Intelligence Artificielle En Réseaux

- Dispensé par Dr. Msc. Ir. **MWAMBA KASONGO Dahouda**
- Docteur en génie logiciel et systèmes d'information
- Machine and Deep Learning Engineer

- Assisté Ass. Grace PWELE

- E-mail : dahouda37@gmail.com

Heure : 08H00 – 12H00

IA (Réseaux et Telecom)

Fiche matière

Universite Protestante de Lubumbashi
Faculté de Sciences Informatiques

Enseignant responsible de la matière : Intelligence Artificielle (reseaux et Telecoms)

Contact: dahouda37@gmail.com/ dahouda37@upl-univ.ac

Matière : Intelligence Artificielle En Reseaux

Domaine/ Filiere/Specialite : Système Informatique (SI)
Crédit: 4 [60H]

Volume horaire d'enseignement hebdomadaire: Cours (Nombre d'heures par semaine): 8H

Objectif du cours

❖ Prérequis

- Connaissance de base des réseaux informatiques.
- Familiarité avec les concepts d'apprentissage automatique et la programmation Python.
- La connaissance des concepts de sécurité des réseaux sera utile mais pas obligatoire

❖ Objectifs généraux

- Comprendre les principes de base de la sécurité des réseaux et des systèmes de détection d'intrusion (Intrusion Detection System : IDS).
- Découvrir comment l'intelligence artficielle peut être appliquée pour détecter les intrusions et les anomalies du réseau informatique.
- Comprendre les différents types de cyberattaques, notamment les logiciels malveillants et les attaques DDoS.
- Mettre en œuvre et évaluer des modèles d'apprentissage automatique pour classer le trafic réseau comme normal ou malveillant.

Objectif du cours

Objectifs spécifiques

- Comprendre le rôle de l'IA dans la mise en réseau : reconnaître comment l'IA peut être intégrée aux réseaux informatiques pour améliorer la sécurité.

- Améliorer la sécurité des réseaux grâce à l'IA : développer des modèles basés sur l'IA pour la détection des intrusions, la détection des anomalies et la prédiction des menaces afin de sécuriser les réseaux.

- Analyser et prétraiter les données réseau (KDD'99, NSL-KDD, CICIDS 2017) pour la détection des intrusions.

- Apprendre a collecter les donnes sur un reseaux informatique grâce a des outils comme Wireshark ou tcpdump.

- Appliquer des techniques avancées, telles que les machine Learning et le Deep Learning, pour améliorer la précision et l'efficacité des systèmes de détection d'intrusion.

- Créer et entraîner un modèle simple à l'aide de techniques d'apprentissage supervisé sur des ensembles de données de trafic réseau.

Fiche matière

Contenu de la matière

CHAPITRE 1 Aperçu général le réseaux

CHAPITRE 2 L'intelligence artificielle dans les Réseaux (Réseaux informatique et Telecom).

CHAPITRE 3 Techniques d'IA utilisées dans le réseaux informatique

CHAPITRE 4 L'IA pour la sécurité des réseaux (IDS)

CHAPITRE 5 Détection des anomalies du trafic réseau avec l'apprentissage automatique (ML)

IA (Réseaux et Telecom)

Fiche matière

Mode D'evaluation : Moyenne et de l'examen Final

Moyenne	Points
Presence au cours	10 pts
TD	10 Pts
TP	10 pts
Interrogation	20 pts
Total Moyenne annuelle	/50 pts

PLAN DU COURS

CHAPITRE 1 Aperçu général des réseaux

Ce chapitre présente une introduction aux réseaux, en distinguant deux types principaux :

- Réseaux Informatiques : Un réseau informatique est un ensemble d'ordinateurs connectés qui partagent des ressources. Cela peut incl ure des fichiers, des imprimantes, ou encore des services comme les applications. Ces réseaux permettent la communication et la colla boration entre différents utilisateurs ou systèmes au sein d'une entreprise ou à travers Internet.
  - Exemples : LAN (réseau local), WAN (réseau étendu), Intranet, Extranet.

- Réseaux de Télécommunications : Ce type de réseau est dédié à la transmission d'informations sous forme de signaux électroniques ou optiques. Cela inclut les réseaux cellulaires (comme 4G, 5G), les réseaux de téléphonie fixe, et les réseaux de fibres optiques qui véhicu lent des données à haute vitesse.
  - Exemples : Réseaux téléphoniques, réseaux mobiles, Internet.

PLAN DU COURS

CHAPITRE 2 L'intelligence artificielle dans les Réseaux

Dans ce chapitre, on explore comment l'IA est intégrée aux réseaux, à la fois pour les réseaux informatiques et les réseaux télécoms.

L'objectif est d'améliorer l'**efficacité**, **la sécurité** et **la gestion des ressources** de ces réseaux.

- Dans les réseaux informatiques : L'IA est utilisée pour l'optimisation de la gestion du trafic, la surveillance en temps réel, la détection des anomalies, et la réponse automatisée aux menaces de sécurité.
- Dans les réseaux télécoms : L'IA peut aider à la gestion automatique de la bande passante, l'optimisation de la couverture réseau, et la prévision des pannes ou des surcharges.

L'IA rend ces réseaux plus adaptatifs et résilients en répondant aux changements de conditions ou aux menaces sans intervention humaine.

PLAN DU COURS

CHAPITRE 3 Techniques d'IA utilisées dans les réseaux informatiques

Ce chapitre aborde les différentes méthodes d'intelligence artificielle couramment utilisées dans la gestion des réseaux informatiques, telles que :

- Apprentissage automatique (Machine Learning - ML) : Utilisé pour analyser les modèles de trafic réseau et prédire les comportements in habituels ou détecter des anomalies. Les algorithmes ML sont capables de reconnaître des schémas d'attaque ou d'anomalies dans les d onnées réseaux.

Exemples : Réseaux de neurones, algorithmes d'apprentissage supervisé ou non supervisé.

- Apprentissage profond (Deep Learning) : Une sous-catégorie de ML qui utilise des réseaux de neurones profonds pour détecter des mod èles complexes dans de grandes quantités de données réseau.

Ces techniques permettent d'améliorer la qualité de service, de détecter des problèmes de sécurité, et de prédire les besoins en ressources réseau

PLAN DU COURS

CHAPITRE 4 L'IA pour la sécurité des réseaux (IDS)

Dans ce chapitre, on examine le rôle de l'IA dans les Systèmes de Détection d'Intrusion (IDS), qui sont des outils essentiels pour la cybersécurité.

Ces systèmes surveillent en permanence le réseau pour détecter toute activité **suspecte** ou **malveillante**.

- **Détection des intrusions** : L'IA permet de reconnaître des comportements anormaux qui pourraient être des attaques, même des attaques inconnues auparavant. Contrairement aux systèmes traditionnels basés sur des signatures d'attaques (qui ne peuvent détecter que des menaces connues), l'IA peut identifier des menaces DDOS.
- **Prévention proactive** : L'IA peut non seulement détecter des intrusions, mais aussi réagir automatiquement pour isoler un réseau, bloquer un accès, ou même corriger des failles de sécurité avant qu'elles ne soient exploitées.

Les systèmes IDS basés sur l'IA sont cruciaux pour renforcer la sécurité des réseaux modernes face à des cyberattaques de plus en plus sophistiquées

PLAN DU COURS

CHAPITRE 5 Détection des anomalies du trafic réseau avec le machine Learning (ML)

Ce dernier chapitre présente une démonstration pratique de l'utilisation de l'apprentissage automatique (ML) pour détecter des anomalies dans le trafic réseau. Le ML est particulièrement adapté pour ce type de tâche, car il peut analyser des volumes massifs de données réseau et détecter des schémas anormaux qui pourraient indiquer une activité malveillante ou une panne imminente.

- **Anomalies dans le trafic réseau** : Cela peut inclure des augmentations soudaines du volume de données, des connexions inhabituelles ou des tentatives d'accès non autorisées à certaines parties du réseau.

- **Outils de ML** : Les algorithmes tels que Random Forest, Decision Tree, Support Vector Machine (SVM), ou les réseaux de neurones sont utilisés pour créer des modèles capables de repérer ces anomalies en temps réel.

Ce chapitre sert à montrer concrètement comment l'apprentissage automatique peut rendre la détection des anomalies plus rapide et plus précise, améliorant ainsi la sécurité et la performance des réseaux.

Références bibliographiques

Références bibliographiques

1. Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Opportunities. Journal of Internet Services and Applications, 9(1), 16.

Une revue récente qui couvre l'utilisation du machine learning pour les réseaux et ses applications dans divers domaines.

2. Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., & Zomaya, A. Y. (2020). Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. IEEE Internet of Things Journal, 7(8), 7457-7469.

Cet article explore comment l'IA est déployée dans les architectures d'edge computing pour les réseaux modernes.

3. Zhang, Z., Li, X., Wang, R., & Jin, Z. (2021). A Survey on Network Anomaly Detection Using Machine Learning Techniques. IEEE Access, 9, 20750–20761.

Un examen complet des méthodes de détection d'anomalies basées sur le machine learning dans les réseaux.

4. Dong, Y., Luo, M., Wang, J., & Li, L. (2022). AI-Empowered Network Intrusion Detection System for IoT Using Blockchain Technology. IEEE Internet of Things Journal, 9(1), 439–447.

Cet article combine l'IA et la blockchain pour renforcer la sécurité des systèmes de détection d'intrusion dans les réseaux IoT.

5. Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, W. (2020). End-to-End Encrypted Traffic Classification With One-Dimensional Convolution Neural Networks. IEEE Access, 8, 38472–38482.

Cet article se concentre sur l'utilisation de réseaux de neurones convolutifs (CNN) pour classer le trafic réseau chiffré.

Références bibliographiques

Références bibliographiques

6. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2022). Network Traffic Anomaly Détection and Prévention: Concepts, Techniques, and Tools. Springer.

Un livre récent qui aborde les concepts de détection et prévention des anomalies dans les réseaux, en mettant l'accent sur les techniques modernes.

7. Nguyen, T. T., & Armitage, G. (2018). A Survey of Techniques for Internet Traffic Classification Using Machine Learning. IEEE Communications Surveys & Tutori als, 10(4), 56-76.

Une revue des méthodes d'apprentissage automatique pour la classification du trafic Internet.

8. Mao, Q., Hu, F. R., & Hao, Q. (2018). Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey. IEEE Communications Survey & Tutorials, 20(4), 2595-2621.

Un guide détaillé sur l'application de l'apprentissage profond dans les réseaux sans fil.

9. Li, H., Ota, K., & Dong, M. (2018). Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing. IEEE Network, 32(1), 96-101.

Cet article discute de l'utilisation de l'apprentissage profond dans le contexte de l'Internet des objets (IoT) avec l'edge computing.

10. Sarker, I. H., Kayes, A., & Badsha, S. (2022). Cybersecurity Data Science: An Overview from Machine Learning Perspective. Journal of Big Data, 9(1), 36.

Un article récent qui met en lumière l'application du machine Learning à la cyber sécurité, en se concentrant sur la détection des intrusions.