probabilité conditionnelle d'une variable du modèle à partir de la structure causale (arbre causes à effets) et les distributions de probabilités associées. Le théorème de Bayes et les lois de probabilités conditionnelles sont au cœur de ce calcul. Selon la complexité du réseau, nous distinguons deux types d'inférences :

11.1 L'inférence exacte

Les techniques d'inférence reposent essentiellement sur l'indépendance des variables entre elles, ce qui permet de factoriser certaines parties du calcul et d'utiliser des techniques de programmation dynamique. Le cas des RB arborescents a été traité par Pearl et permet par un simple passage de message entre les variables de calculer les différentes probabilités jointes. Le cas général a été traité par Jenson avec la construction d'un arbre de jonction [50].

11.2 L'inférence approximative

Lorsqu'il n'est pas possible de faire une inférence exacte, ce qui est le cas des RB où il y a beaucoup de cycle et/ou de parents par noeud.il existe différentes méthodes tell que la méthode Variationelles, méthode de Monte-Carlo, méthode de propagation cyclique [50].

12. La classification et les réseaux Bayésiens

Un classificateur est une fonction qui reçoit en entrée la description d'un exemple et retourne une étiquette. Un classificateur h est donc une fonction : h : X → f {-1, +1}. La fonction h est parfois utilisée sous le terme hypothèse.

Un classificateur bayésien est un RB utilisé pour la classification, qui est un cas particulier d'inférence. Dans un RB utilisé pour la classification, on cherche à inférer la valeur la plus plausible d'une seule variable non observée, appelé classe, les autres variables, sont observables et constituent généralement les attributs des objets de la classe [53].

13. Le Classificateur Bayésiens naïfs

Un classificateur Bayésien naïf représente la forme la plus simple des RB. Il se compose d'un graphe avec un seul parent et plusieurs nouds feuilles, avec une forte hypothèse d'indépendance entre les feuilles dans le contexte de leur parent [53]. La figure 21 présente un RB naïf.

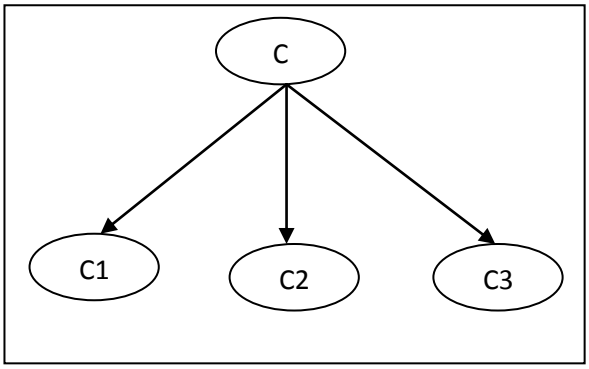

Figure 21: Réseau Bayésien naïf.

14. Les avantages des Réseaux Bayésiens

Les principaux avantages des RB sont [58] :

- ✓ les *RB* peuvent être utilisés pour apprendre des dépendances causales et pour modéliser des phénomènes aléatoires.
- ✓ un *RB* est une représentation graphique compacte et synthétique avec une facilité d'acquisition et d'utilisation de la connaissance.
- ✓ les *RB* peuvent combiner plusieurs aspects à la fois, des statistiques, des probabilités, de l'aide à la décision et le management des connaissances.
- ✓ pour l'utilisation, leur flexibilité permet d'interroger le même modèle graphique pour des objectifs différents, tels que la prédiction ou le diagnostic.
- ✓ de surcroît, ils permettent de modéliser la connaissance par une attribution des probabilités même si les données sont de nature incertaine.
- ✓ les algorithmes dédiés au calcul offrent un outil puissant pour la fusion des données incomplètes avec prise en compte des jugements des experts.

Conclusion

Dans ce chapitre nous avons couvert les principaux aspects concernant les RB. Nous avons vu que ces modèles graphiques sont des outils bien adaptés à la description des problèmes de décisions dans l'incertain, en permettant notamment de tenir compte des connaissances du problème à traité. Après nous avons introduit la notion des arbres de décision ainsi que le Random Forest et le Simple Cart.

Le chapitre suivant est consacré à la présentation de notre approche de détection d'intrusion réseaux.

PARTIE
RESULTATS ET DISCUSSION

Contribution dans la détection d'intrusions réseaux

Implémentation et réalisation

CHAPITRE IV
Contribution dans la détection d'intrusions réseaux

Introduction

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir des IDS, ces derniers sont devenus pratiquement indispensable dû à l'incessant accroissement en nombre et en dangerosité des attaques réseaux depuis quelques années.

Un IDS destiné à surveiller les données qui transitent sur le système, ainsi de détecter les logiciels malveillants, et capables de repérer et signaler à l'administrateur système, toute trace d'activité anormale ou suspecte sur la cible analysée.

Dans le but de la réalisation d'un IDS de haute performance qui maximise le taux de détection (DR) et le taux d'exactitude et minimise le taux de fausses alarmes (FAR) et qui détecte mieux les attaques rares sans perdre leur haute performance sur les autres attaques et le comportement normal.

L'idée de notre contribution est de proposé un modèle d'un IDS hiérarchique et hybride qui intègre plusieurs classificateurs qui ont été choisis selon leurs performances de détection de comportement normal et le comportement anormal (U2r, R2l, Dos, Probe).

1. Description de l'approche proposée

Dans cette section, nous présentons la structure de notre modèle ainsi que le mode de fonctionnement et les différentes étapes de réalisation de notre modèle.

1.1 La structure de notre modèle

Cette section présente les différentes étapes nécessaires pour construire notre modèle qui est basé sur les RB naïf pour fusionner les prédictions de plusieurs classificateurs. Comme il est montré dans la figure 22.

Notre modèle est composé de deux niveaux :

- Le premier niveau : à ce niveau, il s'agit de choisir les classificateurs qui ont le meilleur DR ; Le meilleur taux d'exactitude et avec un FAR le plus bas possible. Ensuite, on associe à chaque type de connexion le classificateur le plus approprié.

Chaque classificateur donne sa prédiction par rapport à un type de connexion pour lequel ce classificateur est sélectionné, ensuite cette prédiction et le classificateur qui lui convient seront fusionnés avec l'ensemble de données de test.

- Le deuxième niveau : à ce niveau, on divise le nouvel ensemble de données résultant de premier niveau en deux ensembles un pour l'apprentissage et l'autre pour le test.

Ensuite, il s'agit d'un classificateur RB naïf qui prend par la suite la décision final, cette décision peut être un comportement normal ou un comportement anormal (attaque).

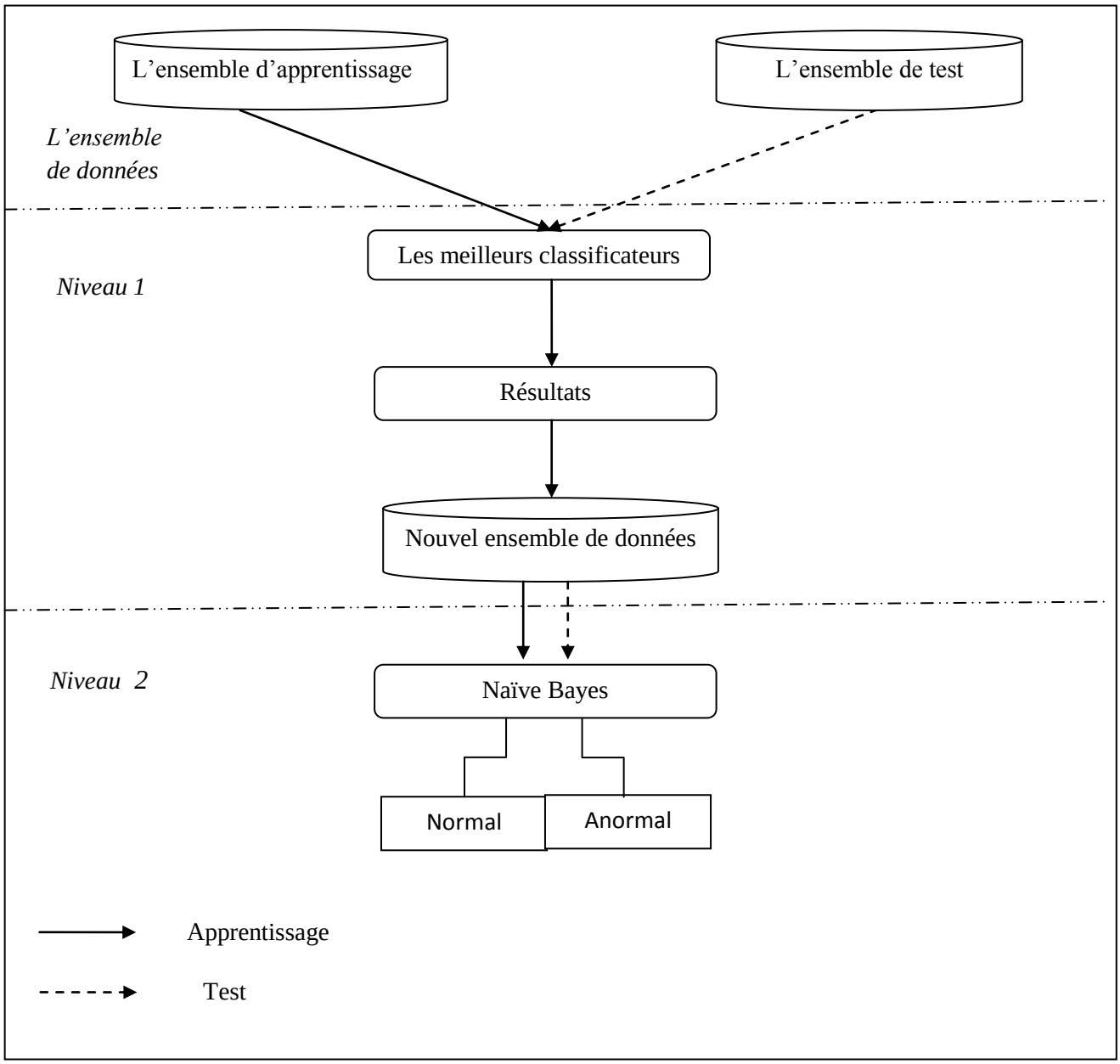

Figure 22: La structure de notre modèle.

1.2 Le mode de fonctionnement de notre modèle

Notre modèle fonctionne en trois étapes : étape de sélection des classificateurs ensuite une étape d'apprentissage enfin une étape de test.

1.2.1 Étape 1 : La sélection des classificateurs

Afin de sélectionner les meilleurs classificateurs de premier niveau, nous effectuons deux études comparatives entre différents types de classificateurs.

Premièrement, nous comparons les différents classificateurs par rapport à leur performance. Nous sélectionnons seulement les classificateurs qui donnent, le meilleur DR de même pour l'exactitude et le FAR le plus bas possible. Cette sélection est faite sur la base de l'optimalité de PARETO [70] pour rechercher les meilleurs classificateurs parmi un ensemble de classificateurs par rapport au taux d'exactitude le plus élevé et le DR le plus élevé et le FAR le plus bas.

Deuxièmement, une deuxième étude comparative sur les classificateurs sélectionnés pour associer a chaque type de connexion (dos, probe ,u2r, r2l, normal) le meilleur classificateur qui lui convient selon le meilleur DR de chaque type de connexion. Puis, nous générons un nouvel ensemble de données à partir des prédictions du premier niveau.

Ensuite, une intégration des prédictions des classificateurs sélectionnés dans un RB naïf.

1.2.2 Étape 2 : La phase d'apprentissage

Une phase d'apprentissage pour notre modèle est indispensable afin de se préparer la phase de test, cette phase est composée de deux étapes :

Première étape : concernant l'apprentissage des classificateurs du premier niveau par l'ensemble de données d'apprentissage, où chaque instance de ce ensemble de données d'apprentissage représente une entrée pour le classificateur.

Deuxième étape : concernant l'apprentissage des classificateurs du deuxième niveau par le nouvel ensemble de données créé à partir des prédictions du premier niveau.

Ce nouvel ensemble de données est créé par la fusion des résultats des prédictions des classificateurs du premier niveau et le classificateur qui lui convient avec l'ensemble de données de test (KDDcup test). Ensuite, nous sélectionnons les instances qui ont l'étiquette correcte.

Ce dernier sera divisé en deux ensembles, le premier ensemble sera utilisé comme base d'apprentissage du deuxième niveau et le deuxième sera utilisé comme base de test du deuxième niveau.

1.2.3 Étape 3 : La phase de test

À cette phase, nous testons les performances de notre modèle pour les deux niveaux.

Concernons le premier niveau, une fois la phase d'apprentissage a été réalisée, nous traitons chaque enregistrement des données de test par les différents classificateurs du premier

niveau. Ensuite, nous utilisons les sorties des prédictions du premier niveau pour réaliser le nouvel ensemble qui sera divisé en ensemble de donné d'apprentissage et ensemble de donné de test, ces derniers seront utiliser comme entrée du deuxième niveau.

Concernons le deuxième niveau, à ce niveau, on va utiliser le nouvel ensemble de test résultant des sorites de premier niveau, et nous traitons chaque enregistrement des données de ce nouvel ensemble de test par le classificateur du deuxième niveau.

2. Expérimentations

Dans cette section, de prime abord, nous parlons de la préparation des données détaillées utilisés dons notre approche. Ensuite en passe à l'identification des différentes étapes de déroulement de notre modèle. Enfin nous affectons une étude comparative entre les résultats de notre modèle et d'autres résultats bien connus.

2.1 Préparation des donnés pour notre modèle

La détection d'intrusion est toujours été l'un des sujets chauds dans le domaine de l'apprentissage par machine.

En vue de l'augmentation des attaques contre les systèmes d'informations, les IDS ont été utilisé avec un certain nombre de techniques qui sont disponibles pour la DI, et L'exploration de données est l'une des techniques efficace parmi eux.

Cette expérience se concentre sur l'outil de manipuler et d'analyse des fichiers de données WEKA 3.7.0 [63][ANNEXES A] et ces différents algorithmes de classification pour expérimenter des méthodes, résoudre des problèmes où nous concentrant sur l'utilisation et les résultats fournis par ces implémentations, sans avoir à réécrire à chaque fois les algorithmes.

De plus, nous concentrons également sur la compétition KDD Cup 99 [64] qui représente l'ensemble de données le plus utilisé dans le domaine de la sécurité des réseaux et le point d'attraction de nombreux chercheurs de domaine de détection d'intrusion de la dernière décennie.

En travaux pratiques, nous utiliserons un PC Windows avec CPU Core i3, 2.40 GHz et 4 giga-octets de RAM.

2.2 Présentation de l'ensemble de formation et de test

Depuis 1999, KDDcup'99 a été l'ensemble de données le plus utilisé pour l'évaluation des méthodes de détection d'anomalie. Cet ensemble de données est préparé par Stolfo et al (2000), [5]. est construit sur la base des données recueillies dans l'évaluation DARPA'98 IDS Programme.

Le programme d'évaluation de la détection des intrusions DARPA en 1998 a été préparé et géré par MIT Lincoln Labs.il contient un ensemble standard de données à auditer, qui comprend une grande variété d'intrusions simulées dans un environnement de réseau militaire. D'où le KDD99 a été dérivé en 1999.DARPA'98 a mis en place neuf semaines pour acquérir les données.

Les données d'apprentissage comptent environ 4 giga-octets de données brutes compressées (binaire) à partir de sept semaines de trafic réseau. qui peut être transformé en environ 5 millions d'enregistrements de connexion chacun avec environ 100 octets. De même, les deux semaines de données d'essai ont donné environ deux millions d'enregistrements de connexion.

L'ensemble de données d'apprentissage KDD comprend environ 4 898 431 célibataires vecteurs de connexion dont chacun contient 41 attributs le tableau 4 montre les différent attribut qui forme une connexion. L'ensemble de données d'apprentissage KDD99 couvre le comportement normal et 22 types d'attaque étiqueté, avec exactement un type d'attaque spécifique. Les attaques simulées appartiennent à l'une des quatre catégories suivantes:

- **L'attaque de déni de service « Denial of Service Attack (DoS) »** : est une attaque dans laquelle l'attaquant essaye de rendre la mémoire d'un système ou la bande passante d'un réseau trop occupée ou trop chargée pour gérer les demandes légitimes, afin d'empêcher les utilisateurs légitimes d'accès à une machine.
- **L'attaque de passage d'un utilisateur à un super utilisateur « User to Root Attack (U2R)** » : est une attaque dans laquelle l'attaquant commence par un accès à un compte utilisateur normal sur le système (peut-être acquise par des mots de passe capturés, une attaque par dictionnaire…etc.) dans le but d'exploiter certaines vulnérabilités pour obtenir un accès Root sur le système.
- **L'attaque distance à local « Remote to Local Attack (R2L) »** : se produit quand un attaquant qui a la capacité d'envoyer des paquets vers une machine sur un réseau, mais qui n'a pas de compte sur cette machine. Il exploite certaines vulnérabilités afin d'obtenir un accès local en tant qu'utilisateur de cette machine.
- **L'attaque d'exploration « Probing Attack »** : elle vise de rassembler des informations sur un réseau d'ordinateurs dans le but de contourner les contrôles de sécurité.

L'ensemble de données de test KDD comprend environ 311029 célibataires Vecteurs de connexion dont chacun contient 41 attribut de même que L'ensemble d'apprentissage KDD99,et couvre le comportement normal et 37 type d'attaque où 17 attaques n'existent pas dans le L'ensemble de données d'apprentissage KDD. Le tableau 04 montre les différent attribut qui forme une connexion.

Nom d'attribut	Description	type
Duration	Longueur de la connexion (second)	continuous
Protocol_type	Type de protocole, e.g. tcp, udp, etc.	discrete
Service	Service réseau de destination, e.g., http, telnet, etc.	discrete
Flag	Statut normal ou erreur de la connexion	discrete
Src_bytes	Nombre d'octets de données de la source à a destination	continuous
Dst_bytes	Nombre d'octets de données de la destination à la source	continuous
Land	1 si une connexion est de / vers le même hôte / port; 0 sinon	discrete
Wrong_fragment	Nombre de fragments « erronées »	continuous
Hot	Nombre d'indicateurs "hot"	continuous
Urgent	Nombre de paquets urgents	continuous
Num_failed_logins	Nombre de tentatives de connexion échouées	continuous
Logged_in	1 si un succès de se connecter, 0 sinon	discrete
Root_shell	1 si le root Shell est obtenu; 0 autrement	discrete
Num_compromised	Nombre de conditions compromises	continuous
Su_attempted	1 si la commande " su root " a été tentée, sinon 0	discrete
Num_root	Nombre de " root " ont accédé	continuous
Num_file_creations	Nombre d'opérations de création de fichiers	continuous
Num_shell	Nombre d'invités du shell	continuous
Num_access_files	Nombre d'opérations sur les fichiers de contrôle d'accès	continuous
Num_outbound_cmds	Nombre de commandes sortantes dans une session FTP	continuous
Is_host_login	1 si la connexion appartient à la liste du 'hot' ; 0 sinon	discrete
Is_guest_login	1 si le login est un login "guest", sinon 0	discrete
Count	nombre de connexions vers la même machine que la connexion en cours dans les deux dernières secondes	continous
Srv_count	Nombre de connexions pour le même service que la connexion en cours dans les deux dernières secondes	continuous
Serror_rate	% Des connexions qui ont des erreurs "SYN" (connexions de la même machine)	continuous
Srv_serror_rate	% Des connexions qui ont des erreurs "SYN" (connexions du même service)	continuous
Rerror_rate	% Des connexions qui ont des erreurs "REJ" (connexions de la même machine)	continuous
Srv_rerror_rate	% Des connexions qui ont des erreurs "REJ" (connexions du même service)	continuous
Same_srv_rate	% des connexions aux mêmes services	continuous
Diff_srv_rate	% de connexions aux différents services	continuous
Srv_diff_host_rate	% de connexions aux différentes machines	continuous
Dst_host_count	compteur pour la machine de destination	continuous

Dst_host_srv_count	Srv_count pour la destination host	continuous
Dst_host_same_srv_rate	Same_srv_rate pour la destination host	continuous
Dst_host_diff_srv_rate	Diff_srv_rate pour la destination host	continuous
Dst_host_same_src_port _rate	Same_src_port_rate pour la destination host	continuous
Dst_host_srv_diff_host_ rate	Diff_host_rate pour la destination host	continuous
Dst_host_serror_rate	Serror_rate pour la destination host	continuous
Dst_host_srv_serror_rate	Srv_serror_rate pour la destination host	continuous
Dst_host_rerror_rate:	Rerror_rate pour la destination host	continuous
Dst_host_srv_rerror_rate	Srv_serror_rate pour la destination host	continuous

Tableau 04: Les différents attributs qui forme une connexion.

Le tableau 05 montre une comparaison ente les attaques qui existent dans L'ensemble de données d'apprentissage KDD99 et L'ensemble de données de test KDD99.

Type d'attaque	Les attaques qui existent dans l'ensemble d'apprentissage	Les attaques qui existent dans l'ensemble de test
DOS	Back, land, Neptune ,Pod, Smurf,Teardrop	Apach2, Mailbomb, Processtable, Udpstorm, Back ,Land, Neptune, Pod, Smurf, Teardrop
Probe	Ipsweep, Nmap, Portsweep, Satan,	Msan, Saint, Ipsweep, Nmap, Portsweep, Satan
R2l	Ftp_write, Guess_passwd, Imap, Multihop, Phf, Spy, Warezmaster, Warezclient	Named,Sendmail,Snmpgetattack,Snmpguess, Worm, Xlock, Xsnoop, ftp_write, Imap, , Phf Guess_passwd, Multihop, Warezmaster
U2r	Buffer_overflow, Loadmodule, Perl, Rootkit	Httptunnel, Ps, Sqlattack, Xterm, Buffer_overflow, Loadmodule, Perl, Rootkit

Tableau 05: Comparaison entre base d'apprentissage et base de test KDDcup'99.

En vue de la grande taille de KDD99, nous avons utilisé le KDD99_10% qui représente 10% des données d'apprentissage KDD99 établies avec la même répartition des attaques et le comportement normal.

Pour réduire la taille de KDD99_10%, nous avons créé un ensemble de données d'apprentissage contenant 30 000 enregistrements. De plus, nous avons supprimé tous les enregistrements redondants. Ensuite, une sélection aléatoire pour les enregistrements normaux et DOS. D'autre part, nous avons supprimé tous les enregistrements redondants de l'ensemble de données de test de KDD99 .Deux attributs (num_outbound_cmds, is_host_login) sont supprimés en raison de leurs valeurs identiques dans le l'ensemble de données d'apprentissage KDD99.

Le tableau 6 montres la répartition des attaques et du comportement normal dans L'ensemble d'apprentissage KDD99 training_10% et dans l'ensemble de test ainsi que résume la répartition des attaques et du comportement normal de notre ensemble de données d'apprentissage.

Type de connexion	KDD'99 10% d'apprentissage			KDD'99 de test	
	All	Sans Duplication	Notre Ensemble	All	Sans Duplication
Normal	97278	87832	8000	60590	47911
Dos	391458	54572	18819	229853	23568
Probe	4107	2130	2130	4166	2680
R2l	1126	999	999	16189	2913
U2r	52	52	52	228	215
All	494021	145585	30000	311029	77287

Tableau 06: Répartition des attaques et du comportement normal dans le KDD'99 10%.

Avant d'expliquer les différentes étapes de notre modelé, nous avons tendance à expliquer les mesures de performance utilisées dans notre approche. On se base sur la matrice de confusion, qui représente le nombre d'instances correctement classées est le nombre d'instances incorrectement classées. Le tableau 07 montre notre matrice de confusion.

		La classe prédite	
		Negative (Normal)	Positive (Attaque)
La classe actual	Negative (Normal)	VN	FP
	Positive (Attaque)	FN	VP

Tableau 07: La matrice de confusion.

Vrai Positive VP : est la classification correcte de la classe positive d'attaque.

Vrai Négative VN : est la classification correcte de la classe négative (normale).

Faux Positive FP : est la mauvaise classification d'une classe négative normale comme une classe positive d'attaque.

Faux Négative FN : est la mauvaise classification de la classe positive (d'attaque) comme une classe négative normale.

Dans notre cas, nous avons basé sur le taux l'exactitude et DR et le FAR comme mesure de performance pour évaluer notre résultat.

$$\text{Le Taux d'exactitude} = \frac{VP + VN}{VP + VN + FP + FN}$$

$$\text{Le Taux de Detection (DR)} = \frac{VP}{VP + FN}$$

$$\text{Le Taux de Fausse Alarme (FAR)} = \frac{FP}{VN + FP}$$

2.3 Les différentes étapes de construction de notre modèle

Notre solution proposée se présente en 2 niveaux majeurs.

2.3.1 Le premier niveau

À ce niveau, nous avons réalisé une étude comparative des différents classificateurs dans le but de sélectionner les meilleurs classificateurs ainsi que la préparation d'un nouvel ensemble de donnée d'entrer pour le deuxième niveau.

2.3.1.1 Etude comparative des classificateurs du premier niveau

Afin de choisir les meilleurs classificateurs du premier niveau, nous avons réalisé deux types de comparaison.

En premier lieu, nous avons effectué une série d'expériences sur les six classificateurs suivants: Simple Cart (SC) ,Decision Tree (J48),Naive Bayes (NB),Randon Forest (RF), Best First Tree (BFTree),RandonTree(RT).D'où chaque classificateur donne ses prédictions pour les cinq catégories de connexion, où nous avons utilisé l'ensemble d'apprentissage KDD99 et l'ensemble de tests KDD99 détaillé dans le tableau 06. Par la suite, nous avons effectué une comparaison sur les résultats de ces expérimentations selon le meilleur DR le meilleur taux d'exactitude et le FAR le plus bas possible.

Cette comparaison fondée sur l'optimalité de PARETO qui représente un puissant outil d'analyse et d'aide a la décision, l'optimalité de PARETO a été introduit pour formuler des

recherches multicritères, ils permettent d'extraire l'ensemble des points les plus intéressants quand différents critères, souvent conflictuels, Elles s'appuient sur le principe de dominance de Pareto.

Ordre de Pareto : On souhaite comparer deux vecteur, V et U tel que V=(V1,..Vn),

U=(U1,…Un). L'ordre de Pareto est défini par la formule suivante :

$$V > Pareto\ U \leftrightarrow (\ \forall i\ vi \geq ui\ et\ \exists\ j\ vj > uj) \quad (14)$$

Exemple : Le tableau 08 résume les résultats d'expérience sur les six classificateurs candidats.

			Les mesures de performances		
			Taux de détection	**Taux d'exactitude**	**FAR**
Classificateurs	**Naive Bayes(NB)**	**V #1**	89,21909	92,685704	5 ,1887875
	Simple cart (SC)	**V #2**	**98,794935**	94,873653	7,5306297
	Random forest (RF)	**V #3**	94,28445	**95,294163**	**4,0867442**
	First Tree (BFTree)	**V #4**	98,788126	94,871065	7,5306297
	Decision Tree (DT)	**V #5**	93,263208	94,649812	4,5000104
	Random Tree(RT)	**V #6**	93,702342	94,783081	4,5542777

Tableau 08: Comparaison entre les classificateurs du premier niveau.

Soit la requête suivante qui consiste a trouvé les classificateurs avec le meilleur DR, le meilleur taux d'exactitude et le FAR le plus bas possible.

Le vecteur de score (v#2) ne peut pas être comparé aux autre vecteurs (v#1) et (v#3) et (v#5) et (v#6) . En utilisant l'ordre de Pareto le résultat est donné comme suite (v#2) >Pareto (v#4) mais (v#2) ne peut être compare ni a vecteurs (v#1) ni (v#3) ni (v#5) et ni (v#6).

Le vecteur de score (v#3) ne peut pas être comparé aux autre vecteurs (v#2) et (v#4) En utilisant l'ordre de Pareto le résultat est donné comme suite(v#3) >Pareto (v#1) et (v#3) >Pareto (v#5) et (v#3) >Pareto (v#6) mais (v#3) ne peut être compare ni a vecteurs v (#2) ni à v(#4)

Donc Le vecteur de score v(#2) et v(#3) sont incomparable, car (v#2) >Pareto (v#4) et (v#3) >Pareto (v#1) et (v#3) >Pareto (v#5) et (v#3) >Pareto (v#6).

Le classificateur SC et Le classificateur RF sont cependant incomparable, car SC et meilleur que RF au regard du taux de détection tandis que le RF est meilleur que SC au regard du taux d'exactitude et FAR.

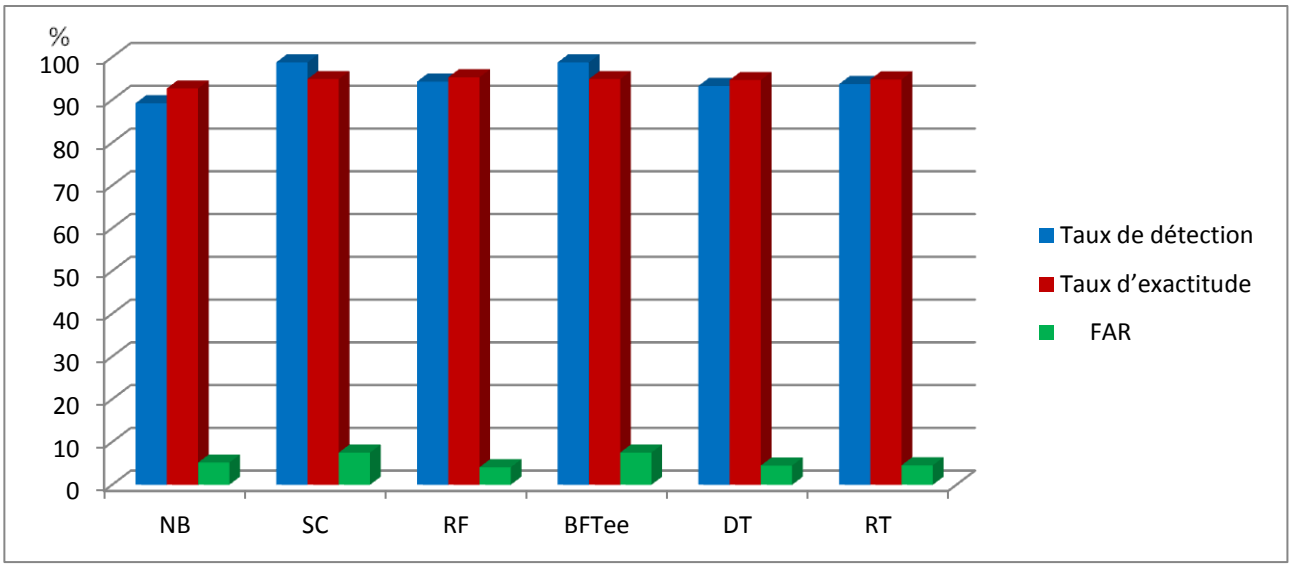

Figure 23 : Une comparaison entre les classificateurs du premier niveau.

En deuxième lieu, nous avons effectué une comparaison sur les classificateurs sélectionnais RF et le SC dans le but d'associé à chaque type de connexion le classificateur le plus approprié selon le meilleur taux de détection.

Le tableau 09 montre une étude comparative entre les deux classificateurs RF et le SC par rapport au DR.

		Random forests		**Simple Cart**	
		Attaque	**normal**	**Attaque**	**normal**
Normal		4,1	**95,9**	7,5	92,5
Attaque	**U2r**	**19,1**	80,9	13,5	86,5
	Dos	**94,9**	5,1	92,9	7,1
	R2l	37,8	62,2	**47,5**	52,5
	probe	63,9	36,1	**83,9**	16,1
All		94,3	5,7	98,8	1,2

Tableau 09: Comparaison entre Randon Forest et Simple Cart.

Compte tenu des résultats de tableau 09, nous remarquons que le SC et meilleur pour le type d'attaque probe et r2l et le classificateur RF et meilleur pour le type d'attaque Dos et u2r et pour le comportement normal.

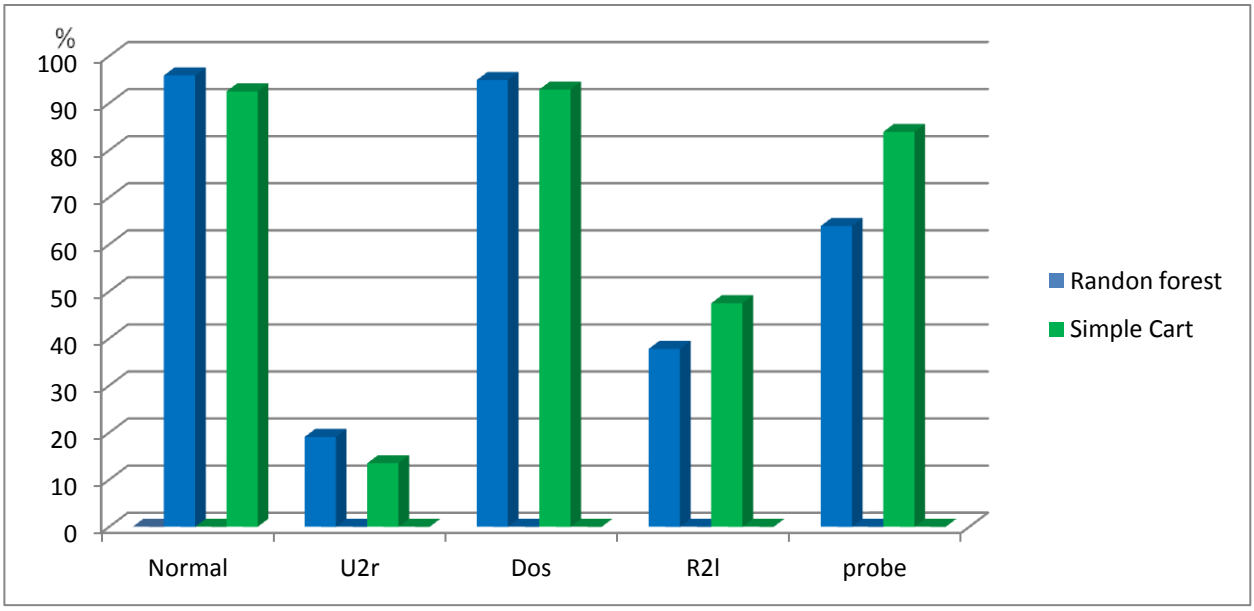

Figure 24 : Une comparaison entre Randon Forest et Simple Cart.

2.3.1.2 Formulation de nouvel ensemble de donné pour le deuxième niveau

Notre solution exhorte la fusion des attributs de l'ensemble de données test avec le classificateur et sa prédiction de sorte que chaque type de connexion fusionne le classificateur et la prédiction du classificateur approprié. Selon la phase de sélection de meilleurs classificateurs pour notre modèle. Enfin, nous gardons que les instances avec l'étiquette correcte.

Le tableau 10 montres la répartition des instances de nouvel ensemble de données d'entre de deuxièmes niveaux.

		Nouvel ensemble
Normal		**45401**
Attaque	**Dos**	**22367**
	Probe	**2249**
	R2l	**1384**
	U2r	**41**
All		**71442**

Tableau 10: Ensemble de données Test / Apprentissage pour le deuxième niveau**.**

Cette description et illustré dans l'exemple suivant :

Les lignes suivantes représentent un échantillon des instances de l'ensemble de tests.

31,tcp,ftp,SF,189,541,0,0,0,3,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,1,1,1,0,1,0,0,0,0,0,**u2r.**

0,tcp,ftp_data,SF,12,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,1,0,0,4,12,1,0,1,0.25,0,0,0,0,**r2l.**

0,icmp,eco_i,SF,18,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,1,27,1,0,1,1,0,0,0,0, **probe.**

0,icmp,ecr_i,SF,1032,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,510,510,0,0,0,0,1,0,0,255,255,1,0,1,0,0,0,0,0, **dos.**

0,tcp,http,SF,227,182,0,0,0,0,0,1,0,0,0,0,0,0,0,0,8,8,0,0,0,0,1,0,0,255,255,1,0,0,0,0,0,0,0, **normal.**

Le tableau suivant explique l'affectation des prédictions des classificateurs approprie sur ces instances.

Type de connexion	Le classificateur	La prédiction de classificateur
R2l	Simple Cart	La prédiction de Simple Cart
probe		La prédiction de Simple Cart
dos	Randon Forests	La prédiction de Randon Forests
U2r		La prédiction de Randon Forests
Normal		La prédiction de Randon Forests

Tableau 11: L'affectation des prédictions des classificateurs.

Les lignes suivantes représentent la structure de notre nouvel ensemble.

31,tcp,ftp,SF,189,541,0,0,0,3,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,1,1,1,0,1,0,0,0,0,0,**u2r,rf,u2r.**

0,tcp,ftp_data,SF,12,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0,0,0,0,1,0,0,4,12,1,0,1,0.25,0,0,0,0,**r2l,sc,r2l.**

0,icmp,eco_i,SF,18,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,1,27,1,0,1,1,0,0,0,0,**probe,sc,probe.**

0,icmp,ecr_i,SF,1032,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,510,510,0,0,0,0,1,0,0,255,255,1,0,1,0,0,0,0,0,**dos,rf,dos.**

0,tcp,http,SF,227,182,0,0,0,0,0,1,0,0,0,0,0,0,0,0,8,8,0,0,0,0,1,0,0,255,255,1,0,0,0,0,0,0,0,**normal,rf,normal.**

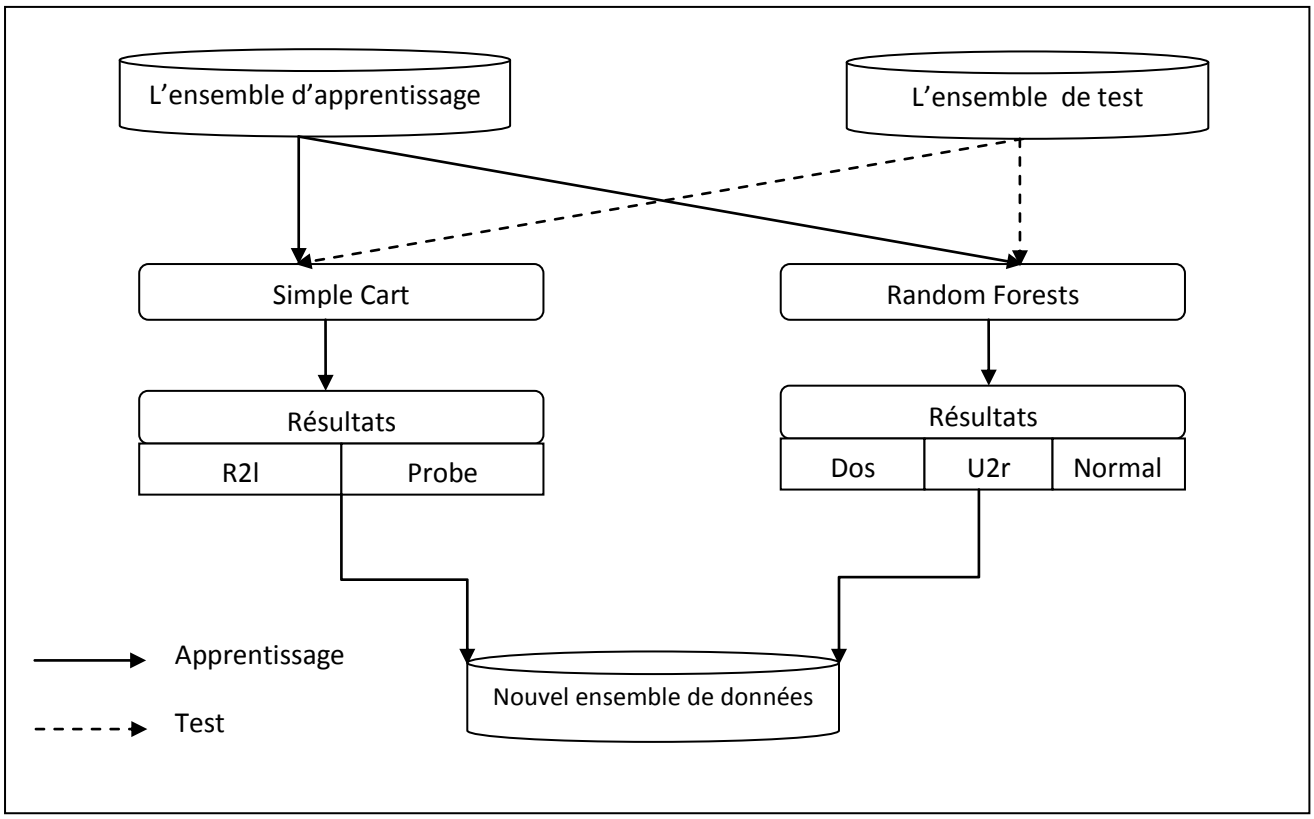

Figure 25 : La structure du premier niveau de notre modèle.

2.3.2 Le deuxième niveau

À ce niveau, nous avons réalisé une phase de prétraitement sur l'ensemble de données d'entrée, nous avons divisé le nouvel ensemble résultant du premier niveau en deux un ensemble pour l'apprentissage et l'autre pour le test. D'une façon qu'il existe des types de connexion seulement dans l'ensemble d'apprentissage et des types de connexion seulement dans le test et des types de connexion dans les deux ensembles d'apprentissage et test.

La figure 24 montre comment nous avons divisé le nouvel ensemble de donnée.

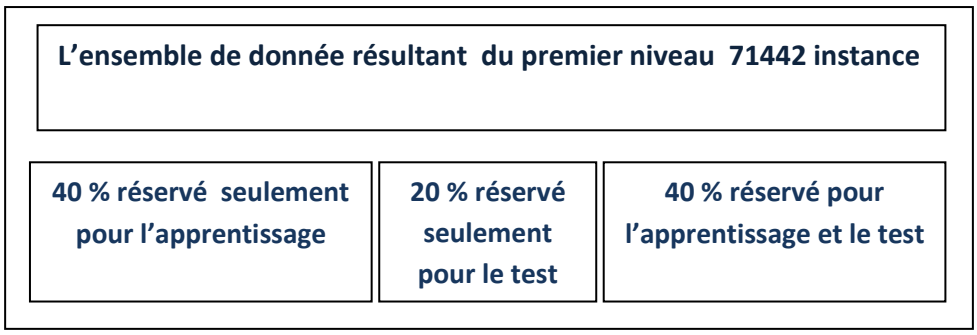

Figure 26: La divisons du nouvel ensemble de donnée

Le tableau 12 montre la composition de l'ensemble d'apprentissage et de l'ensemble de tests du deuxième niveau.

	Train		Test	
Normal	36321		27241	
Dos	17894	20833	13420	15624
Probe	1799		1349	
R2l	1107		830	
U2r	33		25	
All	57154		42865	

Tableau 12: Composition d'ensemble d'apprentissage et d'ensemble de test du 2 niveau.

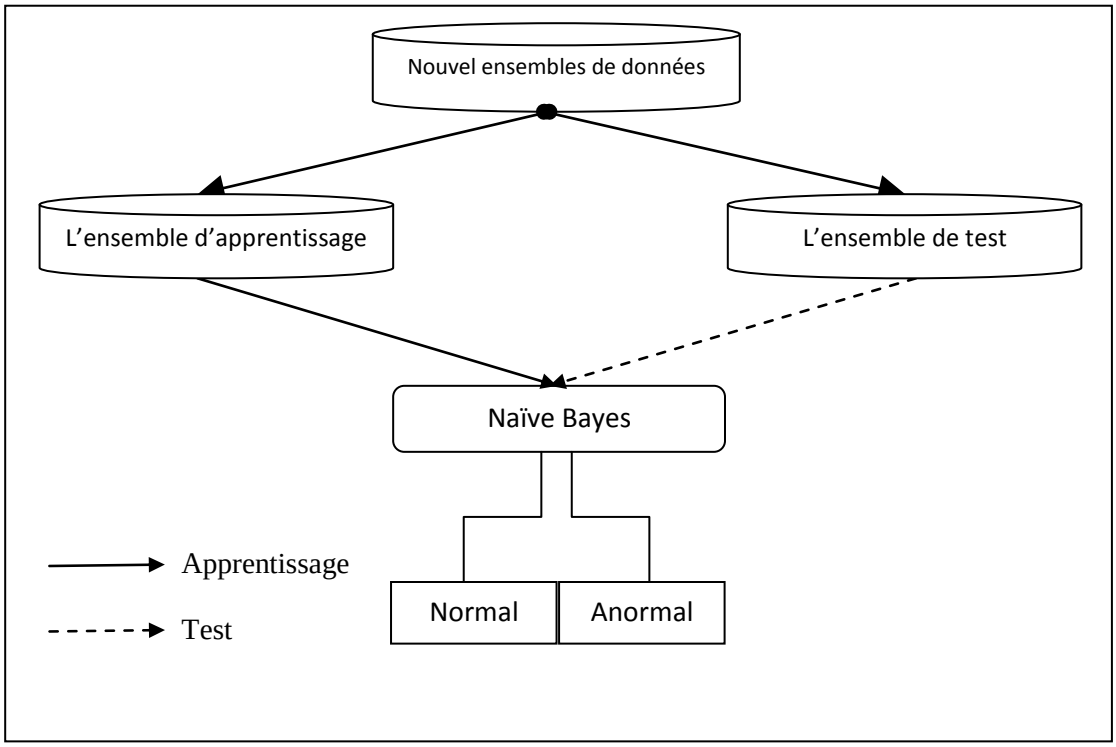

Figure 27: La Structure du deuxième niveau de notre modèle.

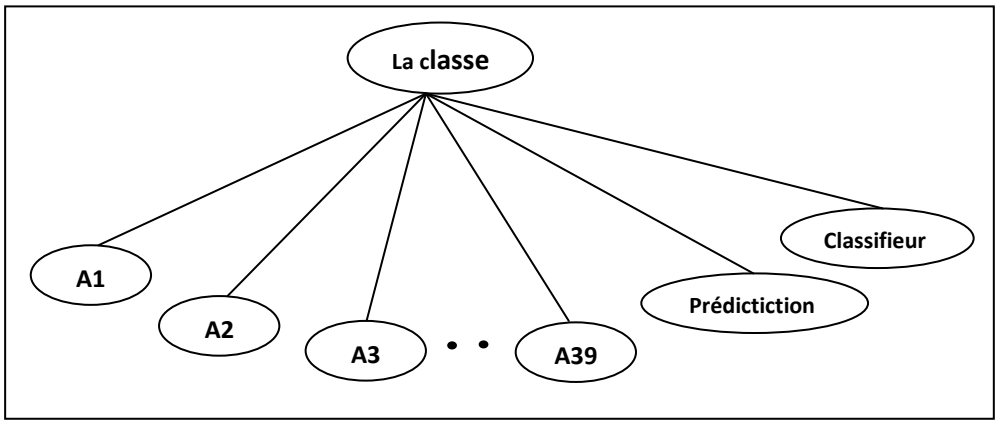

Figure 28: La structure de notre modèle naïve bayes.

Finalement pour évaluer notre approche nous avons affecté une comparaison entre les résultats de notre modèle et d'autres résultats bien connus tels que SC, RF, NB, et NFPHID [16], où nous utilisons les même ensemble d'apprentissage et de test que notre model. Le tableau ci-dessus montre les résultats de la comparaison de notre modèle et d'autre modèle.

		Notre modele		NFPHIDS		Simple Cart		Random forests		Naïve Bayes	
		Attaque	Normal	Attaque	Normal	Attaque	Normal	Attaque	Normal	Attaque	Normal
Normal		2,2	97,8	2,3	97,7	7,5	92,5	4,1	95,9	5,2	94,8
Attaque	U2r	100	0	92,2	7,8	13,5	86,5	19,1	80,9	23,7	763
	Dos	96,8	32	96,6	3,4	92,9	7,1	94,9	5,1	87,6	12,4
	R2l	93,5	65	42,3	57,7	47,5	52,5	37,8	62,2	5	95
	Probe	94,7	53	95,2	4,8	83,9	16,1	63,9	36,1	91,1	8,9
	All	95,5	45	94,1	5,9	98,8	1,2	94,3	5,7	89,2	10,8
DR		95,51971326		94,14836431		98,79493464		94,28444989		89,21909041	
FAR		2,213575126		2,268672496		7,530629709		4,086744171		5,188787544	
Exactitude		96,96022396		96,4252222		94,87365275		95,29416331		92,68570393	

Tableau 13: Comparaison de notre résultat par rapport à d'autres travaux connexes dans la DI.

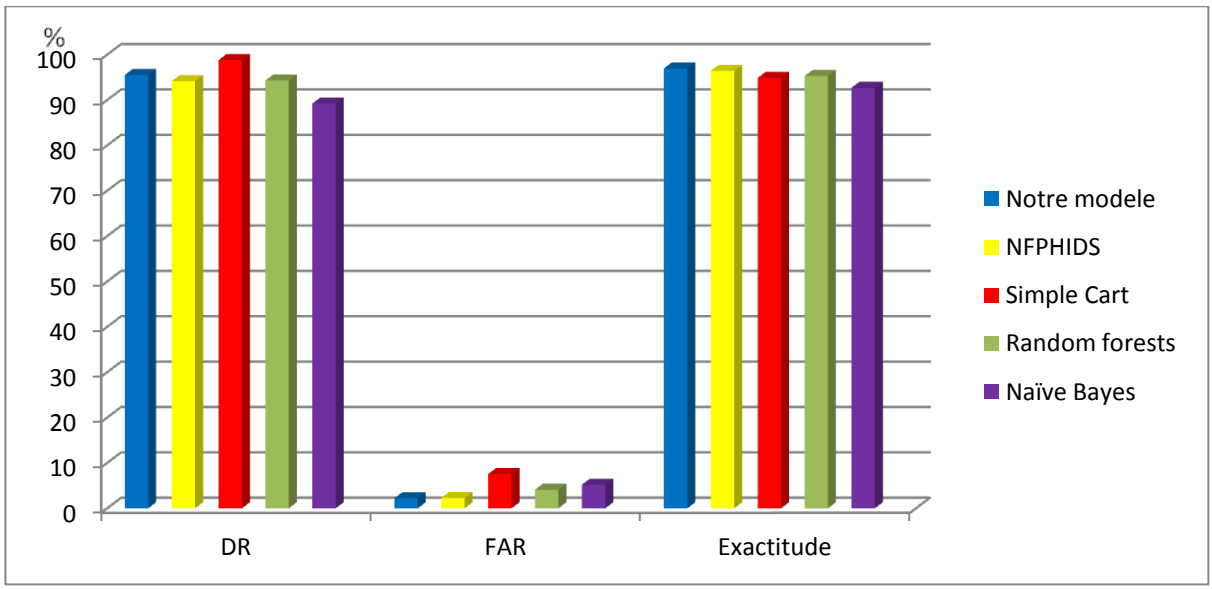

Figure 29: Une comparaison de notre résultat avec d'autres travaux.

Le graphique comparatif des résultats en figure 29 et le tableau 13 permet de souligner les remarques suivantes :

Les résultats obtenus après le calcul des différents critères d'évaluation à savoir le DR et le taux d'exactitude et le taux de fausse d'alarme donne l'avantage de notre solution proposée pour la détection d'intrusion par rapport aux algorithmes de classification RF et NB . En effet, notre approche augmente le taux de détection. Le pourcentage d'amélioration est de (1,24%) par rapport aux RF et de (6,3%) par rapport aux NB.

De même, on peut remarquer une amélioration par rapport aux taux d'exactitude estimée à (1,46%) pour RF de (2,8%) pour SC et de (4,28%) pour le NB.

De plus, l'approche proposée rendre le taux de fausse d'alarme très significatif par rapport au taux obtenu par l'application de RF et SC et NB , en effet, et dans ce cas un pourcentage de réduction (5,32%) est remarqué pour le SC, (1,87%) pour le RF et (2,97%) pour le NB. Afin de disposer non seulement d'une évaluation absolue, mais aussi d'une évaluation relative par comparaison à des solutions existantes dans la littérature, les résultats obtenus par notre approche ont été comparés avec NFPHID (Ahmim Ahmed) [16].

Les résultats du tableau 13 donne l'avantage de notre approche proposée par rapport à l'approche de NFPHIDS En effet, une amélioration de (1,37%) est remarquée pour le taux de détection, de même une légère amélioration de (0,05%) est signalée pour le taux de fausse d'alarme, et une amélioration de (0,54%) pour le taux d'exactitude, ceci est dû à l'intégration d'un classificateur dans un autre.

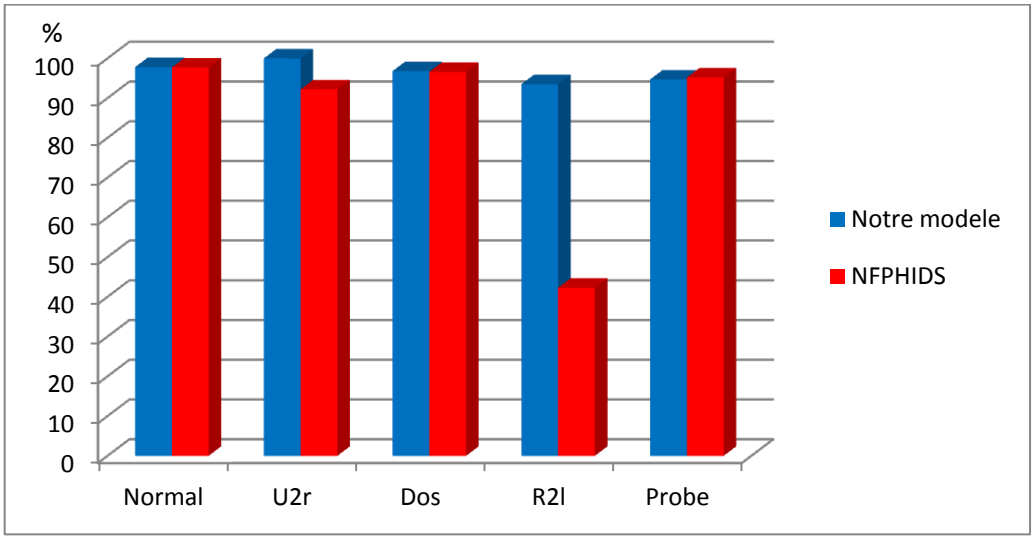

Figure 30: Une comparaison de notre résultat avec NFPHIDS.

Notons aussi que notre système a montré sa grande capacité de détection des attaques rares telles que R2l et U2R.

D'après le tableau 13 et la figure 30 on peut remarquer clairement que les résultats obtenus par notre approche sont meilleures que ceux produits par NFPHIDS.

Notre approche fait varier le taux de détection de comportement normale de (97,7%) à (97,8%) et de (96,6%) à (96,8%) pour les connexion Dos, de même pour les attaques rares de (42,3%) à (93,5%) pour les connexion R2l et de (92,2%) à (100%) pour les connexion U2R.

Conclusion

Dans ce chapitre, nous avons présentés une nouvelle approche pour la détection d'intrusion basée sur la fusion des prédictions résultant de deux différents classificateurs, on utilisant des techniques d'exploration de données y compris des arbres de décision, les prédictions des deux classificateurs sont intégrés dans un classificateurs bayésien naïf.

Notre approche donne des meilleurs résultats et augments les performances d'un IDS par rapport à certains travaux dans la littérature.

CHAPITRE V
Implémentation et réalisation

Introduction

Notre projet comprend une étude et une conception et développement d'un prototype pour un système de détection d'intrusion.

Dans le chapitre précédent, nous avons présenté notre approche de détection d'intrusion. Alors, dans cette section, nous présenterons la partie implémentation de notre prototype ainsi que l'environnement de développement et les technologies utilisées ensuite les principales interfaces qui le composent.

1. Environnement de développement

Notre prototype fonctionne selon l'environnement NetBeans et Weka.

1.1 Présentation de NetBeans

NetBeans IDE est un environnement de développement intégré gratuit qui vous permet de développer des applications bureautiques, mobiles et Web, il prend en charge le développement d'applications dans diverses langues, y compris Java, HTML5, PHP et C ++, comme il offre un support intégré pour le cycle de développement complet, de la création de projet ,gestion des projets, compilation, débogage de code source, profilage au déploiement.

Il comprend les caractéristiques de configuration et gestion de l'interface graphique, un éditeur de différents langages de programmation, traitement du code source (édition, navigation, formatage, inspection ..),fonctions d'import/export depuis et vers d'autres IDE ,accès et gestion de bases de données, fonctionnement sur différentes plates-formes : Windows, Linux, Solaris… etc.

Figure 31 : NetBeans.

1.2 Présentation de Weka

Weka environnement Waikato pour l'analyse de connaissances est une collection d'algorithmes d'apprentissage machine écrite en java pour les tâches d'exploration de données, ces algorithmes peuvent être appliqués directement à un jeu de données ou à partir de votre propre code java.

Weka est un logiciel open source libre développée à l'université de Waikato en Nouvelle-Zélande, délivré sous la Licence publique générale GNU. Il contient des outils pour le prétraitement des données, la classification, la régression, le regroupement, les règles d'association et la visualisation.

Figure 32: Weka.

2. Réalisations

Nous présentons dans ce qui suit notre prototype et un scénario d'utilisation de notre prototype pour vérifier le modèle obtenu, nous exécutons notre prototype, notre première interface est l'interface d'accueil comme on le voit dans la figure 32 , elle est composé de :

- Chargement : la ou on charge les connexions à tester.
- Simple cart et Random forest : l'utilisation de SC et RF sur la connexion choisie.
- New data : l'intégration de la prédiction et le classificateur dans la connexion choisie.
- Naive Bayes : l'utilisation de NaiveBayes sur la nouvelle connexion.
- Comparaison: pour comparer les résultats des déférents classificateurs.
- Testé un fragment : pour testé un fragment.
- Résumé : pour visualiser les prédictions des déférents classificateurs sur un fragment.
- Quitter : pour sortir du prototype.

Figure 33: Interface d'accueil.

L'interface suivante est l'interface chargement la ou on charge notre corpus de test (plusieurs connexions, certaines connexions normales et d'autres anormales (dos, r2l, u2r, probe)).

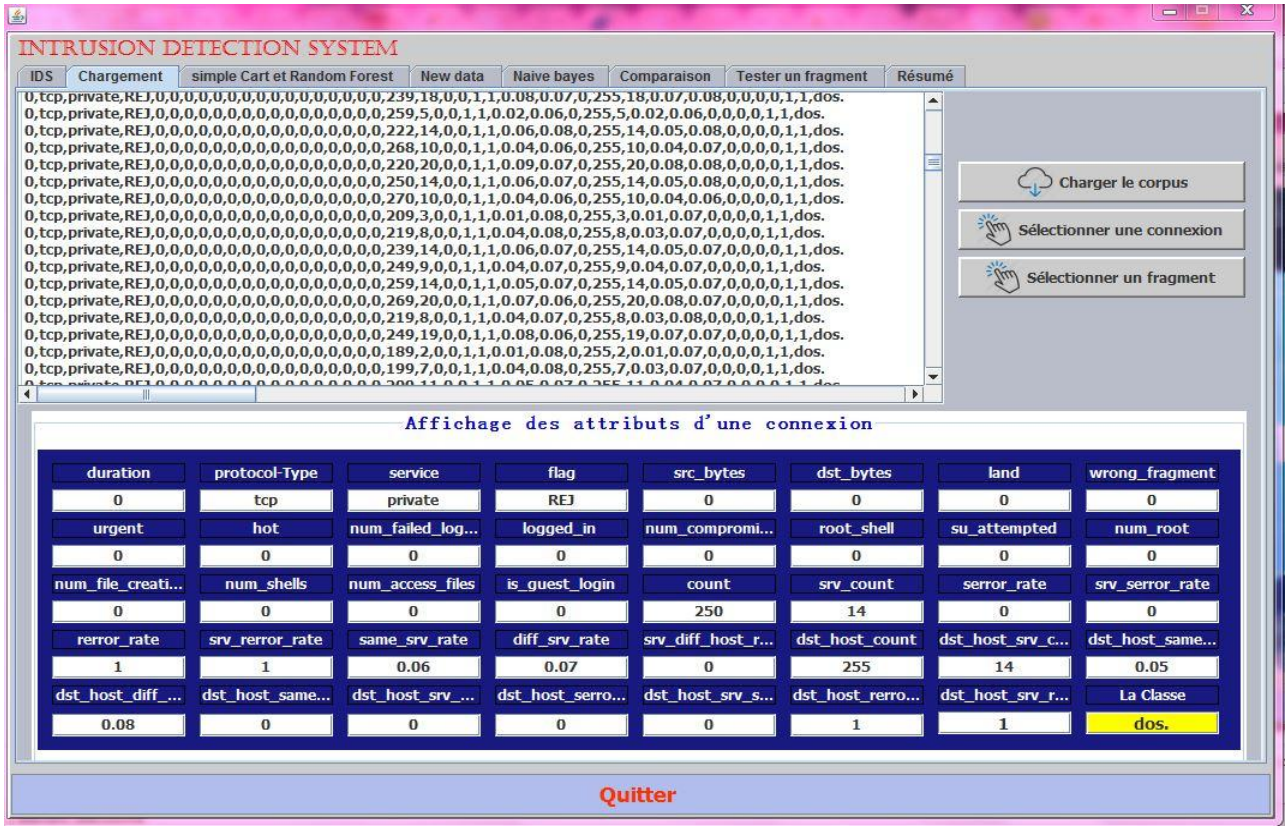

Figure 34: Interface chargement.

Une fois qu'on a choisi une connexion, on passe à L'interface suivante Simple cart et Random forests là où on fait l'appel de SC et RF à l'aide de weka et on donne en entrée la connexion choisie, et comme sortie en reçoit les prédictions des deux classificateurs sur la connexion d'entrée.

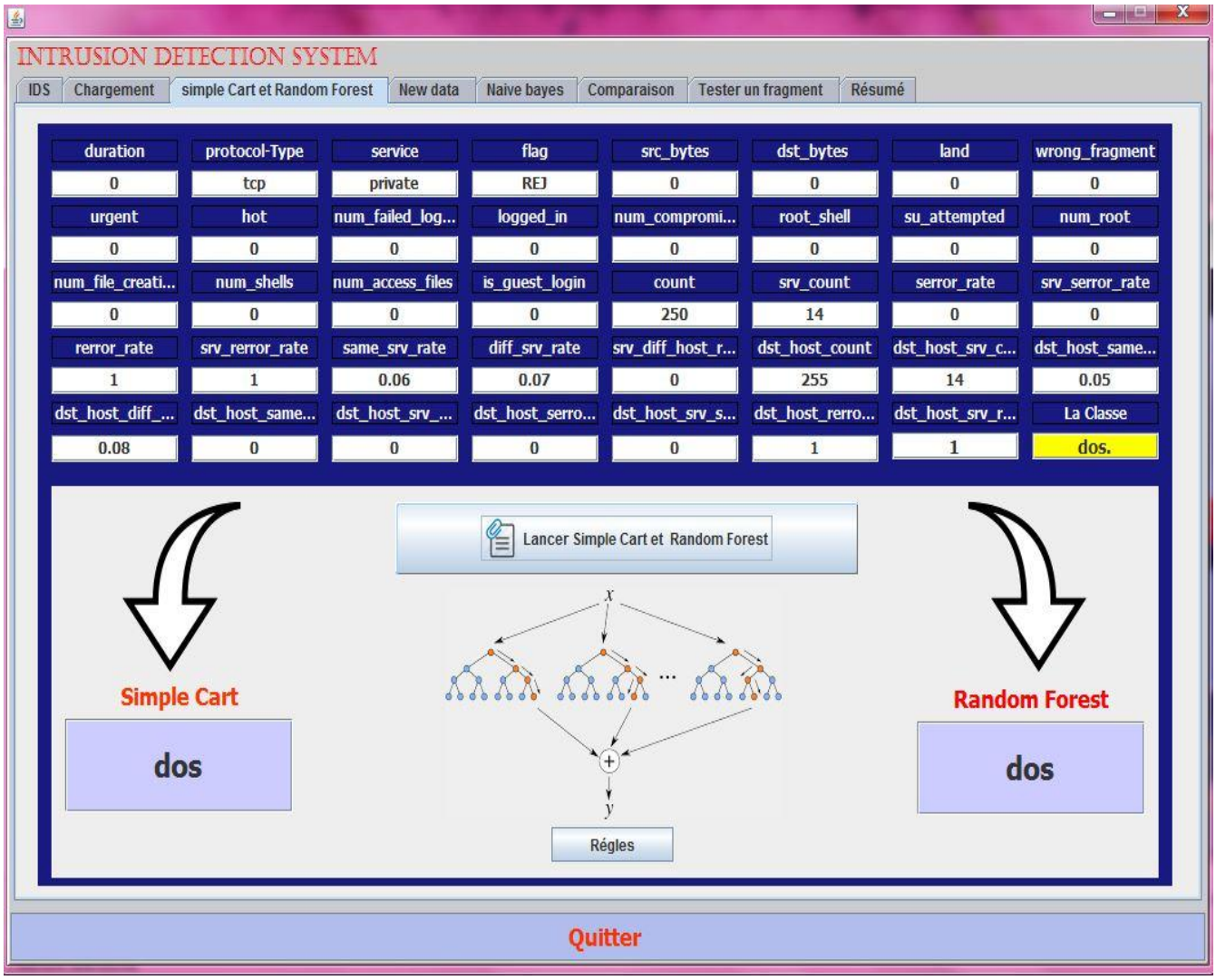

Figure 35: Interface Simple cart et Random Forests

L'étape suivante et l'étape de préparation de nouvel ensemble d'entrée pour notre approche qui représente d'intégration de la prédiction et le classificateur dans la connexion. Ce si est situé dans la figure 35.

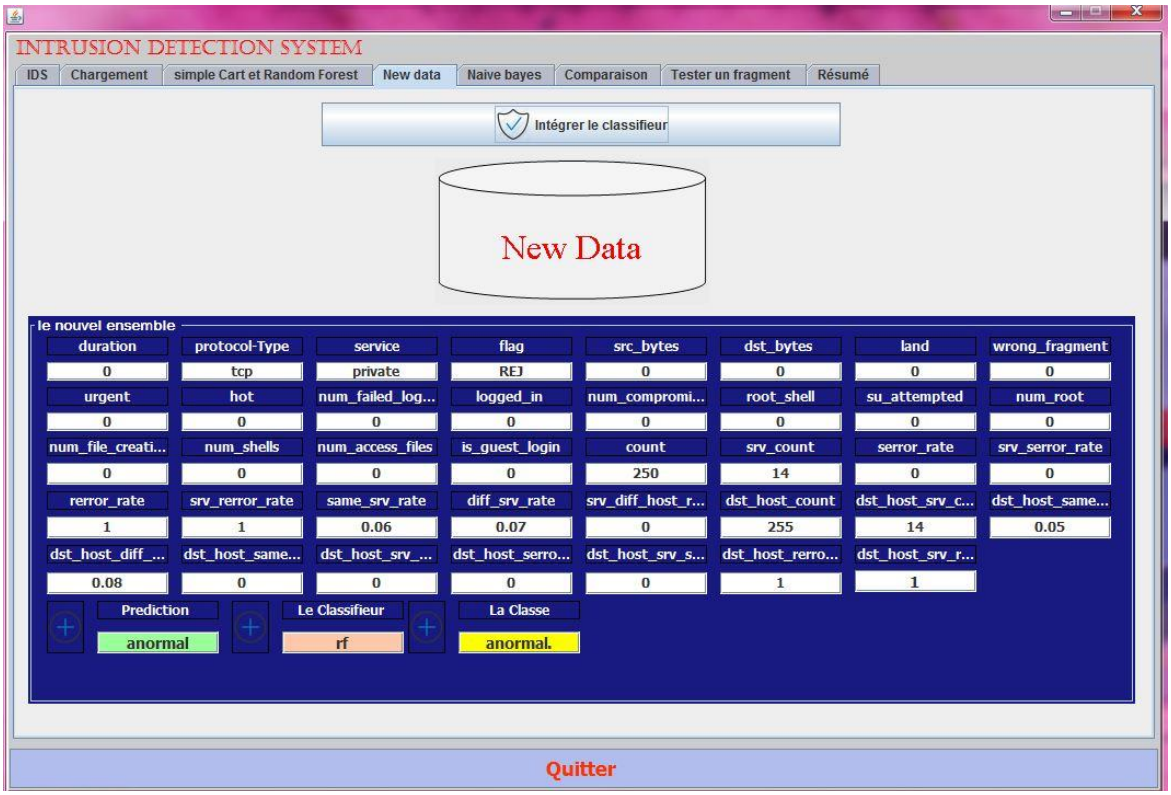

Figure 36: Interface New data.

Cette phase consiste à appliquer l'approche sur la nouvelle donnée, à ce niveau, la connexion et prête pour être testé par notre approche ce qui est présenté dans la figure 35. Notre approche qui se compose d'un réseau bayesien naif va donner sa décision finale sur la connexion soit un comportement normal, soit un comportement anormal.

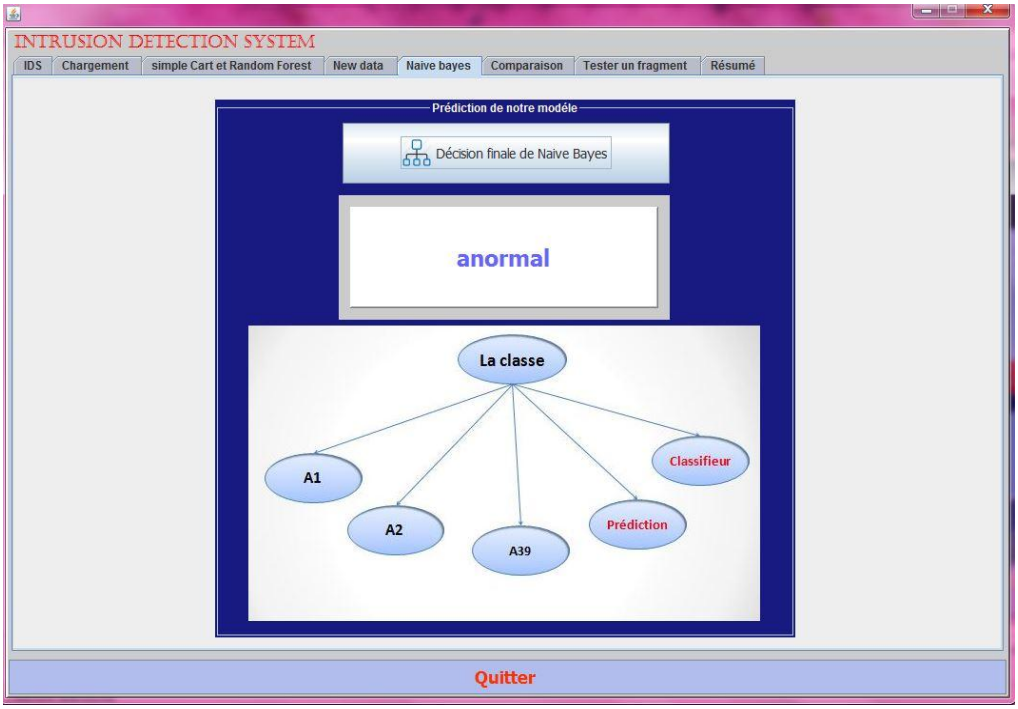

Figure 37: Interface Naive Bayes.

Finalement, la figure 37 représente une dernière interface pour comparer les résultats de notre approche et les résultats de SC et RF. On voit sur la figure la nature de la classe actuelle, la décision de SC, la décision de RF, et la décision de notre modèle.

Figure 38: Interface de comparaison.

Si on désire appliquer ce modèle et consulter les résultats sur un fragment de connexion, on utilise les interfaces Testé un fragment et Résume.

Figure 39: Interface Résumé.

Conclusion

Dans ce chapitre nous avons présenté en premier lieu les outils utilisés pour le développement de notre prototype qui implémente notre approche d'IDS, ensuite nous avons présenté les interfaces de notre prototype avec un exemple d'utilisation. Nous avons montré comment préparé les donné pour notre modèle, et en fin comment obtenir les décisions de notre modèle.

CONCLUSION

Conclusion générale

Dans le monde moderne, et cependant l'actualité présentée par l'évaluation technologique, L'univers des systèmes d'information est devenu un outil primordial qu'on utilise pour effectuer diverses activités comme le travail, l'étude, l'achat en ligne, la communication…ect, cette évaluation soufre des faiblesses qui menacent les informations qui transitent par internet et qui peuvent être importantes, critiques, secrètes et confidentielles.

Aujourd'hui, ces menaces ne se limitent plus aux grandes entreprises, toutes les sociétés sont concernées. Ils visent à se multiplier et devient plus complexe et sophistique et s'adapte a tout type de technologie donc le nombre de ces menaces est en constante progression et les conséquences lient à ses risques peuvent être fatales, il est donc indispensable pour les entreprises de constituer un moyen de se protéger par la préservation de (l'intégrité, la confidentialité et la disponibilité) de ces informations ou de minimiser les risques qui menacent ses ressources informatiques.

Une grande partie de l'intérêt des recherches actuelles porte sur la recherche des solutions pour les menaces polymorphes qui ne sont pas détectables et changent de variante régulièrement pour échapper à la solution a base de signatures.

Cependant, d'autre solution a été proposée à fin de traiter ces problèmes où la détection d'intrusion comportementale à été utilisé est devenue très indispensable et joue un rôle primordial pour la détection de toute activité anormale qui peut présenter un danger.

Malgré la puissance et l'efficacité de cette technique les systèmes de détection d'intrusion souffrent de certaines limites comme la nécessité de préparer les données d'apprentissage, le nombre de fausses alertes, la difficulté de détecter les nouvelles formes d'attaques… etc.

Les systèmes de détection d'intrusion hybride et hiérarchique sont proposés afin de traiter ces limites. De ce fait, nous avons proposé dans ce mémoire, un modèle hiérarchique basé sur deux niveaux, et hybride qui fait coopérer plusieurs classificateurs (simples cart et random forest) ,en intégrant un classificateur et sa prédiction dans un Réseaux Bayésien naif. Notre approche est illustrée en utilisant la base de données KDDcup99 qui est utilisée dans la plupart des travaux, notre approche à montrée sa capacité de minimiser le nombre des

fausses alarmes et augmenter les performances du système par rapport à d'autres travaux de recherche. Ce travail est donc une première approche sur la composition et la valorisation des IDS comportementale qui reste peu exploité en terme de commercialisations, et ce, malgré sa prolifération. À cet effet, ce travail s'inscrit dans les préconisations actuellement souhaitées en matière de recherche sur ce domaine de recherche très actif, intéressant, et défiant.
Comme complément à la présente étude, les points suivants nous semblent pertinents :

- Tester notre approche avec un ensemble de données plus récent.
- Améliorer l'approche et rendre le système adaptatif en détectant les nouvelles formes d'attaques.
- Utiliser d'autre critère de choix des classificateurs pour le premier niveau.
- Penser à sélectionner des attributs pertinents dans l'étape de sélection.

REFERENCES BIBLIOGRAPHIQUES

Bibliographie

[1] : Jean-François Carpentier. La sécurité informatique dans la petite entreprise. Etat de l'art et Bonnes Pratiques. Editions ENI, 3ième édition, 2009 ,265p.

[2] : Sarah Stéphanie .Contribution de l'audit interne a la sécurité de l'information en milieu bancaire .cas de ECOBANK cote d'ivoire. Mémoire de Fin d'Etudes. Centre Africain d'Etudes Supérieures en Gestion. 2011.

[3] : Rodrigue Mpyana. Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP. Cas de Mecelco.IUMM- Ingénieur. 2011.

[4] : Angeline Kone. Conception et déploiement d'une architecture réseau sécurisée : cas de SUPEMIR. SUPEMIR-Ingénieur. 2011.

[5] : Messavussu Adotevi Enyonam, Moumouni Mooussa Harouna. Les strategies de sécurité et système de protection contre les intrusions. Mémoire de recherche de L'ecole supérieure de Gestion d'informatique et des sciences et école supérieur de génie informatique (Graduate School of Management) Paris. Décembre 2008.

[6] : Laurent Bloch, Christophe Wolfhugel, Ary Kokos, Gérôme Billois, Arnaud Soullié, Alexandre Anzala Yamajako, Thomas Debize Préfaces de Christian Queinnec et Hervé Schauer. Avec la contribution de Nat Makarevitch. Ouvrage. Sécurité informatique pour les DSI, RSSI et administrateurs. Editions eyrolles (5 ème edition) .50p.

[8] : Aman-Vladimir .Ouvrage « Concevoir la Sécurité Informatique en Entreprise ».Penser des stratégies efficaces dans la mise en œuvre de la sécurité informatique dans les organisations .publié sous licence Créative Commons. 2014.

[9] : Jean-François Pillou. « Introduction à la sécurité informatique » issu de (www.commentcamarche.net). publié sous licence créative commons. Septembre 2015.

[11] : Karim Tamine, « Sécurité dans les réseaux ». Cours MASTER2 (recherche) Informatique- Décembre 2004.

[13] : Douglas Deschanel Tchana . Network access control avec packet fence. ISTDI – Licence Professionnelle.2012.

[14] : landry Ndjate . Mise en place d'un crypto système pour la sécurité des donnée et la détection d'intrusion dans un supermarché. Université Notre Dame du Kasayi - Graduat 2014.

[16] : Ahmim Ahmed. Système de Détection d'intrusion Adaptatif et distribué . Thèse de doctorat 3 ème cycle . Université badji mokhtar- annaba .2014

[17] : Hubal Pfumtchum .LA pratique de l'audit informatique dans les banques. Mémoire de fin d'études titre d'Ingénieur Maître MIAGE. Université de Douala .2004 -2005.

[19] : Rebiha Hadaoui. Un IDS basé sur un algorithme inspiré du fonctionnement de colonies des fourmis. Mémoire de magister. Université Mohamed Bougara de Boumerdes 2008-2009.

[23] : J Imene Safa, Anissa Zenati . Apports des fonctions de croyance dans les Systèmes de Détection d'Intrusion. Mémoire de fin d'étude. Université d'Ibn Khaldoun– Tiaret.Département Informatique. Spécialité : Génie informatique .2015-2016

[26] : Sonia Saidi. Apports des réseaux bayésiens dans les systèmes de détection d'intrusions. Mémoire de fin d'étude. Université d'Ibn Khaldoun –Tiaret .Département Informatique. Spécialité : Génie logiciel.2015-2016.

[27] : Hatem Bouzayani. Modèle quantitatif pour la détection d'intrusion. Une architecture collaborative IDS-HONEYPOT. Mémoire de Maîtrise. Université de Québec en Outaouais (UQO).

[28] : Tarek Abbes. Classification du trafic et optimisation des règles de filtrage pour la détection d'intrusions. Thèse de doctorat. Université Henri Poincaré. Nancy1.2004.

[29] : Yousef Farhaoui. Evaluation des Systèmes de Détection et de Prévention des Intrusions et la Conception d'un BiIDS. Thèse de doctorat. Université Ibn Zohr Agadir. 2012

[32] : Jabou Chaouki, Schillings Michaël , Hantach Anis. TER Détection d'anomalies sur le réseau . Université paris des cartes.2008-2009.

[33] : Ali Kartit. Une nouvelle approche de détection d'intrusions et étude des problèmes liés au déploiement de politiques de sécurité dans les réseaux informatiques. Thèse de doctorat. Université Mohamed V- AGDAL Faculté des sciences Rabat, Maroc.2011.

[34] : R. Heady, G. Luger, A. Maccabe et M. Sevilla, The architecture of a network level intrusion detection system, Aout 1990.

[35] H. Debar, M. Dacier, et A. Wespi. Towards a taxonomy of intrusion detection systems. Computer Networks, Elseiver, 1999.

[36] : Mimoun Imene. Détection d'intrusions par les réseaux Bayésiens. Memoire de fin d'étude .Université d'Ibn Khaldoun. Tiaret. 2012-2013.

[37] : Dorothy E. Denning ,An intrusion-detection model. IEEE Trans. Softw. Eng, Piscataway, NJ, USA, 13(2):222-232, 1987.

[38] : J. Anderson. Computer security threat monitoring and surveillance. Technical Report 56, Box 40 Fort Washington, pa. 19034, February 26, 1980.

[40] : Lynn Bogovich. Host-Based Intrusion Systems for Solaris. SANS Institute Reading Room. Interested in learning more about security. Version: 1.2f GSEC Practical Assignment.2002.

[43] : Forensics George Mohay. Alison Andeson. byron Collie Olivier de vel . rodney MsKemmish. Computer and Intrusion. Inc. artech house .boston .london.2003.

[50] : Akila Djebbar zaidi .Optimisation de la recherche d'un cas Bayésien. thése de doctorat. Université badji mokhtar –annaba .2013

[51] : Jimmy Vandel. Apprentissage de la structure de réseaux bayésiens. Application aux données de génétique-génomique. Thése de doctorat. Université Toulouse III - Paul Sabatier. 7 Décembre 2012.

[52] : David Bellot. Fusion de données avec des réseaux bayésiens pour la modélisation des systèmes dynamiques et son application en télémédecine. Thése de doctorat. Université Henri Poincaré - Nancy 1.26 Novembre 2002

[53] : Tayeb Kenaza. Modèles graphiques probabilistes pour la corrélation d'alertes en détection d'intrusions. Thése de doctorat. Université Houari Boumediene

[54] : J. Pearl. Probabilistic reasoning in intelligent systems : networks of plausible inference. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA,1988.

[55] : A. Darwiche. Modeling and Reasoning with Bayesian Networks. Cambridge.University Press, New Y ork, USA, 2009.

[56] : F.V. Jensen. Introduction to Bayesian networks. UCL Press, London, 1996.

[57] : Embarki miloud. Etude comparative entre réseaux bayésien et autre méthodes de classification appliqué sur une base cardiologue. Mémoire de fin d'études Master . Université Abou Bakr Belkaid– Tlemcen.2011-2012.

[58] : Salima Zeghdani. Modélisation de l'état d'un système de production sur la base d'une approche Bayésienne. Etude de cas : Entreprise COTITEX – BATNA. Mémoire de Magister. Université Hadj Lakhdar Batna.2014 – 2015.

[59] : Zied Elouedi. Réseaux bayésiens naïfs et arbres de décision. Article in Techniques et sciences informatiques.February.2006.

[60] : Fabien Moutarde. Arbres de décision et Forêts aléatoires, CAOR, MINES Paris Tech, PSL Fév.2017.

[61] : Que Tran. Improving Random Forest Algorithm through Automatic Programming. Master Halden, Norway. May 15, 2015.

[62] : Sushilkumar Kalmegh. Analysis of WEKA Data Mining Algorithm REPTree, Simple Cart and RandomTree for Classification of Indian News, Department of Computer Science, Sant Gadge Baba Amravati University Amravati, Maharashtra- 444602, India. IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 2, February 2015.

[66] : Groupe de travail de l'utilisation de techniques modernes en météorologie aéronautique le relevant de la Commission de météorologie aéronautique. « techniques d'interprétation des produits de prévision numérique du temps pour la météorologie aéronautique ». NOTE TECHNIQUE N° 195. Secretariat de "Organisation mereorologique moudiaIe - Geneve, Suisse 1994.p65

[67] : Alexandre Mornet. Contributions à l'évaluation des risques en assurance tempêté et automobile. Thèse de doctorat. Université Claude bernard lyon I. (L.S.F.A). 2006 .

[68] : Sujata Joshi, S. R. Priyanka Shetty. Performance Analysis of Different Classification Methods in Data Mining for Diabetes Dataset Using WEKA Tool. International Journal on Recent and Innovation Trends in Computing and Communication ISSN Volume:3 .2015.

[69] : Lamiche Chaabane. Fusion et fouille de donnees guidees par les : Application a l'analyse d'image. Thése de doctorat. Université Mohamed khider Biskra. 2013.

[70] : W. Siberski, U. Güntzer, W-T Balke. Restricting Skyline Sizes using Weak Pareto Dominance. Informatik – Forschung und Entwicklung manuscript. 2007.

[71] : I. Witten, E. Frank and M. Hall, "Data Mining: Practical Machine Learning Tools and Techniques", Elsevier Inc, 2011.

Webographie

[7] : https://www.doc-etudiant.fr/Informatique/Securite-des-systemes-informatiques/Cours-Audit-de-la-securite-de-linformation-9231.html, Consulté le 05/01/2017.

[10] : http://www.funinformatique.com/les-risques-informatiques/ Consulté le 11/02/2017.

[12] :http://cyberzoide.developpez.com/securite/methodes-analyse-risques/, Consulté le 15/02/2017.

[15]:https://www.securiteinfo.com/services/securite_informatique_quels_enjeux_pour_votre_entreprise.shtml., Consulté le 15/01/2017.

[18]:https://tpesecuriteinformatique.wordpress.com/les-differentes-attaques-informatiques/ Consulté le 17/02/2017.

[20]: https://support.kaspersky.com/fr/614, Consulté le 08/02/2017.

[21]: http://www.commentcamarche.net/contents/42-attaque-du-ping-de-la-mort,Consulté le 14/02/2017.

[22]: https://www.securiteinfo.com/divers/lexique.shtml, Consulté le 25/01/2017.

[24]:https://www.ibm.com/support/knowledgecenter/fr//SSB2MG_4.6.1/com.ibm.ips.doc/concepts/wap_injection_attacks.htm, Consulté le 14/02/2017.

[25]: https://linux.developpez.com/secubook/node42.php Consulté le 16/02/2017.

[30]: http://www-igm.univ-mlv.fr/~dr/XPOSE2001/liyun/IDS.html Consulté le 9/03/2017.

[31]: http://dbprog.developpez.com/securite/ids/#LIII-A, Consulté le 9/03/2017.

[39]:http://www.voxtechnologies.com/enterasys_files/pdf/overview-datasheet.pdf, Consulté le 10/02/2017

[41] : https://www.giac.org/paper/gsec/726/dragon-intrusion-detection-system/101614 [Global.Information.Assurance.Certification.Paper] Consulté le 10/02/2017

[42]: http://www.nongnu.org/tiger/ Consulté le 15/02/2017

[44]: https://www.snort.org/ Consulté le 09/04/2017

[44]: https://www.snort.org/ Consulté le 09/04/2017

[45]: https://korben.info/ids-windows-patriot.html Consulté le 09/04/2017

[46]: http://hank.sourceforge.net/docs/lwn.html Consulté le 09/04/2017

[47]: https://fr.wikipedia.org/wiki/Prelude_SIEM Consulté le 09/04/2017

[48]:http://www.scaramanga.co.uk/firestorm/,Consulté le 09/04/2017

[49]:https://www.ossir.org/sur/supports/2007/bro-ids-ossir-sur-16012007.pdf, Consulté le 19/04/2017

[63]: http://www.java2s.com/Code/Jar/w/Downloadweka370jar.htm Consulté le 22/05/2017

[64]:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[The KDD CUP 1999 Data] Consulté le 17/05/2017.

[65]: http://www.cs.waikato.ac.nz/ml/weka/ Consulté le 09/06/2017

ANNEXES

Annexe A : L'utilisation de weka 3.7.0

WEKA est un logiciel libre dédié au Data Mining, parmi les fonctionnalités qu'il couvre, on trouve les arbres de décision. Il permet de modéliser simplement, graphiquement et rapidement un phénomène mesuré plus ou moins complexe. Sa lisibilité, sa rapidité d'exécution et le peu d'hypothèses nécessaires à priori expliquent sa popularité actuelle. Il est écrit en java, disponible sur le web téléchargé à partir du site officiel de WEKA [65] pour le WEKA 3.7.0 disponible sur [63], et s'appuie sur le livre *Data Mining, practical machine learning tools and techniques* [71].

On peut utiliser WEKA à trois niveaux :

- Via l'interface graphique.
- Invoquer un algorithme sur la ligne de commande.
- Utiliser les classes définies dans ses propres programmes pour créer d'autres méthodes, implémenter d'autres algorithmes, comparer ou combiner plusieurs méthodes.

a) Installation

L'installation de WEKA est facile et rapide, Charger l'archive zip à partir du site de Weka puis d´ecompressez-le (les classes sont dans weka.jar et les sources dans weka-src.jar).

Après l'avoir lancé à partir du menu démarrer en cliquant sur weka 3.7.0, vous obtenez la fenêtre intitulée *Weka GUI Chooser* :

Figure 40: Weka GUI Chooser.

b) Préparation du fichier de données de Weka

Les formats de fichiers supportés par WEKA sont le CSV et le ARFF (Attribute-Relation File Format) Le plus utilisé sous WEKA. Pour convertir un fichier en format arff il faut passer par des outils ou un programme java qui fait cette conversion (Il y a même un convertisseur inclus dans Weka du format CSV vers le format ARFF).

c) L'utilisation de WEKA

On cliquant sur *Explorer* sur la première fenêtre apparue lors du lancement de WEKA. Une nouvelle fenêtre qui s'ouvre et présente six onglets :

- *Preprocess* : pour choisir un fichier, inspecter et préparer les données.
- *Classify* : pour choisir, appliquer et tester différents algorithmes de classification : là, il s'agit d'algorithmes de classification supervisée.
- *Cluster* : pour choisir, appliquer et tester les algorithmes de segmentation.
- *Associate* : pour appliquer l'algorithme de génération de règles d'association.
- *Select Attributes* : pour choisir les attributs les plus prometteurs.
- *Visualize* : pour afficher (en deux dimensions) certains attributs en fonctions d'autres.

Ensuite, cliquer sur Open file de l'onglet *Preprocess* .Dans la fenêtre qui s'ouvre choisir le type de fichier arff ou csv, et naviguer jusqu'à votre fichier et cliquer sur ouvrir. Vous aurez un aperçu du genre :

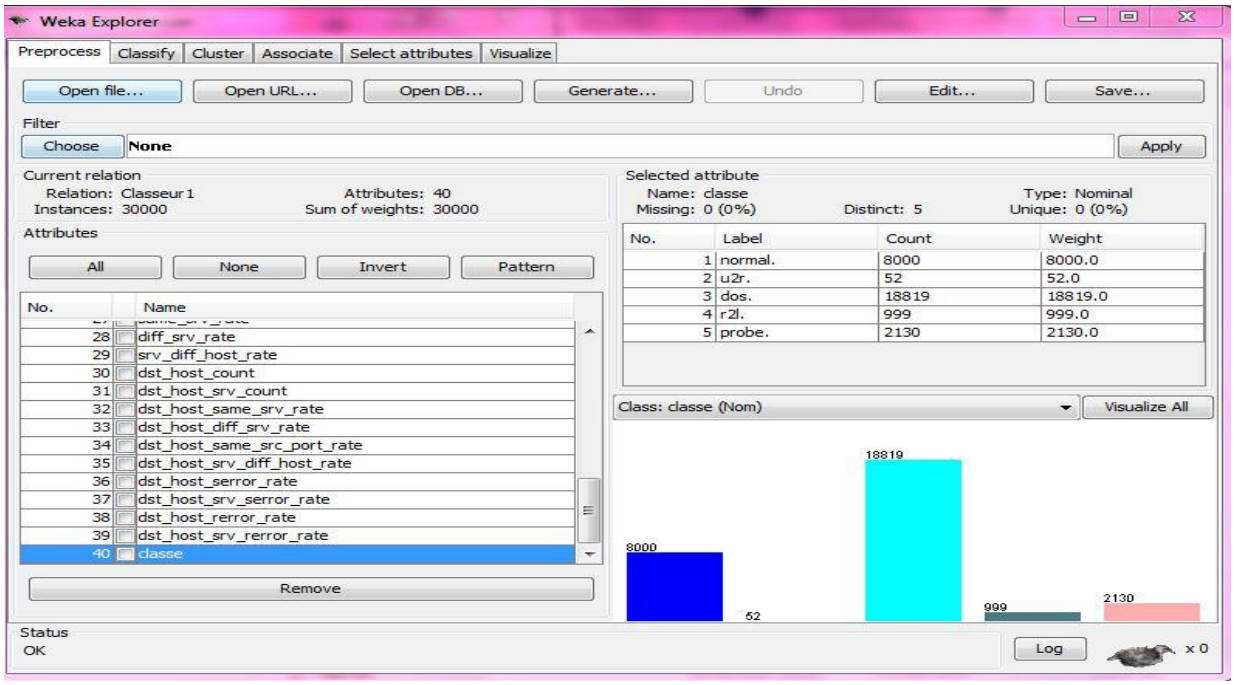

Figure 41: La fenêtre principale de l'explorer WEKA.

Cet aperçu comporte plusieurs parties. On y trouve :

La partie *Current relation* : qui montre :

- *Relation* : Le nom du fichier csv ou arff utilisé, dans ce cas c'est Classeur1.
- *Instances* : Le nombre d'instances du fichier, dans ce cas c'est 30000.
- *Attributes* : Le nombre d'attributs traités, dans ce cas c'est 40.

La partie Attributes : qui explicite les attributs figurant dans le fichier à traiter. L'utilisateur peut à tout moment cocher un attribut et cliquer sur le bouton *Remove* pour l'enlever de l'analyse.

La partie Selected attribute : qui donne des statistiques sur l'attribut sélectionné dans la partie Attributes (le nom de l'attribut, son type, nombre d'occurences distinctes,...).

d) La classification par WEKA

Cliquer sur l'onglet *Classify*, La zone *Test options* permet de choisir de quelle façon l'évaluation des performances du modèle appris se fera selon L'option *Use training set*, L'option *Supplied test set* ,l'option *Cross-validation* ,l'option *Percentage split.*

Ensuite, cliquer sur le bouton *Choose* pour choisir l'algorithme parmi ceux proposés par WEKA. Dans mon cas je vais utiliser l'algorithme NaiveBayes .Les résultats de classification sont présentés sur la figure suivante on cliquant sur « *Start* ».

Dans la partie *Classifier output* vous avez des statistiques sur le fichier exploité, à savoir le nombre d'instances de votre fichier, le nombre d'instances correctement classifiées et incorrectement classifiées et autres statistiques à découvrir. Sur le même écran on peut déduire la matrice de confusion.

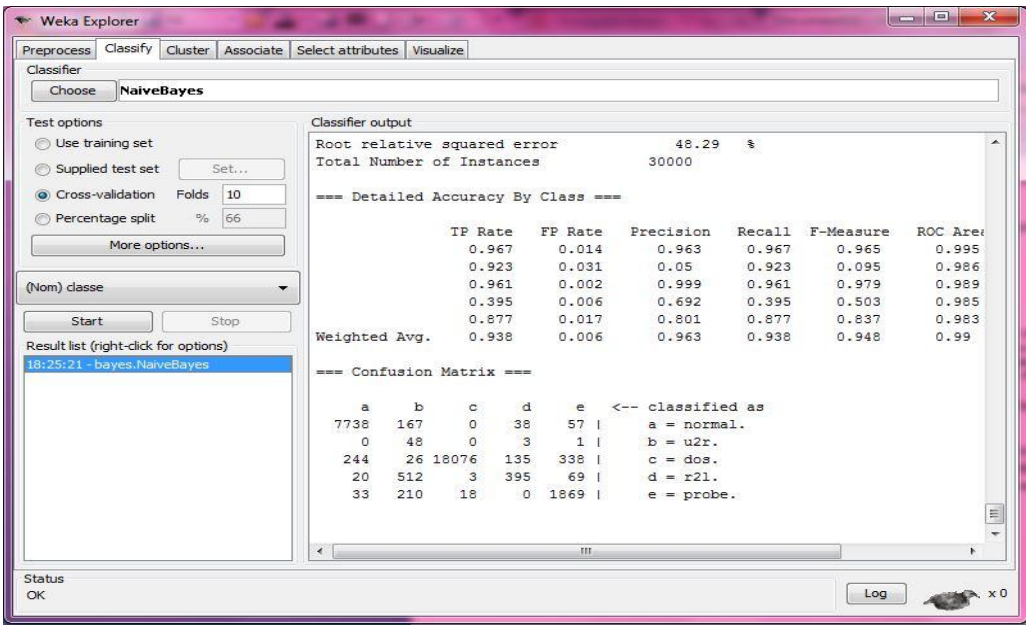

Figure 42: La fenêtre classifier output.

Résumé :

Au cours de ces dernières années, notre civilisation devient de plus en plus numérique et nous propose des formidables opportunités liées à l'usage des nouvelles technologies dans divers domaines, mais cette évaluation apporte avec elle son lot de risque. Une grande partie de l'intérêt des recherches actuelles porte sur la recherche des solutions pour se protéger face à ces risques et d'aboutir la sécurité des informations qui transitent par internet et qui peuvent être importantes, critiques, secrètes et confidentielles.Et comme tout système, l'internet contient des faiblesses, certains utilisateurs mal intentionnés peuvent exploiter les vulnérabilités d'internet pour essayer d'accéder à ces informations sensibles dans le but de les lire, les modifier ou les détruire. Des mécanismes de protection existent, mais il est souvent nécessaire d'ajouter à ces systèmes des mécanismes de détection d'intrusion afin de compléter les fonctions de sécurité. Dans la sécurité des systèmes d'information, les systèmes de détection d'intrusions (IDS) jouent un rôle primordial pour la détection de toute violation de la politique de sécurité. Cependant, les IDSs sont bien connus pour générer de grandes quantités d'alertes dont la plupart sont fausses et redondantes. Notre travail a visé à faire une étude sur le problème de la détection d'intrusion à base de modèles graphiques probabilistes (Réseaux bayésien naif) où nous avons considérer les systèmes de détection comportementale. L'idée est de faire coopérer plusieurs modules de détection, en intégrant un classificateur dans un Réseaux Bayésien naif. Donc la richesse de cette approche est de minimiser le nombre des fausses alarmes et augmenter les performances du système et de détecter les nouvelles attaques par excellence. Notre approche est illustrée en utilisant la base de données KDDcup99 qui est très connue et qui a montré de très bons résultants.

Mots-clés : IDS, Réseau bayésien naif, sécurité, approche comportementale,weka.

Abstract :

During the last years, our civilization became more and more digital and offers us of enormous opportunities in the use of the new technologies in diverse domains, but this evaluation brings its part of risk. The interest of the current search is to look for solutions to protect itself against these risks and to reassure the information security which passes by Internet and which can be important, critical, secret and confidential. And as any system, Internet contains weaknesses, certain hostile users can exploit the vulnerabilities of Internet to try to reach this sensitive information to read them, modify them or destroy them. Mechanisms of protection exist, but it is often necessary To add mechanisms of detection of intrusion to these systems to complete the functions of security. In the information system security, intrusion detection system (IDS) plays an essential role in the detection of any violation of the safety policy. However, the IDS is well known to generate big quantities of alerts, among which most are false and redundant. Our work aimed at making a study on the problem of the detection of intrusion based on probability graphic models (Bayesian networks) where we consider the systems of behavioral detection. The idea is to make cooperate several modules of detection by integrating a classifier into a naïve bayesian network. The wealth of this approach thus is to minimize the number of false alarms and to increase the performances of the system and to detect new archetypal attacks. Our approach is illustrated by using the database KDDcup99 which is very known and which presents very good results.

Keywords : IDS, bayesian network,security, behavioral approach,Weka.