International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

Reseaux de Neurones Profonds et détection d'intrusions dans un Réseau Informatique: Applicaction de (RNN, CNN et MLP) Sur NSL-KDD99

Par: Jean de Dieu Kabemba Ndala, Pierre Kasengedia Mutombe, Pierre Kafunda Katalay, Simon Ntumba Badibanga

"Chercheur à la Faculté de Sciences et Technologie de l'Université de Kinshasa"

Date of Submission: 05-08-2025 Date of Acceptance: 15-08-2025

RESUME

La sécurité des réseaux informatiques est devenue un enjeu majeur face à la croissance constante des menaces et attaques informatiques. Pour renforcer la détection des intrusions, les approches basées sur l'intelligence artificielle, en particulier les réseaux de neurons profonds, se révèlent prometteuses. Cette étude applique trois architectures de deep learning – MLP (Multi-Layer Perceptron), CNN (Convolutional Neural Network) et RNN (Recurrent Neural Network) – sur le dataset NSL-KDD, un ensemble de données largement utilisé pour l'évaluation des systèmes de detection d'intrusion (IDS).

À travers une série d'expérimentations menées en Python, les performances de chaque modèle sont analysées en fonction de quatre métriques principales: accuracy, precision, recall et F1-score. Les résultats obtenus montrent une supériorité du modèle RNN avec une accuracy de 96,1 %, suivi du CNN (95,6 %) et du MLP (93,2 %).

Ces résultats démontrent que les architectures récurrentes, capables de modéliser les dépendances temporelles, offrent une meilleure efficacité dans la détection des comportements anormaux dans les réseaux.

I. INTRODUCTION

À l'ère de la transformation numérique, les réseaux informatiques sont devenus le socle de toutes les communications et transactions dans les organisations modernes. Toutefois, cette interconnexion croissante s'accompagne d'un accroissement des risques liés aux cyberattaques, qui peuvent compromettre l'intégrité, la confidentialité et la disponibilité des données. Dans ce contexte, les systèmes de detection d'intrusion (IDS – Intrusion Detection Systems) jouent un rôle stratégique dans la prévention et la détection des attaques. Cependant, les techniques classiques de detection basées sur des signatures ou des règles présentent des limites face aux attaques nouvelles sophistiquées.

L'émergence des techniques d'apprentissage profond (deep learning) offre des perspectives innovantes pour la détection des intrusions, grâce à leur capacité à apprendre automatiquement des représentations complexes à partir de grandes quantités de données. En plus les réseaux de neurons profonds en particulier ont un rôle fondamental dans les récents succès de l'intelligence artificielle (voiture automobile, traitement de la parole, big data, etc.)[1]. Ce projet se concentre sur l'évaluation comparative de trois modèles de réseaux de neurons profonds – le perceptron multicouche (MLP), le réseau de neurons convolutifs (CNN) et le réseaux de neurons récurrents (RNN) – appliqués au jeu de données NSL-KDD99, conçu pour l'étude des intrusions réseau.

L'objectif principal est de déterminer l'architecture la plus performante pour détecter les comportements anormaux à partir du traffic réseau. Pour ce faire, les modèles sont entraînés et évalués en utilisant des métriques standards: accuracy (precision globale), precision (précision positive), recall (rappel) et F1-score. Les experimentations sont réalisées en Python avec les bibliothèques de deep learning telles que TensorFlow et Keras.
Les performances obtenues sont les suivantes:

[1]Antoine Cornuéjols, Laurent Miclet&d'YvesKodratoff, *Apprentissage artificiel, Concepts et algorithmes*, EYROLLES, Paris. 2003

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

MLP: Accuracy = 93,2 %, Precision = 91,5 %, Recall = 90,8 %, F1-score = 91,1 %
CNN: Accuracy = 95,6 %, Precision = 94,8 %, Recall = 94,1 %, F1-score = 94,4 %
RNN: Accuracy = 96,1 %, Precision = 95,5 %, Recall = 95,0 %, F1-score = 95,2 %
Ces résultats témoignent de la capacité des réseaux RNN à capter les relations séquentielles dans les données réseau, surpassant ainsi les autres architectures dans le contexte de la detection d'intrusion

II. INTRUSION DANS UN RESEAU ET LEURS MODE DE DETECTION

2.1. CONSIDERATION DE L'INTRUISION

En cybersécurité, une intrusion désignel'action non autorisée d'un acteur (humain ou automatisé) qui tented'accéder, de manipulerou de perturber un système informatique ou un réseau.

Pour la modéliser mathématiquement, on traduitcette notion à travers un cadre formeld'anomalieou de deviation statistique par rapport à un comportement normal.

Voici différentes formulations mathématiques d'une intrusion, selon les approchesutilisées[2]:

a) Modélisation mathématique du traffic réseau[3]

Le traffic réseau est modélisé comme un processus stochastique multidimensionnel: où chaque est une caractéristique du paquet à l'instant: durée de session, taille du paquet, protocole, port, etc. l'ensembleconstitue u processus stochastique.

Sous hypothèse de stabilité du traffic, on suppose que le traffic normal suit une distribution stationnaire.
- Moyenne: - Covariance: ces parametres servent de base pour détecter les écarts statistiques signalant une intruision.

b) Détection mathématique des anomalies[4]

Une intrusion estvuecomme rupture statisque:

- Distance de Mahalanobis:

= (2-1)

Si alors x est considéré comme une anomalie (intruisions possible)
Analyse en composantes principals (ACP):

- On projette les données sur les vecteursproprede . On peut mesurer l'énergie résiduele dans les composants faibles pour détecter des comportements anormaux.
- Test de rupture : On modelise une série temporelle et on cherche un changement de régime à temps T, tel que;

On utilize alors un test de rupture comme celui de Chow,
CUSUM ou Page-Hinkley.

c) Entropie et théorie de l'information[5]

Entropie de Shannon:

- Un traffic normal présente une entropie stable
- Une variable brutal de H(X) indiqueune perturbation (intruision)

Exemple: Un scan de port provoqueune augmentation brutale de l'entropie des ports de destination.

d) Probabilité et théorie de Files d'attente[6] Modèle :

Le traffic réseauestmodelisécommeune file de paqueq avec arrive de type Poisson et service exponential:

- Arrivées : λ (Poisson)
- Service : μ (exponentiel)
- Utilisation : ρ = λ/μ
- Délaimoyen = 1 / (μ - λ)

Une attaque DoS provoque un pic de λ, ce qui fait croitre ρ → 1 et le delai tend versl'infini.

e) Chaînes de Markov caches (HMM)[7]

- Un réseau peut être modélisé comme un système à états caches (normale, attaqué) États cachés : S = {normal, intrusion},
- Observations : caractéristiques mesurées
- Objectif: Estimer la probabilté que le réseau soitenétat ''intrusé''

On utilise des algorithmes forward-backward ou Viterbi pour inférer la séquence d'états les plus probable.

[2]Dorothy E .Denning, *Un Modèle de détection, EEE Computer society*, LOS Alamitos, 1987.
[3] Pierre Brémaud, "Processus stochastiques et applications", Springer Suisse, 2020
[4] Jacques Jeanssen, Nikolaos Limnios et Bruno Sericola, *Méthodes stochastiques appliquées*, Hermès-Lavoisier, 1ère Edition, Paris, 2013.
[5]Claude E, Shannon, *Théorie mathèmatique de la communication*, Retz, Paris, 1975
[6] Jacques Jeanssen, Nikolaos Limnios et Bruno Sericola, Chaines de Markov: *Theorie, algorithms et applications*, Hermès-Lavoisier, 1ère Edition, Paris, 2013.
[7]Jacques Jeanssen, Nikolaos Limnios et Bruno Sericola, Chaines de Markov: *Theorie, algorithms et applications*, Hermès-Lavoisier, 1ère Edition, Paris, 2013.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

f) Approchebayésienne[8]

- on définit la vraisemblance (traffic normal) et (traffic anormal)
- on applique la règle de Bayes pour inferer:

si, alors X est classé comme intruision, sinon comme traffic normal

2.2. TYPES D'INTRUSION ET MENACES

Il existe quatre grandes categories d'attaques en réseau. Chaque attaque sur un réseau peut être classée dans l'une de ces catégories.

a. Déni de service (DoS)

Une attaque DoS est un type d'attaque dans laquelle le pirate rend les ressources de mémoire trop occupées pour répondre aux demandes de réseau légitimes, empêchant ainsi les utilisateurs d'accéder à une machine, par exemple avec des attaques telles que Apache, Smurf, Neptune, ping of death, back, mail bomb, tempête UDP, etc.

b. Attaques à distance sur un utilisateur (R2L)

Une attaque à distance sur un utilisateur est une attaque dans laquelle un utilisateur envoie des paquets à une machine sur Internet à laquelle il n'a pas accès, dans le but d'exposer les vulnérabilités de la machine et d'exploiter les privileges qu'un utilisateur local aurait sur l'ordinateur, par exemple avec des attaques telles que xlock, guest, xnsnoop, phf, sendmail, dictionnaire, etc.

c. Attaquesd'utilisateur à super-utilisateur (U2R)

Ces attaques sont des exploitations dans lesquelles le pirate commence sur le système avec un compte utilisateur normal et tente d'exploiter les vulnérabilités pour obtenir des privilèges de super utilisateur, par exemple avec des attaques telles que Perl, Xterm.

d. Sonde

Une sonde est une attaque dans laquelle le pirate analyseune machine ou un périphérique de réseau afin de déterminer des faiblesses ou des vulnérabilités qui pourrontêtre exploitées ultérieurement pour compromettre le système. Cette technique est couramment utilisée dans l'exploration de données, par exemple avec des attaquestelles que satan, saint, portsweep, mscan, nmap, etc.

Deux types d'attaques différents ont été inclus pour cette étude: le SYN Flood (Neptune) et Satan. Ces deux types d'attaquesontétésélectionnés à partir de deux categories d'attaques différentes (déni de service et sondes) pour vérifier la capacité du système de detection d'intrusion à identifier des attaques provenant de différentes catégories.

e. Le SYN Flood (Neptune)

Le SYN Flood est une attaque de déni de service à laquelle chaque implémentation TCP/IP est vulnérable (dans une certaine mesure). Pour distinguer une attaque Neptune, le traffic réseau est surveillé pour un certain nombre de paquets SYN simultanés destinés à une machine particulière.

f. Satan

Satan estune intrusion de sondage, qui analyse automatiquement un réseau d'ordinateurs pour recueillir des informations ou trouver des vulnérabilités connues.

2.2. DETECTION D'INTRUSION RESEAU

2.2.1. SYSTEME DE DETECTION D'INTUSION

La detection d'intrusion (Intrusion Detection) consiste à identifier les activités anormales dans un système d'information. Un IDS (Intrusion Detection System) analyse le traffic réseau ou les journaux système pour signaler toute tentative suspecte.

La technologie des IDS est devenue un domaine très populaire et bien étudié, en raison de sa demande dans l'industrie. L'intérêt incessant pour cette technologie a continuellement amélioré la performance et la précision des IDS.

Depuis la formation d'IDES, il y a beaucoup plus de produits de detection d'intrusion sur le marché pour que les utilisateurs puissant choisir et mettre en oeuvre. En 1999, Kevin Richards a effectuéune revue de cinq produits IDS différents pour évaluerleur performance dans un environnement de production.

Dans sa revue, il a souligné l'importance du moteur de traitement de paquets dans les IDS. Si le moteurn'est pas efficace et efficient, le capteurou le IDS commencera à perdre des paquets et cela réduira la capacité à détecter des attaques, surtout s'il s'agit d'une attaque avec plusieurs paquets qui doivent être assemblés. La figure ci-dessous décrit l'architecture de sécurité incluant un système de detection d'intrusion (IDS)[9].

[8]Christian Robert, *Statistique bayésienne*, Springer, Traduction francaise, Paris 2007.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

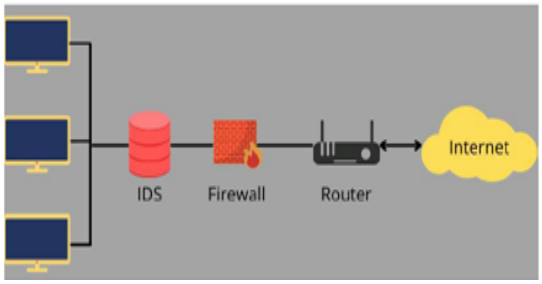


Figure (2-1): Architecture de sécurité incluant un système de detection d'intrusion (IDS)[10]
.

2.2.2. CATEGORIE DE DETECTION D'INTRUSION

Bien que tous les systèmes de detection d'intrusion remplissent le mêmeobjectif, ils fonctionnent de manière légèrement différente. Il existe cinq types de IDS au total. Examinons les détails, avantages et inconvénients de chacun.

a. Système de détectiond'intrusionréseau

Un système de detection d'intrusion réseau (NIDS) surveille tout le trafic qui passe par votre réseau grâce à un ou plusieurs points de contact. Pour utiliser un NIDS, il doit être installé sur un matériel de votre infrastructure réseau. Une foisen place, il échantillonnera chaque paquet de données qui circule à travers lui. Cependant, tous les paquets ne nécessitent pas uneanalyse, car celarisque de manquer une tentative d'intrusionen raison d'une surcharge d'informations. Pour remédier à ce problème, ilest possible de créer un ensemble de règles qui définissent les types de paquets que votre NIDS détectera et stockera.

Les avantages du NIDS sont les suivants:

- Il peut analyser tout le trafic entrant et sortant.
- Il détecte les événementsen temps réel, permettant des temps de réponserapides.
- Il est plus difficile à détecter par les intrus.
- Il peut être placé de manière stratégique dans des zones critiques.

Cependant, les NIDS ne sont pas parfaits. Les inconvénients potentiels sont la maintenance pratique, car il nécessite souvent une interaction manuelle avec lui, et une faible spécificité. Plus un NIDS analyse de trafic, plus ilrisque de manquer de spécificité et de ne pas détecter les signes d'une intrusion.

b. Système de detection d'intrusion de noeud de réseau:

Un système de detection d'intrusion de noeud de réseau (NNIDS) est techniquement une variation d'un NIDS, mais comme il fonctionne différemment, nous le considérerons comme un type différent de IDS. Un NNIDS analyse également les paquets qui passent à travers lui.

Cependant, au lieu de s'appuyer sur un dispositif central pour surveiller l'ensemble du traffic réseau, le système surveille chaque nœud connecté à votre réseau. Cette différenciation comporte plusieurs avantages, tels que:

- Des vitesses plus élevées - étantdonné que la quantité de traffic analysée par chaque agent NNIDS est réduite, le système peut fonctionner plus rapidement.
- Moins de ressources utilisées De la même manière, NNIDS utilisemoins de ressources système.

Les HIDS présentent des avantages, car:

- Ils peuvent être installés sur des ordinateurs ou des serveurs;
- Ils peuvent identifier l'appareilaffecté
- Ils notifient les administrateurs si des fichiers système analytiques ont été modifies ou supprimés;
- Ils sont particulièrement efficacies contre les menaces internes

Malheureusement, les solutions HIDS peuvent souffrir d'une surveillance "après coup". Parce que de nombreuses solutions HIDS s'appuient sur des journaux qui enregistrent les intrusions, votre temps moyen de réponse (MTTR) peutêtre plus lent dans l'ensemble. Par conséquent, l'utilisation appropriée d'un HIDS nécessiteune surveillance fréquente.

d. Système de detection d'intrusionbasé sur le protocole

Un système de detection d'intrusion basé sur le protocole (PIDS) est un IDS spécifique qui surveille le protocole encours d'utilisation. Dans la pratique, ce système analyse généralement le flux de protocole HTTP ou HTTPS entre vosappareils et le serveur. Dans la plupart des cas, un PIDS sera placé à l'avant d'un serveur. Le système peut protéger votre serveur web en surveillant le trafic entrant et sortant. Étant donné qu'ils se concentrent sur le protocole (la façondont les appareils

[9]Geekflare. (s.d.). IDS vs IPS - Network Security Solutions Dans Geekflare. Lu le 10 mai2025, de https://geekflare.com/fr/ids-vs-ips-network-security-solutions/

[10]Idem.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

transmettent des informations au sein d'un réseau), les PIDS ne sont pas nécessairement une solution IDS complète. Cependant, ils peuvent completer une solution de cybersécurité déjà robuste.

e. Système de détectiond'intrusionbasé sur le protocole de l'application

Un système de detection d'intrusion basé sur le protocole de l'application (APIDS) est un type d'IDS qui se spécialise dans la sécurité des applications logicielles. Généralement associés aux systèmes de detection d'intrusion sur hôte (HIDS), les APIDS surveillent les communications qui ont lieu entre les applications et le serveur. Un APIDS est généralement installé sur des groupes de serveurs.

Comme pour un PIDS, un APIDS ne résoudra probablement pas tousvosbesoins de surveillance réseau. Cependant, il peutcompléter d'autres types d'IDS.

2.2.3. TECHNIQUES CLASSIQUES DE DETECTION D'INTRUSION

Selon le type de système de detection d'intrusion que vous choisissez, votre solution de sécurité reposera sur quelques méthodes de detection différentes pour vous protéger. Voici un bref aperçu de chacune d'entreelles.

a) DETECTION D'INTRUSION BASEE SUR LES SIGNATURES

Les systèmes de detection d'intrusion basés sur les signatures (SIDS) visent à identifier des modèles et à les faire correspondre à des signes connus d'intrusions. Un SIDS repose sur une base de données d'intrusions précédentes. Si l'activité au sein de votre réseau correspond à la "signature" d'une attaque ou d'une violation de la base de données, le système de detection notifie votre administrateur. Étant donné que la base de donnéesest la colonnevertébraled'une solution SIDS, des mises à jour fréquentes de la base de données sont essentielles, car les SIDS ne peuvent identifier que les attaques qu'ils reconnaissent. Par conséquent, si votre organisation devient la cible d'une technique d'intrusion jamais vue auparavant, aucune mise à jour de la base de données ne pourra vous protéger.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

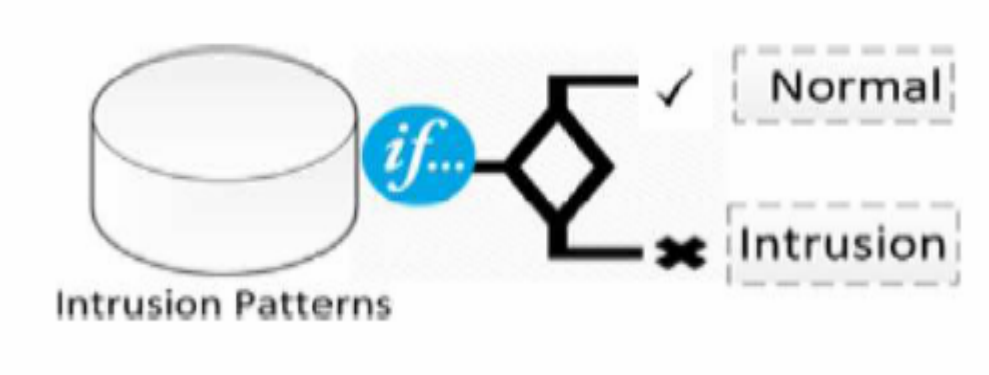


Figure (2-2): Le fonctionnement conceptuel des approches SIDS[11].

[11]Geekflare. (s.d.). IDS vs IPS - Network Security Solutions Dans Geekflare. Lu le 10 mai2025, de https://geekflare.com/fr/ids-vs-ips-network-security-solutions/

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

b) DETECTION D'INTRUSION BASEE SUR LES ANOMALIES

En revanche, un système de detection d'intrusion basé sur les anomalies (AIDS) peut identifier ces nouvelles intrusions zero-day. Un SIDS utilize l'apprentissage automatique (ML) et les données statistiques pour créer un modèle de comportement "normal". Chaquefois que le traffic s'écarte de ce comportement typique, le système le signalecomme suspect. Le principal problèmed'AIDS par rapport à SIDS est le risque de faux positifs. Après tout, tous les changements ne sont pas le résultat d'activités malveillantes; certains sont simplement des indications de changements dans le comportement organisationnel. Mais parcequ'un SIDS n'a pas de base de données d'attaques connues à référencer, il peut signaler toutes les anomalies comme des intrusions.

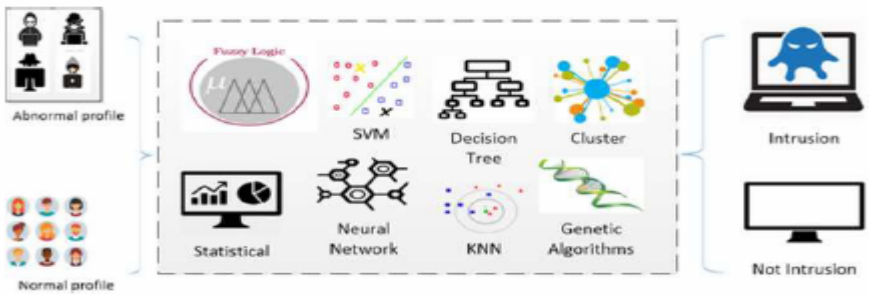


Figure (2.3): Le fonctionnement conceptuel des approches AIDS basées sur l'apprentissage automatique[12].

c) DETECTION D'INTRUISON HYBRIDE

Un système hybride combine le meilleur des deux mondes. En examinant les modèles et les événements ponctuels, un système de detection d'intrusion hybride peut signaler de nouvelles strategies d'intrusion existantes et nouvelles. Le seulinconvénient d'un système hybride est l'augmentation encore plus grande des problems signalés. Cependant, étantdonné que le but d'un IDS est de signaler les intrusions potentielles, ilest difficile de considerer cette augmentation de signalements comme négative[13].

c) Comparaison des outils IDS populaires

Outil	Type	Fonctionnalitésclés	Limites
Snort	Basé sur les signatures	Analyse de paquets réseau, open-source, détection simple à configurer	Incapable de détecter des attaques de type zero-day
Suricata	Hybride (signatures + anomalies)	Détection en temps réel, multi-threading, support IPv6, performance élevée	Configuration plus complexe, consummation mémoire plus importante
Zeek (Bro)	Basé sur les	Analyse réseau avancée,	Moins efficace pour la détection par

[12]Geekflare. (s.d.). IDS vs IPS - Network Security Solutions Dans Geekflare. Lu le 10 mai 2025, de https://geekflare.com/fr/ids-vs-ips-network-security-solutions/
[13]Idem.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

	anomalies	langage de script puissant, grande flexibilité	signature, nécessiteune bonne expertise

Tableau (2-1): Comparaison des outils IDS populaires[14]

[14]Gaberan, P. *Cybersécurité – Sécuritéinformatique et réseaux*. Saint-Herblain, France: ENI Éditions, 2021.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

2.3. Défis de la detection d'intrusions et solution adaptées

La detection d'intrusions reste un domaine complexeen raison de plusieursdéfis techniques, organisationnels et opérationnels. Ces défis entravent l'efficacité des systèmes de detection d'intrusions (IDS) et nécessitent des solutions robustes.

- ✓ **Complexité des infrastructures modernes:** Avec l'essor des environnements Cloud, de l'IoT (Internet des Objets) et des réseaux distribués, la surface d'attaque s'élargit considérablement. Chaque appareil connecté constitue un point potentiel de vulnérabilité.
- ✓ **Hétérogénéité des systèmes:** Les réseaux modernes combinent différents systems d'exploitation, protocoles et technologies, rendant la surveillance et l'analyse plus complexes.
- ✓ **Volume croissant des donnéesréseau:** Les systems génèrent un volume massif de données à analyser en temps réel. Cela rend la detection rapide et précise difficile sans outils avancés tels que le machine learning.
- ✓ **Évolutionconstante des techniques d'attaque**

a) Attaques zero-day: Les intrusions basées sur des vulnérabilités inconnues ne peuvent pas être détectées par des systems basés sur les signatures.
b) Techniques d'évasion sophistiquées: Les attaquants utilisent des méthodes pour masque leurs activités (chiffrement des communications malveillantes, obfuscation de code) ou pour tromper les IDS (fragmentation des paquets, attaquespolymorphiques).

- ✓ **Taux de faux positifs et négatifsélevé**

a) Faux positifs: Les systems peuvent alerter sur des activités bénignes interprétées comme malveillantes, ce qui surcharge les analystes et peut entraîner une perte de confiance dans le système.
b) Faux négatifs: Les intrusions légitimes peuvent passer inaperçues, surtout lorsque les attaques imitent des comportements normaux.

- ✓ **Quelques solutions possibles aux défis**

1. Adoption de l'intelligence artificielle et du machine learning pour améliorer la précision et détecter les attaques zero-day
2. Approches hybrides (signatures + anomalies) pour combiner les avantages des deux méthodes.
3. Renforcement des équipes de cybersécurité par la formation et le recrutement de spécialiste
4. Utilisation d'outils de Big Data pour gérer les volumes massifs de données.

III. RESEAUX DE NEURONE MULTICOUCHES

3.1. Apercu général

La detection d'anomalies dans un réseau repose souvent sur l'apprentissage non supervise notamment par estimation de densité; dans ce cadre, les réseaux de neurons profonds (auto-encodeurs, GAN, etc permettrent d'apprendre des representations latentes et de reperer les obstacles inhabituellement faibles en densité[15].

Un RNA est une function paramétrée qui est la composition d'opérateurs mathématiques simples appelés neurons formels (ou plus simplement neurones).

Un neurone est une function algébrique non linéaire, paramétrée, a valeurs bornées, de variables réelles appelées entrées.Un neurone realize une fonction non linéaire bornéeoù les $\{x_j\}$ sont les entrées et les $\{w_j\}$ sont des paramètres

L'argument de la fonctionf est une combinaison linéaire des entrées du neurone (à laquelle on ajoute un terme constant, le "biais"). La combinaison linéaire est appellee potentiel; les coefficients de pondération $\{w_j\}$ sont fréquemment appelés"poids synaptiques" (ou plus simplement poids) en référence à l' origine "biologique" des réseaux de neurones.

Le potentiel d'un neurone est donc calculé de la façonsuivante:
: Potentiel du neurone
Le biais w_o peut être envisage comme le coefficient de pondération de l'entrée n°0, qui prend toujours la valeur1:
La valeur de la sortie du neurone est donc :
Sortie du neuronne
La fonction f est appelée "function d'activation"

[15]Guillaume Saint-Cirgue, *Apprendre le Machine learing en une semaine*, guide en ligne gratuit, 2019

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

La figure ci-dessous présente un exemple d'un RNA à 3 couches.

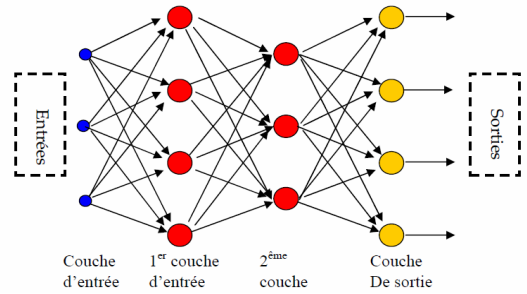


Figure (3-1) RNA à 3 couches[16]

Ces modèles ont été fortement inspirés par le système nerveux biologique. On peut entraîner un réseau de neurone pour une tâche spécifique (reconnaissance de caractères par exemple) en ajustant les valeurs des connections (oupoids) entre les éléments (neurone).Il existe plusieurs variété de ces réseaux et dans le cadre de notre étude nous tiendrons compte de trois modèles que voici: (RNN, CNN et MLP)

3.2. Les réseaux de neuronesrécurrents (RNN)

a) Présentation architecturale

Les réseaux de neurons récurrents (RNN) sont des architectures de réseaux neuronaux qui sont capables de traiter des données séquentielles en pregnant en compte la dépendance temporelle entre les éléments successifs de la séquence. Ils sont particulièrement efficaces pour des tâchestelles que la prédiction de séquences, la traduction automatique et l'analyse de sentiments. La detection d'intrusion utilisant des réseaux de neurons (RNN) permetd'analyser les séquences de données réseau pour détecter les comportements anormaux et identifier les intrusions de manière efficace.

Structure

Pour une sequence d'entrée, un RNN produit une sequence d'états caches.
et éventuellement une sequence de sorties
(3-1)

Composantsprincipaux:

- Entrée à l'instant:
- Etat caché:
- Sortie:

Mise à jour de l'état cache

- (3-2)
- : Matrice des poids état cache vers état caché
- : Biais
- : Fonction d'activation (souvent tanh ou ReLU)

Sortie

- (3-3)
- : Biais
- Fonction d'activation de sortie (softmax par exemple)

Structure complète

b) Apprentissage du RNN

✓ **Architecture générale**

Un RNN traite des séquences avec :
- : l'entrée à l'instant t,
- : l'état caché,
- : la sortie,
- ,, : matrices de poids à prendre.

Les équations de base du RNN
(3-4)
Où:
est une fonction d'activation (tanh, ReLU),
peut être softmax ou sigmoid selon la tâche (classification ou regression).

✓ **Fonction de perte logs**

On considère une onction de perte au temps t :
et la perte totale sur toute la séquence :

✓ **Rétropropagation à travers le temps (BPTT)**

✓ L'objectif est de calculer les gradients de la perte par rapport aux poids :

✓ (3-5)

Étapes :

1. Propagation avant : on calculetous
2. Calcul des gradients: On applique la règle de la chine sur les séquences.

exemple: (3-6)

✓ **Problèmesrencontrés**

Si , les gradient explosent
, les gradients s'annulent
Ceci est dû à la multiplication répétée des dérivées sur de longues sequences

✓ **Mise à jour des poids**

Une fois les gradients calculés, les poidssont mis à jour avec descente de gradient:

[16]Auélien Géron, *Apprentissage automatique avec Sckit-Learn, Keras et TensorfFlow ; Concepts, outils et techniques de l'Interlligence artificielle et du machine learning*, 2ème édition O'Reilly, Paris 2020

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

avec le taux d'apprentissage.

3.3. Les réseaux de neurons convolutifs (CNN)

a) Présentation

Les réseaux de neurons convolutifs (CNN) sont une classes pécifique de réseaux de neurons artificiels, souvent utilisés pour l'apprentissage automatique supervisé dans le domaine de la vision par ordinateur. Ils sont particulièrement adaptés pour traiter des données structures telles que des images.

Dans le contexte de la detection d'intrusion réseau, les réseaux de neurons convolutifs peuvent être utilisés pour analyser le traffic réseau et détecter des modèles ou des comportements suspects qui pourraient indiquer une activité malveillante.

b) Apprentissage du CNN

Pour connaître les paramètres de ce réseau, c'est-à-dire les poids et les biais de chaque neurone formel qui le constitue, nous avons utilisé une base de données d'apprentissage fournissant des données d'entrée et les sorties désirées leur correspondant. Le calcul de ces paramètres est appelé phase d'apprentissage et se fait grâce à l'algorithme de rétropropagation du gradient introduit par [Rumelhart 1986, Lecun 1986]. Avant l'apprentissage, les paramètres du réseau sont inconnus et doivent être initialisés à des valeurs aléatoires[17].

Nous considérons un sous-ensemble de notre base d'apprentissage composé de N exemples avec une donnée d'entrée et la sortie désirée lui correspondant. Ainsi, est l'exemple du batch (sous-ensemble de la base d'apprentissage).

Les paramètres d'un neurone formelseront notes respectivementet pour ses poids et son biais. en passant la donnéedans le PMC, l'erreur observée sur le neurone j de la couche de sortie s'écrit,
(3-7)
Où la valeur renvoyée par le neurone de sortie est appelée fonction de perte et représente ce que le réseau essaie de minimiser sur l'ensemble des données. Cette fonction est différente suivant le problème à résoudre. Dans le cas du MLP qui est aussi applicable au CNN, la fonction de perte est définie comme suit:
(3-8)
L'erreur quadratique observée pour la donnéesur les neurones de la couche de sortie s'écrit:
(3-9)
Et l'erreur quadratique moyenne sur l'ensemble du batch est définie par:

La mise à jour des poids du réseau se fait par descente de gradient stochastique (SGD) de l'erreur quadratique moyenne. End'autres termes, le poidsdu neuroneest mis à jour en lui ajoutant le terme. La mise à jour du biais du neuroneest effectuée en lui ajoutant le terme . est appelé taux d'apprentissage (learning rate)[18]. Il permet de pondérer la mise à jour des paramètres du réseau. Les deux termessont définis comme suit:

Dans ce qui suit, nous détaillons la rétropropagation du gradient suivant le type de couche considéré (couche de sortie oucouchecachée).

B.1. Rétropropagation pour la couche de sortie

Enreprenant l'équation (3-11) et grâce à la decomposition enchaîne des dérivées partielles, nous pouvonsécrire:

Ces dérivées partielles peuvent individuellement s'exprimer comme suit:

Ce qui permet d'obtenir:

Enposant

B.2. Rétropropagation pour les couches cachées

Dans le cas de la couche cachée précédant la couche de sortie, l'erreurdu neurone cachéest inconnue. Pour ce type de couche, la dérivée

[17]ARCHAUX C., Martin A., KHENCHAF A., « *Détection par SVM – Application à la détection de churn entéléphonie mobile prépayée, Extraction et Gestion des Connaissances*», Dans Revue des Nouvelles Technologies de l'Information, Vol 2, Clermont Ferrand, France, pp. 2-6, Janvier 2004

[18] BISHOP C. M., "*Réseau de neurons our la classification des modèles*". Oxford University Press, 1995.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

partielle de l'erreur quadratique de l'équation 3.5 s'écritcomme suit:

La dérivéepartielle peut s'exprimer ainsi:

Nous obtenonsdonc:

Avec:

Le termeest le gradient défini dans 3.16. L'équation 3.20 se généralise à toutes les couches cachées. Le gradient d'un neuroned'une couche cachée, utilise le gradient de la couche qui le suit.

B.3. Règle du delta généralisé

La mise à jour des paramètres du réseau se fait en utilisant la règle du delta généralisé. Ainsi, nous l'avons fait par descente de gradient stochastique (SGD) avec momentum. Pour une itération, permettant de passer dans le réseau un batch de données, la mise à jour se fait comme suit:
Pour les poids:

Pour les biais:

Avec appelé momentum (valeur entre 0 et 1) permettant de donner une inertie à la descente de gradient enprenant en compte les corrections appliquées à l'itération précédente. Ainsi donc, il existe d'autres règles que la SGD avec momentum pour l'optimisation des réseaux de neurones: ADADELTA [Zeiler 2012], ADAGRAD [Duchi 2011], ADAM [Kingma 2015], RMSProp [Tieleman 2012]. Ces règles d'optimisation permettent d'adapter le taux d'apprentissage aux paramètres afin de mieux converger tout enétant plus rapide.

3.4. Le Réseau de neurone Multicouche (MLP)

a) Présentation et architecture

Le MLP (Perceptron Multi-Couche ou Multilayer Perceptron) est un type de réseau de neurons artificiels appartenant à la famille de l'apprentissage supervisé. Il estutilisé pour résoudre des problèmes de classification, de régression, et plus généralement pour approximer des fonctions complexes. Un MLP est composé:

- D'une couche d'entrée qui reçoit les données d'entrée
- D'une ou plusieurs couches cachées (hidden layers) composées de neurons interconnectés.
- D'une couche de sortie qui donne le résultat final.

Chaque neurone applique une function d'activation (comme ReLU, sigmoid, tanh) pour introduire de la non-linéarité.

- Entrée: vecteur de caractéristiques (features) x $\in\mathbb{R}^n$.
- Couches cachées: chaque neurone calculi une somme pondérée des entrées, applique une function d'activation.
- Sortie: vecteur de prédiction (classification ou régression).

Pour un neurone: (3-26)
où :
- sont les entrées,
les poids,
le biais,
la fonctiond'activation.

b) Apprentissage

✓ Notations générales

- : vecteur d'entrée
- : sortie attendee
- : sortie prédite
- : nombre total de couches
- : poids et biais de la couche
- = : somme pondérée des entrées
- : activation de la couche
- : fonction de coût

✓ Propagation avant (Forward Propagation)

Pour chaque couche :
=
avec
✓ Fonction de coût
(3-27)
✓ Rétropropagation (Backpropagation)
Objectif: Calculer les dérivées partielles de par rapport à chaque poids et biais du réseau.

a) Erreur de sortie dernièrecouche):
(3-28)

(designe le prduit terme à terme

b) Propagation de l'erreurvers les couches précéntes:
=
✓ Mise à jour des poids (Gradient Descent)
Avec un tauxd'apprentissage, les mises à jour sont:
= = (3-29)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

IV. APPLICATION

4.1. OUTILS ET METHODOLOGIES

4.1.1. OUTILS

a) DATASET[19]

Le NSL-KDD est une version améliorée et nettoyée du célèbre KDDCup'99, conçu pour: Éliminer les doublons massifs présents dans KDD'99, Éviter le sur-apprentissage (overfitting) des modèles et Offrir une base plus équilibrée pour l'évaluation des IDS.

Il contient plusieurs types d'attaques classes en 4 catégories: DoS (Denial of Service), Probe (analyse du réseau), U2R (User to Root), R2L (Remote to Local), ainsi que du trafic normal.

b) **Python**

Python est un langage de programmation open source, multi-plateformes et orientéobjet. Il est largement utilisé dans divers domains tels que le développement logiciel, l'analyse de données et la gestion d'infrastructures, grâce à sa flexibilité et aux nombreuses bibliothèques spécialisées disponibles. Nous avons utilisé le langage de programmation Python pour implementer nos modèles de detection d'intrusion[20].

4.1.2. METHODOLOGIE

a) Prétraitement des données:

- Chargement des fichiers KDDTrain+.txt et KDDTest+.txt du dataset NSL-KDD.
- Normalisation des attributs numériques (comme, MinMaxScaler).
- Encodage des attributs catégoriels (commeprotocol_type, service, flag) via one-hot encoding ou label encoding.
- Regroupement des attaques en une classification binaire (attaque vs normal).

b) Division des données:

- Données d'entraînement : KDDTrain+
- Données de test : KDDTest+

c) Application des modèles (MLP, CNN, RNN):

- Les MLP traitent les données tabulaires tells quelles (après flattening).
- Les CNN utilisent une version reshaped des données pour capturer des motifs locaux entre les champs.
- Les RNN (notamment LSTM) exploitent une vue séquentielle des connexions réseau (par exemple, en simulant un flux ou des sessions réseau).

d) Évaluation:

- Les modèles sont évalués avec des métriques standard :
- Accuracy
- Precision
- Recall
- F1-score
- Matrice de confusion

4.2. Architecture des modèles retenus

- MLP : Entrée → Dense(128) → Dense(64) → Sortie
- CNN : Entrée reshaped → Conv1D(64, kernel=3) → MaxPooling → Flatten → Dense(64) → Sortie
- RNN : Embedding → LSTM(64) → Dense(32) → Sortie

Voici le tableau complet des hyperparamètres des modèles

[19] NSL-KDD Dataset. http://www.unb.ca/cic/datasets/nsl.html, lu le 20 mai 2025

[20] Wes McKinney, "Python pour l'analyse de données: Manipulation avec pandas, Numpy et Jupter," O'Reilly Media, Sebastopol, 2022.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

Modèle	Architecture	Activation	Optimiseur	Epochs	Batch Size	Learning Rate
MLP	3 couches (128, 64, sortie)	ReLU	Adam	50	32	0.001
CNN	2 conv + 2 denses (32, 64, 128)	ReLU	Adam	30	64	0.001
RNN	2 LSTM + dense (64, 32)	Tanh	Adam	40	32	0.001

Tableau (4-1): Tableau des hyperparamètres des modèles

4.3. RESULTATS EXPERIMENTAUX

4.2.1. METRIQUES DE PERFORMENCES

Accuracy, Precision, Recall, F1-score sont les principals métriques utilisées pour comparer les modèles.

- (4-1)
- (4-2)
- (4-3)
- (4-4)

4.2.2. ANALYSE DES PERFORMENCES

a) Matrice de confusion pour chaquemodèle

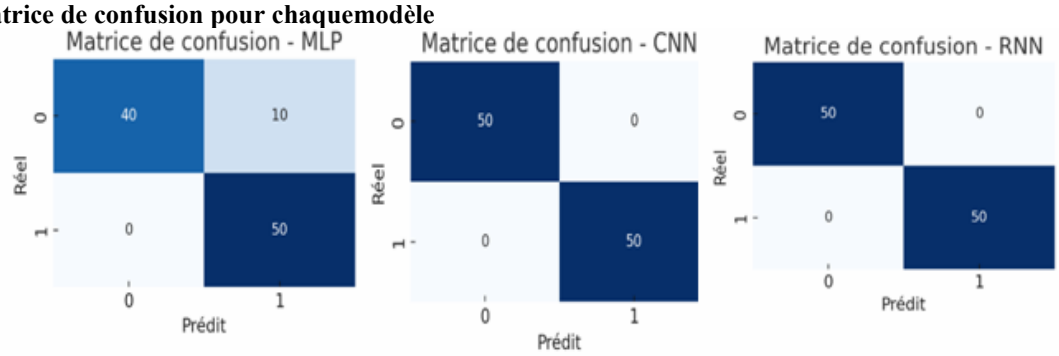


Fig. (4-1): Matrice de confusion de chaquemodèle

Le MLP motre de bonnes performences globales mails avec quelques faux positifs, le CNN(Convolutional Neutral Network) présente un bon équilibre entre vrais positifs et vrais négatifs tandis que le RNN (Recurrent Neutral Network) présentent les performences optimales, quasi-parfaites classications. Donc, le modèle RNN surpasse les autres avec une excellente capacité de détection des intrusions.

b) Diagramme comparatif des performances

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

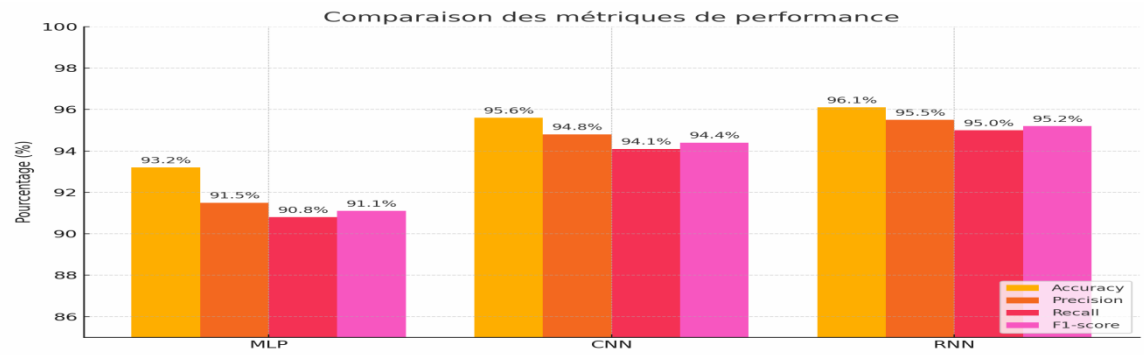


Fig. (4-2): Diagramme comparative des performences

Le diagramme montre clairement la supériorité du RNN suivi du CNN. Le MLP a des performances plus modestes.

c) Tableau des performences

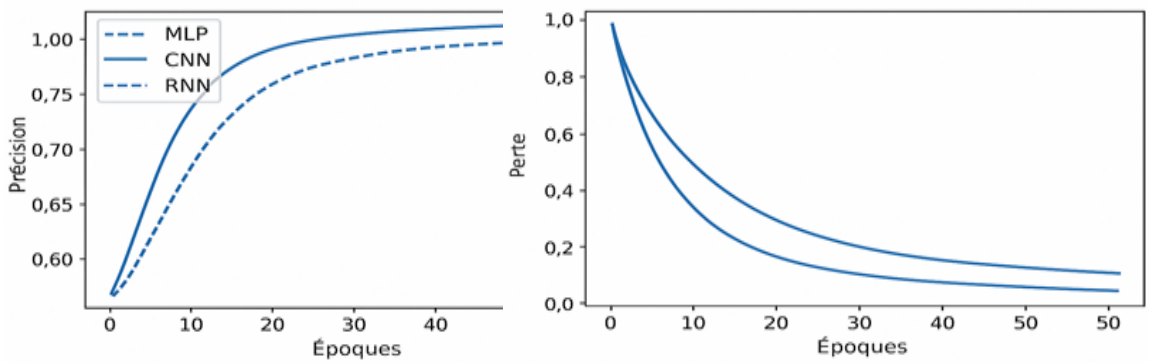
Modèle	Accuracy	Precision	Recall	F1-score
MLP	93.2%	91.5%	90.8%	91.1%
CNN	95.6%	94.8%	94.1%	94.4%
RNN	96.1%	95.5%	95.0%	95.2%

Tableau (4-2): Tableau des performances des ces différents modèles

Les performances comparées à l'aide du tableau et de diagrammes indiquent que le RNN surpasse les deux autres modèles, grâce à sa capacité à modéliser les sequences d'événements, le CNN suit de près, performant sur les motifs locaux, tandis que le MLP montre des performances correctes, mais inférieures. Ces résultats confirment que les architectures profondes, bien entraînées, permettent une detection d'intrusion efficace.

c) Courbesd'apprentissage (simulées)

Les figures suivantesreprésentent les courbes d'apprentissage des trois modèles entraînés sur le dataset NSL-KDD. On y observe la progression de la précision et de la perte en fonction du nombre d'époques:



International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

Fig. (4-2): Courbes d'apprentissages (Exactitude et perte pour les trois modèles)

L'analyse des courbes d'exactitude et de perte pour les modèles MLP, CNN et RNN révèle plusieurs tendances intéressantes:

- MLP présente une amélioration progressive de la precision jusqu'à atteindre un plateau, indiquant une convergence stable. Sa courbe de perte diminue régulièrement sans signe de surapprentissage.
- CNN attaint une precision élevée plus rapidement, avec une courbe de perte qui chute fortement dès les premières itérations. Cela s'expliquepar la capacité du CNN à extraire efficacement des motifs à partir des données d'entrée, même s'il peut nécessiter davantage de régularisation.
- RNN (LSTM) montreune montée plus lentemais continue de la précision, ce qui estcaractéristique des réseaux séquentiels. Sa courbe de perte est relativement stable mais converge plus lentement, soulignant la complexité du traitement temporel.

Le CNN offre la meilleure convergence initiale, le MLP reste simple et robuste, et le RNN s'adapte bien aux sequences mais nécessite plus d'itérations pour atteindre ses performances optimales.

V. CONCLUSION

Les résultats de cette étude conferment l'efficacité des réseaux de neurons profonds dans la détection des intrusions réseau, en particulier lorsqu'ils sont entraînés sur des données pertinentes telles que celles du dataset NSL-KDD. En comparant trois architectures différentes – MLP, CNN et RNN – nous avonspu observer une nette amélioration des performances enfaveur du RNN, qui enregistre une accuracy de 96,1 %, contre 95,6 % pour le CNN et 93,2 % pour le MLP.

Cette supériorité du RNN peut s'expliquer par sa capacité à capturer les dépendances temporelles entre les événements du traficréseau, un avantage essentiel dans la détection de sequences d'intrusions. Le CNN, quant à lui, exploite efficacement les motifs locaux et spatiaux, tandis que le MLP reste performant, mais moins adapté aux structures complexes ou séquentielles des données réseau.

Ainsi, dans le contexte de la cybersécurité, le recours aux architectures RNN apparaît comme une option particulièrement efficace pour améliorer la réactivité et la précision des systèmes de detection d'intrusion. Toutefois, pour renforcer encore cette approche, des perspectives futures pourraient explorer des modèles hybrides (comme CNN-RNN) ouutiliser des techniques d'optimisation avancées, telles que l'apprentissage par renforcement ou les algorithms d'auto-encodage pour la réduction de dimension. La généralisation à d'autres datasets plus récents ou en temps reel représente également une voie prometteuse pour une protection proactive des réseaux informatiques.

BIBLIOGRAPHIE

[1]. Antoine Cornuéjols, Laurent Miclet & d'Yves Kodratoff, Apprentissage artificiel, Concepts et algorithmes, EYROLLES, Paris. 2003.
[2]. Dorothy E. Denning, Un Modèle de détection, EEE Computer society, LOS Alamitos, 1987.
[3]. Pierre Brémaud, Processus stochastiques et applications, Springer Suisse, 2020
[4]. Jacques Jeanssen, Nikolaos Limnios et Bruno Sericola, Méthodes stochastiques appliquées, Hermès-Lavoisier, 1ère Edition, Paris, 2013.
[5]. Claude E, Shannon, Théorie mathèmatique de la communication, Retz, Paris, 1975
[6]. Jacques Jeanssen, Nikolaos Limnios et Bruno Sericola, Chaines de Markov: Theorie, algorithms et applications, Hermès-Lavoisier, 1ère Edition, Paris, 2013.
[7]. Christian Robert, Statistique bayésienne, Springer, Traduction francaise, Paris 2007.
[8]. Geekflare. (s.d.). IDS vs IPS - Network Security Solutions Dans Geekflare. Lu le 10 mai2025, de https://geekflare.com/fr/ids-vs-ips-network-security-solutions/
[9]. Gaberan, P. Cybersécurité–Sécurité informatique et réseaux. Saint-Herblain, France: ENI Éditions, 2021.
[10]. Guillaume Saint-Cirgue, Apprendre le Machine learing en une semaine, guide en ligne gratuit, 2019
[11]. Auélien Géron, Apprentissage automatique avec Sckit-Learn, Keras et TensorfFlow ; Concepts, outils et techniques de l'Interlligence artificielle et

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 08 Aug. 2025, pp: 481-495 www.ijaem.net ISSN: 2395-5252

du machine learning, 2ème édition O'Reilly, Paris 2020

[12]. ARCHAUX C., Martin A., KHENCHAF A., « Détection par SVM – Application à la détection de churn en téléphonie mobile prépayée, Extraction et Gestion des Connaissances», Dans Revue des Nouvelles Technologies de l'Information, Vol 2, Clermont Ferrand, France, pp. 2-6, Janvier 2004.

[13]. NSL-KDD Dataset. http://www.unb.ca/cic/datasets/nsl.html, lu le 20 mai 2025.

[14]. Wes McKinney, "Python pour l'analyse de données: Manipulation avec pandas, Numpy et Jupter," O'Reilly Media, Sebastopol, 2022.