Université Mohamed Khider Biskra

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département d'informatique

Thèse

Présentée pour l'obtention du diplôme de

docteur en sciences

par

Mourad Belhadj

Sécurité des réseaux informatiques basée sur la théorie de danger

---

Spécialité : Informatique

Soutenue le devant un jury composé de :

Président du jury	**Pr. Mohamed Chaouki Babahanini**	Université de Biskra
Rapporteur	**Pr. Foudil Cherif**	Université de Biskra
Examinateur	**Dr. Akram Zine Eddine Boukhamla**	Université de Ouargla
Examinateur	**Dr Amine Khaldi**	Université de Ouargla

ملخص

نظام المناعة الاصطناعي هو نوع فرعي من تعلم نظام الذكاء الاصطناعي بناءً على قواعد مستوحاة من أنظمة المناعة لدى الفقاريات. تعتمد هذه الخوارزميات عادةً على خصائص الجهاز المناعي عندما يتعلق الأمر بالتعلم والذاكرة واستخدامهما في حل المشكلات. تسعى لأنظمة المناعة الاصطناعية لتبسيط نشاط وبنية الجهاز المناعي من أجل إنشاء نماذج حاسوبية، واستخدام هذه النماذج لحل المشكلات الحسابية في مجالات الرياضيات والهندسة وتكنولوجيا المعلومات والاتصالات. هذه الأنظمة هي مجال فرعي من علم الأحياء المستوحاة والحوسبة الطبيعية، مع تقارب للتعلم الآلي وسياق أوسع للذكاء الاصطناعي. تعد خوارزمية الخلية الشجيرية مثالاً على خوارزمية تم تطويرها باستخدام نهج شامل. كان يعتمد على نموذج الخلية المتغصنة. يخضع لعملية فحص جوانب مختلفة من نشاط الخلايا التغصنية، من الشبكة الجزيئية الموجودة داخل الخلية إلى سلوك مجموعة الخلايا كمجموعة.

يتم تقديم وارزمية الخلية الشجيرية كخوارزمية مناعة اصطناعية جديدة. تتناول هذه الأطروحة التحدي المتمثل في تحسين مرحلة ما قبل المعالجة. في هذه الطريقة، تقلل خوارزمية الخلية التغصنية الأبعاد باستخدام طريقة تقليل الأبعاد: تحليل المصفوفة على أساس عامل المصفوفة غير السلبي. يقلل عامل المصفوفة غير السالب من حجم البيانات عن طريق تحويل البيانات الأصلية واستخراج الميزات المهمة من خلال المساحة الكامنة ذات الأبعاد المخفضة. تحدث الخوارزمية المقترحة في خطوتين: أولاً ، القيام بتحويل البيانات الأصلية عن طريق التحليل إلى عوامل غير سالبة. بينما يتمثل الثاني في تخصيص الفضاء المختزل لفئة الإشارة المناسبة لها. أظهرت النتائج التجريبية أن هذه الخوارزمية الجديدة تحسن بشكل كبير مرحلة المعالجة المسبقة لخوارزمية الخلية المتغصنة من حيث وقت التنفيذ مع الحفاظ على معدل دقة أعلى.

الكلمات المفتاحية: نظام المناعة الاصطناعي، خوارزمية الخلية الشجيرية، المرحلة القبلية، تحليل المصفوفة لعوامل غير سالبة

Abstract

Artificial immune system (AIS) is a subtype of learning artificial intelligence system based on rules inspired by vertebrate immune systems. The algorithms are usually based on the characteristics of the immune system when it comes to learning and memory and their use in problem solving. AIS strive to simplify the activity and structure of the immune system to create computer models, and use these models in favor of solving computational problems in the fields of mathematics, engineering and information and communication technologies. these systems are a subfield of biology inspired by biology and natural computing, with an affinity for machine learning and a broader context for artificial intelligence. The Dendritic Cell Algorithm (DCA) is an example of an algorithm developed using a comprehensive approach. It was based on a model of dendritic cell (DCs). DCA undergoes a process of examining various aspects of dendritic cell activity (DC), from the molecular network that is within the cell to the behavior of a cell group as a group.

DCA is presented as a new artificial immunity algorithm. This thesis addresses the challenge of improving the preprocessing phase. In this method, the dendritic cell algorithm reduces dimensionality using the dimensionality reduction method: matrix factorization based on non-negative matrix factorization. Non-negative matrix factorization reduces data size by transforming the original data and extracting important features through reduced dimensional latent space. The proposed algorithm takes place in two steps: First, transform the original data by factorization. While the second is to assign the reduced space characteristics to their appropriate signal category. The experimental results show that this new algorithm significantly improves the preprocessing phase of the dendritic cell algorithm in terms of execution time while maintaining a higher accuracy rate.

Keywords: Artificial immune system, Dendritic cell algorithm, Preprocessing phase, Non negatice matrix factorization.

Résumé

Le système immunitaire artificiel (AIS) est un sous-domaine de système de l'intelligence artificielle et d'apprentissage basé sur des règles inspirées du système immunitaire des vertébrés. Ces algorithmes sont généralement basés sur les caractéristiques du système immunitaire en ce qui concerne l'apprentissage et la mémoire ainsi que leur utilisation dans la résolution de problèmes. Un système immunitaire artificiel simplifie l'activité et la structure du système immunitaire pour créer des modèles informatiques et utilise ces modèles pour résoudre des problèmes dans les domaines des mathématiques, de l'ingénierie et des technologies de l'information et de la communication. ces systèmes sont aussi un sous-domaine de la biologie inspiré et de l'informatique naturelle, avec une affinité pour l'apprentissage automatique et un contexte plus large pour l'intelligence artificielle. L'algorithme des cellules dendritiques (DCA) est un exemple d'algorithme développé à l'aide d'une approche globale. Il était basé sur un modèle de cellule dendritique (CD). Le DCA subit un processus d'examen de divers aspects de l'activité des cellules dendritiques (DC), du réseau moléculaire qui se trouve dans la cellule au comportement d'un groupe de cellules en tant que groupe.

Le DCA est présenté comme un nouvel algorithme d'immunité artificielle. Cette thèse aborde le défi d'améliorer la phase de prétraitement. Dans cette méthode, l'algorithme des cellules dendritiques réduit la dimensionnalité à l'aide de la méthode de réduction de la dimensionnalité : factorisation matricielle basée sur une factorisation matricielle non négative. La factorisation matricielle non négative réduit la taille des données en transformant les données d'origine et en extrayant les caractéristiques importantes grâce à un espace latent dimensionnel réduit. L'algorithme proposé se déroule en deux étapes : Premièrement, transformer les données originales par factorisation. Alors que la seconde consiste à attribuer les caractéristiques d'espace réduit à leur catégorie de signal appropriée. Les résultats expérimentaux montrent que ce nouvel algorithme améliore significativement la phase de prétraitement de l'algorithme des cellules dendritiques en termes de temps d'exécution tout en maintenant un taux de précision plus élevé.

Mots-clé: Système immunitaire artificielle, Algorithme de cellule dendritique, phase de prétraitement, factorisation matricielle non négative

Remerciements

Je voudrais dans un premier temps remercier, mon directeur de thèse Pr. Foudil Cherif, professeur en informatique à l'université de Biskra, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à enrichir mes connaissances.

Je remercie également Pr. Mohamed Cheriet, Professeur en informatique et directeur de laboratoire Syncromedia à ETS, Université du Québec ainsi que tous les membres de ce laboratoire en particulier Pr. Rachid Hadjam pour ses précieux conseils et directions.

Je remercie profondément tout enseignant qui m'a bien encadré et soutenu pendant mes années d'études.

Un très grand merci, à M. Abdelhakim Cheriet pour son support et conseil, M. Khaled Djaber pour son encouragement, M. Abdellah Bensayah pour les précieuses discussions et suggestions, Pr. Mohamed Lamine Kherfi pour son aide ainsi que tous les collègues de l'université de Ouargla.

Sans oublier Pr. Ahmed Bouterfaia pour son support et encouragement qui m'a permis de progresser dans ce travail.

Je remercie également le président de jury Pr. Babahanini Mohamed Chaouki, ainsi que les membres du jury : Dr. Amine Khaldi et Dr. Akram Boukhalma qui ont accepté d'évaluer ce travail.

Je remercie aussi tous ceux qui ont contribué de prêt ou de loin à la réalisation à ce modeste travail.

A tous, Merci

Dédicace

Á ma mère et à mon père.
Á ma chère tente Zoulou.
A ma petite famille
Á mes frères et soeurs.

Table des matières

Table des figures

Liste des tableaux

*

Introduction

La révolution de l'outil informatique a permis de faciliter la vie de l'humanité, et de rendre les tâches qui étaient laborieuse dans le passé par des taches faciles à réaliser, cependant cet outil n'étant que le reflet des idées de l'être humain qui rend ses systèmes imparfaits même avec la prise de toutes les précautions possibles soit physique ou logique.

D'un autre Coté, l'utilisation d'internet se développe considérablement et devenue un point essentiel aussi bien que pour les particuliers que pour les entreprises afin d'étendre leurs activités et augmentent leurs productivités, la disponibilité d'internet à faible coût a permis de trouver virtuellement n'importe qui sur le réseau, cette facilité de manipulation a introduit un nouveau type de criminalité : cybercriminalité [56], qui se développe en exponentiel depuis la démocratisation du réseau internet [52].

L'information est un atout essentiel dans l'entreprise [67], à cet effet, on aperçoit que la sécurité est devenue une priorité fondamentale pour le bon fonctionnement d'un ordinateur en général, et particulièrement l'intégrité du réseau au sein de l'entreprise qui étend son activité à travers internet.

De plus, le développement accéléré de l'informatique laisse place à une autre technologie en parallèle qui est le piratage informatique, les grandes firmes commercialisent leurs produits et les pirates essayent toujours de contourner les mécanismes de protection et de la sécurité. Plus grave encore, les entreprises et les organisations qui manipulent des informations de hautes importances (domaine militaire, économique, énergétique ...) doivent toujours sécuriser ses données et mettre en évidence que ces derniers soient une cible potentiel à l'extérieur.

La détection d'intrusion est une problématique qui ne cesse d'exister qui prend une grande partie dans la sécurité informatique. Les technologies classiques qui étaient efficaces dans le passé deviennent inutile contre les attaques actuelles. Pour cela chaque système informatique doit avoir une politique de sécurité qui doit garantir la sécurité tout en respectant trois objectifs qui doivent être satisfaits :

— Confidentialité de l'information : Les données de l'organisme ne doivent pas être divulguées à des personnes non autorisées.
— Disponibilité des données : L'accès à l'information de l'entreprise par le personnel autorisé doit être garanti.
— Intégrité de l'information : La politique de sécurité doit garder l'intégrité de l'information.

Ainsi qu'apparaissent les systèmes de détection d'intrusion (en anglais IDS Intrusion Detection System) pour combler les manques identifiés dans la sécurité, mais malgré ces systèmes qui peuvent détecter les anomalies et les accès non autorisés, de nouvelles attaques apparaissent à chaque fois.

Plusieurs techniques ont été adoptées pour détecter les intrusions. La nature est parmi les inspirations pour traiter la sécurité en informatique, elle est le monde physique qui nous entoure en particulier et la vie en général. Elle a un potentiel immense à explorer, analyser et enquêter. En observant attentivement la nature, on peut déduire sa perfection, structuration et créativité. C'est en raison des caractéristiques attrayantes intrinsèques des systèmes biologiques que de nos jours, de nombreux chercheurs sont engagés dans la production de nouveaux paradigmes de conception pour relever les défis des différents systèmes comme les réseaux informatiques et les techniques de sécurité basées sur des systèmes biologiques. Les approches d'inspiration biologique semblent prometteuses lorsqu'un haut niveau de robustesse et d'adaptabilité est requis.

L'un des systèmes biologiques est le système immunitaire qui a une immense capacité de lutter contre les corps étrangers dans le corps. Il a deux couches protectrices, à savoir la couche innée et une couche adaptative, ce qui aide à faire face aux différents types d'attaques où la couche innée opère dans la peau, le mucus et dans les larmes, alors que la couche adaptative comprend des cellules B et des cellules T. De plus, il a une particularité intéressante de se souvenir des corps étrangers qui attaquent le corps humain. Cette fonction les aide à gagner du temps pour faire face aux intrusions.

En effet, Le système immunitaire est un système distribué, adaptatif, auto-organisé par nature, conserve la mémoire des expériences passées et a la capacité d'apprendre continuellement de nouvelles attaques. D'un point de vue informatique, le système immunitaire peut faire une révolution dans plusieurs domaines en prenant compte ses système comme une source d'inspiration. Ces dernières années, il y a eu un intérêt croissant pour l'utilisation du système immunitaire naturel appliqué pour la création de nouvelles solutions aux différents problèmes informatiques. Ce domaine de recherche est appelé Système Immunitaire Artificiel (AIS) [6].

Ce travail met en lumière le système immunitaire humain basé sur la théorie de danger (DCA Algorithme de cellules dendritiques). En outre, il explique comment l'utilisation de la réduction d'espace basé sur la factorisation matricielle peut aider à optimiser l'algorithme DCA original et réduire le temps de détection de ce dernier comparé aux travaux de l'état de l'art.

Le DCA est relativement un nouvel algorithme d'immunité artificielle. En tant que nouvel algorithme, davantage travaux doivent être effectués sur l'algorithme afin de vérifier ses propriétés et ses performances en tant que filtrage de données binaires. L'objectif principal de ce travail est d'étudier la faisabilité d'appliquer la réduction d'espace de données par la technique de réduction de d'intentionnalité en utilisant la factorisation matricielle non-négative sur la phase de prétraitement de l'algorithme DCA. Il s'agit d'améliorer les performances de cet algorithme, l'accessibilité ainsi que la précision du DCA aux futurs utilisateurs. Pour satisfaire cet objectif, un ensemble de contributions sont présentées dans cette thèse comme suit : Après une étude détaillée du comportement du DCA. Nous avons remarqué que l'algorithme a deux principales limitations critiques. La première limitation est liée à la phase de prétraitement des données DCA. La deuxième limitation est liée au temps d'exécution de l'algorithme par rapport à sa phase de prétraitement, c'est-à-dire que le DCA est conçu à être un algorithme léger. Afin d'obtenir une précision et performance satisfaisante ces deux lacunes et les solutions proposées sont mises en évidence dans la phase de prétraitement automatisées lors de l'étude de cette phase du DCA, nous avons remarqué que cette phase n'est pas robuste dans le cas où elle est basée sur l'utilisation de la technique d'analyse en composantes principales (ACP). En fait, l'application de l'ACP ne garantit pas que les premières composantes principales sélectionnées capturent la majeure partie de la variance sont les attributs les plus adéquats à retenir [20]. De plus, l'application de l'ACP détruit la signification sous-jacente des attributs présentes dans l'ensemble de données utilisés. Cependant, perdre la sémantique des fonctionnalités contredit le fondement du DCA car il est important de connaître la source (fonctionnalité) de chaque catégorie de signal en fonction de sa signification. L'utilisation d'autres techniques de sélection d'attributs comme réduction de dimensionnalité en utilisant la théorie des ensembles et la théorie de la logique floue [62] a permis d'améliorer la précision de filtrage de l'algorithme DCA, cependant, le temps de traitement de cette solution rend l'algorithme trop long et le rend dans certain cas paralysé face à la taille importante de données. Par conséquent, nous nous concentrons sur l'étude de la phase de prétraitement des données DCA tout en proposant de nouvelle

technique de prétraitement automatisés robustes. Pour ce faire, nous utilisons la factorisation matricielle non négative comme technique d'extraction d'attributs puissantes dans la phase de prétraitement des données DCA.

Cette thèse est structurée comme suit : L'état de l'art détaillant les définitions, concepts et aspects théoriques de cette étude.

1. Chapitre 1 : Dans ce chapitre, une brève définition des systèmes de détection d'intrusion avec les différentes techniques utilisées dans ce domaine et les domaines d'applications sont présentés
2. Chapitre 2 : Comme le système immunitaire est un système naturel détection d'anomalie et vu son efficacité, ce chapitre vise à éclairer les notions de base et les métriques utilisées pour évaluer de tels situations
3. Chapitre 3 : Liste les systèmes immunitaires artificiels et identifié les principales caractéristiques des systèmes immunitaires.
4. Chapitre 4 : Approfondi les définitions et points clés de l'algorithme DCA tout en mettant la lumière sur la théorie de danger qui est une théorie controversée dans l'immunologie.

Dans le chapitre 5, nous présentons la solution proposée basée sur la réduction de dimensionnalité par projection des données originales dans un espace réduit en utilisant la factorisation matricielle non-négative, cette solution combine la factorisation matricielle avec la réduction d'attributs en gardant la qualité des données originales. Enfin, notre thèse se termine par une conclusion et perspectives. La conclusion résume l'ensemble du travail présenté et propose d'autres travaux à réaliser avec l'algorithme des cellules dendritiques dans les futurs travaux de recherches.

Chapitre 1

Système de détection d'intrusion

Les systèmes de détection d'intrusion (IDS Intrusion détection system) sont soit un système logiciel dans la plupart des cas ou matériel qui permet d'automatiser le processus de la surveillance des événements qui se produisent dans un système d'ordinateur ou un réseau. Comme les attaques des réseaux informatiques ont augmenté d'une façon considérable avec des méthodes plus sévères l'utilisation des IDSs est devenue une nécessité obligatoire dans l'infrastructure de la sécurité dans les entreprises. Ce chapitre présente des définitions et des concepts qui sont en relation avec les IDSs, en des méthodes utilisées pour détecter les intrusions et enfin quelques technologies existantes en cours d'exploitation.

1 Définition d'un système de détection d'intrusion

La détection d'intrusion fait référence à un dispositif logiciel ou matériel qui automatise la surveillance et l'analyse d'un système ou d'un réseau afin de détecter des signes d'intrusion [8] il peut être un processus actif ou passif [73] qui permet de détecter le trafic indésirable sur un réseau ou un périphérique [94]. Une intrusion est définie comme une tentative de compromettre la confidentialité, la vie privée, l'intégrité et disponibilité des informations ou simplement contourner les politiques de sécurité dans un ordinateur ou dans un réseau. Les attaques sont effectuées par des utilisateurs qui ont accès de l'internet, des utilisateurs autorisés qui veulent acquérir plus de privilège non autorisé ou des utilisateurs qui exploitent mal leurs propres privilèges. Un groupe scientifique de la DARPA appelé IDWG (Intrusion Detection Working Group), travaillant sur les IDSs ont élaboré une architecture générale d'un IDS [39], la figure 1.1

Selon l'architecture proposée par [39], un IDS est composé de quatre types de

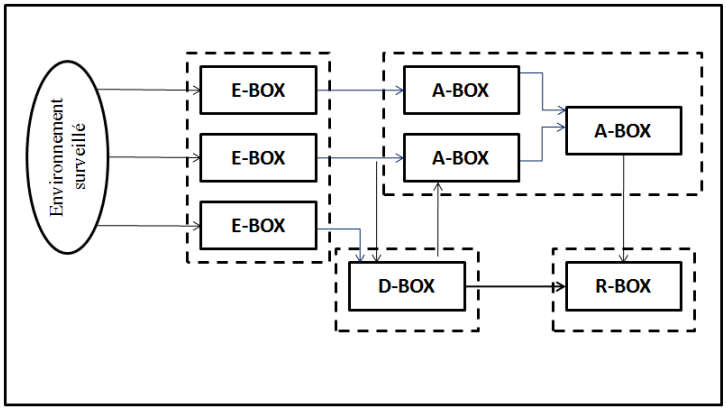

FIGURE 1.1 – Architecture générale d'un système de détection d'intrusion

composants fonctionnels :

- **E-box :** Bloc des événements : Ce type de bloc est composé de capteurs qui surveillent le système cible, et permet l'acquisition des informations sur les événements pour être analysé par autres blocs
- **D-box :** Bloc de base de données : comporte les éléments envoyés par E-BOX
- **R-box :** Bloc de réponse : Sa fonction principale est d'exécuter les procédures de contrattaque dans le cas d'intrusion
- **A-box :** Bloc d'analyse : Lance le processus d'analyse d'événement et génère une alerte dans le cas de détection d'un comportement hostile ou pour d'autre l'engagement d'un traitement spécial.

En plus de cette architecture, la définition d'un protocole d'échange d'informations entre les différents modules ce protocole est appelé IDXP (Intrusion Detection eXchange Protocole, RFC 4767) au format de données IDMEF, (Intrusion Detection MEssage Format, RFC 4765). La source d'information du bloc A dépend du type d'IDS basé hôte ou basé réseau, celui basé sur l'hôte les informations collectées (événements) sont par exemple les processus en cours, les programmes utilisés, nombre de fenêtres ouvertes, et celui basé sur le réseau les événements sont les adresses IP, la bande passante, les ports ouverts et les protocoles utilisés ... Le Bloc A procède selon la méthode de détection, il existe deux méthodes [18] : la première basée sur les anomalies (comportementale) alors que la deuxième basée sur la signature, ces deux approches seront expliquées dans les prochains paragraphes.

2 Objectifs des IDSs

Les IDSs ont imposé leurs existences au sein de l'infrastructure de sécurité, derrière ce puissant outil quelques caractéristiques que doit satisfaire et veille à ce qu'ils sont maintenus [8], on citera les points suivants :

- Détecter les intrusions et les violations d'accès qui ont contourné les autres dispositifs de sécurité
- Fournir des informations utiles pour les intrusions qui ont lieu pour mieux améliorer les nouvelles détections
- Prévention des problèmes de comportement, en améliorant les techniques de détections
- Détecter et traiter les attaques connues (comme les sondes réseau ou les explorations des audits)
- Agir comme un contrôle de qualité pour le système de sécurité et l'administration diagnostics, récupérer et corriger les failles.
- Enregistrer les menaces existantes dans une entreprise

3 Les faux négatifs et les faux positifs

Tel que les systèmes ont été conçus, on ne peut jamais trouver un système parfait, autant plus pour les IDSs à cause de la complexité du trafic réseau par exemple. Un IDS peut faire deux types d'erreurs, la première erreur qui est le **faux positif** qui consiste à signaler une intrusion qui n'est pas vraiment une intrusion, et la deuxième appelée **faux négatif** c'est de ne pas signaler une intrusion réelle. Ces deux types d'erreurs présentent un problème d'administration et la re-calibration du système est peut-être indispensable [94], un nombre important de faux négatifs qui sont générés, ce type d'alerte est généralement acceptable avec de lourdes tâches à faire par l'administrateur, cependant, les faux positives sont les plus dangereuses, elles ne dérangent pas l'administrateur mais elles menacent la sécurité.

4 Méthodes de détection d'intrusion

Les audits de sécurité ont été invoqués la première fois dans un rapport technique en 1980 [5], qui a fait une démonstration sur l'importance des audits dans un système de surveillance et du fait qu'il a défini les violations des politiques de sécurité, notre intérêt est l'attaque, en d'autres termes, les tentatives de violations qu'elles soient réussite ou pas. Donc la tâche d'un IDS est

de détecter ces tentatives et de prendre des contre-mesures si nécessaire. Les IDSs existants se basent sur deux méthodes qui sont :

4.1 Méthode de détection basée signature

Cette méthode repose sur le fait que les attaques connues sont traitées et éradiquées, c'est à dire que la connaissance des attaques est indispensable pour ce type de détection. La signature citée est vue comme un motif, si une attaque a une signature qui correspond à un motif présent dans l'IDS alors elle sera traitée, un IDS de ce type se compose de plusieurs modules :

- Les sondes : Dispositif qui permet de générer des événements qui seront analysés par d'autres modules, ça peut être une seule sonde ou plusieurs.
- Base de signature : Cette base contient les motifs des attaques existantes, ces signatures sont utilisées exactement pour la détection de virus, elles sont construites par des experts informatiques et basées sur les règles qui permettent d'identifier facilement les attaques et envoi une alarme dans le cas d'intrusion, quelques travaux dans la littérature [17] permettent la génération automatique des motifs avec un modèle formel. La Base de signature doit être maintenue à jour, en ajoutant les nouvelles attaques qui ont été signalées par les communautés et la suppression des signatures qui ne présente aucune menace (exemple : les mises à jour du système d'exploitation)
- Système de reconnaissance de motifs : ce module identifié le motif existant dans la base de motifs à partir du flux d'événement acquis, pour identifier une intrusion, plusieurs approches existent, l'une de ses techniques est de comparer les motifs identifiés en utilisant une simple approche ou une approche complexe (comparaison de chaîne de caractères, système expert ou modélisation des états).

Cette méthode est performante et a une pertinence de détection des attaques connues, en plus, ce système est facile à déployer. Une limitation évidente est l'incapacité de détecter les nouvelles attaques.

4.2 Méthode de détection basée comportement

Cette deuxième prend en considération les *profils* utilisateurs du système et de voir si c'est un comportement normal ou pas, ce concept a été étudié par [85]. Cette approche passe par deux étapes, une phase d'apprentissage et une autre d'analyse qui évalue la similarité du profil en cours par-rapport au profil dit normal. Néanmoins, L'hypothèse de changement de comporte-

ment n'est pas toujours valable, car il existe des comportements rares qui sont catégorisés à des anomalies alors qu'ils sont normaux et en conséquence la génération des faux positifs ce qui est acceptable dans le cas d'un nombre d'alerte raisonnable. Plusieurs techniques ont été utilisées pour la détection comportementale, parmi ces techniques : (Modèle statique, Système expert, réseaux de neurones et approche immunitaire). Cette approche permet par contre à la première de détecter les nouvelles attaques, puisque l'identification des intrusions est effectuée à partir d'un profil, et qu'une intrusion génère dans la plupart du temps une anomalie, ce qui permet de rendre ce type d'IDS fiable. Cependant, la détection basée comportement souffre de quelques points faibles, durant la phase d'apprentissage il faut bien s'assurer que le système surveillé ne comporte pas d'intrusion, dans le cas contraire, l'IDS met cette intrusion comme un comportement normal. Un deuxième problème se situe au niveau du profil normal, car ce dernier évolue dans le temps en conséquence la mise à jour d'IDS doit être assuré et donc ce système de détection doit apprendre au cours du temps l'évolution du profil.

5 Quelques technologies existantes

Les pirates utilisent plusieurs types d'attaques, certaines attaques utilisent les failles réseaux, d'autres les failles de programmation, c'est ainsi qu'il est nécessaire de connaître tous les types d'attaques existantes en plus de leurs techniques, un résultat évident de cet acte la diversité des IDSs, le paragraphe suivant expose quelques technologies de détection d'intrusion, il existe d'autres qui n'ont pas été cités.

5.1 L'IDS réseaux NIDS

Network intrusion detection system (NIDS) permet d'analyser le trafic réseau sur toutes les couches du modèle OSI et prend la décision concernant les activités malicieuses, la plupart des NIDS sont faciles à déployer dans le réseau et peut être surveiller depuis plusieurs systèmes en même temps. Un autre terme est nouvellement utilisé est WIDS (Wifi intrusion detection system) qui décrit un dispositif réseau qui permet d'analyser un réseau sans fil pour intrusion et prend des contre-mesures.

5.2 L'IDS basés sur l'hôte HIDS

Hybrid intrusion detection system (HIDS), cet IDS s'intéresse aux machines connectées au réseau, il permet de surveiller tout l'ensemble (ou une partie) des comportements dynamiques et l'état d'une machine, un HIDS permet de savoir si un programme utilise les bonnes ressources ou pas, par exemple un logiciel de traitement de texte soudainement sans explication commence à modifier le mot de passe d'une base de données. Il existe plusieurs techniques pour localiser les anomalies, parmi ces techniques :

Comportement des utilisateurs : Chaque utilisateur a un profil d'utilisation de sa machine (horaire d'utilisation, programmes utilisés, exploration des fichiers...) si le profil en cours ne correspond pas alors ça peut être un risque d'intrusion.

Comportement des programmes : Il permet de contrôler les accès aux ressources ou autres programmes et de signaler les accès non autorisés.

L'état des ressources et du système : On peut détecter des anomalies à partir des ressources utilisées [94, 18], le nombre de fenêtre ouvertes [85], fichier journal, processus en cours, fichiers utilisés ...

5.3 WIDS

Ce système de détection ressemble à NIDS, sauf que celui-là ajoute une analyse du trafic sans fil incluant les utilisateurs qui essayent de se connecter à un point d'accès [57], ainsi les attaques visant le réseau sans fil sont traitées, et comme les réseaux informatiques supportent de plus en plus les réseaux sans fil dans différents points de topologies, les WIDS joueront un rôle plus important dans la sécurité des organismes.

5.4 Détection des anomalies de comportement dans le réseau

Cet IDS moniteur le réseau en temps réel et déclenche une alarme dans le cas d'une détection, il intègre l'analyseur de comportement réseau qui est un module de plus dans la sécurité que celui offert par les firewalls ou d'autres outils, il utilise différents critères pour le comportement du réseau, comme par exemple : le volume du trafic, la bande passante et l'utilisation des protocoles...

6 Conclusion

L'intrusion indésirable est un problème à l'échelle de l'industrie qui affecte la sûreté, la sécurité, la fiabilité des systèmes et la productivité. Le problème à ce sujet a été abordé avec une variété de techniques. Ces derniers traitent à la fois de la prévention et de la détection et incluent les systèmes de détection d'intrusion. Dans ce chapitre, on a cité les concepts de base de la détection et de la prévention d'intrusion appliquée dans le domaine informatique aussi bien que d'autres domaines. Les stratégies pour améliorer la détection des intrusions emploient invariablement une combinaison de mesures. La probabilité de succès de la mise en œuvre de toute stratégie liée à la sécurité est augmentée lorsqu'elle est abordée avec la même discipline associée à un projet. Une telle discipline garantira un examen complet des problèmes et des alternatives.

Chapitre 2

Détection d'anomalie

La détection d'anomalie est l'identification de motifs dans des données qui ne sont pas conformes aux comportements attendus(normaux) [88]. Ces motifs sont souvent appelés anomalies, ou une autre appellation selon le domaine d'application. La détection d'anomalie trouve une utilisation étendue dans une grande variété d'applications telles que la détection de fraude pour les cartes de crédit, les assurances ou les soins de santé, la détection d'intrusion pour la cybersécurité, la détection de fautes dans les systèmes critiques de sécurité et la surveillance militaire des activités de l'ennemi. La détection d'anomalies est devenue un axe de recherche très important depuis l'automatisation de plusieurs processus.

La détection d'anomalies dans les données acquises par des capteurs, d'une image ou d'un signal est une tâche complexe qui fait intervenir d'autres domaines scientifiques comme les statistiques, machine learning, intelligence artificielle, etc. L'importance de la détection d'anomalies est due au fait que les anomalies dans les données se traduisent par des informations importantes et critiques pouvant être utilisées dans une grande variété de domaines d'application. Par exemple, le trafic anormal dans un réseau informatique est peut-être traduit par un ordinateur piraté qui transmet des informations confidentielles à une personne inconnue [96], Une image anormale d'IRM peut indiquer la présence de tumeurs malignes [38], une transaction de carte de crédit anormale est peut-être une fraude ou un vol d'identité [3] ou encore la lecture de données de capteurs peut-être une défaillance dans un composant dans une chaîne de production.

La détection d'anomalies dans les données a été étudiée dans la communauté des statistiques dès le $19^{éme}$ siècle [34]. Au fil du temps, diverses techniques de détection d'anomalie ont été développées dans plusieurs domaines de recherche. Beaucoup de ces techniques ont été spécifiquement développées

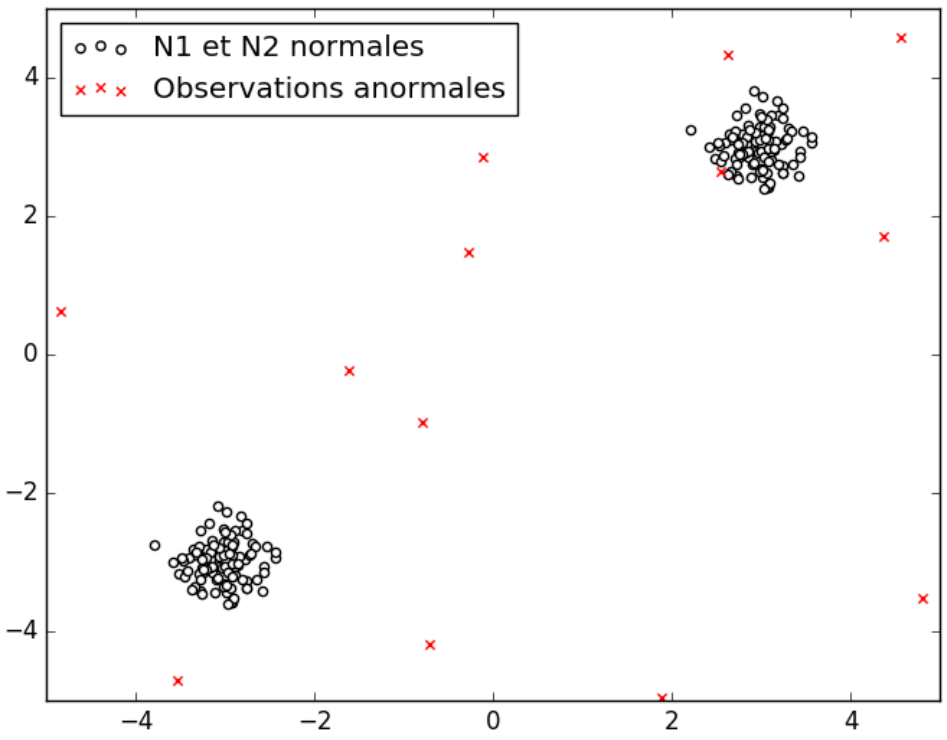

FIGURE 2.1 – Exemple d'anomalie

pour certains domaines d'application, tandis que d'autres sont plus génériques.

1 Notion d'anomalie

Les anomalies sont des motifs de données qui ne sont pas conformes à un comportement normal. La figure 2.1 illustre des anomalies dans un ensemble de simples données bidimensionnelles. Les données ont deux régions normales, $N1$ et $N2$, puisque la plupart des observations se situent dans le même nuage de ces deux régions. Les points qui sont éloignés des régions $N1$ et $N2$, les autres points (représentés par x) se distinguent par la distance entre le point et l'un des deux nuages $N1$ et $N2$, donc les points notés x sont considérés comme des anomalies. Les anomalies peuvent être induites dans les données pour diverses raisons, telles que les activités suspectes et malveillantes, par exemple, la fraude de carte de crédit, l'intrusion de réseau ou d'ordinateurs, les activités dans la télésurveillance ou la panne de système, mais toutes les raisons citées ont une caractéristique commune elles intéressent l'analyste. La curiosité dans la vie réelle des anomalies est un point clé de la détection des

anomalies [88].
Notant bien que la détection d'anomalies n'est pas un bruit, puisque le bruit est un phénomène dans les données qui alourdi l'analyste par le nettoyage de données que ce soit des données manquantes ou impertinentes. Un autre point essentiel qui concerne la détection de nouveau motif [74], définie comme une détection de nouveaux motifs émergeant dans les données, par exemple, l'apparition d'un nouveau phénomène climatique. La différence avec la détection d'anomalies est que les nouveaux motifs sont généralement classés comme des motifs normaux.

2 Problématique

Une des approches de détection d'anomalie consiste à définir une région de comportement normal et à déclarer une anomalie tout comportement hors cette région normale. Mais plusieurs facteurs rendent cette simple approche difficile à mettre en œuvre :

- La définition de comportement normal n'est pas évidente lorsqu'une action malveillante est manœuvré, car la personne malveillante adapte son action à un comportement normal.
- La définition exacte d'une anomalie change selon le domaine d'application et/ou l'environ, ainsi on ne peut pas appliquer une seule technique de détection d'anomalies sur plusieurs problèmes, par exemple, les fluctuations de la température corporelle pourrait être une anomalie, alors qu'une déviation similaire dans le domaine boursier pourrait être considérée comme normale.
- En général, les données contiennent du bruit qui tend à être similaire aux anomalies et donc il est difficile de les distinguer et de les supprimer.
- Dans de nombreux domaines, le comportement normal évolue dans le temps, ce qui insuffisant pour représenter le comportement normal.
- La définition d'une région normale qui englobe tous les comportements normaux possibles est très difficile voire impossible. En outre, la limite entre comportement normal et anormal est souvent imprécise. Ainsi, une observation anormale qui se rapproche de la normale peut effectivement être normale.

Vu l'importance des défis exposés précédemment, le problème de détection d'anomalie sous sa forme la plus générale n'est pas facile à résoudre. En fait, la plupart des techniques de détection d'anomalie existantes donne une solution spécifique à un problème bien défini. La solution est induite par divers

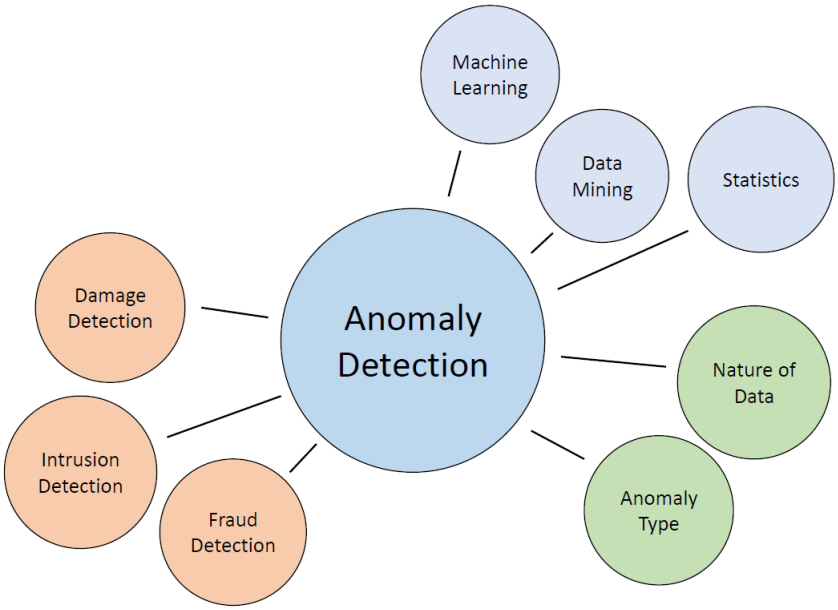

FIGURE 2.2 – Techniques de détection d'anomalies

facteurs tels que la nature des données, la disponibilité des étiquettes (données libellées), le type d'anomalies à détecter, etc. Souvent, ces facteurs sont déterminés selon le domaine d'application dans lequel les anomalies doivent être détectées. Les chercheurs ont adopté des concepts de diverses disciplines telles que les statistiques, machine learning, data mining, théorie de l'information, la théorie spectrale qui ont été appliqués à des problèmes spécifiques. La figure 2.2 montre les composants essentiels décrits ci-dessus associés à toute technique de détection d'anomalies.

3 Aspects de la détection d'anomalies

Comme mentionné précédemment, une formulation spécifique du problème est déterminée par plusieurs facteurs différents tels que la nature des données d'entrée, la disponibilité (ou l'indisponibilité) des étiquettes ainsi que les contraintes et les exigences induites par le domaine d'application.

3.1 Nature de données

La nature de données est un atout indéniable les techniques de détection d'anomalies. L'entrée est généralement une collection de données (vecteur). Chaque instance de données peut être décrite à l'aide d'un ensemble d'attributs ou variables. Les attributs peuvent être de différents types tels que binaire, symbolique ou continu. Les attributs peuvent être du même type ou peuvent

constituer un mélange de différents types de données.

La nature des attributs détermine l'applicabilité des techniques de détection d'anomalie. Par exemple, pour les techniques statistiques, différents modèles statistiques doivent être utilisés pour des données continues et symboliques. De même, pour les techniques basées sur le plus proche voisin, la nature des attributs déterminerait la mesure de distance à utiliser.

Les données d'entrée peuvent également être catégorisées en fonction de la relation présente entre les instances de données [14]. La plupart des techniques de détection d'anomalie existantes traitent des données d'enregistrement (ou des données ponctuelles), dans lesquelles aucune relation n'est prise en compte dans les instances de données.

En général, les instances de données peuvent être liées l'une à l'autre. Certains exemples sont des données séquentielles, des données spatiales et des données graphiques. Dans les données séquentielles, les instances de données sont ordonnées de manière linéaire, par exemple, des données de séries temporelles, des séquences génomiques, des équations protéiques. Dans les données spatiales, chaque instance de données est liée à ses instances voisines, par exemple, des données de circulation des véhicules, des données écologiques. Alors que les données spatiales comportent un composant temporel (séquentiel), elles sont appelées données spatio-temporelles, par exemple, des données climatiques. Dans les données graphiques, les instances de données sont représentées sous forme de sommets dans un graphique et sont connectées à d'autres sommets avec des bords.

3.2 Types d'anomalies

La nature de données définie la technique utilisée pour trouver les anomalies, ce qui conduit à la question : de quel type est cette anomalie ? ce qui argumente plus le choix de techniques à appliquer. On peut trouver trois catégories définies comme suit :

Anomalie ponctuelle

Si une instance de données individuelles peut être considérée anormale par rapport au reste des données, l'instance est appelée une anomalie ponctuelle. C'est l'anomalie la plus simple et fait l'objet de la majorité des recherches sur la détection des anomalies. Par exemple, dans la figure 2.1, les points X se situent en dehors de la limite des régions normales $N1$ $N2$ et, par conséquent, sont des anomalies ponctuelles puisqu'elles sont différentes des points

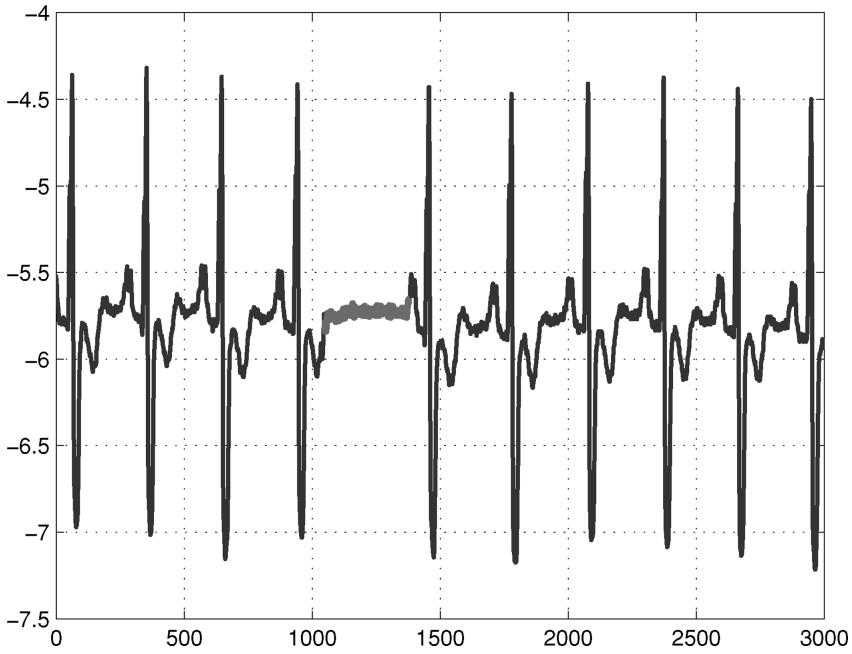

FIGURE 2.3 – Anomalie collective correspondant à une contraction prématurée auriculaire d'un électrocardiogramme ECG humain

de données normaux. Prenant l'exemple de transaction bancaire, et soit des données qui correspond aux transactions de la carte de crédit, tout en supposant que les données sont définies en utilisant une seule caractéristique : le montant dépensé. Une transaction pour laquelle le montant dépensé est très élevé par rapport à la gamme normale de dépenses pour cette personne sera une anomalie ponctuelle.

Anomalie contextuelle

C'est une anomalie détectée dans un contexte spécifique. La notion de contexte est induite par la structure dans l'ensemble de données et doit être spécifiée comme une partie de la formulation du problème. Prenant l'exemple de la température corporelle si elle dépasse 37 degrés, elle est considérée comme anormale. Alors que dans un autre contexte (météo), elle est normale.

Anomalie collective

Cette anomalie est détectée si une collection d'instances de données liées est anormale par rapport à l'ensemble de données. Les cas individuels de données dans une anomalie collective peuvent ne pas être des anomalies par elles mêmes, mais leur apparition ensemble comme une collection est anormale.

La figure 2.3 illustre un exemple qui montre une sortie d'ECG humain [43]. La région en surbrillance représente une anomalie car la même valeur faible

existe pour un temps anormalement long (correspondant à une contraction prématurée auriculaire. Notant bien que cette faible valeur par elle-même n'est pas une anomalie. bien que des anomalies ponctuelles puissent se produire dans n'importe quel ensemble de données, les anomalies collectives ne peuvent se produire que dans les données dans lesquels les instances de données sont liées. En revanche, l'apparition d'anomalies contextuelles dépend de la disponibilité des attributs contextuelles dans les données. Une anomalie ponctuelle ou une anomalie collective peut également être une anomalie contextuelle si elle est analysée par rapport à un contexte. Ainsi, un problème de détection d'anomalie ponctuelle ou un problème de détection d'anomalie collective peut-être transformé en un problème de détection d'anomalie contextuelle en intégrant les informations de contexte.

3.3 Étiquetage de données

Les étiquettes (libellé) associées à une instance de données indiquent si cette instance est normale ou anormale. Il convient de noter que l'obtention de données marquées qui est exacte et représentative de tous types de comportements est souvent coûteuse. L'étiquetage est souvent effectué manuellement par l'expertise humaine et nécessite donc des efforts considérables pour obtenir l'ensemble de données d'apprentissage étiquetées. En règle générale, l'obtention les instances de données anormales qui couvrent tout comportement anormal possible est plus difficile que d'obtenir des étiquettes pour un comportement normal. En outre, le comportement anormal est souvent de nature dynamique, par exemple, de nouveaux types d'anomalies peuvent survenir. Dans certains cas, comme la sécurité du trafic aérien, les cas anormaux se traduiraient par des événements catastrophiques et, par conséquent, seraient très rares. En fonction de la mesure dans laquelle les étiquettes sont disponibles, les techniques de détection d'anomalie peuvent fonctionner dans l'un des trois modes suivants :

Détection supervisée : Ces techniques supposent la disponibilité de données d'entraînement qui comportent les instances étiquetées de classe normale ainsi que celle anormale. Une approche typique dans de tels cas est de construire un modèle prédictif pour les classes normales et les anomalies. Toute instance de données non visualisée est comparée au modèle pour déterminer à quelle classe elle appartient. Il existe deux problèmes majeurs surviennent dans la détection supervisée. Tout d'abord, les anomalies sont moins nombreuses par rapport aux instances normales dans les données d'entraînement. Les problèmes liés à la distribution de classe déséquilibrées ont été abordés

dans la littérature [64, 99, 87, 107, 104]. Deuxièmement, l'obtention d'étiquettes précises et représentatives, en particulier pour la classe d'anomalie, est généralement difficile. Un certain nombre de techniques ont été proposées qui injectent des anomalies artificielles dans un ensemble de données normal pour obtenir des données d'entraînement libellé, ce problème a été traité dans [101, 1, 97].

Détection semi-supervisée : Les techniques qui fonctionnent sous un mode semi-supervisé supposent l'étiquetage des données d'entrainement comportant les instances de la classe normale uniquement. Par exemple, dans la détection de défauts spatiaux [38], un scénario d'anomalie signifierait un accident, ce qui n'est pas facile à modéliser. L'approche typique utilisée dans de telles techniques consiste à construire un modèle pour la classe correspondante au comportement normal et à utiliser le modèle pour identifier les anomalies dans les données de test. Néanmoins, Il existe une minorité de techniques de détection d'anomalie qui supposent la disponibilité des cas d'anomalie seuls pour les données d'entrainement [29, 30, 32]. De telles techniques ne sont pas couramment utilisées, principalement parce qu'il est difficile d'obtenir tous les comportements anormaux possibles qui peuvent se produire dans les données.

Détection non-supervisée : Les techniques qui fonctionnent en mode non surveillé n'exigent pas de données d'entraînement et sont donc les plus applicables. Les techniques de cette catégorie supposent implicitement que les instances normales sont beaucoup plus fréquentes que les anomalies dans les données de test. Si cette hypothèse n'est pas vraie alors, de telles techniques souffrent d'un taux de fausses alarmes élevé. De nombreuses techniques semi-supervisées peuvent être adaptées pour fonctionner en mode non surveillé en utilisant un échantillon de de données non libellé. Une telle adaptation suppose que les données de test contiennent très peu d'anomalies et le modèle appris pendant la formation est robuste aux anomalies existantes.

3.4 Résultats de la détection d'intrusion

Un aspect important pour toute technique de détection d'anomalie est la manière dont les anomalies sont signalées. Généralement, Le résultat produit par les techniques de détection d'anomalie est l'un des deux types suivants :

		Prédiction	
		Classe 0	Classe 1
Réalité	Classe 0	VP	FN
	Classe 1	FP	VN

TABLE 2.1 – Matrice de confusion.

Score

Cette technique attribue un score d'anomalie à chaque instance dans les données de test en fonction du degré auquel cette instance est considérée comme une anomalie. Ainsi, le résultat de ces techniques est une liste classifiée d'anomalies. Un analyste peut choisir d'analyser les premières anomalies ou d'utiliser un seuil pour sélectionner les anomalies.

Étiquetage

Les techniques de cette catégorie attribuent une étiquette (**normale** ou **anormale**) à chaque instance de test. Les techniques de détection d'anomalie basées sur le score permettent à l'analyste d'utiliser un seuil spécifique au domaine pour sélectionner les anomalies les plus pertinentes. Les techniques qui fournissent des étiquettes binaires aux instances de test ne permettent pas directement aux analystes de faire un tel choix, mais cela peut être contrôlé indirectement par des choix de paramètres au sein de chaque technique. Généralement, ces techniques s'appuient sur les méthodes de classification.

Métriques de performance

Matrice de confusion Une matrice de confusion résume la performance de classification d'un classificateur par rapport à quelques données de tests [93]. Pour évaluer la précision de la classification, il est courant de créer une matrice de confusion. La force d'une matrice de confusion est qu'elle identifie la nature des erreurs de classification, ainsi que leurs quantités. Dans la détection d'anomalies, on trouve deux classes, une classe normale et une autre anormale, d'où la matrice de confusion contient deux colonnes, comme illustré dans le tableau 2.1.

Matrice de confusion Elle est construite à partir de quatre éléments, ses éléments sont obtenus des données de référence et de la classification, définis

comme suit :

Vrai positif VP : Elément de la classe 1 correctement prédit

Vrai négatif VN : Elément de la classe 0 correctement prédit

Faux positif FP : Elément de la classe 1 mal prédit

Faux négatif FN : Elément de la classe 0 mal prédit

Á partir de cette matrice, il est possible de calculer plusieurs indicateurs. Par exemple si nous souhaitons rendre compte de la qualité de la prédiction sur la classe 1, on définit :

La sensibilité : permet de mesurer la capacité à donner un résultat positif lorsqu'une hypothèse est vérifiée, elle s'oppose à la spécificité. Elle peut être calculer par : $Sensibilité = \frac{VP}{VP+VN}$

La spécificité : mesure la capacité d'un test à donner un résultat négatif lorsque l'hypothèse n'est pas vérifiée, $Spécificité = \frac{VN}{VP+VN}$.

L'exactitude elle est définit en décrivant une combinaison des deux types d'erreur d'observation aléatoire et systématique, ou encore, la proximité de l'accord entre un résultat d'essai et la valeur de référence acceptée [82]. Comme illustré dans la figure 2.4, il faut rappeler que la précision et l'exactitude ne sont pas les mêmes, car lorsqu'on répète la mesure plusieurs fois avec le même résultat la précision est plus élevée. L'exactitude d'une mesure est d'autant plus élevée que la mesure donnera un résultat proche de la réalité. La valeur de l'exactitude (accuracy en anglais) $Exactitude = \frac{VP+VN}{\sum population}$ alors que la $precision = \frac{TP}{TP+FP}$.

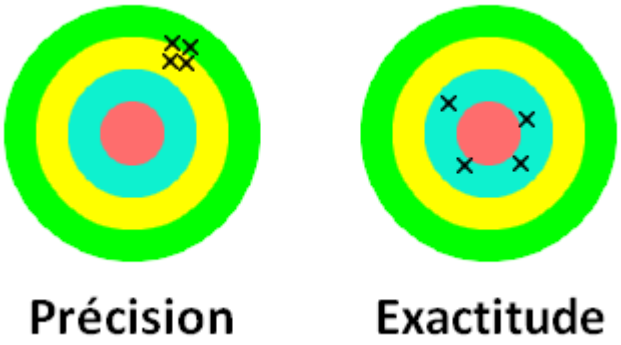

FIGURE 2.4 – Précision et exactitude selon l'iso5725.

4 Domaine d'applications

4.1 Détection d'intrusion

Le comportement du réseau est un paramètre majeur sur lequel reposent les systèmes de détection d'anomalies. Si le comportement du réseau est dans un comportement prédéfini, alors la transaction réseau est acceptée ou bien elle déclenche une alerte dans le système [57]. Les performances réseau acceptables peuvent être prédéterminées ou apprises grâce à des spécifications ou des conditions définies par l'administrateur.

L'étape cruciale de la détermination du comportement concerne la capacité du système de détection à utiliser plusieurs protocoles à chaque niveau. L'IDS doit être capable de comprendre le processus des protocoles et son objectif. Malgré le fait que l'analyse du protocole est très coûteuse en termes de calcul, les avantages tels que l'augmentation de l'ensemble de règles aident à réduire les niveaux de fausse alarmes positives.

La définition des ensembles de règles est l'un des principaux inconvénients de la détection basée sur les anomalies. L'efficacité du système dépend de la mise en œuvre et du test efficaces des ensembles de règles sur tous les protocoles. En outre, une variété de protocoles utilisés par différents fournisseurs a un impact sur la règle définissant le processus.

En plus, les protocoles personnalisés ajoutent également de la complexité au processus de définition des règles. Pour une détection précise, l'administrateur doit clairement comprendre les comportements acceptables du réseau. Cependant, avec une forte incorporation de règles et de protocoles, la procédure de détection des anomalies serait susceptible de fonctionner plus efficacement.

Cependant, si le comportement malveillant relève du comportement accepté, dans de telles conditions, il peut passer inaperçu. Le principal avantage du système de détection basé sur les anomalies réside dans l'étendue de la détection de nouvelles attaques. Ce type d'approche de détection d'intrusion pourrait également être faisable, même si l'absence de modèles de signature correspond et fonctionne également dans des conditions qui dépassent les modèles de trafic réguliers.

4.2 Détection de fraude

La fraude est l'utilisation délibérée de la tromperie pour mener des activités illicites. La détection automatique des fraudes implique l'analyse de gros volumes de données pour découvrir des modèles d'utilisation frauduleuse, et

en tant que telle, elle est bien adaptée aux techniques d'exploration de données [35].

4.3 Traitement d'image

Avec la prolifération actuelle des données, d'énormes volumes de données structurées et non structurées existent. La raison pour laquelle la détection des anomalies est importante est que les anomalies sont importantes et contiennent des informations intéressantes qui sont généralement d'intérêt dans la majorité des domaines d'application. Pour la détection d'anomalies dans les images, les approches exigent une formation libellée [45]. Des techniques appropriées de reconnaissance de formes ou de classification peuvent être appliquées à la tâche de détection supervisée des anomalies, car elles se traduisent essentiellement par un problème de classification binaire (également appelé un classificateur de classe unique où une classe est la classe normale sans anomalies et l'autre classe contient ce qui nous appelons des anomalies). Deux des défis majeurs de la détection des anomalies sont le manque de données étiquetées et les cas d'anomalies faibles. L'apprentissage en profondeur et en particulier les réseaux de neurones convolutifs (CNN) qui sont une classe de réseaux de neurones artificiels, sont devenus des outils très puissants pour les applications de vision par ordinateur, en particulier pour les tâches de classification. La formation de ces réseaux nécessite d'énormes volumes de données et la formation à partir de zéro s'avère souvent irréalisable. L'apprentissage par transfert est l'un des outils qui permet de surmonter ces défis. Les résultats obtenus sur les ensembles de données CIFAR10 [8], MNIST [9] et Concrete Crack [10] montrent que cette approche surpasse plusieurs techniques de pointe pour la détection d'anomalies dans les images.

4.4 Détection dans les capteurs réseau sans fil

Les réseaux mobiles et véhiculaires et les réseaux de capteurs et d'actionneurs sont composés de nombreux appareils distribués qui communiquent le plus souvent à l'aide de la technologie sans fil. Les appareils connectés à de tels réseaux sans fil sont particulièrement sujets aux attaques cybernétiques, et leur sécurité est parmi les principales préoccupations qui affectent leur convivialité [98, 4].

4.5 Détection d'anomalies dans un texte

Les techniques de détection d'anomalie dans ce domaine détectent principalement de nouveaux sujets ou événements ou nouvelles dans une collection de documents. Les anomalies sont causées par un nouvel événement intéressant ou un sujet anormal. Les données dans ce domaine sont généralement de grande dimension et très éparses. Elles ont également un aspect temporel puisque les documents sont collectés au fil du temps. Le défi dans ce domaine est de gérer les grandes variations dans les documents appartenant à une catégorie ou un sujet [91].

4.6 Autres domaines

La détection d'anomalie a également été appliquée à plusieurs autres domaines [88] tels que la reconnaissance de parole, la détection de la nouveauté dans le comportement du robot, la surveillance du trafic, la détection des fautes dans les applications Web, La détection d'anomalies dans les données biologiques, la détection d'anomalies dans le recensement, la détection d'associations entre activités criminelles, la détection d'anomalies chez le client, les données de gestion des relations (CRM), la détection d'anomalies dans les données astronomiques et la détection des perturbations de l'écosystème.

5 Conclusion

Le monde étant de plus en plus axé sur les données et sans approche générique pour la détection des anomalies, le problème de la dimensionnalité élevée est inévitable dans de nombreux domaines d'application. De plus, la perte de précision est plus grande et plus complexe sur le plan du calcul à mesure que le volume de données augmente. Identifier les points de données anormaux dans de grands ensembles de données. Ce chapitre a fourni un aperçu complet des techniques de détection. Pour résoudre les problèmes de la détection d'anomalies, il faut s'adapter aux changements technologiques et les nouvelles techniques de recherche consistant à construire un nouveau cadre permettant d'identifier les points de données anormales sur de grands volumes de données avec des problèmes de dimensionnalité élevée. La principale contribution dans les futures recherche est d'optimiser la détection des anomalies efficacement avec un volume de données important dans un temps très réduit afin de garantir l'intégralité et la sécurité des systèmes.

Chapitre 3

Système immunitaire artificiel

La nature est une source d'inspiration pour l'être humain, cette inspiration a permis de résoudre plusieurs problèmes cruciaux, aussi bien que dans la vie quotidienne que dans des domaines scientifiques, les chercheurs se sont inspirés des structures et des fonctions des systèmes biologiques et de leurs mécanismes. Depuis le milieu du XXe siècle, la simulation des systèmes biologiques a pris du terrain, en particulier les mécanismes et systèmes des êtres humains. Par exemple, le réseau neuronal artificiel simule la structure du système nerveux du cerveau humain, le contrôle flou est très semblable à la nature de la pensée floue et au raisonnement inexact des êtres humains, ainsi que plusieurs d'autres systèmes inspirés des théories, observations, expérimentations des systèmes biologiques. Au cours des dernières années, le système immunitaire biologique est devenu une zone émergente de recherche en bio-informatique [92]. Le système immunitaire étant un système complexe composé d'organes, de cellules et de molécules capable de reconnaître la stimulation du soi et du non-soi, faire une réponse précise et conserver la mémoire [76, 100, 16]. Les algorithmes utilisés exploitent les caractéristiques essentielles du système immunitaire comme la mémorisation, l'apprentissage, reconnaissance des formes, la diversité, la tolérance aux pannes et la détection distribuée [10, 55], pour résoudre les problèmes. Ces propriétés attrayantes du système immunitaire biologique ont attiré l'attention des chercheurs en ingénierie qui ont proposé de nombreux algorithmes et techniques novateurs basés sur les principes de l'immunologie. Après cette innovation, de nombreux chercheurs ont obtenu de plus en plus de résultats prometteurs, tels que dans la sécurité des réseaux informatiques, les robots intelligents, le contrôle intelligent, la reconnaissance des formes et la détection d'anomalies [100]. Ces efforts et ces applications peuvent non seulement nous aider à mieux comprendre le système immunitaire lui-même, mais aussi à réexaminer et résoudre des problèmes d'ingénierie

pratique dans la perspective du traitement de l'information dans le système immunitaire biologique. La construction de système de sécurité informatique utilisant les principes du système immunitaire ouvre un nouveau domaine de recherche sur la sécurité de l'information [59]. Utiliser le système immunitaire et ses mécanismes ont permis une avancée technologique sur la sécurité informatique, comme la diversité des anticorps, la dynamicité et la distribution. Ces caractéristiques sont les racines et les sources d'origine pour la construction des systèmes de sécurité informatique performant.

1 Caractéristiques des systèmes immunitaires biologique

Le système immunitaire artificiel (SIA) est un système bionique inspiré des principes du système immunitaire biologique. La clé de la conception du système immunitaire artificiel est de tirer pleinement profit des principes de l'immunologie et de reproduire l'efficacité et la capacité de ce système dans les systèmes informatiques. Un système immunitaire biologique présente un certain nombre de caractéristiques d'inspiration dont le système immunitaire artificiel peut encapsuler, on cite :

Distribution

les lymphocytes dans le système immunitaire biologique sont capables de détecter l'anomalie de manière indépendante, avec un contrôle centralisé, ce qui signifie qu'ils constituent un système fortement distribué. Lors de la conception d'un système immunitaire artificiel, cette fonctionnalité est très utile pour l'autoprotection et la robustesse des IAS. L'architecture basée sur les agents a été proposée pour simuler la distribution du système immunitaire [51, 72].

Multicouche

le système immunitaire biologique a une structure multicouche. Une seule couche du système immunitaire biologique ne peut pas protéger l'organisme de toutes les menaces, mais la coopération entre plusieurs couches permet d'assurer la protection de sécurité du système. Les études et les implémentations de la fonctionnalité multicouche dans le système immunitaire artificiel pour les systèmes informatiques peuvent grandement améliorer la sécurité des systèmes informatiques [78].

Diversité

Bien que les corps protégés par le système immunitaire biologique soient les mêmes dans l'ensemble, chaque corps a ses propres différences. La diversité des différents corps est également très utile pour la protection contre les invasions. La diversité vient de la diversité du corps et la diversité du système immunitaire biologique. La combinaison des deux aspects augmente considérablement la diversité qui est très importante pour protéger notre corps. Dans le domaine de la sécurité des systèmes informatiques, la mise en œuvre de la diversité peut également être réalisée dans deux aspects : la diversité des systèmes d'exploitation informatiques et la diversité du SIA.

Autonomie

Le système immunitaire biologique ne nécessite pas un nœud de contrôle central. Les cellules immunitaires peuvent reconnaître et détruire automatiquement les antigènes envahissants le corps.

Adaptabilité

Le système immunitaire biologique est capable de connaître de nouveaux agents pathogènes envahissants et de les mémorisés. Ainsi la vitesse de réponse à la même invasion du chemin sera accélérée. Ces mécanismes d'apprentissage sont très importants pour le système immunitaire artificiel. Le SIA ne doit pas seulement se souvenir de l'information immunologique anormale trouvée dans le passé, mais aussi apprendre dynamiquement pour gérer les anomalies émergentes inconnues.

Détection d'anomalie

Le système immunitaire biologique est capable de reconnaître le pathogène qui n'a pas était traité auparavant. Cette fonctionnalité est propice au système immunitaire artificiel pour atteindre la fonction de détection d'anomalies inconnues ou de trouver de nouveaux virus dans le domaine de la sécurité informatique [102, 92].

2 Système immunitaire artificiel

Le système immunitaire artificiel (AIS) est un système d'intelligence computationnelle inspiré des principes du système immunitaire biologique. Sur la

base de l'idée de faire connaître la sagesse de la nature, et en simulant le mécanisme des systèmes immunitaires biologiques, les systèmes immunitaires artificiels réussissent à atteindre de nombreux avantages du système immunitaire biologique, y compris la plupart des caractéristiques du système immunitaire biologique [16, 100]. Les SIA sont une discipline liée à l'intelligence artificielle qui s'est développée et attiré l'attention de nombreux chercheurs. Il existe plusieurs algorithmes et modèles de système immunitaires artificiels. La plupart des algorithmes tentent d'utiliser les mécanismes d'apprentissage et de mémoire des systèmes immunitaires biologiques pour la résolution les problèmes. Dans un algorithme immunitaire artificiel, l'antigène correspond à la fonction objective pour résoudre les problèmes et les contraintes, l'anticorps correspond à la solution candidate et le degré d'affinité des anticorps et des antigènes correspond à la solution candidate avec fonction objective. Les étapes générales d'un algorithme immunitaire artificiel sont présentées dans l'a. Dans l'algorithme 1, lorsqu'il a été suspendu, c'était la meilleure correspondance avec l'anticorps antigène, qui a été optimisé pour la solution qui résout le problème avec succès.

Entrée : Antigène
Initialiser la population des anticorps;
*Calcul d'affinité de chaque anticorps;
Vérifier le cycle de vie de chaque anticorps;
si *condition d'arrêt* **alors**
| aller à : * ;
sinon
| aller à : ** ;
fin
****Sortie :** anticorps ;

Algorithme 1 : Étapes générales d'un algorithme immunitaire artificiel [100].

La première proposition de cet algorithme [36] basée sur la sélection négative des systèmes immunitaires biologiques, ils ont d'abord proposé un algorithme de sélection négatif [36], pour la détection d'anomalie dans les systèmes informatiques. Cet algorithme est l'un des algorithmes AIS les plus importants et présente une très bonne robustesse dans l'identification de soi et de la "variante", cet algorithme peut être utilisée pour détecter des antigènes inconnus. Il est particulièrement adapté à surveiller la sécurité informatique, au diagnostic des erreurs dans des environnements dynamiques, à la détection des malwares, à la détection des anomalies, à la détection d'intrusion, etc. cet algorithme sera détaillé dans les sections qui suivent.

L'application du mécanisme de la diversité biologique dans le système immunitaire contribue à améliorer la capacité de recherche avec des algorithmes optimaux et accélère leur vitesse de convergence. D'autres mécanismes comme l'auto-organisation et l'apprentissage non supervisé peuvent nous fournir des mécanismes pour connaître les environnements inconnus en utilisant des informations connues. La mémoire immunitaire qui peut rappeler des connaissances acquises est très importante et essentielle pour un système intelligent. Au milieu du développement rapide d'algorithmes immunitaires artificiels, beaucoup de personnes continuent à présenter une variété d'algorithmes et modèles immunitaires artificiels pour de nombreux problèmes du monde réel.

Les systèmes immunitaires artificiels ont été appliqués avec succès à de nombreux domaines pratiques, y compris la sécurité informatique, l'optimisation, le diagnostic et la reconnaissance des formes. En particulier, la détection des d'anomalies et d'intrusion basée sur l'immunité artificielle a été développée rapidement et a permis de d'avoir des résultats satisfaisants et de nouvelles perspectives, attirant de plus en plus de chercheurs dans ce domaine. Néanmoins, ces systèmes immunitaires artificiels ne sont pas parfaits. La plupart d'entre eux ont des lacunes, ce qui stimule les chercheurs à explorer des modèles et des algorithmes plus efficaces.

3 Modèles et algorithme des systèmes immunitaires artificiels

Plusieurs théories et modèles existent dans l'immunologie, ses théories ont fait un sujet d'abstraction dans le domaine de l'informatique, dans cette section on liste quelques modèles d'immunité artificielle.

3.1 Algorithme de sélection négative (ASN)

Les auteurs de cet algorithme l'ont inspiré du processus de génération des cellules T dans les systèmes immunitaires, dans leur article [36], ils ont proposé l'ASN. Basé sur un concept biologique qui est la capacité de distinguer entre les cellules soi et les cellules non-soi, ce qui permet de reconnaître les antigènes envahissants. Les cellules T jouent un rôle crucial dans ce processus. La génération de cellules T comprend deux stages : un stage de génération initiale et les étapes de sélection négatives. Pour le premier, les récepteurs des cellules T sont générés par une combinaison aléatoire de gènes. Afin d'éviter la reconnaissance erronée de soi, les cellules T sont filtrées dans le thymus (c'est-à-dire un

processus de sélection négatif). Les lymphocytes T identifient et suppriment les cellules du soi, tandis que les autres cellules considérées comme étrangères par les cellules T, elles peuvent participer à la réponse immunitaire.

Les travaux dans la littérature [36] ont adopté le même principe de distinction de soi et de non-soi dans les systèmes informatiques. Ils ont généré le détecteur défini par le processus de sélection négatif pour reconnaître le non-soi qui a envahi les ordinateurs.

L'ASN comme illustré dans l'algorithme 1 comprend l'étape de génération de l'ensemble de détecteurs et l'étape de détection du non-soi. Dans la génération d'ensemble de détecteurs, la collection des gènes du soi est construite à partir de fichiers propres aux cellules du soi. Ensuite, l'ensemble de détecteurs est généré de manière aléatoire. Les détecteurs qui correspondent à l'ensemble de soi sont supprimés des détecteurs selon le principe de sélection négatif. Le rôle principal de l'ensemble de détecteurs est qu'il peut couvrir entièrement l'espace de données non-soi. Par conséquent, le nombre de détecteurs a tendance à être plus important. Dans l'étape de la détection non-soi, l'algorithme cherche une correspondance entre l'échantillon et l'ensemble de détecteurs un par un. Une fois qu'une correspondance (matching) se produit, l'échantillon sera étiqueté comme non-soi.

Plusieurs chercheurs ont travaillé sur la perspective de trouver les deux fonctions de la section négative (la représentation de détecteurs et la fonction de correspondance) [63]. Les auteurs [28] ont représenté les détecteurs comme une fonction porte (rectangular function) dans l'espace de nombres réels, cette méthode permettait de calculer le degré d'anomalie. L'analyse des limites de la représentation de chaîne binaire et son processus de correspondance a permis de montrer que le type de détecteur de type binaire n'est pas capable de bien caractériser la structure spatiale des données de certains problèmes [44]. [9] a mené une enquête sur de multiples formes de détecteurs dans l'espace de valeurs réelles : super rectangle, super sphéricité, super sphéroïdité, etc. De plus, ils ont donné un modèle de sélection négatif uniforme. [28] a adopté la distance euclidienne en tant que fonction correspondance du détecteur dans l'espace de valeurs réelles et a ajusté dynamiquement la valeur de seuil de correspondante en fonction de la longueur des détecteurs. Dans l'algorithme traditionnel de sélection négative, le détecteur mis en place pour le soi est généré aléatoirement. Cette méthode aléatoire non supervisée consomme beaucoup de ressources. En outre, l'algorithme traditionnel de sélection négative est plus préoccupé par le caractère non-soi des échantillons, alors que le système immunitaire biologique prend en considération le danger des antigènes. Dans la détection d'anomalies,

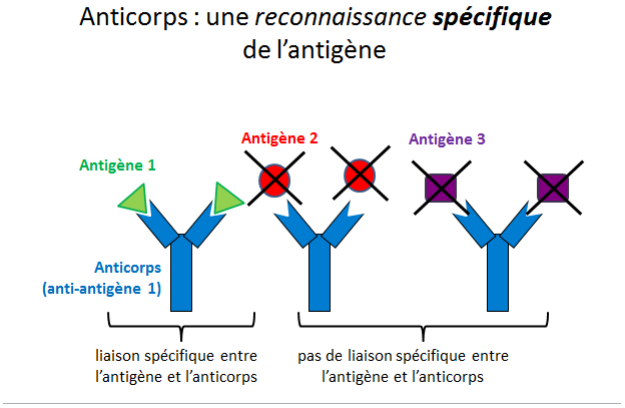

FIGURE 3.1 – La relation entre antigène et anticorps

le risque se situe dans l'échantillonnage.

3.2 Algorithme de sélection clonale (ASC)

En immunité, chaque cellule B produit une sorte d'anticorps, afin d'identifier l'antigène correspondant. Lorsque l'anticorps et l'antigène correspondent (liaison voire figure 3.1) et reçoivent un signal de stimulation émis par les cellules T auxiliaires, les cellules B correspondantes sont activées et clonées et différenciées en cellules plasmatiques et cellules B de mémoire. Lorsque les cellules B de la mémoire rencontrent le même antigène, elles généreront beaucoup d'anticorps avec des affinités élevées. [19] a proposé la théorie biologique de sélection clonale pour expliquer le processus de clonage et la relation entre prolifération et différenciation des cellules immunitaires et les affinités. Á partir de ce concept, [31] ont proposé l'algorithme de sélection clonale. L'idée centrale de cet algorithme est de sélectionner et cloner les cellules avec des affinités élevées et d'effacer les cellules avec de faibles affinités, avec le clonage et la mutation des cellules ayant affinités des antigènes et des anticorps.

L'algorithme 2 est une implémentation de sélection clonal présenté par [16] pour traiter un problème de minimisation. Le modèle général de CLONALG [31] implique la sélection d'anticorps (solutions potentielles) en fonction de l'affinité soit en combinant un modèle d'antigène, soit par évaluation d'un modèle par une fonction de coût. Les anticorps choisis sont soumis à un clonage proportionnel à l'affinité, tant dis que la mutation des clones est inversement proportionnelle à l'affinité du clone. L'ensemble clonal qui en résulte est en concurrence avec la population d'anticorps existante pour être membre de la prochaine génération. En outre, les membres de la population à faible affinité

Entrées : $Population_{taille}$, $Selection_{taille}$, $Prob_{taille}$, $CellulesAleatoire_{num}$, $Clone_{freq}$, $Mutation_{freq}$
Sortie : Population
Population ← `GénérerCelluleAléatoirement(`$Population_{taille}$, $Prob_{taille}$`)`;
tant que ¬`ConditionDarrêt()` **faire**
  pour chaque $p_i \in$ Population **faire**
    `Affinité(`p_i`)`;
  fin
  $Population_{select}$ ← `Selectionner(`Population, $Selection_{taille}$`)`;
  $Population_{clones} \leftarrow \emptyset$;
  pour chaque $p_i \in Population_{select}$ **faire**
    $Population_{clones}$ ← `Cloner(`p_i, $Clone_{freq}$`)`;
  fin
  pour chaque $p_i \in Population_{clones}$ **faire**
    `Hypermutate(`p_i, $Mutation_{freq}$`)`;
    `Affinité(`p_i`)`;
  fin
  Population ← `Selectionner(`Population, $Population_{clones}$, $Population_{taille}$`)`;
  $Population_{rand}$ ← `GénérerCelluleAléatoirement(`$CellulesAleatoire_{num}$`)`;
  `Remplace(`Population, $Population_{rand}$`)`;
fin
retourner Population;

Algorithme 2 : Algorithme de sélection clonale [16]

sont remplacés par des anticorps générés aléatoirement. La variation de reconnaissance de motif de l'algorithme comprend la maintenance d'un ensemble de solutions de mémoire qui, dans son intégralité, représente une solution au problème. Un schéma de codage binaire est utilisé pour la reconnaissance de motif avec une fonction de d'optimisation continue, et un schéma de permutation de nombre réel est utilisé pour le problème du TSP.

Plusieurs travaux ont été réalisé pour améliorer de cet algorithme, y compris l'ajout de paramètres et leur mise à jour automatique [27], la distribution de l'algorithme et ses performances en cas de l'implémentation parallèle [106], Les mêmes auteurs [106] ont discuté l'influence de la mutation gaussienne et celle de cauchy, ainsi une comparaison entre codage binaire et avec des valeurs réelles. Une implémentation de Framework de la sélection clonale proposé par [9] et compare la sélection clonale artificielle avec les algorithmes évolutionnaires.

3.3 Réseau immunitaire artificiel

Le réseau immunitaire artificiel (RIA) est inspiré de la théorie proposée par [90]. Il suggère que le système immunitaire peut être considéré comme un réseau, dans lequel les cellules immunitaires interagissent les unes avec les autres même lors de l'absence des antigènes. Les interactions peuvent être initialisées non seulement entre les antigènes et les anticorps, mais aussi entre les anticorps qui peut induire des réponses immunitaires stimulantes ou suppressives, ce qui entraîne une série de comportements immunologiques, y compris la tolérance et l'émergence de la mémoire. Il existe trois facteurs majeurs qui affectent le niveau de stimulation des cellules B [58] : la contribution de la liaison de l'antigène, la contribution des cellules B voisines et la suppression des cellules B voisines. La quantité de clones que la cellule B produit augmente en conséquence de l'augmentation du niveau de stimulation d'une cellule B augmente. Au niveau de la population, il en résulte un ensemble diversifié de cellules B. En outre, trois mécanismes de mutation sont introduits, y compris le croisement, la mutation inverse et ponctuelle, contrairement aux algorithmes de sélection clonale.

L'un des premiers travaux proposés par [60] qui ont exposé une méthode de réseau immunitaire artificiel et l'ont appliqué à la reconnaissance de séquence d'ADN. Leur principe s'articule sur les lymphocytes B qui sont corrélés en fonction du degré d'affinité et d'inhibition. La population des cellules B comprend deux sous-ensembles : la population initiale et la population clonée. Dans la phase d'entraînement, l'ensemble de formation est divisé en deux parties, l'une pour générer le réseau initial de cellules B, et l'autre partie est utilisée comme antigène pour stimuler le réseau de cellules B. Lorsque l'affinité entre un antigène et une cellule B dépasse un seuil prédéterminé, la cellule B est excitée et sera clonée et mutée. Les cellules B générées rejoignent alors le réseau et seront ajustées dynamiquement par l'état excité du réseau. Ce travail a trouvé les caractéristiques fondamentales de la théorie du réseau immunitaire. En ce qui concerne les mécanismes du réseau immunitaire et la méthode de représentation des cellules B, les chercheurs ont proposé une variété d'approches du réseau immunitaire artificiel [103].

Les RIA ont gagné une grande popularité pour résoudre les problèmes d'optimisation [7, 26]. Cependant, une analyse théorique de RIA réalisée par [80] a souligné que l'algorithme RIA avait des faiblesses pour les problèmes qui impliquent le partitionnement de données distribués non uniformes. Ceci est dû à la métrique basée sur le mécanisme suppressif dans l'algorithme, ce qui entraîne une perte de l'information significative causée par la compression

Entrées : $Population_{taille}$, $Problem_{taille}$, N_{clones}, $N_{Aleatoir}$, $Seuil_{Affinit}$
Sortie : $S_{meilleur}$
$Population \leftarrow$ `InitialiserPopulation(`$Population_{taille}$, $Problem_{taille}$`)`;
tant que ¬`Condition d'arrêt()` **faire**
  `EvaluerPopulation(`$Population$`)`;
  $S_{meilleur} \leftarrow$ `meilleurSolution(`$Population$`)`;
  $Resultat \leftarrow \emptyset$;
  $Cout_{Moy} \leftarrow$ `CalculerCoutMoyenPopulation(`$Population$`)`;
  tant que `CalculerCoutMoyenPopulation(`$Population$`)` > $Cout_{Moy}$ **faire**
    pour chaque $Cellule_i \in Population$ **faire**
      $Clones \leftarrow$ `Cloner(`$Cellule_i$, N_{clones}`)`;
      pour chaque $Clone_i \in Clones$ **faire**
        $Clone_i \leftarrow$ `MuterSelonFitnessParent(`$Clone_i$, $Cellule_i$`)`;
      fin
      `EvaluerPopulation(`$Clones$`)`;
      $Resultat \leftarrow$ `meilleurSolution(`$Clones$`)`;
    fin
  fin
  `SupprimerCelluleFaibleAfinité(`$Resultat$, $Seuil_{Affinit}$`)`;
  $Resultat \leftarrow$ `CreerCelluleAleatoire(`$N_{Aleatoir}$`)`;
  $Population \leftarrow Resultat$;
fin
retourner $S_{meilleur}$;

Algorithme 3 : Algorime de réseau immunitaire artificiel [16]

ou la représentation redondante de données. D'autres algorithmes basés sur le réseau immunitaire [108] qui a utilisé le mécanisme d'apprentissage à court terme présenté dans le réseau immunitaire appliqué sur des robots mobiles. Une approche combinée à court terme et à long terme fondée sur les comportements du réseau immunitaire a été proposée [109]. Cette méthode a été appliquée pour résoudre les problèmes de navigation des robots mobiles, qui sont présentés et testés à la fois en simulation et sur des robots réels.

3.4 Algorithme de cellules dendritiques

Le modèle du soi et non-soi prédominant en immunologie depuis les années 1950, a commencé à rencontrer des problèmes à la fin des années 1980, lorsque les immunologistes ont su que les lymphocytes T dépendent d'autres cellules pour collecter et ensuite les présenter pour avoir une réponse, et que la réponse de la cellule T dépend si l'autre cellule (connue sous le nom de cellules présentatrices d'antigène CPA) envoie des signaux d'activation aux cellules T.

En s'appuyant sur les idées de Thomas Kuhn, Charles Janeway [61] a proposé que l'ancien paradigme immunologique ait atteint ses limites. Il a soutenu que le système immunitaire inné était le véritable contrôleur même si le système immunitaire n'a pas répondu. Il a également soutenu que le système immunitaire inné utilisait des anciens récepteurs de reconnaissance de formes pour prendre ces décisions - reconnaissant un pathogène par ses caractéristiques immuables.

4 Conclusion

Dans ce chapitre, nous avons présenté en bref les systèmes immunitaires artificielles qui existent. Les caractéristiques attrayantes de ses systèmes ont été aussi présentées et enfin l'introduction de DCA qui sera présenté en détails dans le prochain chapitre, exposant le concept biologique ainsi que l'abstraction de tel système inspiré en informatique.

Chapitre 4

Théorie de danger et Algorithme de cellules dendritiques

Comme dans l'immunité, plusieurs algorithmes AIS sont basés sur la théorie de «soi non-soi». Il a été remarqué que ces algorithmes ne peuvent pas produire les mêmes performances élevées que le système immunitaire humain. Par conséquent, la théorie du danger a été proposée. Elle indique que la reconnaissance d'un pathogène est basée sur le contexte environnemental (signaux) plutôt que sur le simple principe du soi-non-soi. Aussi, elle est dédiée aux problèmes de classification est basée sur le fonctionnement des cellules immunitaires dendritiques. Une inspiration de ces cellules a permis le développement de l'algorithme des cellules dendritiques (DCA) [2]. Le DCA est basé sur le principe des cellules dendritiques, ou elles classent chaque antigène comme étant normal ou anormal. Le DCA a été appliqué avec succès à une large gamme d'applications où il a été démontré que l'algorithme peut traiter la classification des données tout en générant des résultats de classification avec un taux élevé et précis.

L'objectif de cette thèse est de proposer un nouvel algorithme optimisé qui peut améliorer les propriétés de classification du DCA.

1 Fondement de la théorie de danger

1.1 Concepts fondamentaux

L'objectif primaire du système immunitaire est de protéger le corps des entités envahissantes qui causent des dommages et des maladies. Au départ, les immunologistes pensaient que la protection se faisait en distinguant le soi et le non-soi à l'intérieur du corps et en éliminant le non-soi. Cependant, il

a été remarqué que le corps humain était incapable de s'adapter totalement à cette théorie dû aux situations que cette théorie n'a pas pu assurer une explication satisfaisante comme (la puberté, les tumeurs, les greffes ...) [76, 75]. Les immunologistes ont découvert de plus en plus des défauts dans la réflexion traditionnelle sur soi-même ainsi que la nouvelle théorie du danger émerge. Cette théorie souligne qu'il doit y avoir une discrimination qui va au-delà de l'auto-discrimination, par exemple :

- Il n'y a pas de réaction immunitaire aux bactéries étrangères présentes dans l'intestin ou aux aliments que nous mangeons bien que les deux soient des entités étrangères.
- Le corps humain change au cours de sa vie et, par conséquent, s'auto-change également. Par conséquent, la question se pose à savoir si les défenses contre des corps étrangers tôt dans la vie pourraient être auto-réactives plus tard.
- D'autres aspects qui semblent en contradiction avec le point de vue traditionnel sont les maladies auto-immunitaires, certains types de tumeurs combattues par le système immunitaire et des greffes réussies.

La théorie de danger offre une alternative à l'approche du soi non-soi. Elle stipule que le système immunitaire discrimine en fait un soi de certain non-soi. La réponse immunitaire se fait par réaction à un danger et non pas au non-soi [76].

1.2 Description du concept de danger

La mort cellulaire est un processus systémique qui peut être trouvée dans différentes parties du corps. Néanmoins, il existe deux types de morts cellulaires, le premier type de mort cellulaire qui n'apparaît pas dangereux pour le système immunitaire est normal (elle est une mort cellulaire programmée) et s'appelle « apoptose ». Les cellules mourantes causées par l'apoptose sont récupérées par des cellules spécialisées : Qu'on appelle cellule CPA (Cellule présentatrice d'antigène). Immunologiquement, en cas d'apoptose, les cellules envoient des signaux aux APC de récupération à proximité pour les dévorer. Ce phénomène empêche la cellule mourante de libérer des toxines nocives (voir la figure 4.1).

Un autre type de mort cellulaire est appelé « nécrose », Contrairement à la première, cette mort se traduit par une mort non programmée, les cellules sont tuées accidentellement par des agents pathogènes nocifs ou par endommagement directe des cellules. Cette mort désordonnée n'envoie pas de signaux qui informent les phagocytes voisins d'engloutir les cellules lésées. Cela rend

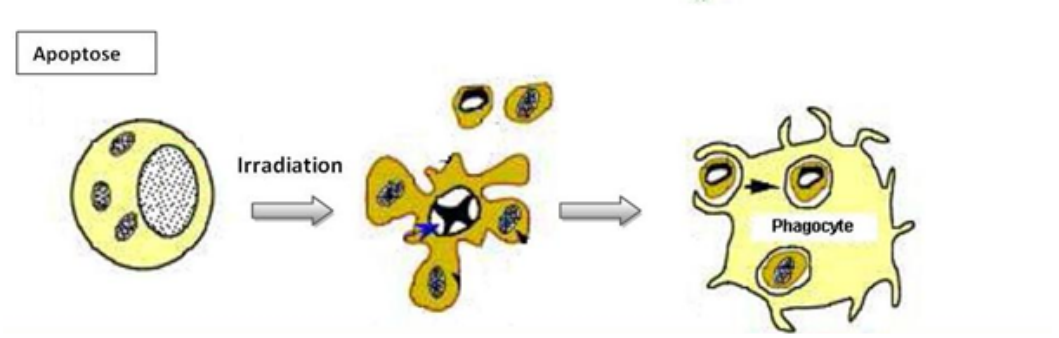

FIGURE 4.1 – Processus d'apoptose

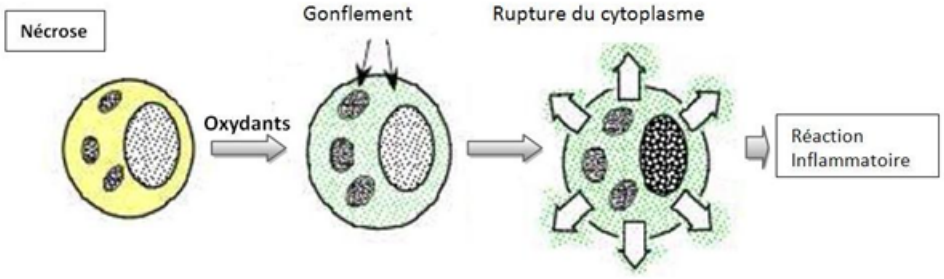

FIGURE 4.2 – processus de la nécrose

difficile pour les cellules de nettoyage (phagocytes) de localiser et de digérer les cellules qui meurent à cause de la nécrose. La membrane cellulaire stocke des enzymes digestives spéciales. Ainsi, la libération de cette toxine nocive accélère la réaction chimique non organisée (voir Figure 4.2). Le modèle de danger a été construit sur la base que le contenu libéré par toute cellule endommagée était en fait une forme de signaux de danger qui alertaient les cellules APC voisines (les cellules dendritiques) et les activaient. Seules les cellules qui meurent de nécrose enverraient des signaux d'alerte au danger. Les cellules saines et les cellules issues de l'apoptose ne devraient pas envoyer ce type de signaux.

1.3 Les signaux de danger

— Signaux PAMP : Modèles moléculaires associés pathogéniques, signatures moléculaires d'agents pathogènes (bactérie ou virus) qui sont reconnus par les récepteurs de type Toll (TLR) à la surface des cellules dendritiques, et ils ont une grande influence sur la transition de l'état immature à l'état mature. Les anomalies sont susceptibles d'exister lorsque ce type de signaux sont présents

— Signaux sains : Ces signaux sont dérivés des cellules de mort programmé naturellement, le TNF-α (Tumor Necrosis Factor) est un candidat des signaux sains, ils contribuent à la maturation des cellules dendritiques

de l'état immature à l'état semi-mature, leurs présences indiquent que le système est sûr et qu'aucune anomalie n'est présente.

— Signaux de danger : Signaux libérées par des cellules tissulaires endommagées sujettes à une nécrose (mort cellulaire non programmée), elles ont un effet plus faible que les PAMP sur la maturation vers l'état mature, car ces signaux sont moins importants pour les autres. Les cellules endommagées envoient des signaux de danger, leur présence augmente une situation anormale mais a une puissance inférieure à celle du PAMP.

— Stimulations inflammatoires : L'inflammation est un processus par lequel les globules blancs du corps et les éléments qu'ils fabriquent permet de protéger le corps contre l'infection des envahisseurs extérieurs, tels que les bactéries et les virus. L'inflammation peut produire : rougeur, douleur, gonflement et augmentation de température.

Pendant l'état immature, les cellules dendritiques collectent également des débris dans les tissus qui sont ensuite combinés avec les signaux environnementaux. Certains des débris « suspects » collectés sont appelés antigènes, et ce sont des protéines provenant d'entités potentiellement envahissantes. Les cellules dendritiques combinent les antigènes « suspects » avec des preuves sous forme de signaux pour indiquer correctement au système immunitaire adaptatif de répondre ou de devenir tolérant aux antigènes présentés [71].

2 Fonctionnement de cellules dendritiques

Selon [75] fondateur de cette théorie, qui a proposé que les cellules présentatrices d'antigène sont responsables d'envoyer une alarme ou un signal de danger de la cellule ou du tissu endommagé(cellules exposées à des pathogènes, toxine, dommage physique ...), ces faits sont purement théoriques et ont conduit à un résultat évident : il existe plusieurs signaux envoyés, en plus, les cellules issues de l'apoptose(processus de mort cellulaire programmée normal) se font nettoyer puis désintégrer alors que celles de la nécrose (mort non programmée des cellules) vident leurs contenus et tous produits intracellulaires générant un signal de danger. L'importance dans ces signaux qu'ils ne soient pas issus d'une cellule saine ou morte d'une façon physiologique, la figure 4.3 résume les différents états de cellule dendritique.

Les cellules dendritiques DC sont un type de cellule présentatrice d'antigène. Les DC sont chargés de détecter, identifier, capturer, traiter et révéler les antigènes aux lymphocytes T. Ils expriment également des récepteurs sur leurs surfaces pour recevoir des signaux de leur voisinage. Le comportement

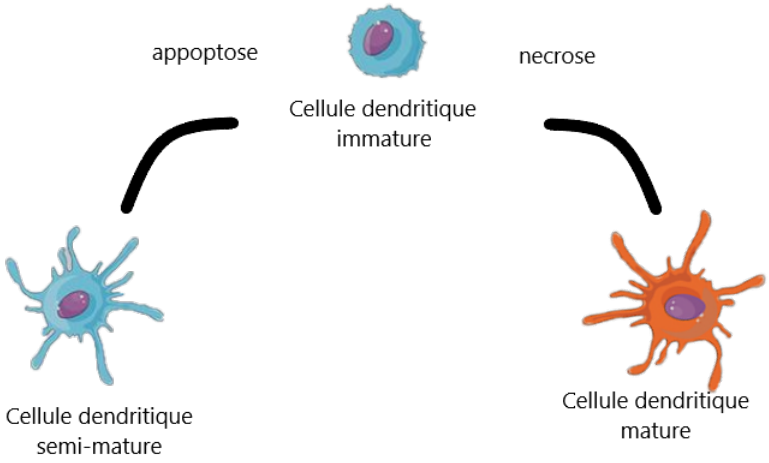

FIGURE 4.3 – Maturation de la cellule dendritique

des DC dépend de la concentration des signaux reçus. En conséquence, ils se différencient en trois niveaux de maturité [71] différents décrits comme suit :

Cellules immatures : A leur arrivée dans le tissu, les DC se trouvent dans un état immature. Ici, les DC immatures (iDC) collectent des antigènes qui pourraient être une molécule « sûre », dangereuse ou quelque chose d'étranger. De plus, la DC peut collecter et détecter les divers signaux qui peuvent être présents dans le tissu. La réception de signaux entraîne des modifications de la fonction, de la morphologie et du comportement de l'iDC. En d'autres termes, les proportions relatives et la puissance des différents signaux conduisent à un état de maturation totale ou partielle d'immaturité.

Cellules matures : Pour qu'une iDC devienne une « DC mature » (mDC), l'iDC doit être exposée à une plus grande concentration de PAMP et (ou) de signal de danger que de signal sain. Une exposition suffisante signaux amène la DC à cesser la collecte d'antigène et à migrer du tissu vers le ganglion lymphatique. Plus important encore, les mDC produisent une cytokine inflammatoire appelée « interleukine-12 » qui stimule l'activation des cellules T afin d'être réactives à la présentation de l'antigène. De plus, les mDC produisent des molécules co-stimulatrices (CSM) qui sont connues pour faciliter le processus de présentation d'antigènes.

Cellules semi-matures : En présence de conditions d'apoptose, l'exposition aux signaux sains détourne l'état de l'iDC pour devenir une « DC semi-mature » (smDC). Les smDC semblent morphologiquement très

similaires aux mDC et peuvent présenter un antigène, mais ils n'ont pas la capacité d'activer les lymphocytes T (le mécanisme d'activation du système immunitaire). La smDC produit «l'interleukine-10» qui supprime les lymphocytes T correspondant à l'antigène présenté. Les antigènes collectés avec les signaux sains sont présentés dans un contexte tolérogène et conduisent à une absence de réponse à ces antigènes.

Le passage d'un état DC à un autre dépend de la concentration de différents signaux tout au long de l'état initial (iDC). Comme l'illustre à la figure 4.3. La migration vers l'état mature ou vers l'état semi-mature dépend de la concentration des signaux d'entrée reçus de l'environnement. Immunologiquement, si la concentration de signaux sains est supérieure aux autres catégories de signaux, alors les DC migrent vers l'état semi-mature. Cependant, si la concentration de PAMP et de signaux de danger est supérieure à la concentration de signaux sains, alors les DC migrent vers le contexte mature.

3 Algorithme de cellule dendritique DCA

Phase de prétraitement et d'initialisation

L'application du DCA nécessite souvent une phase de prétraitement des données pour catégoriser de manière appropriée un domaine de problème donné à l'espace d'entrée de l'algorithme. L'étape de prétraitement comprend deux étapes principales : la réduction des attribues et la catégorisation du signal. Le processus de réduction d'attributs et de catégorisation des signaux implique la sélection et l'extraction des caractéristiques les plus intéressantes de l'ensemble de données originales du problème, puis la catégorisation consiste à attribuer ces caractéristiques dans l'une des catégories de signaux définies du DCA : PAMP, signal de danger ou signal sain. Certains travaux sur cette phase ont traité l'implication des utilisateurs ou d'experts afin de sélectionner ou d'extraire les attributs représentatifs et de les mettre dans les catégories de signaux appropriées. D'autres travaux de sur cette phase appliquaient, principalement, la méthode statistique d'analyse en composantes principales (ACP) pour une tâche de prétraitement automatisé des données [54]. Plus précisément, pour la réduction des caractéristiques, l'algorithme applique l'ACP qui sélectionne les attributs des composants principaux qui révèlent la structure interne des données en mettant l'accent sur la variance des données. Une fois les attributs sélectionnées, l'ACP est appliqué pour attribuer chaque attribut à son type de signal spécifique. D'autres méthodes favorisaient l'utilisation de la théorie des ensembles et la logique floue

Pour la catégorisation des signaux, certaines versions DCA utilisaient un attribut parmi l'ensemble sélectionné des attributs et l'affectent à la fois à PAMP et au signal sain car ils sont tous deux considérés comme des indicateurs positifs d'anomalie et normalité. L'utilisation d'un attribut pour ces deux signaux nécessite de définir un seuil : les valeurs supérieures à ce seuil peuvent être classées comme normales sinon comme anormales. Quant à l'attribution d'attributs signal de danger et puisque ce signal est moins important que certain d'être anormal, la combinaison du reste des attributs sélectionnés est choisie pour la représenter. D'autres travaux DCA gèrent l'étape de catégorisation des signaux en utilisant la procédure de classement ACP. Ceci est réalisé en utilisant le classement des attributs ACP en termes de variabilité. Une fois le classement effectué, les attributs sont mappés dans les catégories de signaux d'entrée DCA en corrélant le classement ACP avec le classement des catégories de signaux qui est dans l'ordre Sain, PAMP et Danger.

3.1 Détail de l'algorithme

Données : Identifiants d'antigènes et tous les signaux (Signal sain, signal PAMP, signal de danger et antigènes).

Résultat : Valeur de contexte antigène (normal/anormal)

//Phase de pré-traitement et d'initialisation

//Convertir les données en signaux appropriés (signal sain, signal de danger et Signal Pamp). //Phase d'initialisation

pour *i = 1 .. maxDC* **faire**
  initialiser DC_i
fin

//Phase de détection

répéter
  Échantillonner_antigène()
  Mise_à_jour_sommes()
jusqu'à $Csm >= Seuil$;

//Phase d'évaluation de contexte

si *cellule_mature* < *cellule_semi_mature* **alors**
  Contexte ← 0
sinon
  Contexte ← 1
finsi

//Phase de filtration : * cellules maturées

pour *i = 1 .. max_antigène* **faire**
  si *Contexte(antigène[i])=1* **alors**
    compte(antigène[i])++
    re-init_DC
  finsi
fin

//Phase de filtrage : ** MCAV_Seuil

pour *i = 1 .. max_antigène* **faire**
  MCAV(antigène[i]) ← nombre_cellule_mature / nombre_cellule_échantillonnées
  si *MCAV_Seuil > MCAV(antigène[i])* **alors**
    classe(antigène[i]) ← *normal*
  sinon
    classe(antigène[i]) ← *anormal*
  finsi
fin

Algorithme 4 : Algorithme de cellule Dendritique [48]

Phase de détection

Après l'achèvement de l'étape de prétraitement des données DCA terminée, l'algorithme calcule les valeurs des signaux : sain, PAMP et danger [47] induisant une base de données de signaux et adhère à ces signaux et antigène pour identifier le contexte de chaque cellule dendritique. Ces opérations sont élaborées pendant la phase de détection. En effet, les signaux d'entrée du système qui sont pré-catégorisés comme PAMP, danger et sain sont traités par l'algorithme afin d'obtenir trois signaux de sortie : signal de co-stimulation (CSM), signal semi-mature (smDC) et le signal mature (mDC). La phase de détection se produit dans les cellules dendritiques de l'état immature. Le contrôleur de domaine a les trois fonctions suivantes qui sont exécutées chaque fois qu'un seul contrôleur de domaine est mis à jour :

Échantillon d'antigène : La cellule recueille en même temps les signaux et les antigènes d'une source externe (dans ce cas, du tissu) et place l'antigène dans sa propre structure de données de stockage d'antigène.

Mise àjour des signaux d'entrées : La cellule dendritique collecte les valeurs de tous les signaux d'entrée présents dans la zone de stockage des signaux.

Calcul des signaux de sortie intermédiaires : à chaque itération, chaque cellule calcule trois valeurs de signal de sortie temporaires à partir des signaux d'entrée reçus. Ces signaux sont utilisés pour évaluer l'état de la cellule dendritique à la fin cette phase, on détermine la durée de vie de la cellule dendritique en passant de l'état immature à l'un de deux autres états. Les trois signaux de sortie d'un DC remplissent deux rôles, pour déterminer si un type d'antigène est anormal et pour limiter le temps passé à échantillonner les données. Pour calculer les signaux de sortie intermédiaires, DCA applique l'équation de somme pondérée suivante :

$$C = \left(\frac{(W_{PAMP} * \sum_i PAMP_i) + (W_{SS} * \sum_i SS_i) + (W_{DS} * \sum_i DS_i)}{(W_{PAMP} + W_{SS} + W_{DS})} \right) * (1 + I) \quad (4.1)$$

Supposant qu'il existe plusieurs signaux par catégorie, ($PAMP_i$, DS_i , SS_i) sont les valeurs de signaux d'entrée de la catégorie PAMP, danger et sain pour tous les signaux (i) de cette catégorie. W_{PAMP}, W_{SS} et W_{DS} représentent les poids utilisés pour PAMP, SS et DS, respectivement. I représente le signal d'inflammation. Cette équation est répétée trois fois, une fois par signal de sortie. Ceci permet de calculer les valeurs de signal de sortie intermédiaires pour la sortie CSM, la sortie smDC

	Csm	Mature	Semi-mature
Pamp	2	1	2
Danger signal	0	0	3
Safe signal	2	1	-1

TABLE 4.1 – Matrice de poids prédéfinie

et la sortie mDC. Ces valeurs sont cumulées au fil du temps [47, 48]. Les pondérations utilisées par le DCA sont soit dérivées empiriquement des données, soit sont des valeurs définies par l'utilisateur. Par défaut, l'auteur de l'algorithme a proposé une matrice de poids selon les observations expérimentales illustrée dans la table 4.1 [48].

Chaque cellule dendritique de la population se voit attribuer une valeur de seuil de migration lors de sa création. Suite à la mise à jour des signaux de sortie cumulés, une cellule dendritique compare la valeur qu'elle contient pour la valeur CSM avec la valeur qui lui est assignée comme son seuil de migration. Si la valeur de CSM dépasse la valeur du seuil de migration, alors la cellule se retire de la zone d'échantillonnage et sa durée de vie est terminée.

Phase d'évaluation du contexte

Une fois qu'une cellule a migré, et à travers la phase d'évaluation du contexte, chaque cellule a la capacité de traiter et de collecter des signaux et des antigènes. Grâce à la génération de signaux de sortie cumulatifs, la cellule dendritique forme un contexte cellulaire qui est utilisé pour effectuer la détection d'anomalies dans l'évaluation des antigènes. En fait, lors de la migration, les signaux de sortie cumulés sont évalués et le plus grand signal de sortie entre semi-mature et mature devient le contexte de cellule. Ce contexte de cellule est utilisé pour étiqueter tous les antigènes collectés par la cellule avec la valeur de contexte dérivée de 1 ou 0. Cette information est finalement utilisée dans la génération d'un coefficient d'anomalie qui sera traité dans l'étape finale, c'est-à-dire la phase de filtrage (classification).

Phase de filtrage (classification)

La valeur dérivée du contexte cellulaire est utilisée pour dériver la nature de la réponse en mesurant le nombre de cellule dendritique qui sont pleinement matures et est représentée par la valeur d'antigène de contexte mature (MCAV). Le MCAV est utilisé pour évaluer le degré d'anomalie d'un antigène donné. Plus le MCAV est proche de 1, plus la probabilité que l'antigène soit

anormal est élevée. En appliquant des seuils à différents niveaux, une analyse peut être effectuée pour évaluer les capacités de détection d'anomalies de l'algorithme. Les antigènes dont les MCAV sont supérieurs au seuil anormal sont classés dans la catégorie anormale tandis que les autres sont classés dans la catégorie normale. La valeur de MCAV peut être calculer pour chaque antigène selon l'équation 4.2.

$$MCAV = \frac{cellules\_matures}{cellules\_echatillonees} \tag{4.2}$$

4 Exemple d'application du DCA

Cet exemple consiste à montrer l'application du DCA sur un problème financier pour évaluer le risque de crédit bancaire. Un extrait de l'ensemble de données pour cet exemple est présenté dans la table 4.2.

Client	Âge	Revenu	Nombre de carte de crédit	Durée de prêt	Crédit
Client1	24	650	1	30	non
Client2	30	1000	3	10	non
Client3	36	1300	3	8	oui
Client4	20	600	1	20	non
Client5	32	900	2	13	oui

TABLE 4.2 – Extrait de données évaluation de risque de crédit bancaire

Le DCA transforme les données brutes en données sous forme de signaux, sélectionne tout d'abord certains attributs et les pré-catégorise comme PAMP, DS et SS. Ensuite, l'ensemble de données obtenu est transformé en un ensemble de données de signal. Dans cet exemple, l'ensemble extrait de de données de signaux est illustré dans la table 4.3. Pour afficher les calculs dans différentes

Client (antigène)	PAMP	SS	DS
Client1	100	100	0
Client2	0	0	100
Client3	20	50	40

TABLE 4.3 – Extrait de signaux après transformation

conditions de signal d'entrée, trois itérations (cycles) avec trois ensembles de signaux sont affichés. Les valeurs de signal de sortie dérivées sont utilisées pour montrer comment effectuer le calcul MCAV pour trois types d'antigènes différents Ag1 (client 1), Ag2 (client 2) et Ag3 (client 3). Dans cet exemple, trois (cellule dendritique) DC sont nécessaires, un pour chaque itération, appelés DC1, DC2 et DC3 à des fins d'identification. Chaque DC se voit attribuer

une valeur de seuil de migration identique (seuil Csm) qui est fixée à 100. Les ensembles de signaux utilisés dans cet exemple sont présentés dans le tableau 4.3. Les équations de traitement du signal sont les suivantes :

	PAMP	SS	DS
CSM	2	1	2
smDC	0	0	1
mDC	2	1	- 1.5

TABLE 4.4 – Matrice de poids pour l'exemple

$$C_{Csm} = \left(\frac{(W_{PAMP1} * \sum_i PAMP_i) + (W_{SS1} * \sum_i SS_i) + (W_{DS1} * \sum_i DS_i)}{(W_{PAMP1} + W_{SS1} + W_{DS1})} \right)$$

$$C_{mature} = \left(\frac{(W_{PAMP2} * \sum_i PAMP_i) + (W_{SS2} * \sum_i SS_i) + (W_{DS2} * \sum_i DS_i)}{(W_{PAMP2} + W_{SS2} + W_{DS2})} \right)$$

$$C_{semi-mature} = \left(\frac{(W_{PAMP3} * \sum_i PAMP_i) + (W_{SS3} * \sum_i SS_i) + (W_{DS3} * \sum_i DS_i)}{(W_{PAMP3} + W_{SS3} + W_{DS3})} \right)$$

Les poids sont issus de la matrice prédéfinie dans la table 4.4, avant de commencer et comme dans la réalité, on doit procéder à la multiplication des antigènes dans le tissu. Le déroulement de l'algorithme sera comme suit :

1. On se suppose que le vecteur d'antigènes (A) est le suivant :
   A={Ag1 ; Ag1 ; Ag1 ; Ag1 ; Ag1 ; Ag2 ; Ag2 ; Ag2 ; Ag2 ; Ag3 ; Ag3 ; Ag3}
2. Cycle l = 0 :

   — DC échantillonne les antigènes du vecteur A aléatoirement, donc DC1 :
   a(m) ={Ag1 ; Ag1 ; Ag1 ; Ag2 ; Ag2}
   — DC échantillonne les signaux d'entrée, donc DC1 :
   s(m) = {100 ; 100 ; 0} DC calcule les signaux de sortie, donc les sorties DC1 :

$$C_{CSM} = (100 * 2) + (100 * 1) + (0 * 2) = 300$$

$$C_{smDC} = (100 * 0) + (100 * 0) + (0 * 1) = 0$$

$$C_{mDC} = (100 * 2) + (100 * 1) + (0 * -1,5) = 300$$

— Pour DC1, t(m) = 100, donc ce DC a maintenant dépassé son seuil de migration car la valeur pour C_{CSM} est supérieure à t(m).
De plus, $C_{smDC} < C_{mDC}$ et donc DC1 se voient attribuer une valeur de contexte de cellule de 1 indiquant que ses antigènes collectés peuvent être anormaux.

3. En supprimant les antigènes utilisés par DC1, le vecteur d'antigènes se compose désormais de :
   A = {Ag1 ; Ag1 ; Ag2 ; Ag2 ; Ag3 ; Ag3 ; Ag3}
4. Cycle l = 1 :

— DC échantillonne les antigènes au hasard, donc DC2 contient :
a(m) = {Ag2 ; Ag2 ; Ag1}
— DC échantillonne les signaux d'entrée, donc DC2 :
s(m) = {0 ; 0 ; 100}
— DC calcule les signaux de sortie, donc les sorties DC2 :

$$C_{CSM} = (0 * 2) + (0 * 1) + (100 * 2) = 200$$

$$C_{smDC} = (0 * 0) + (0 * 0) + (100 * 1) = 100$$

$$C_{mDC} = (0 * 2) + (0 * 1) + (100 * -1,5) = -150$$

— Pour DC2, t(m) = 100, donc ce DC a maintenant dépassé son seuil de migration car la valeur pour C_{CSM} est supérieure à t(m).
De plus, $CsmDC > CmDC$ et donc DC2 se voient attribuer une valeur de contexte de cellule de 0 indiquant que ses antigènes collectés sont susceptibles d'être normaux.

5. Le vecteur d'antigénes se compose maintenant de :
   A = {Ag1 ; Ag3 ; Ag3 ; Ag3}
6. Cycle l = 2 :
   — DC échantillonne les antigènes, donc DC3 :
   a(m) = {Ag1 ; Ag3 ; Ag3 ; Ag3}
   DC échantillonne les signaux d'entrée, donc DC3 :
   s(m) = {20 ; 50 ; 40}
   DC calcule les signaux de sortie, donc les sorties DC3 :

$$C_{CSM} = (20 * 2) + (50 * 1) + (40 * 2) = 170$$

$$C_{smDC} = (20 * 0) + (50 * 0) + (40 * 1) = 40$$

Antigène	présentations tissu	présentations maturées	MCAV
Ag1	5	3	0.6
Ag2	4	2	0.5
Ag3	3	0	0.0

TABLE 4.5 – Calcul MCAV de l'exemple

$$C_{mDC} = (20 * 2) + (50 * 1) + (40 * -1,5) = 30$$

Pour DC3, t(m) = 100, donc ce DC a maintenant dépassé son seuil de migration car la valeur pour C_{CSM} est supérieure à t(m).
En effet, $C_{smDC} > C_{mDC}$ et donc DC3 se voient attribuer une valeur de contexte de cellule de 0.

7. Les antigènes peuvent maintenant être analysés et les coefficients MCAV dérivés sont indiqués dans le tableau 4.5.
8. Pour effectuer la détection d'anomalies, un seuil doit être appliqué aux MCAV. Ce seuil est un paramètre défini par l'utilisateur qui nécessite des connaissances d'expert pour être défini et qui est spécifique à l'application. Dans ce cas, le seuil d'anomalie est défini par le responsable de la banque et est fixé à 0,47. Par conséquent, client1 (Ag1) et client2 (Ag2) sont classés comme anormaux (ils ne sont pas autorisés à avoir un crédit). Cependant, client3 (Ag3) est classé comme normal.

5 Avantages de l'algorithme de cellules dendritiques

Le DCA ainsi que ses versions ont été appliqués avec succès sur un large éventail d'applications. Cela est dû aux caractéristiques exprimées par le DCA car il présente plusieurs caractéristiques intéressantes et potentiellement bénéfiques pour les problèmes de classification binaire. En premier, l'algorithme effectue une corrélation temporelle qui relie les anomalies identifiées à leurs causes potentielles [50, 49]. Un autre avantage est que le DCA est capable de générer le coefficient (MCAV) pour chaque antigène. L'utilisateur ou l'expert peut prendre des décisions adéquates sur la manière de réagir contre l'antigène observé.

6 Inconvénients de l'algorithme de cellules dendritiques

Bien que le DCA ait des avantages, ça n'empêche pas qu'il existe des faiblesses de l'algorithme qui limitent son application aux problèmes. Les principales limitations du DCA sont présentées comme suit : La première est liée à la phase de prétraitement des données. La phase de prétraitement des données DCA est effectuée soit manuellement par les utilisateurs en fonction de leur connaissance approfondie d'un domaine de problème donné, soit automatiquement en utilisant essentiellement l'ACP, théorie des ensembles ou logique floue. Dans le cas où l'étape de prétraitement est effectuée manuellement, cela fait que l'algorithme dépend de l'application. Dans le cas où la phase de prétraitement est effectuée à l'aide du ACP, cela ne garantit pas que les premiers composants principaux sélectionnés seront les éléments les plus adéquats pour le filtrage. De plus, le processus de catégorisation DCA est basé sur le classement des attributs ACP en termes de variabilité. Cependant, ce processus de catégorisation ne peut être considéré comme une procédure de catégorisation cohérente. Dans le cas de sélection d'attributs en utilisant la théorie des ensembles et la logique floue et bien que cette méthode ait considérablement améliorée la phase de prétraitement, elle souffre d'être très lente vis à vis l'une des caractéristiques essentielles de cet algorithme est qu'il soit léger en termes de temps d'exécution.

Une autre limitation de l'algorithme est liée à ses poids utilisés pour la transformation du signal, vu dans la phase de détection de l'algorithme. Ces poids sont attribués statiquement ou sont des paramètres définis par l'utilisateur. Cela pourrait considérablement limiter la capacité de l'algorithme à s'adapter pleinement à un domaine de problème donné.

Une autre critique du DCA est le respect obligatoire de l'ordre des données dans les jeux de tests de données. En d'autres termes, l'algorithme ne doit être appliqué qu'aux ensembles de données ordonnés, les donnes doivent être ordonnées tous de classe 1 suivis de tous les éléments de données de classe 2, pour obtenir des résultats de filtrage satisfaisants.

De plus, l'application du DCA est essentiellement limitée aux problèmes de classification binaire. Depuis son développement, l'algorithme n'a été appliqué qu'aux problèmes de classification binaire où une classe est «normale» et l'autre «anormale». Cette restriction est due au fondement de l'algorithme lié au fait de classer chaque antigène soit comme un élément normal, soit comme un élément dangereux.

Le DCA dès son fondement n'a pas été conçu pour qu'il soit un algorithme de classification, les auteurs de cet algorithme ont bien précisé que cet algorithme est un algorithme de corrélation et de filtrage adaptatif, il n'a aucune capacité de recherche. Il s'appuie sur des connaissances d'experts (ou de méthode automatique qui n'est pas propre à l'algorithme) pour définir les paramètres et produire une catégorisation du signal.

7 Conclusion

Dans ce chapitre, nous avons présenté les notions de base de la théorie du danger et fondamentalement les concept clés du DCA. Nous avons détaillé les différentes phases de l'algorithme et également discuté des principaux travaux effectués sur la phase de prétraitement du DCA tout en identifiant les points forts et les faiblesses de l'algorithme. Dans le prochain chapitre, nous présenterons une autre solution qui permet de réduire la dimensionnalité de données tout en gardant leurs propriétés, cette solution comme étant un outil d'alléger l'algorithme dans pour la phase de prétraitement et garder un taux de précision élevé.

Chapitre 5

Algorithme de cellules dendritiques basé sur la factorisation matricielle non-négative

L'algorithme de cellule dendritique est composé de quatre phases qui sont illustrées dans la figure 5.1, comme mentionné dans les sections précédentes l'amélioration de l'algorithme était sur la partie prétraitement, où on a appliqué la technique de sélection d'attributs en utilisant l'ACP [54], la théorie des ensembles [21, 22, 24] ou encore la logique floue [23]. Pour chaque méthode appliquée, on a remarqué qu'elle souffre de quelques inconvenants dont on essaie d'améliorer le fonctionnement de cet algorithme par rapport à la phase du prétraitement en gardant un taux de précision et en réduisant le temps de traitement.

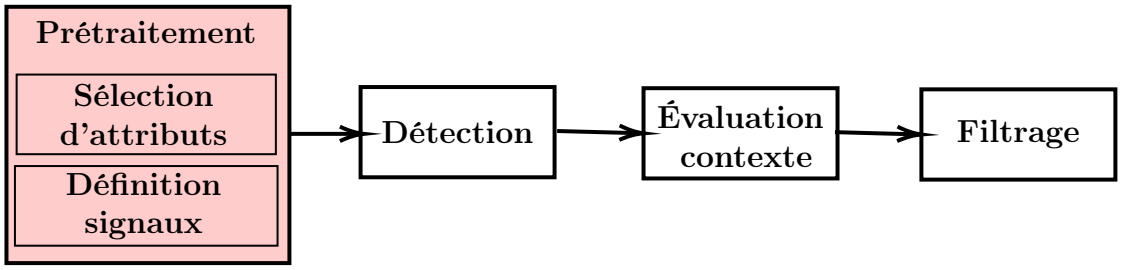

FIGURE 5.1 – Phases du DCA

1 Problématique

Les premières versions du DCA nécessitait l'intervention manuelle des experts du domaine pour extraire des connaissances afin de les assigner à leurs propres signaux, et le processus devient plus difficile à gérer dans les grandes dimensions et en fonction du domaine appliqué. Dans [54], les auteurs ont appliqué l'analyse en composantes principales (ACP) pour automatiser la phase de prétraitement en fonction de sa pertinence et de son importance [9], pour maximiser la variance des attribues importants sélectionnées et ainsi réduire le bruit et la redondance des données. Cette première étape est la sélection des attribues, suivie de la catégorisation des signaux (PAMP, SS, DS), en projetant le ACP en fonction de leur variabilité, par rapport à l'analyse de corrélation et au gain d'information [53]. Le ACP permet l'automatisation avec un taux de précision acceptable [54]. L'utilisation de l'ACP présente l'inconvénient de la projection vers l'espace de réduit à partir des attribues originales.

Une version plus récente de DCA est présentée dans [21] pour contourner les inconvénients rencontrés dans l'ACP en introduisant le concept de théorie des ensembles approximatifs [25] REDUCT and CORE et en présentant le RST-DCA [6,8]. Le concept a été appliqué pour sélectionner les attribues dans la phase de prétraitement de DCA en conservant ceux qui sont informatifs et en supprimant ceux qui ne sont pas nécessaires en utilisant le concept des ensembles approximatifs. Le REDUCT conserve la même qualité que les données d'origine. Il attribue des signaux pratiques en utilisant une fonction attribuée à la fois à PAMP et à SS car ils représentent les signaux les plus significatifs. Les autres caractéristiques désignées comme DS (signaux de danger) Dans la même perspective, pour sélectionner des fonctionnalités informatives, [25, 22] a proposé le RC-DCA et modifier le processus de catégorisation en affectant chaque attribut à sa propre catégorie de signal. Il montre dans [25] que RST-DCA et RC-DCA ont effectué des calculs inutiles et ont consommé plus temps et de ressources pour faire face à cet inconvénient. L'auteur a montré qu'une seule réduction serait suffisante pour réduire les données. Tel que défini dans le DCA original, il est censé être un algorithme léger. QR-DCA a donc géré cela en implémentant l'algorithme Quickreduct pour réduire considérablement le temps de gain et optimiser davantage de ressources et de temps. Les solutions citées sont réalisées en termes de précision et mettent en évidence l'amélioration du DCA. Le DCA original a été conçu pour être un algorithme léger. Alors que l'utilisation de la théorie des ensembles approximatifs ou la théorie des ensembles flous dans la phase de prétraitement prend un temps considérable [23, 66] et affecte les avantages de nature de cet algorithme. D'autre part,

en temps réel, les données peuvent être progressivement affinées, et les informations concernant le domaine du problème peuvent activement ajouter ou supprimer des connaissances, et la nature des données modifiée. Et certaines fonctionnalités peuvent changer leur influence sur les données au fil du temps.

2 Factorisation matricielle non-négative

La factorisation matricielle non négative (NMF) [69] est un algorithme de réduction d'espace et d'extraction d'attributs de pointe relativement nouveau proposé pour découvrir des structures latentes de faible dimension intrinsèques à un espace de données de haute dimension en fournissant une représentation non négative des données originales et basée sur des parties. [13, 42, 70, 69, 112]. L'idée de base est similaire à la décomposition inférieure supérieure connue comme les analyses en composantes principales (PCA) [110] et la quantification vectorielle [46] (VQ).

De la figure 5.2, prenant une matrice de données initiale $V = v_1, v_2, ..., v_n \in R^{n \times m}$. Le but de la factorisation NMF est de trouver deux matrices non négatives $W = [w_{ik}] \in R^{n \times r}.H = [h_{kj}] \in R^{r \times m}$ qui se rapproche de la matrice originale V avec la minimisation de l'erreur. La factorisation WH peut être écrite en termes de vecteurs colonnes : $v \approx Wh$ où v et h sont les vecteurs colonnes correspondantes de V et H. La combinaison linéaire de colonnes de W pondérée par les composantes de h représente l'approximation de la colonne correspondante de v, vu W comme contenant des vecteurs de base optimisés de l'approximation linéaire de V [69] (La matrice W est appelée matrice de base et matrice d'encodage H matrice de coefficient).

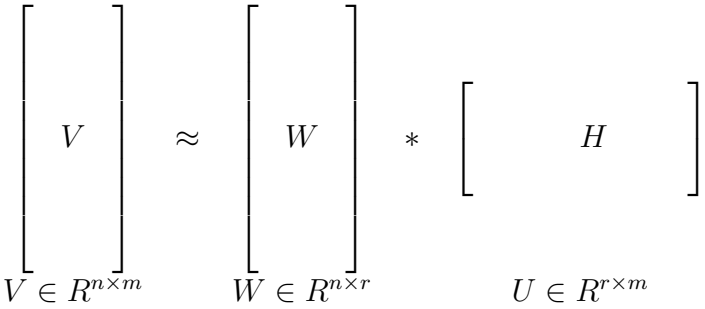

FIGURE 5.2 – Factorisation matricielle non négative

NMF est un relativement nouvel outil pour réduire la dimensionnalité des données par la combinaison linéaire des bases (W) et des poids (H). L'avantage d'utiliser NMF au lieu des autre méthodes de factorisation telle que la décomposition en valeurs singulières (SVD) ou l'analyse en composantes prin-

cipales (ACP) est dû à ses avantages [40]. Premièrement, le NMF est facilement interprétable. D'après [69], la contrainte de non-négativité produit une représentation additive de partie, et par conséquent, les facteurs W, H sont en général naturellement creuse. De plus, NMF interprète ses facteurs de façon remarquable, Grâce au premier avantage, par rapport aux autres techniques de factorisation, NMF permet d'économiser plus de stockage et de ressource en termes de facteurs denses [68]. La factorisation matricielle n'étant pas une solution unique et ne pouvant être résolue analytiquement en général, la solution est donc une approximation numérique, et elle consiste à résoudre un problème d'optimisation non linéaire dans l'équation 5.1 :

$$min \parallel V_{(n\times m)} - W_{(n\times r)}H_{(r\times m)} \parallel^2 /V, W, H \geq 0 \tag{5.1}$$

Le rang r est défini par l'utilisateur empiriquement suivant la règle générale $r < \frac{nm}{n+m}$ [81, 41] et la fonction de coût pour mesurer l'erreur entre la matrice d'origine V et ses facteurs W et H comme mentionné dans l'équation 5.2, elle représente une norme qui est appelée norme de Forbenius (distance euclidienne carrée entre deux matrices) [84], avec la possibilité d'utiliser d'autres fonctions de coût alternatives [69, 33, 83].

$$ER = \parallel V - WH \parallel^2 = \sum_{i,j}(x_{i,j} - \sum_{r=1}^{r} w_{ir}h_{rj})^2 \tag{5.2}$$

Pour trouver la factorisation $V \approx WH$, nous pouvons utiliser l'une des approches itératives suivant les règles proposées dans [70]. Les itérations se poursuivent jusqu'à la convergence vers le minimum local satisfaisant la fonction de coût.

$$W_{ir} = W_{ir}\frac{[VH^T]_{ir}}{[WHH^T]_{ir}} \quad H_{rj} = H_{rj}\frac{[W^TV]_{rj}}{[W^TWH]_{rj}} \tag{5.3}$$

Initialement, le NMF peut être lent à converger vers un minimum global [15], pour les données à grande échelle V, car W et H ne sont pas uniques. Le problème de minimisation est non-convexe, des travaux comme [79, 65, 41] sont venus pallier les inconvénients et mieux améliorer cette méthode. Le NMF a été appliqué avec succès dans des domaines [105] tels que l'imagerie hyperspectrale, le traitement d'image, l'exploration de texte et d'autres applications, notamment le regroupement de documents, les systèmes de recommandation, l'analyse musicale, la biologie informatique et l'environnement.

3 Solution proposée

Dans cette section, on va présenter un modèle qui est basé sur la factorisation matricielle non négative [12] pour automatiser la phase de prétraitement du DCA. Pour cela, la solution comprend les deux étapes, la sélection des attributs transformés et la catégorisation de ses attributs vers les signaux appropriés. En plus, les capacités humaines montrent leurs limites lorsque la taille de données s'élargisse, alors que des efforts importants et des recherches faites pour gérer et aider les humains à analyser et à extraire des informations utiles et latents. Une des solutions, le mécanisme de réduction de dimensionnalité est évident et essentiel pour faire face à la malédiction de la dimensionnalité et réduire l'effort humain à réduire la complexité.

Le processus de réduction de dimensionnalité obtient un nouvel espace réduisant la dimension des données d'origine, ce qui optimise les ressources et le temps, tout en augmentant les performances de classification et réduisant la complexité des données.

La réduction de dimensionnalité a montré son efficacité dans différents domaines. Deux techniques dominantes existent dans la réduction de dimensionnalité : la sélection et l'extraction d'attributs. La sélection d'attributs est le processus de sélection d'un sous-espace contenant les attributs les plus informatives et pertinentes à partir des données originales, et le nouvel espace réduit peut mieux décrire l'espace original, le processus de sélection d'attributs réduit les coûts de calcul tout en gardant un équilibre entre efficacité et précision de classification, ce qui est fortement recommandé pour gérer les données de large dimension.

D'autre part, on utilise des méthodes de réduction d'attributs pour trouver les facteurs minimaux faiblement corrélés ou non corrélés et extraire les propriétés cachées des données. Cette technique peut mieux décrire les données originales tout en ajoutant des propriétés cachées d'attributs. Le processus de réduction des fonctionnalités se fait en transformant les données originales vers un nouvel espace réduit composé de nouvelles fonctionnalités de valeur tout en réduisant la complexité de calcul en termes de temps et d'espace de stockage, en plus de la découverte d'une structure latente cachée dans les données, et ainsi obtenir l'avantage de la réduction de dimension.

En plus des avantages mentionnés ci-dessus, NMF évite le surajustement dans un contexte de prédiction. Cet avantage est essentiel pour réduire les faux positifs/négatifs, ce qui implique que NMF exprime mieux le problème d'évolutivité et d'éparsité améliorant les performances de prédiction. NMF a été principalement utilisée pour factoriser la matrice de données sous contrainte

non négative. Par conséquent, il peut extraire automatiquement des facteurs épars facilement interprétable. Comparé à l'ACP, NMF ne supprime pas la signification de données, ce qui conduit à des valeurs non négatives. Par conséquent, il peut conserver plus d'informations que l'ACP [89].

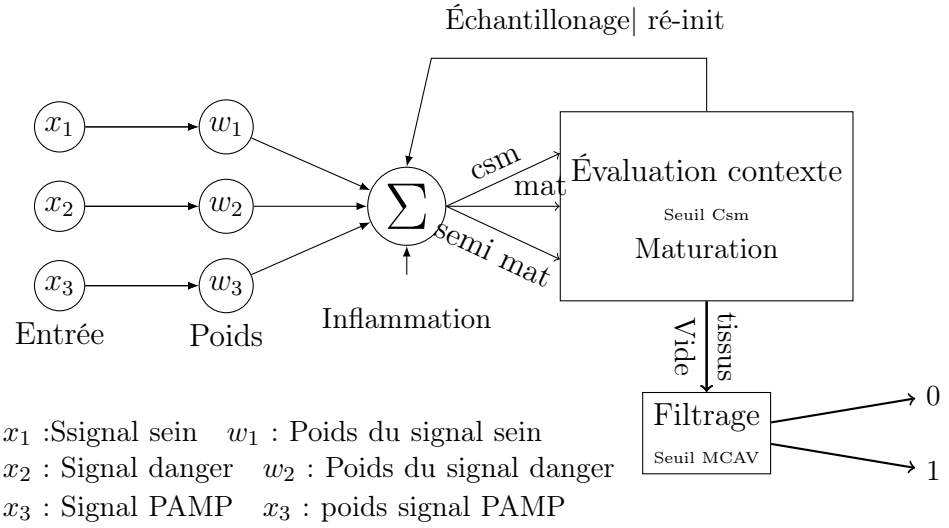

FIGURE 5.3 – Résumé de l'abstraction du DCA

La figure 5.3 [11] résume l'algorithme 4 et illustre l'abstraction du fonctionnement de la cellule dendritique. La motivation de travailler sur la phase du prétraitement est justifiée par le fait que les entrées des signaux (seins, danger et PAMP) doivent représenter les données originales le plus possible tout en s'adaptant à l'équation 4.1, la concentration de chaque signal représentera son importance dans une cellule dendritique, cette importance est supportée par le poids adéquat mentionné dans la matrice des poids par défaut (voir la table 4.1).

La solution proposée surmonte la limitation du temps d'exécution et l'utilisation de ressource en introduisant la factorisation matricielle non négative, en améliorant la factorisation des données d'origine et en réduisant les données d'origine sans affecter ou perdre une partie des données. En outre, NMF n'a besoin d'aucune hypothèse statistique sur les données d'origine mais repose sur la contrainte non négative, qui est plus pratique pour représenter les données [69].

Pour faciliter et alléger le processus de la factorisation NMF sur le DCA, on peut faire un prétraitement sur les données originales à fin d'avoir un espace réduit de qualité, il consiste à traiter les données de base, pour cela on on peut appliquer les techniques suivantes :

— Préparation et le nettoyage de données qui est un processus de détection

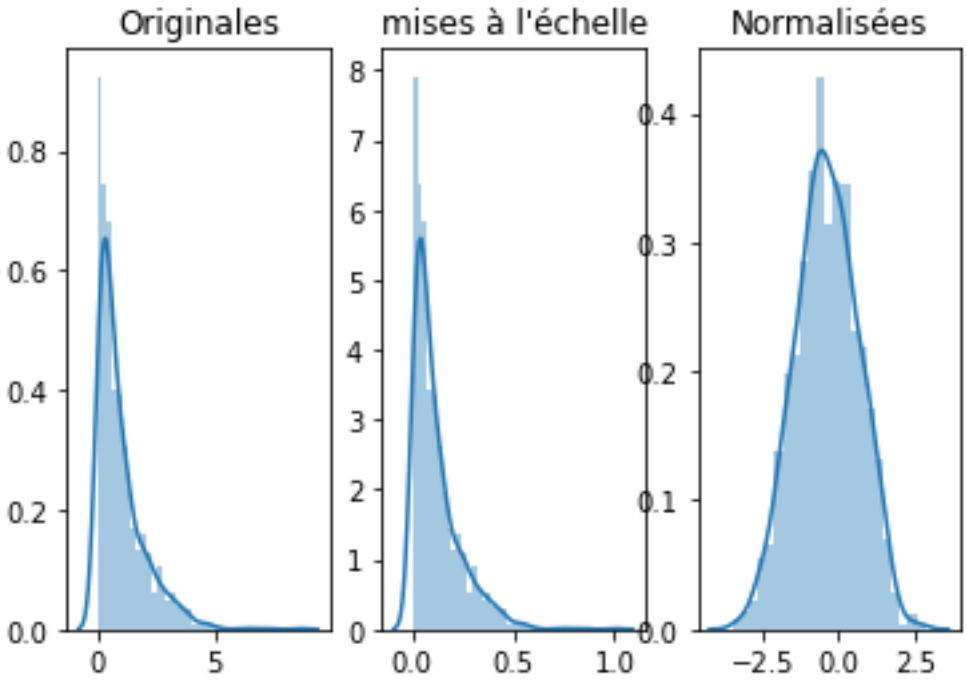

FIGURE 5.4 – Différence entre normalisation et mise à l'échelle

et de correction (ou certains cas la suppression) de lignes ou colonnes corrompues, inexactes, incomplètes ou impertinentes des données, puis remplacer, modifier supprimer les données grossières.

— Mise à l'échelle et normalisation : La mise à l'échelle des attributs est essentiellement utilisée pour les algorithmes d'apprentissage automatique qui calculent les distances entre les données, par conséquence, la portée de toutes les entités doit être mise à l'échelle afin que chaque entité contribue approximativement proportionnellement métrique finale. La normalisation consiste à à diviser par une norme de l'attribut. Il se réfère également souvent à la remise à l'échelle par le minimum et la plage du vecteur (attribut), pour que tous les éléments se situent généralement entre 0 et 1, ramenant ainsi toutes les valeurs des colonnes numériques de l'ensemble de données à une échelle commune. La différence entre les deux techniques est que lors de la mise à l'échelle, on modifie la plage des données tandis que dans la normalisation, on modifie la forme de la distribution des données, un exemple concret illustré par la figure 5.4 qui montre que la mise en échelle ne modifie pas la distribution de données alors que la normalisation le fait. Cette technique permet de rendre tous les éléments de la matrice originale positifs pour la factorisation NMF.

3.1 Transformation d'espace de données

Dans de nombreuses situations, lorsqu'on tente de modéliser un phénomène particulier, les valeurs négatives sont simplement insignifiantes. Par exemple, une hauteur négative pour les personnes ou un nombre négatif de visites sur un site Web ne sont que quelques-unes des variables discrètes-continues ou discrètes qui sont tout à fait absurdes en termes d'estimation finale.

NMF donne une meilleure projection des données tout en conservant la structure de données d'origine préservée. Après avoir effectué une préparation de données par comparaison avec d'autres méthodes de factorisation en raison de ses contraintes non négatives, il décompose les données en produit de deux matrices de rang inférieur non négatives W et H. La matrice de base contenue dans la sous-matrice W et la matrice H contient des poids (coefficients). L'algorithme NMF commence à modifier W et H jusqu'à atteindre la convergence. L'algorithme garantit que les deux matrices W et H sont non négatives et s'approchent des données originales approximativement, étant donné que les valeurs aberrantes peuvent avoir un impact significatif sur la factorisation. Pour améliorer la factorisation matricielle tout en bénéficiant de la normalisation, il faut diminuer la tolérance d'erreur. Initialement, NMF doit commencer par une initiation ((c'est-à-dire une valeur initiale pour $W0$ et (ou) ou $H0$) indiquant le début des itérations car il n'y a pas de minimum global et la dimensionnalité des données est considérablement large, il est crucial d'avoir une initialisation appropriée pour obtenir des résultats significatifs. On lance l'initialisation (seed) de façon aléatoire afin que W et H prennent une distribution uniforme.

Le choix du rang réduit de factorisation r est défini par l'utilisateur de manière empirique, en utilisant des connaissances d'experts ou simplement, dans notre cas, l'essai et erreur [41] est utilisé. On teste r choisi dans une plage allant de 2 à $min(m, n)$ où m est le nombre d'attributs et n le nombre d'échantillons des données (instances). Dans chaque valeur choisie, on calcul la fonction de coût de distance euclidienne entre les données d'origine et le produit de ses facteurs W et H (équation 5.1), on choisit la valeur de distance minimale.

En résumé, la solution proposée améliore la phase de prétraitement du DCA, en tenant compte de la force de la décomposition matricielle ou cette technique scinde les données (en tant que matrice V) en un produit de deux matrices W et H. L'objectif ici est d'obtenir la matrice H qui représente les données dans une dimension réduite avec des caractéristiques équivalentes, et de sorte que leur multiplication matricielle nous donne la matrice V. La figure

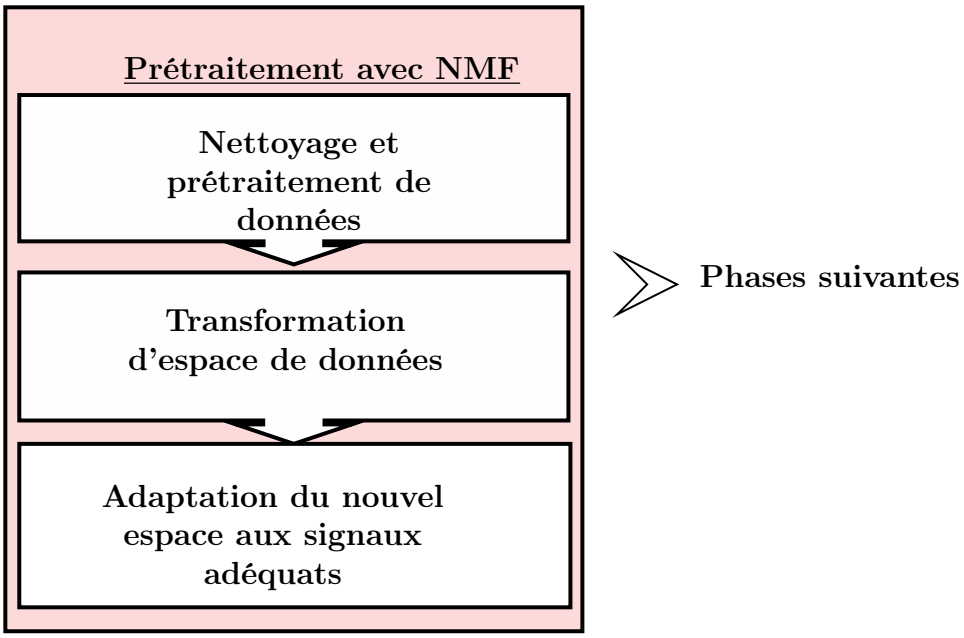

FIGURE 5.5 – Phases du DCA avec NMF

5.5 illustre la solution proposée en sous phases dont la première est de nettoyer et prétraiter les données, la deuxième consiste à transformer les données issues de la première sous phase en un espace réduit par le biais de la factorisation matricielle non négative, et finalement, la troisième sous phase affecte le nouvel espace de données dans sa catégorie du signal adéquat (SS, DS ou PAMP).

3.2 Catégorisation du signal

Après avoir transformé les attributs originaux en utilisant la réduction NMF dans la phase de prétraitement et comme souligné dans la section précédente où une réduction d'espace a été traitée pour transformer les données d'origine en un espace de rang plus bas, la deuxième étape consiste à affecter les signaux ou les attributs transformés à leur signal approprié. Ce processus reflète l'importance de chaque colonne résultante affecté au bon signal, rappelant les points vitaux suivants pour les signaux existants dans l'algorithme DCA :

- Signaux PAMP : des anomalies sont susceptibles d'exister lorsque ces signaux sont présents
- Signaux saines (SS) : indiquent que le système est sûr et qu'aucune anomalie n'est présente
- Signaux de danger (DS) : ces signaux sont moins importants pour les autres. La cellule qui subit des dégâts envoie un signal de danger, leur présence augmente une la probabilité d'anomalie mais inférieure que le

signale PAMP.

Selon l'étendue du signal de danger DS, il ne suffit pas de définir un contexte final pour l'antigène comme normal ou anormal car sa présence peut signifier une anomalie mais avec une faible probabilité car elle peut être normale. Cependant, la concentration de deux autres signaux PAMP et SS peut définir un contexte de conclusion d'antigène. Ceci est traduit par l'équation 4.1 si on considère la matrice de poids par défaut dans [48]. Dans le tableau 4.1 qui montre que les poids de la première colonne (sortie co-stimulatrice) contiennent des poids élevés sont donnés au signal SS et PAMP tandis que le poids du signal de danger est moins important. Cela donne un signal PAMP and SS plus important pour décider s'il y a une anomalie ou non. La matrice de base W est l'espace réduit des données originales. Il représente les informations essentielles pondérées par la matrice de coefficients H, considérant cette matrice comme cachée. La première colonne représente donc une partie à forte concentration de la signification de données originales. En d'autres termes, le premier vecteur est le plus informatif, on l'affecte donc ce vecteur aux deux signaux SS et PAMP car ils représentent des signaux informatifs et significatifs.

L'algorithme calcule automatiquement un seuil pour générer une concentration pour PAMP et SS, par rapport à chaque élément de la matrice W. Si sa valeur est inférieure au seuil, nous attribuons la concentration de PAMP à la valeur correspondante et on attribut zéro au signal SS, et s'il est supérieur au seuil, le signal de sécurité prend la valeur et PAMP est mis à zéro.

L'importance des autres colonnes restantes dans la matrice de base est moins critique que la première, et on combine les colonnes restantes de nouvelles attributs transformés pour former le signal de danger (DS).

4 Évaluation expérimentale

L'objectif principal de ce travail est de montrer que la solution proposée, utilisant la factorisation matricielle dans la phase de prétraitement de l'algorithme DCA, peut être utilisée et améliorer la capacité de détection du DCA en moins de temps. L'expérience est réalisée sur un ensemble de données. Ces données sont des classes binaires sélectionnées dans la base de données WBC [37] et d'autres données avec des valeurs numériques, ils sont répertoriés dans le tableau 5.1. L'expérience a été réalisée sur un processeur Dell Intel (R) Xeon (R) E5-2670 v2 à 2,50 GHz , codé en langage Python 3,6 / 64 bits.

On a gardé le même environnement d'expérimentation les travaux de l'état de l'art [54, 24]. L'expérience a été réalisée sur une population de cent cellules

TABLE 5.1 – Description de données

Nom	Ref	Instances	Attributs
Breast cancer wisconsin (Original)	Breast 10	699	10
Breast cancer wisconsin (Diagnostic)	Breast 32	569	32
SPECTF Heart	Spectf	267	44
Red wine quality	Red wine	1599	12
Sonar, mines vs. Rocks	Sonar	208	60
Congressional voting	Vote	435	16
Statlog (Heart)	heart	270	16
Liver disorders	Bupa	345	7

et dix cellules dendritiques échantillon le vecteur antigénique à chaque cycle. Le seuil de maturation (Csm) est généré automatiquement pour chaque DC à chaque cycle [50]. Nous avons également utilisé la matrice de poids prédéfinie utilisée pour la transformation du signal du DCA identique à celle définie dans la plupart des travaux (voir tableau 4.1).

4.1 Description de données

Pour montrer l'efficacité du NMF dans la phase de prétraitement du DCA, on a comparé à deux méthodes la première et celle des ensembles approximatifs : l'algorithme Quick-reduct (QR-DCA), elle a été choisie pour sa rapidité d'exécution par rapport les autres méthodes existantes, et la deuxième méthode est l'application de l'ACP dans le prétraitement. Rappelant que l'objectif principal de cette étude est de montrer la faisabilité d'utiliser la réduction de dimensionnalité basée sur la factorisation matricielle non négative et qu'elle permet de donner un taux de précision élevé tout en optimisant le temps d'exécution.

4.2 Métriques d'évaluation

Précision

La précision est une métrique pour évaluer les modèles de classification. De manière informelle, la précision est la fraction des prédictions que notre modèle

Vrai positif (TP) : Situation : Maligne Prédiction du modèle : Maligne Nombre de résultat TP : 2	Faux positif (FP) Situation : Benigne Prédiction du modèle : Maligne Nombre de résultat FP : 2
Faux Negatif (FN) : Situation : Maligne Prédition du modèle : Benigne Nombre de résultat FN : 16	Vrai negatif (TN) : Situation : Benigne Prédition du modèle : Benigne Nombre de nombre TN : 180

TABLE 5.2 – Un exemple de précision

a obtenues correctement. Formellement, la précision a la définition suivante :

$$Précision = \frac{Nombre \quad de \quad prédictions \quad correctes}{Nombre \quad total \quad de \quad prédictions} \tag{5.4}$$

La précision est également utilisée comme mesure statistique dans laquelle un test de classification binaire identifie ou exclut correctement une condition. Autrement dit, la précision est la proportion de prédictions correctes (à la fois vraies positives et vraies négatives) parmi le nombre total de cas examinés. Dans ce contexte, [77] compare les estimations de la probabilité avant et après le test. La formule pour quantifier la précision binaire est :

$$Précision = \frac{TP + TN}{TP + TN + FP + FN} \tag{5.5}$$

où :

— TP = Vrai positif.
— FP = faux positif.
— TN = Vrai négatif.
— FN = faux négatif.

Prenant un exemple résumé dans la table 5.2 pour calculer la précision pour le modèle suivant qui a classe 200 tumeurs comme malignes (classe positive) ou bénignes (classe négative). La précision est égale à

$$Précision = \frac{TP + TN}{TP + TN + FP + FN} = 91\%$$

Notant bien que les concepts de précision tels que définis par l'ISO 5725-1 ne sont pas applicables. Une des raisons est qu'il n'y a pas une seule «valeur vraie» d'une quantité, mais plutôt deux valeurs vraies possibles pour chaque cas, alors que la précision est une moyenne dans tous les cas et prend donc en compte les deux valeurs. Cependant, le terme précision est utilisé dans ce

contexte pour désigner une métrique différente issue du domaine de la recherche d'informations.

Sensibilité

Elle mesure la proportion de positifs qui sont correctement identifiés (c'est-à-dire la proportion de ceux qui ont une condition (affectée) qui sont correctement identifiés comme ayant la condition, en d'autres termes Taux de vrais positifs), elle calculé par l'équation suivante :

$$Sensibilité = \frac{TP}{TP + FN} \tag{5.6}$$

La sensibilité fait référence à la capacité du test à détecter correctement les patients malades qui en sont atteints. Dans l'exemple, la sensibilité du test est la proportion de personnes dont le test est positif pour la maladie parmi celles qui en sont atteintes. Si on prend l'exemple précédant. La sensibilité est égale à : 11.11%

Spécificité

La spécificité mesure la proportion de négatifs correctement identifiés (c'est-à-dire la proportion de ceux qui n'ont pas la condition (non affectés) qui sont correctement identifiés comme n'ayant pas la condition, ou le taux de vrai négatif), elle se calcule par l'équation :

$$Spécificité = \frac{TN}{TN + FP} \tag{5.7}$$

La Spécificité de l'exemple précédant vaut 90%. En général, les tests à haute sensibilité ont une faible spécificité. En d'autres termes, ils sont bons pour attraper des cas réels de la maladie, mais ils sont également accompagnés d'un taux assez élevé de faux positifs. Les mammographies sont un exemple de test qui a généralement une sensibilité élevée (environ 70-80%) et une faible spécificité [86]. En plus des métriques citées, On ajoute le temps de calcul pour que l'algorithme termine toutes les phases, la phase qui nous intéresse le plus est la phase de prétraitement.

4.3 Application et comparaison des résultats

Pour commencer, on fait une préparation de données, cette étape est nécessaire pour exécuter l'algorithme NMF en raison de sa contrainte non négative, la préparation est poursuivie en appliquant des fonctions de normalisation et

	Précision			Sensibilité			Spécificité			Temps (secs)	
	NMF	QR	PCA	NMF	QR	PCA	NMF	QR	PCA	NMF	QR
Breast 10	98.92	79.80	89,95	99.50	78.61	98,24	98.88	82.26	85,60	3.06	11.62
Breast 32	98.85	90.50	97,28	98.96	93.99	94,96	99.00	74.52	98,66	4.15	44.08
Vote	96.09	93.97	89,45	98.4	98.97	72,16	94.09	89.94	99,71	1.46	3.84
Bupa	94.73	99.42	68,11	90.97	98.62	81,50	97.26	99.01	49,65	1.10	1.2
Stat heart	91.08	75.36	58,14	86.31	83.52	11,66	93.49	65.35	95,33	1.27	3.34
Red wine	89.63	79.92	84,35	92.12	74.72	58,96	87.37	90.75	99,43	2.10	22.54
Spectf	84.81	91.98	86,08	94.04	69.68	63,78	85.04	91.64	80,40	1.05	6.58
Sonar	67.31	80.23	85,06	93.67	97.94	61,79	59.12	97.3	98,87	0.69	8.56

TABLE 5.3 – Résultats comparatifs

de mise à l'échelle. La fonction de normalisation commence par calculer la matrice de base (nouvelle matrice de faible dimension) puis en utilisant le concept d'essai et d'erreur pour trouver le rang inférieur r, la meilleure approximation de la distance entre les données originales et la matrice de produit factorisée (norme de Forbenius) de qui est choisie en calculant min $\| V - WH \|^2$.

L'étape suivante consiste à définir pour chaque nouvel attribut de la nouvelle matrice sa catégorie de signal adéquate (PAMP, SS ou signal de danger), car la présence du signal PAMP et du signal de sécurité indique une anomalie dans le tissu la première colonne est attribuée aux deux PAMP et le signal de sécurité et d'autres colonnes sont attribués à la moyenne du signal de danger.

Ensuite, on utilise les nouvelles données obtenues à partir du processus précédant et effectuer le processus de multiplication [47] pour préparer plusieurs signaux fusionnés avec des marqueurs antigéniques à utiliser dans l'étape de maturation. Les seuils de filtrage sont générés automatiquement à partir de données d'origine. Le résultat est représenté par la moyenne de 10 exécutions.

Le premier ensemble de données "Breast Cancer Wisconsin (Original)" extrait du référentiel d'apprentissage automatique UCI [37] est un ensemble de données de classification binaire, qui enregistre les mesures des cas de cancer du sein. Il existe deux classes, bénignes et malignes. Cet ensemble de données a une dimensionnalité 9 attributs normalisés et misent à l'échelle prenant des valeurs entre 0-10. La classe maligne de ces données prenne la valeur 1, tandis que les points de la classe bénigne prennent la valeur 0. Nous avons choisi cet ensemble de données parce que le DCA a été appliqué [48] sur ces données par un prétraitement manuel effectué par des experts dans le domaine d'oncologie.

Pour déterminer l'efficacité de la factorisation matricielle non négative sur l'algorithme des cellules dendritiques en tant que phase de prétraitement et surmonter la limitation du temps d'exécution comparant les travaux antérieurs, nous avons appliqué une réduction des attributs sur l'ensemble de données de

classe binaires, et ordonnés (classe 1 suivie de classe 2). Cette transformation est basée sur une factorisation matricielle NMF non négative et utilisait les nouvelles données réduites comme signal d'entrée (SS, PAMP et signal de danger) vers le DCA.

La table 5.3 issue des travaux [12], illustre les résultats de la nouvelle méthode en les comparant avec deux méthodes de l'état de l'art la première étant considérée comme rapide et efficace basée sur la théorie des ensembles [24] qui est l'algorithme *Quick reduct* [62] et la deuxième basée la sélection des attributs en utilisant ACP [54]. Nous avons ajouté aux métrique usuelles le temps de calcul pour les deux méthodes essentiellement NMF et QR. Pour le premier jeu de données, breast10 à partir des résultats du tableau 5.3, qui montrent un haut taux de précision avec plus de 98% en 3 secondes. La sensibilité et la spécificité sont supérieures à 98% . Par rapport à l'algorithme QRDCA, la précision était d'environ 79,80% inférieure à la NMF en termes de précision, traitée en 11,62 secondes pour terminer l'exécution. La précision de données breast32 dépasse 98% avec une sensibilité de 97,68% et une spécificité de 99% en un temps total de 4,15 secondes, tandis que QRDCA a pris plus de 44 secondes avec une précision de 90,50.

Les données vote donne également un résultat cohérent avec une précision de 96,06% et une sensibilité de 98,40% . En même temps, la spécificité a diminué. On a également remarqué qu'il fallait 1,46 seconde pour réaliser la tâche, en comparant le QRDCA qui l'a fait en 3,84 secondes. Contrairement à l'ensemble de données Bupa, la précision du QRDCA a surpassé le NMFDCA avec une sensibilité de 99,42%, 98,62% et une spécificité de 99.01% en 1,20 seconde, tandis que la précision du NMFDCA était inférieure à la précédente avec 94,73% en contournant le QRDCA en 1,10 secondes.

La précision de l'ensemble de données Redwine était d'environ 89,63%, 92,12% de sensibilité et 87,37% de spécificité traités en 2,10 secondes. De plus, la précision était d'environ 79,92% pour QRDCA obtenue en 22,54 secondes. Remarquablement, les taux de jeu de données Spectf utilisant QRDCA surpassent NMFDCA avec un taux de précision de 91,98% contre 84,81 et 85,04% contre 91,64% de spécificité. Cependant, la sensibilité NMFDCA était plus importante avec 94,04% contrairement au QRDCA avec 69,68%.

Pour l'utilisation du ACP dans la phase de prétraitement du DCA, On a remarqué que l'ACP a surmonté QRDCA dans les deux premières données Breast10 et Breast 32, par plus de 89% et 97%, alors que dans les data-sets Vote, Bupa et Stat heart l'ACP n'a pas pu surpasser le QRDCA, NMFDCA a enregistré le taux le plus élevé de la précision par rapport les deux autres

méthodes. Sauf pour Spectf et sonar, avec 91.98% pour QRDCA et 86.08% pour l'ACP. Pour le data-set Sonar l'ACP a pris l'avantage par rapport les deux autres méthodes.

4.4 Discussion et analyse

Dans le premier jeu de données, breast10, l'excellente précision avec 98,54% se traduit par la haute qualité de la factorisation, où elle donne une représentation très proche des données d'origine, ce qui signifie que l'erreur est insignifiante. Par rapport à l'ensemble approximatif [24], le processus de sélection des fonctionnalités utilisant l'ensemble approximatif a pris plus de 11,62 secondes pour sélectionner les fonctionnalités pertinentes avec un taux de précision de 79,80% tandis que NMF n'a pris que 3,06 secondes pour réaliser l'ensemble du processus. Dans ce cas, le processus de sélection des fonctionnalités n'a pas été en mesure de catégoriser les fonctionnalités sélectionnées selon le signal approprié, en particulier le signal sûr et le signal sonore, le signal le plus significatif et crucial pour les résultats finaux.

Parce que QRDCA sélectionne la première fonctionnalité émise par l'algorithme de sélection de fonctionnalités QR comme signal sûr et la seconde comme PAMP ne signifie pas que nous ne pouvons pas attribuer d'autres fonctionnalités au signal choyé ou sûr. Le processus de sélection des fonctionnalités n'était donc pas suffisant pour catégoriser les fonctionnalités sélectionnées.

Le sein32 prend le même chemin que le premier avec un taux de précision raisonnable, mais a pris plus de temps qu'une seconde par rapport au premier en raison du numéro de fonction alors qu'il a fallu plus de 44,08 secondes pour obtenir la sélection de la fonctionnalité sur le processus QR, ce qui est une amélioration significative de NMFDCA. Cet ensemble de données montre une différence significative de temps de traitement, compte tenu du nombre d'entités mais aussi en termes de précision avec 98,92% contre 90,50% . La factorisation NMF donne une image presque identique aux données d'origine avec un espace réduit, de sorte que le processus de catégorisation sera affecté par la qualité de la factorisation.

Quant au vin rouge avec 1599 instances et 12 caractéristiques, la précision était d'environ 89,63% en 2,10 secondes. Le nombre de cas était considérablement plus important que les précédents. De plus, une moindre qualité de la factorisation en raison du problème mal posé ou de l'impossibilité d'obtenir l'erreur optimisée a affecté le processus de catégorisation, a diminué le taux de précision par rapport aux ensembles de données sur le cancer du sein, qui sont considérés comme des problèmes bien posés avec une bonne qualité de

factorisation et erreur optimisée.

Notez que la factorisation NMF n'est pas une solution unique, et qu'elle souffre d'être très mal posée [41] la précision peut être moindre sauf si ce problème apparaît. Pour obtenir une meilleure précision, nous devons le transformer en un problème bien posé et minimiser $\| V - WH \|^2$. Cependant, en termes de temps d'exécution, lors de l'application du processus de sélection de fonctionnalités à l'aide de la méthode de réglage approximatif, le temps a augmenté de manière incroyable avec plus de 22 secondes, ce qui ralentit le DCA et dérive de son caractère principal en tant qu'un algorithme léger.

Le QRDCA peut donner un meilleur taux de précision par rapport au NMFDCA selon le tableau 5.3, il montre que le processus de sélection d'entités s'appliquant aux ensembles de données Spectf et Sonar en utilisant un ensemble approximatif peut être efficace pour classer les entités sélectionnées dans sa catégorie appropriée, mais a pris un temps considérable pour mener à bien le processus de sélection. Alors que la factorisation NMF a donné un moins de précision par rapport aux deux ensembles de données cités, on observe que le temps de prétraitement était clairement moins. Ainsi, l'utilisation de la factorisation matricielle non négative permet de conserver le caractère léger du DCA. La factorisation NMF sera nettement efficace pour le prétraitement du DCA seulement lorsque on gère correctement les problèmes mal posés de la factorisation.

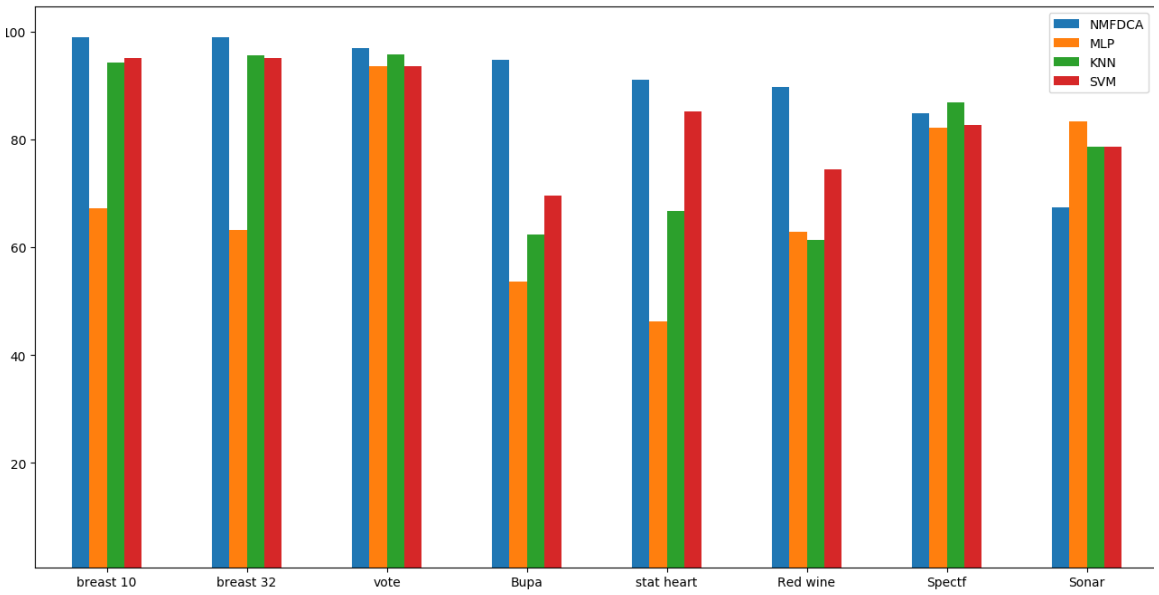

FIGURE 5.6 – Comparaison avec les classifieurs svm, knn et mlp

4.5 Comparaison avec d'autres méthodes

Outre la comparaison avec le QR-DCA, l'expérimental confirmait l'amélioration du temps d'exécution tout en gardant un meilleur taux de précision. Pour donner plus d'objectivité à notre étude, nous avons comparé notre méthode à quatre classificateurs : multi layer perceptron(mlp), k-nearest neighbors(knn) and support vector machine (svm). Nous avons utilisé 5-folds cross validation pour tester les classificateurs.

Comme le montre la figure 5.6, le taux de précision du breast10 en utilisant MLP était d'environ 67,14% , 94,28% et en utilisant KNN et SVM était de 95% . Alors que le NMF était d'environ 98,92% , ce résultat est interprété par la bonne qualité de la factorisation. La faible précision du MLP peut résulter de nombreux points tels que le nombre de neurones, le nombre de couches cachées, l'initialisation du poids ou la fonction d'activation. En retour, KNN et SVM ont donné des taux de précision acceptables. Les résultats de l'ensemble de données du breast32 étaient approximativement les mêmes que le premier en termes de taux de précision avec l'observation que le MLP enregistre toujours un faible taux de précision.

En testant les classificateurs sur l'ensemble de données vote, nous avons observé que MLP l'emporte sur SVM et approche les résultats de KNN. Le taux de précision NMF était environ 96% plus élevé que les autres classificateurs. Le taux de précision de l'ensemble de données Bupa était inférieur à celui des autres données, en raison de la qualité de la factorisation matricielle. Cependant, garder un meilleur résultat que les autres classificateurs. stat avec un taux de précision de 91,08% NMF, 46,29% MLP, 66,66% KNN et 86,18% SVM, ceci est dû par le fait que l'erreur de factorisation est minimisée, la bonne qualité de la factorisation et donc très proche des données d'origine. Alors qu'avec d'autres classificateurs, le taux de précision était plus faible.

Nous sommes conscients que cette méthode peut avoir des limites. Lorsque les données sont un problème mal posé pour la factorisation, l'erreur $\| V - WH \|^2$ augmente et donne des faibles taux, où nous observons que les classificateurs dépassent notre méthode : les jeux de données Spectf et Sonar. Pour remédier à ce problème, pour se faire nous devons gérer et régulariser les données mal posées par les méthodes appropriés.

5 Conclusion

L'algorithme proposé utilise la méthode NMF pour convertir les données d'origine en réduction d'espace en utilisant la factorisation matricielle et ca-

tégorise les nouvelles données dans son signal correspondant. Ce processus optimise la phase de prétraitement et conserve l'efficacité de l'algorithme des cellules dendritiques. Les nouvelles données optimisées à base de NMF transformées nous permettent d'obtenir des informations qui aide à atteindre une précision élevée. En comparaison avec d'autres approches de pointe, des évaluations expérimentales vérifient l'efficacité de l'approche suggérée par rapport à QR-DCA et DCA-PCA en termes de temps d'exécution et de taux de précision. Il a été démontré que la nouvelle approche surpasse les autres classificateurs (MLP, SVM et KNN). En perspective, une analyse comparative entre l'algorithme des cellules dendritiques et l'algorithme du perceptron continuerait d'être étudiée en profondeur pour comprendre le processus d'apprentissage dans les deux algorithmes.

Conclusion générale et perspectives

Le but de cette thèse est d'étudier la faisabilité d'utiliser la réduction d'attributs par la factorisation matricielle sur la phase de prétraitement du DCA à la fois du point de vue théorique et empirique, afin d'améliorer son applicabilité et son accessibilité. L'étude théorique menée tout au long de cette thèse implique une formalisation et des analyses d'exécution de l'algorithme. Il révèle des idées théoriques qui non seulement rendent l'algorithme plus accessible aux futures, mais qui constituent également une base mathématique en ce qui concerne l'étude empirique. En conséquence, l'accessibilité de l'algorithme est améliorée par l'investigation théorique. L'enquête empirique menée dans le chapitre 5 utilise la détection d'intrusion basée sur des anomalies comme une application concrète du problème de détection et de filtrage d'anomalies. Il s'agit d'intégrer des techniques d'autres domaines, dans notre cas, l'apprentissage automatique et la factorisation matricielle non-négative, avec le DCA. L'expérimentation montre que le système intégré devient plus applicable aux problèmes, où la détection sur données diverses sont impliquées, cette application a permis d'automatiser et de s'adapter aux cas où expertise du domaine de problème donné est difficile, voire impossible à obtenir, vu le nature de données. En conséquence, l'applicabilité de l'algorithme est améliorée grâce à l'enquête empirique. Dans le reste de cette conclusion.

Le (dendritic cell algorithm) DCA est présenté relativement comme un nouvel algorithme AIS. Le développement de cet algorithme a connu plusieurs étapes qui commençaient de la conception et l'abstraction à partir de l'immunité humaine vers un système informatique et passaient vers l'automatisation et l'optimisation de cet algorithme. Le processus d'abstraction impliquait de déterminer que les cellules dendritiques sont une unité de contrôle majeure au sein du système immunitaire humain. L'abstraction du fonctionnement de la cellule dendritique a été développé et formalisé en tant qu'algorithme. Cela montre que des informations biologiques détaillées peuvent être traduites en

un algorithme utilisable. L'algorithme résultant est modèles abstraits de cellules immunitaires adaptatives et effectue une filtration sur la base de signaux de contexte, et non sur la structure de l'antigène.

L'investigation empirique pour la phase de prétraitement automatisé a permis de montrer une remarquable amélioration sur la précision du DCA. Les résultats expérimentaux montrent les indications suivantes. Les méthodes de prétraitement automatisées basée sur la méthode NMF en particulier, pourraient produire des performances de filtrage nettement meilleures que la méthode manuelle, ainsi que les deux entre méthodes : théorie des ensembles et la théorie de la logique floue. Cela montre qu'il est possible d'utiliser une combinaison de techniques de réduction de dimensionnalité et de factorisation matricielle par la décomposition matricielle en deux matrices que leur produit donne les données originales, pour remplacer les méthodes manuelles reposant sur l'expertise d'un domaine de problème donné. De plus, parmi les méthodes de prétraitement automatisées existantes, la méthode basée sur le NMF semble produire les performances de classification les plus élevées. En effet, NMF combine toutes les fonctionnalités d'origine pour générer de nouvelles fonctionnalités, ce qui pourrait potentiellement minimiser la perte d'informations lors du prétraitement des données. En conséquence, la méthode basée sur le NMF est avantageuse par rapport aux autres méthodes de prétraitement des données (manuelles ou automatisées) en termes de performance et de précision. Des recherches plus avancées devraient être poursuivies pour tester les méthodes actuellement développées sur un plus grand nombre de données, ainsi que pour développer des méthodes plus avancées et plus performantes. D'autre part, aucune preuve suffisante ne peut être trouvée pour suggérer que l'une des méthodes liées à DCA pourrait surpasser les techniques d'apprentissage automatique standard. Même s'il semble que la méthode basée sur le NMF pourrait produire des performances de détection aussi bonnes que les techniques d'apprentissage automatique. Par conséquent, se concentrer uniquement sur le développement de méthodes de prétraitement automatisées plus efficaces des données pourrait ne pas suffire.

Pour les travaux futurs, on peut également envisager de modifier les fondements de base de l'algorithme pour améliorer fondamentalement sa capacité de détection et le rendre un algorithme d'apprentissage automatique pur. Cependant, de telles modifications ne peut pas être traitée dans cette thèse. En résumé, le module de prétraitement automatique des données pourrait être développé pour remplacer les modules manuels, afin de faire une interface entre l'espace d'entrée du DCA et le domaine d'application de problème donné

sans l'implication d'une expertise manuelle. Dans ce travail on a montré la possibilité de combiner des techniques de réduction de dimensionnalité et la factorisation matricielle qui sont couramment utilisées dans l'apprentissage automatique et la modélisation mathématique, pour automatiser la phase de prétraitement des données du DCA. Cela pourrait potentiellement rendre l'algorithme plus applicable à un plus grand ensemble de problèmes dans lesquels les connaissances d'experts sont difficiles ou impossibles à extraire.

Un certain nombre de problèmes qui limitent l'applicabilité et l'accessibilité du DCA ont été identifiées, et les solutions correspondantes sont proposées et examinées de manière théorique et empirique. Une discussion est à mener sur les travaux futurs qui permettront d'améliorer les performance et l'applicabilité du DCA, pour montrer les extensions possibles de cette thèse, en termes de perspective à court terme. Il se compose de trois parties, à savoir le post-traitement en ligne et le prétraitement automatisé. Un module d'analyse en ligne pourrait augmenter la précision de détection de l'algorithme pour l'ensemble de données testé. Un tel module permettra au système d'effectuer une analyse continue et périodique en parallèle avec la détection. La vitesse de détection qui reflète le temps nécessaire pour produire les résultats de détection finaux peut également être améliorée. En conséquence, ce module d'analyse en ligne basé sur la segmentation pourrait améliorer la capacité de détection de l'algorithme. La taille du segment est liée à deux facteurs des données d'entrée, à savoir la fréquence de l'antigène et la concentration du signal. Pour cela, il faut développer ce mécanisme qui permet de modifier la taille du segment par rapport aux valeurs de ces deux facteurs lors de la détection.

Les méthodes automatisées basées sur des techniques de réduction de dimensionnalité et la factorisation matricielle visent à évaluer la possibilité d'automatiser la phase de prétraitement des données du DCA. Les résultats expérimentaux montrent que la version modifiée avec des méthodes automatisées produisent des performances de filtrages similaires ou du moins pas pires que les méthodes manuelles. Le principe pour garantir des performances et précision élevées du DCA est de générer de produire des signaux adéquats au cours de la phase de prétraitement des données. La production de signaux appropriés peut simplement être les signaux qui, une fois entrés dans le DCA, l'algorithme est capable d'estimer une frontière de décision qui sépare correctement la normalité et les anomalies contenues dans le problème donné. Il s'agit généralement d'un problème de séparabilité (en quelque sorte linéaire) d'un ensemble de données, qui est un problème général en apprentissage automatique. Par exemple, si les données d'un problème de classification binaire sont linéairement sépa-

rables, il est facile pour un classificateur linéaire de trouver un hyperplan qui sépare les deux classes. Par conséquent, les performances de classification du DCA pourraient être déterminées par la séparabilité des signaux générés qui sont réellement traités par l'algorithme mais pas par celle des données brutes. Intuitivement, toute méthode de prétraitement de données capable de générer des signaux facilement ou linéairement séparables est considérée comme utile pour l'algorithme. Pour les données séparables non linéairement, de nouvelles méthodes peuvent être introduites dans le DCA comme moyen de prétraitement. Ces méthodes impliquent généralement de représenter un algorithme linéaire en un algorithme non linéaire, dans un espace d'attributs de dimension éventuellement plus élevée qui est lié non linéairement à l'espace d'entrée. Tout algorithme linéaire réalisable en termes de produits scalaires peut être rendu non linéaire en substituant un noyau choisi a priori [95], ainsi, on peut appliquer la factorisation matricielle non-négative et non linéaire sur les problèmes non linéaires [111].

L'étude dans cette thèse s'intéressait sur l'application de la réduction de dimensionnalité en utilisant la factorisation matricielle non-négative dans la phase de prétraitement du DCA. Cependant, il existe encore plusieurs problèmes avec l'algorithme qui pourraient impliquer la modification des composants de base de l'algorithme. On souhaite que ces problèmes soient résolus éventuellement, si on veut développer l'algorithme en une solution système d'immunité artificielle principale capable de rivaliser avec les techniques conventionnelles. Premièrement, la dimensionnalité de l'espace d'entrée est limitée à trois, ce qui pourrait fortement affecter l'efficacité du prétraitement des données. En outre, les poids pour la transformation du signal sont attribués statiquement (ou empiriquement), ce qui pourrait limiter la capacité de l'algorithme à s'adapter pleinement à un domaine de problème donné. De plus, la fonction de transformation du signal est basée sur une application linéaire, qui pourrait être extrêmement limitée par la séparabilité linéaire d'un domaine de problème donné. Les solutions potentielles à ces problèmes sont l'expansion de l'espace d'entrée, le réglage automatisé des paramètres et l'introduction de perceptrons multicouches.

En effet, le DCA comporte plusieurs paramètres qui doivent être définie par l'utilisation (la matrice de poids, les seuils de maturation et les seuils de filtrage MCAV). L'espace d'entrée de l'algorithme doit être un espace à plus de 3 dimensions (m dimensions). Cela signifie que toute la fonction de transformation du signal doit être modifiée, car la matrice de poids tridimensionnelle d'origine n'est plus applicable. Si le mode linéaire de transformation de signal

est utilisé, une nouvelle matrice de poids 2 m doit être créée pour transformer m signaux d'entrée en deux signaux de sortie. En conséquence, les heuristiques dérivées de l'immunologie qui définissent la relation entre les catégories de signaux d'origine du DCA ne peuvent plus être appliquées. La nouvelle matrice de poids doit être acquise à travers une forme d'apprentissage basée sur les attributs sous-jacents des données. L'expansion de l'espace d'entrée n'élimine pas la nécessité d'utiliser des techniques de réduction de dimensionnalité pour transformer l'espace d'original de données. Une réduction efficace de la dimensionnalité peut réduire la complexité des données d'entrée tout en mettant l'accent sur les caractéristiques cachées de données, de sorte que la difficulté de créer un modèle pour classer correctement les instances de données est réduite en conséquence. La probabilité d'une perte d'information significative par le processus de réduction de dimensionnalité peut également être diminuée.

L'automatisation et l'optimisation des différents paramètres du DCA en utilisation l'algorithme MLP (multi layer perceptron) pour définir et affiner les valeurs de ses paramètres, le mappage entre les signaux d'entrée et de sortie devient non linéaire et les poids associés peuvent être ajustés automatiquement par une fonction d'erreur basée sur le gradient grâce à l'apprentissage. Au lieu d'agréger un signal transformé par une fonction plutôt centralisée à partir de chaque instance de signal d'entrée, chaque DC agrégerait individuellement l'instance de signal d'entrée de son propre chef et présenterait ces moyennes au classificateur du répertoire sur l'échelle de temps la plus similaire à celle de la durée de vie de DC. Les classificateurs dans le répertoire peuvent être n'importe quel type de classificateurs non linéaires, tels que les réseaux à base de perceptron multicouche.

La compréhension des systèmes immunitaires comme un système de détection et de défense a permis le développement de plusieurs systèmes artificiels construites à partir des théories dans le domaine l'immunité biologique. Ces systèmes n'ont pas connu un intérêt par la communauté scientifique comme l'intérêt des réseaux de neurones, ce manque d'intérêt est probablement en relation avec la difficulté et la complexité d'abstraction de ce genre de système en un système, en plus, le fondement de l'immunité est purement basé sur des théories très sensible à l'expérimental. Vu que les fondements et l'abstraction du DCA est faite sur la base de la théorie de danger. Une recherche plus approfondie sur cette théorie avec l'avancée clinique et les nouvelles techniques dans ce domaine peut être envisagée pour étudier de près l'immunité comme un système par des divers spécialistes et scientifiques (mathématiques biologiste, immunologiste, informatique).

Bibliographie

[1] Naoki Abe, Bianca Zadrozny, and John Langford. Outlier detection by active learning. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, volume 2006, pages 504–509. ACM, 2006.

[2] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod. Danger theory : The link between AIS and IDS ? In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 2787, pages 147–155. Springer, 2003.

[3] Emin Aleskerov, Bernd Freisleben, and Bharat Rao. CARDWATCH : A neural network based database mining system for credit card fraud detection. In *IEEE/IAFE Conference on Computational Intelligence for Financial Engineering, Proceedings (CIFEr)*, pages 220–226. IEEE, 1997.

[4] Iman Almomani, Bassam Al-Kasasbeh, and Mousa Al-Akhras. WSN-DS : A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. *Journal of Sensors*, 2016, 2016.

[5] J P Anderson. Computer security threat monitoring and surveillance. Technical Report 98–17, James P Anderson Co., FortWashington, Pennsylvania,USA, 1980.

[6] Alex M. Andrew. Introduction to Evolutionary Computing, 2004.

[7] Paul S. Andrews and Jon Timmis. On diversity and artificial immune systems : Incorporating a diversity operator into aiNet. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 3931 LNCS, pages 293–306. Springer, 2006.

[8] Rebecca Bace and Peter Mell. NIST special publication on intrusion detection systems. *Nist Special Publication*, SP-800-3 :1–51, 2001.

[9] Sankalp Balachandran, Dipankar Dasgupta, Fernando Nino, and Deon Garrett. A framework for evolving multi-shaped detectors in negative

selection. In *Proceedings of the 2007 IEEE Symposium on Foundations of Computational Intelligence, FOCI 2007*, pages 401–408. IEEE, 2007.

[10] B. J. Bejoy, T. V. Bijeesh, and S. Janakiraman. Artificial immune system based frameworks and its application in cyber immune system : A comprehensive review. *Journal of Critical Reviews*, 7(2) :552–560, 2020.

[11] Mourad Belhadj and Foudil Cherif. Dendritic Cell Algorithm and Multilayer Perceptron : A Comparative Study. In *8th International Conference on the Theory and Practice of Natural Computing*, 2019.

[12] Mourad Belhadj, Foudil Cherif, and Mohamed Cheriet. NMF-DCA : An Efficient Dendritic Cell Algorithm Based on Non-Negative Matrix Factorization. *International Journal of Computing and Digital Systems*, 10(1) :575–583, 4 2021.

[13] Michael W. Berry, Murray Browne, Amy N. Langville, V. Paul Pauca, and Robert J. Plemmons. Algorithms and applications for approximate nonnegative matrix factorization. *Computational Statistics and Data Analysis*, 52(1) :155–173, 2007.

[14] Parteek Bhatia. *Introduction to Data Mining*. Pearson Education India, 2019.

[15] C. Boutsidis and E. Gallopoulos. SVD based initialization : A head start for nonnegative matrix factorization. *Pattern Recognition*, 41(4) :1350–1362, 2008.

[16] Jason Brownlee. *Clever Algorithms - Nature-Inspired Programming Recipes*. Lulu.com, 1st edition, 2011.

[17] David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha. Towards automatic generation of vulnerability-based signatures. In *Proceedings - IEEE Symposium on Security and Privacy*, volume 2006, pages 2–16, 2006.

[18] David Burgermeister, Jonathan Krier, and Jonathan Krier David Burgermeister. Les systèmes de détection d'intrusions, 2006.

[19] F. M. Burnet and William B. Bean. The Clonal Selection Theory of Acquired Immunity. *Archives of Internal Medicine*, 105(6) :973, 6 1960.

[20] Erick Cantú-Paz. Feature subset selection, class separability, and genetic algorithms. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3102 :959–970, 2004.

[21] Zeineb Chelly and Zied Elouedi. RC-DCA : A new feature selection and signal categorization technique for the dendritic cell algorithm based

on rough set theory. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7597 LNCS, pages 152–165. Springer, 2012.

[22] Zeineb Chelly and Zied Elouedi. RST-DCA : A dendritic cell algorithm based on rough set theory. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7665 LNCS, pages 480–487. Springer, 2012.

[23] Zeineb Chelly and Zied Elouedi. A fuzzy-rough data pre-processing approach for the dendritic cell classifier. In Linda C van der Gaag, editor, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7958 LNAI, pages 109–120, Berlin, Heidelberg, 2013. Springer, Springer Berlin Heidelberg.

[24] Zeineb Chelly and Zied Elouedi. QR-DCA : A new rough data pre-processing approach for the dendritic cell algorithm. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7824 LNCS, pages 140–150. Springer, 2013.

[25] Zeineb Chelly and Zied Elouedi. A survey of the dendritic cell algorithm. *Knowledge and Information Systems*, 48(3) :505–535, 2016.

[26] Guilherme P. Coelho and Fernando J. Von Zuben. omni-aiNet : An immune-inspired approach for omni optimization. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 4163 LNCS, pages 294–308. Springer, 2006.

[27] V Cutello and G Nicosia. Multiple learning using immune algorithms. In *Proceedings of 4th International Conference on Recent Advances in Soft Computing, RASC 2002*, pages 102–107. Nottingham Trent University Press, 2002.

[28] Dipankar Dasgupta and Fabio González. An immunity-based technique to characterize intrusions in computer networks. *IEEE Transactions on Evolutionary Computation*, 6(3) :281–291, 2002.

[29] Dipankar Dasgupta and Nivedita S. Majumdar. Anomaly detection in multidimensional data using negative selection algorithm. In *Proceedings of the 2002 Congress on Evolutionary Computation, CEC 2002*, volume 2, pages 1039–1044. IEEE, 2002.

[30] Dipankar Dasgupta and Fernando Nino. Comparison of negative and positive selection algorithms in novel pattern detection. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, volume 1, pages 125–130. IEEE, 2000.

[31] Leandro Nunes De Castro and Fernando Jose von Zuben. The Clonal Selection Algorithm with Engineering Applications. In *Gecco*, volume 2000, pages 36–37, 2000.

[32] Patrik D'haeseleer, Stephanie Forrest, and Paul Helman. Immunological approach to change detection : algorithms, analysis and implications. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pages 110–119. IEEE, 1996.

[33] Inderjit S. Dhillon and Suvrit Sra. Generalized nonnegative matrix approximations with Bregman divergences. In *Advances in Neural Information Processing Systems*, pages 283–290, 2005.

[34] F.Y. Edgeworth. XLI. On discordant observations . *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 23(143) :364–375, 1887.

[35] Tom Fawcett and Foster Provost. Adaptive fraud detection. *Data Mining and Knowledge Discovery*, 1(3) :291–316, 1997.

[36] Stephanie Forrest, Lawrence Allen, Alan S. Perelson, and Rajesh Cherukuri. Self-nonself discrimination in a computer. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pages 202–212. Ieee, 1994.

[37] A Frank and A Asuncion. {UCI} Machine Learning Repository, 2010.

[38] Ryohei Fujimaki, Takehisa Yairi, and Kazuo Machida. An approach to spacecraft anomaly detection problem using Kernel Feature Space. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 401–410. ACM, 2005.

[39] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez. Anomaly-based network intrusion detection : Techniques, systems and challenges. *Computers and Security*, 28(1-2) :18–28, 2009.

[40] James Gentle. *Matrix Analysis and Applied Linear Algebra, Numerical Linear Algebra, and Applied Numerical Linear Algebra*, volume 96. Siam, 2001.

[41] Nicolas Gillis. Sparse and unique nonnegative matrix factorization through data preprocessing. *Journal of Machine Learning Research*, 13(Nov) :3349–3386, 2012.

[42] Nicolas Gillis. The Why and How of Nonnegative Matrix Factorization. *Regularization, Optimization, Kernels, and Support Vector Machines*, 12(257) :275–310, 2020.

[43] Ary L. Goldberger, Luis A. N. Amaral, Leon Glass, Jeffrey M. Hausdorff, Plamen Ch. Ivanov, Roger G. Mark, Joseph E. Mietus, George B. Moody, Chung-Kang Peng, and H. Eugene Stanley. PhysioBank, PhysioToolkit, and PhysioNet. *Circulation*, 101(23) :e215–e220, 2000.

[44] Fabio González, Dipankar Dasgupta, and Jonatan Gómez. The effect of binary matching rules in negative selection. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 2723, pages 195–206. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[45] Nico Görnitz, Marius Kloft, Konrad Rieck, and Ulf Brefeld. Toward supervised anomaly detection. Technical report, 2013.

[46] Robert M. Gray. Vector Quantization. *IEEE ASSP Magazine*, 1(2) :4–29, 1984.

[47] Julie Greensmith. *The Dendritic Cell Algorithm.* PhD thesis, Citeseer, 2007.

[48] Julie Greensmith, Uwe Aickelin, and Steve Cayzer. Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection. In *Lecture Notes in Computer Science*, volume 3627, pages 153–167. Springer, 2005.

[49] Julie Greensmith, Uwe Aickelin, and Steve Cayzer. Detecting danger : The dendritic cell algorithm. *Robust Intelligent Systems*, pages 89–112, 6 2008.

[50] Julie Greensmith, Uwe Aickelin, and Jamie Twycross. Articulation and clarification of the dendritic cell algorithm. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4163 LNCS :404–417, 10 2006.

[51] Volker Grimm, Eloy Revilla, Uta Berger, Florian Jeltsch, Wolf M. Mooij, Steven F. Railsback, Hans Hermann Thulke, Jacob Weiner, Thorsten Wiegand, and Donald L. DeAngelis. Pattern-oriented modeling of agent-based complex systems : Lessons from ecology. *Science*, 310(5750) :987–991, 2005.

[52] Jens Grossklags, Nicolas Christin, and John Chuang. Security and insurance management in networks with heterogeneous agents. In *Procee-*

dings of the ACM Conference on Electronic Commerce, EC '08, pages 160–169, New York, NY, USA, 2008. ACM.

[53] F GU. *Theoretical and Empirical Extensions of the Dendritic Cell Algorithm.* PhD thesis, University of Nottingham, 2011.

[54] Feng Gu, Julie Greensmith, Robert Oates, and Uwe Aickelin. PCA 4 DCA : The Application of Principal Component Analysis to the Dendritic Cell Algorithm. *SSRN Electronic Journal*, 2016.

[55] Fabio Guigou. The artificial immune ecosystem : a scalable immune-inspired active classifier , an application to streaming time series analysis for network monitoring To cite this version : HAL Id : tel-02316897 The Artificial Immune Ecosystem : a scalable immune-inspi, 2019.

[56] Barbara Guttman and EA Roback. An Introduction to Computer Security : The NIST Handbook - Chapter 16, "Identification and Authentication". Technical report, Washington, 1995.

[57] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. Anomaly-based intrusion detection using mobility profiles of public transportation users. *2005 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob'2005*, 2 :17–24, 2005.

[58] Emma Hart and Jon Timmis. Application areas of AIS : The past, the present and the future. *Applied Soft Computing Journal*, 8(1) :191–201, 2008.

[59] S. A. Hofmeyr and S. Forrest. Architecture for an artificial immune system. *Evolutionary computation*, 8(4) :443–473, 2000.

[60] John E. Hunt and Denise E. Cooke. Learning using an artificial immune system. *Journal of Network and Computer Applications*, 19(2) :189–212, 1996.

[61] C. A. Janeway. Approaching the asymptote ? Evolution and revolution in immunology. *Cold Spring Harbor Symposia on Quantitative Biology*, 54(1) :1–13, 1989.

[62] Richard Jensen and Qiang Shen. Fuzzy-rough sets for descriptive dimensionality reduction. In *IEEE International Conference on Fuzzy Systems*, volume 1, pages 29–34, 2002.

[63] Zhou Ji and Dipankar Dasgupta. Revisiting negative selection algorithms. *Evolutionary Computation*, 15(2) :223–251, 2007.

[64] Mahesh V. Joshi, Ramesh C. Agarwal, and Vipin Kumar. Mining needles in a haystack : Classifying rare classes via two-phase rule induction.

SIGMOD Record (ACM Special Interest Group on Management of Data), 30(2) :91–102, 2001.

[65] Jingu Kim and Haesun Park. Fast nonnegative matrix factorization : An active-set-like method and comparisons. *SIAM Journal on Scientific Computing*, 33(6) :3261–3281, 2011.

[66] Maciej Kopczyński and Jarosław Stepaniuk. Hardware Implementations of Rough Set Methods in Programmable Logic Devices. In *Intelligent Systems Reference Library*, volume 43, pages 309–321. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[67] Khaled Labib. Computer security and intrusion detection. *XRDS : Crossroads, The ACM Magazine for Students*, 11(1) :2–2, 2004.

[68] Amy N. Langville, Carl D. Meyer, Russell Albright, James Cox, and David Duling. Algorithms, Initializations, and Convergence for the Nonnegative Matrix Factorization. Technical report, Tech. rep. 919. NCSU Technical Report Math 81706., 2014.

[69] Daniel D. Lee and H. Sebastian Seung. Learning the parts of objects by non-negative matrix factorization. *Nature*, 401(6755) :788–791, 1999.

[70] Daniel D. Lee and H. Sebastian Seung. Algorithms for non-negative matrix factorization. In T K Leen, T G Dietterich, and V Tresp, editors, *Advances in Neural Information Processing Systems*, pages 556–562. MIT Press, 2001.

[71] Manfred B. Lutz and Gerold Schuler. Immature, semi-mature and fully mature dendritic cells : Which signals induce tolerance or immunity ?, 9 2002.

[72] C. M. MacAl and M. J. North. Tutorial on agent-based modelling and simulation. *Journal of Simulation*, 4(3) :151–162, 2010.

[73] Frédéric Majorczyk. *Détection d'intrusions comportementale par diversification de COTS : application au cas des serveurs web*. PhD thesis, Universit{é} Rennes 1, 2009.

[74] Markos Markou and Sameer Singh. Novelty detection : a review—part 1 : statistical approaches. *Signal processing*, 83(12) :2481–2497, 2003.

[75] P. Matzinger. Tolerance, Danger and the Extended Family. *Annual Review of Immunology*, 12(1) :991–1045, 1994.

[76] Polly Matzinger. The danger model : A renewed sense of self. *Science*, 296(5566) :301–305, 2002.

[77] Charles E. Metz. Basic principles of ROC analysis. *Seminars in Nuclear Medicine*, 8(4) :283–298, 10 1978.

[78] Melanie Middlemiss. Positive and negative selection in a multilayer artificial immune system. *The Information Science Discussion Paper Series*, 2006/03, 2006.

[79] Shoichi Nakano, Kazumasa Yamamoto, and Seiichi Nakagawa. Fast NMF based approach and improved VQ based approach for speech recognition from mixed sound. In *2012 Conference Handbook - Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2012*, pages 1–4. IEEE, 2012.

[80] Peter Ndajah, Hisakazu Kikuchi, Masahiro Yukawa, Hidenori Watanabe, and Shogo Muramatsu. An investigation on the quality of denoised images. In *International Journal of Circuits, Systems and Signal Processing*, volume 5, pages 423–434. IEEE, 2011.

[81] Oleg G. Okun. Non-negative matrix factorization and classifiers : Experimental study. In *Proceedings of the Fourth IASTED International Conference on Visualization, Imaging, and Image Processing*, pages 550–555, 2004.

[82] International Standards Organization. *Accuracy (trueness and precision) of measurement methods and results - Part 3 Alternative methods for the determination of the precision of a standard measurement method*, volume ISO 5725-4. International Organization for Standardization, 1994.

[83] Pentti Paatero. Least squares formulation of robust non-negative factor analysis. *Chemometrics and Intelligent Laboratory Systems*, 37(1) :23–35, 1997.

[84] Pentti Paatero and Unto Tapper. Positive matrix factorization : A non-negative factor model with optimal utilization of error estimates of data values. *Environmetrics*, 5(2) :111–126, 1994.

[85] Grant Pannell and Helen Ashman. Anomaly detection over user profiles for intrusion detection. In *Proceedings of the 8th Australian Information Security Management Conference*, pages 81–94. Australian Information Security Management Conference, 2010.

[86] Rajul Parikh, Annie Mathai, Shefali Parikh, G. Chandra Sekhar, and Ravi Thomas. Understanding and using sensitivity, specificity and predictive values. *Indian Journal of Ophthalmology*, 56(1) :45–50, 2008.

[87] Clifton Phua, Damminda Alahakoon, and Vincent Lee. Minority report in fraud detection. *ACM SIGKDD Explorations Newsletter*, 6(1) :50–59, 2004.

[88] Nadipuram R. Prasad, Salvador Almanza-Garcia, and Thomas T. Lu. Anomaly detection. *Computers, Materials and Continua*, 14(1) :1–22, 2009.

[89] Bin Ren, Laurent Pueyo, Guangtun Ben Zhu, John Debes, and Gaspard Duchêne. Non-negative Matrix Factorization : Robust Extraction of Extended Structures. *The Astrophysical Journal*, 852(2) :104, 2018.

[90] P. H. Richter. A network theory of the immune system. *European Journal of Immunology*, 5(5) :350–354, 1975.

[91] Lukas Ruff, Jacob R. Kauffmann, Robert A. Vandermeulen, Gregoire Montavon, Wojciech Samek, Marius Kloft, Thomas G. Dietterich, and Klaus Robert Muller. A Unifying Review of Deep and Shallow Anomaly Detection. *Proceedings of the IEEE*, 109(5) :756–795, 2021.

[92] S Forrest S. Hofmeyr. Immunity by design : an artificial immune system. In *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 99)*, page 12891296. Morgan Kaufmann Publishers Inc., 1999.

[93] Claude Sammut and Geoffrey I Webb. *Encyclopedia of Machine Learning*. Springer Science & Business Media, 2010.

[94] Karen Scarfone and Peter Mell. Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology*, 800-94(February) :127, 2007.

[95] Bernhard Schölkopf, Sebastian Mika, Chris J.C. Burges, Philipp Knirsch, Klaus Robert Müller, Gunnar Rätsch, and Alexander J. Smola. Input space versus feature space in kernel-based methods. *IEEE Transactions on Neural Networks*, 10(5) :1000–1017, 1999.

[96] Clay Spence, Lucas Parra, and Paul Sajda. Detection, synthesis and compression in mammographic image analysis with a hierarchical image probability model. In *Proceedings of the Workshop on Mathematical Methods in Biomedical Image Analysis*, pages 3–10. IEEE, 2001.

[97] Ingo Steinwart, Don Hush, and Clint Scovel. A classification framework for anomaly detection. *Journal of Machine Learning Research*, 6(Feb) :211–232, 2005.

[98] Milos Stojmenovic. *Routing in wireless ad hoc and sensor networks*. 2011.

[99] Pei Sun and Sanjay Chawla. On local spatial outliers. In *Proceedings - Fourth IEEE International Conference on Data Mining, ICDM 2004*, pages 209–216. IEEE, 2004.

[100] Ying Tan. *Artificial Immune System : Applications in Computer Security*. Wiley, 2016.

[101] James P. Theiler and D. M. Cai. Resampling approach for anomaly detection in multispectral images. In *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery IX*, volume 5093, page 230, 2003.

[102] J. Timmis, T. Knight, L. N. de Castro, and E. Hart. An Overview of Artificial Immune Systems. In *Artificial immune systems and their applications*, pages 51–91. Springer, 2004.

[103] J. Timmis and M. Neal. A resource limited artificial immune system for data analysis. *Knowledge-Based Systems*, 14(3-4) :121–130, 2001.

[104] Ricardo Vilalta and Ma Sheng. Predicting rare events in temporal domains. In *Proceedings - IEEE International Conference on Data Mining, ICDM*, pages 474–481. IEEE, 2002.

[105] Yu Xiong Wang and Yu Jin Zhang. Nonnegative matrix factorization : A comprehensive review. *IEEE Transactions on Knowledge and Data Engineering*, 25(6) :1336–1353, 2013.

[106] Andrew Watkins, Xintong Bi, and Amit Phadke. Parallelizing an immune-inspired algorithm for efficient pattern recognition. *Intelligent Engineering Systems Through Artificial Neural Networks*, 13 :225–230, 2003.

[107] Gary M Weiss and Haym Hirsh. Learning to Predict Rare Events in Categorical Time-Series Data. In *AAAI Workshop*, pages 83–90, 1998.

[108] Amanda Whitbrook, Uwe Aickelin, and Jonathan Garibaldi. An idiotypic immune network as a short-term learning architecture for mobile robots. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5132 LNCS :266–278, 2008.

[109] Amanda M. Whitbrook, Uwe Aickelin, and Jonathan M. Garibaldi. Two-timescale learning using idiotypic behaviour mediation for a navigating mobile robot. *Applied Soft Computing Journal*, 10(3) :876–887, 2010.

[110] Svante Wold, Kim Esbensen, and Paul Geladi. Principal component analysis. *Chemometrics and Intelligent Laboratory Systems*, 2(1-3) :37–52, 1987.

[111] Zhirong Yang and Erkki Oja. Linear and nonlinear projective nonnegative matrix factorization. *IEEE Transactions on Neural Networks*, 21(5) :734–749, 5 2010.

[112] Zhong Yuan Zhang. Nonnegative Matrix Factorization : Models, Algorithms and Applications. In *Intelligent Systems Reference Library*, volume 24, pages 99–134. Springer, 2012.