

Université Constantine 2 - Abdelhamid MEHRI

Faculté des Nouvelles Technologies de l'Information et de la Communication - NTIC

Département d'Informatique Fondamentale et ses Application - IFA



Approche résiliente pour l'identification et la détection des attaques DDoS dans les réseaux IoT

Présenté par :

Japhet DIARRA

Mamadou DIARRA MAKADJI TB

Sous la Direction de :

M^r Amir DJENNA

20 septembre 2020

Table des matières

1. INTRODUCTION

Contexte

Problématique

Objectif

2. APERÇU SUR L'ÉTAT DE L'ART

IoT

DDoS

IDS

3. CONTRIBUTIONS

Deep Learning

Approche proposée

Résultats

Comparaison

4. CONCLUSION GÉNÉRALE

Conclusion

Perspectives

1. INTRODUCTION

Contexte
Problématique
Objectif

2. APERÇU SUR L'ÉTAT DE L'ART

IoT
DDoS
IDS

3. CONTRIBUTIONS

Deep Learning
Approche proposée
Résultats
Comparaison

4. CONCLUSION GÉNÉRALE

Conclusion
Perspectives

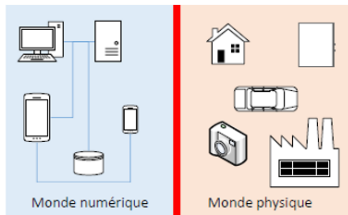
Contexte

Les progrès fulgurants des Technologies de l'Information et de la Communication(TIC) et les nombreuses Innovations dans les communications réseaux ainsi que le besoin de faire collaborer des objets ont conduit à un concept moderne qui est l'Internet des objets(IoT).

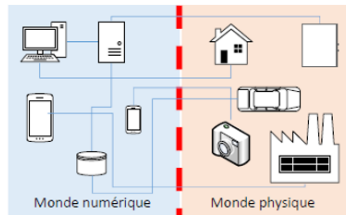
Contexte

Les progrès fulgurants des Technologies de l'Information et de la Communication(TIC) et les nombreuses Innovations dans les communications réseaux ainsi que le besoin de faire collaborer des objets ont conduit à un concept moderne qui est l'Internet des objets(IoT).

Avant l'internet des objets



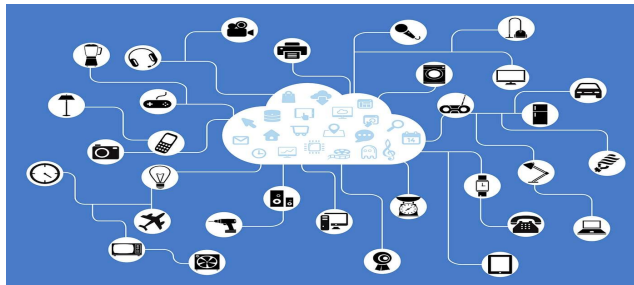
Aujourd'hui



Contexte(suite)

Selon les experts de CISCO, le nombre d'objets connectés dans le monde est actuellement estimé à 30 milliards et ce nombre atteindrait les 75 milliards d'objets connectés en 2025.

Selon les experts de CISCO, le nombre d'objets connectés dans le monde est actuellement estimé à 30 milliards et ce nombre atteindrait les 75 milliards d'objets connectés en 2025.



Problématique

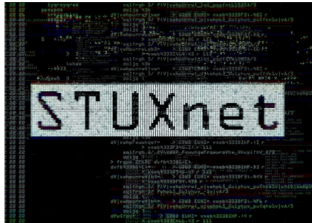
Problèmes

Cependant la collaboration des objets connectés ouvre de nouvelles portes d'attaques aux hackers qui effectuent des attaques de plus en plus sophistiquées. Parmi ces nouvelles portes d'attaques, on peut retenir le DDoS, considéré comme la plus grande menace visant l'IoT. En plus de ces problèmes, s'ajoutent les faibles capacités des composants IoT en terme :

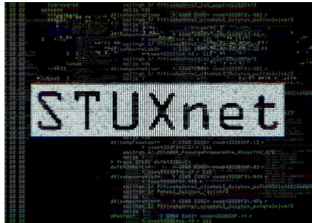
- ▶ D'énergie
- ▶ D'espaces de stockage

Rendant la gestion de leur sécurité plus complexe.

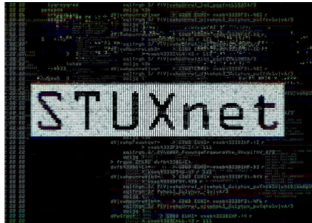
Constat et réalité



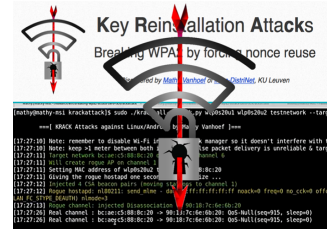
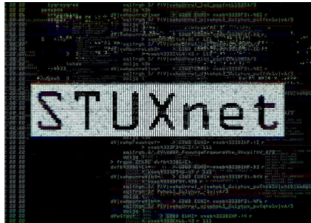
Constat et réalité



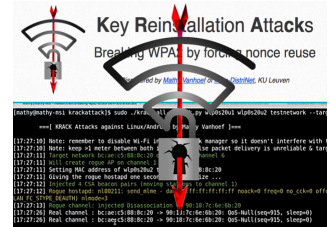
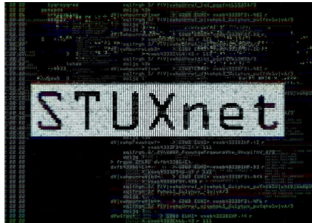
Constat et réalité



Constat et réalité



Constat et réalité



Une Priorité

Diminuer les risques de sécurité notamment ceux dû aux attaques **DDoS** révèle d'une priorité primordiale aussi bien pour les entreprises que pour les opérateurs.

Objectif

L'objectif principal

Réaliser une approche résiliente pour l'identification et la détection des attaques DDoS dans les réseaux IoT en vue d'empêcher les intrusions.

L'idée Consiste à intégrer l'IA plus précisément le DL afin d'avoir une précision de détection efficace.

Par ailleurs cette approche inclue l'utilisation séquentielle de l'auto-encodeur(AE) et des réseaux de neurones profonds(DNN).

1. INTRODUCTION

Contexte
Problématique
Objectif

2. APERÇU SUR L'ÉTAT DE L'ART

IoT
DDoS
IDS

3. CONTRIBUTIONS

Deep Learning
Approche proposée
Résultats
Comparaison

4. CONCLUSION GÉNÉRALE

Conclusion
Perspectives

IoT

Définitions

Définitions

- ▶ L'Internet des Objets est défini comme un ensemble d'objets inter connectés, disponibles et offrant des services en permanence à travers l'internet.

IoT

Définitions

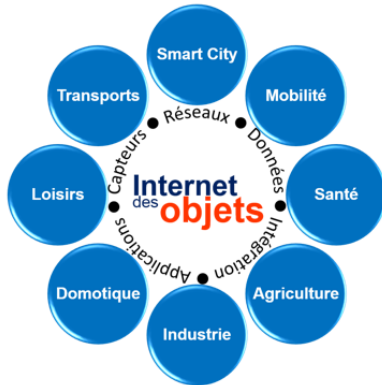
Définitions

- ▶ L'Internet des Objets est défini comme un ensemble d'objets inter connectés, disponibles et offrant des services en permanence à travers l'internet.
- ▶ Un Objet connecté est un appareil possédant la capacité d'échanger des données via internet avec d'autres entités physiques ou numériques.



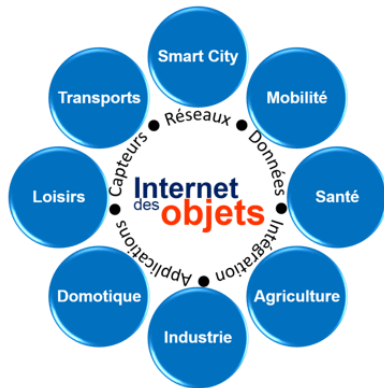
IoT

Domaines d'applications



IoT

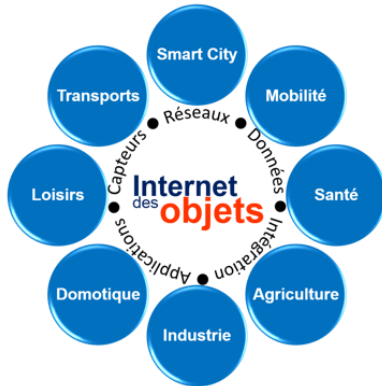
Domaines d'applications



Exemples

IoT

Domaines d'applications

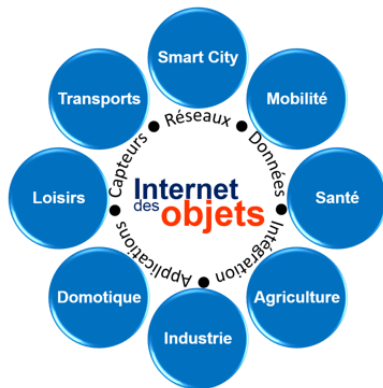


Exemples

- Villes intelligentes : Singapour, Oslo

IoT

Domaines d'applications

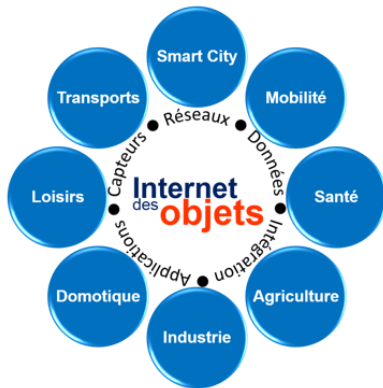


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée

IoT

Domaines d'applications

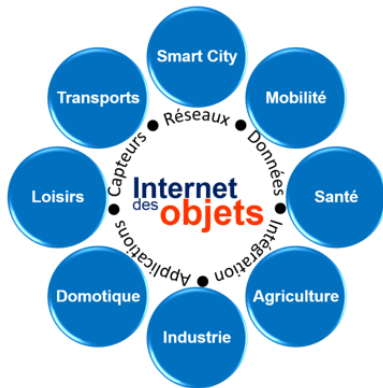


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,

IoT

Domaines d'applications

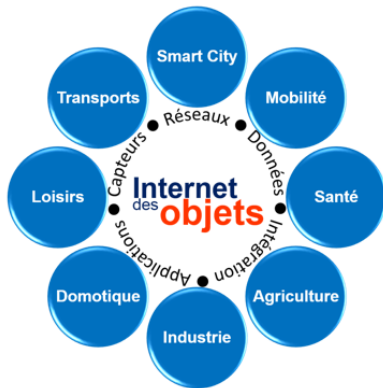


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,
- ▶ Agriculture : Drones agricoles,

IoT

Domaines d'applications

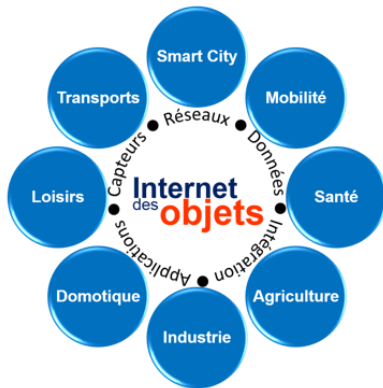


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,
- ▶ Agriculture : Drones agricoles,
- ▶ Industrie : Robot connecté

IoT

Domaines d'applications

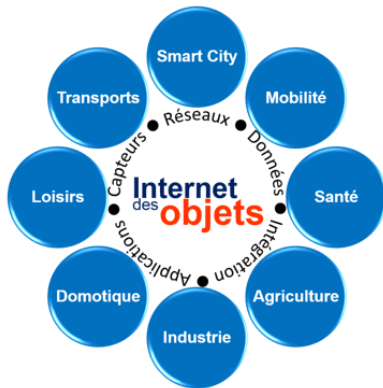


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,
- ▶ Agriculture : Drones agricoles,
- ▶ Industrie : Robot connecté
- ▶ Domotique : Réfrigérateur connecté

IoT

Domaines d'applications

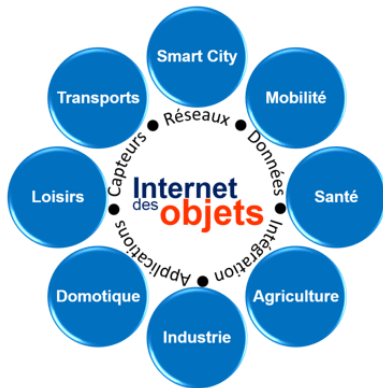


Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,
- ▶ Agriculture : Drones agricoles,
- ▶ Industrie : Robot connecté
- ▶ Domotique : Réfrigérateur connecté
- ▶ Loisirs : Télévision connectée

IoT

Domaines d'applications



Exemples

- ▶ Villes intelligentes : Singapour, Oslo
- ▶ Mobilité : voiture connectée
- ▶ Santé : Tensiomètre connecté,
- ▶ Agriculture : Drones agricoles,
- ▶ Industrie : Robot connecté
- ▶ Domotique : Réfrigérateur connecté
- ▶ Loisirs : Télévision connectée
- ▶ Transports : Gestion de la circulation

IoT

Avantages et Inconvénients de l'IoT

Avantages

- ▶ Amélioration de la productivité
- ▶ Amélioration de nos quotidiens
- ▶ Diminution des erreurs humaines
- ▶ Sécurisation des domiciles
- ▶ Surveillance de sa santé
- ▶ Aide aux personnes âgées

IoT

Avantages et Inconvénients de l'IoT

Avantages

- ▶ Amélioration de la productivité
- ▶ Amélioration de nos quotidiens
- ▶ Diminution des erreurs humaines
- ▶ Sécurisation des domiciles
- ▶ Surveillance de sa santé
- ▶ Aide aux personnes âgées

Inconvénients

- ▶ Gestion complexe de la **sécurité** des objets et des données
- ▶ Interopérabilité et hétérogénéité
- ▶ Génération d'une grande masse de données
- ▶ Faible protection de la vie privée

DDoS

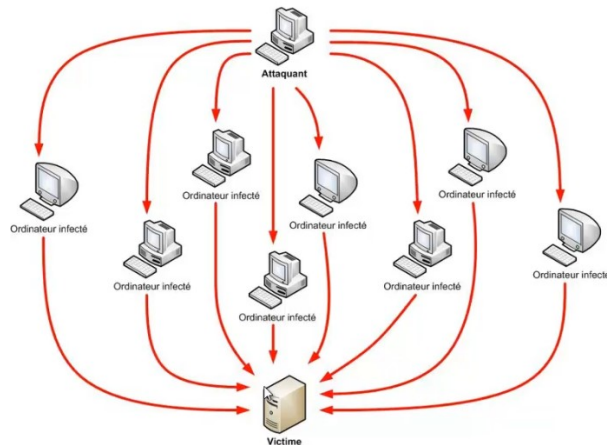
Définition

Le **DDoS** est l'attaque visant à rendre un service ou une ressource indisponible à ses utilisateurs légitimes. Elle est mise en œuvre à travers un botnet c'est à dire un réseau d'objets infectés

DDoS

Définition

Le **DDoS** est l'attaque visant à rendre un service ou une ressource indisponible à ses utilisateurs légitimes. Elle est mise en œuvre à travers un botnet c'est à dire un réseau d'objets infectés



DDoS

Chronologie des attaques DDoS



IDS

Solution pour se protéger contre les attaques DDoS

Une méthode efficace pour protéger les réseaux IoT contre les attaques DDoS est de détecter les attaques et de se défendre avant même qu'elles ne se produisent :

IDS

Solution pour se protéger contre les attaques DDoS

Une méthode efficace pour protéger les réseaux IoT contre les attaques DDoS est de détecter les attaques et de se défendre avant même qu'elles ne se produisent :
utilisation des Systèmes de Détection d'Intrusion(IDS)

IDS

Définition et les différents types d'IDS

Définition

Un IDS est un composant logiciel ou matériel spécialisé, dont le rôle est de surveiller l'activité d'un réseau ou d'un hôte en vue de détecter toute effraction dans l'utilisation des ressources.

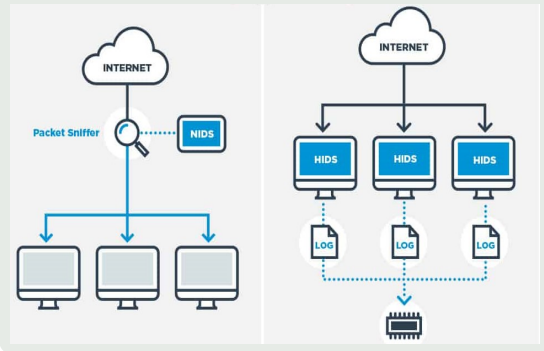
IDS

Définition et les différents types d'IDS

Définition

Un IDS est un composant logiciel ou matériel spécialisé, dont le rôle est de surveiller l'activité d'un réseau ou d'un hôte en vue de détecter toute effraction dans l'utilisation des ressources.

Les Différents types d'IDS



1. INTRODUCTION

Contexte
Problématique
Objectif

2. APERÇU SUR L'ÉTAT DE L'ART

IoT
DDoS
IDS

3. CONTRIBUTIONS

Deep Learning
Approche proposée
Résultats
Comparaison

4. CONCLUSION GÉNÉRALE

Conclusion
Perspectives

Deep Learning

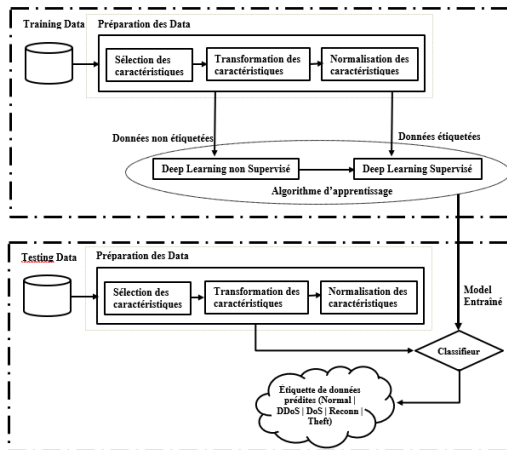
Deep Learning

L'application des techniques d'apprentissage profond pour la détection d'intrusion donne des Résultats très efficaces par rapport aux IDS classiques.

- ▶ Taux de détection élevés,
- ▶ Moins de faux positifs

Approche proposée

Architecture du modèle



Approche proposée

Choix du Dataset

Datasets

- 1 Bot IoT
- 2 NSL-KDD

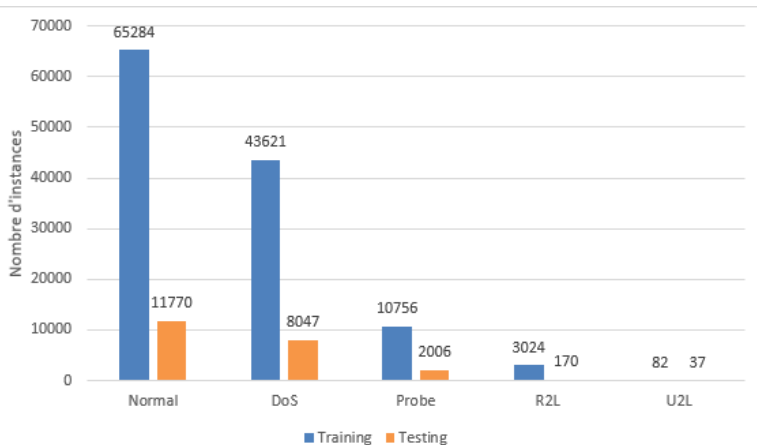


Approche proposée

Choix du Dataset

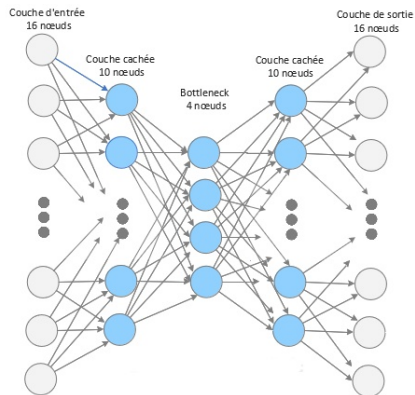
Datasets

- 1 Bot IoT
- 2 NSL-KDD



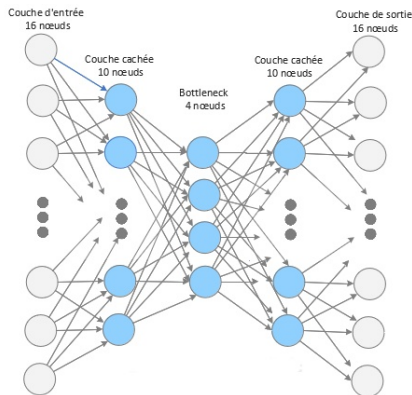
Approche proposée

Définition du modèle Auto Encodeur(AE)



Approche proposée

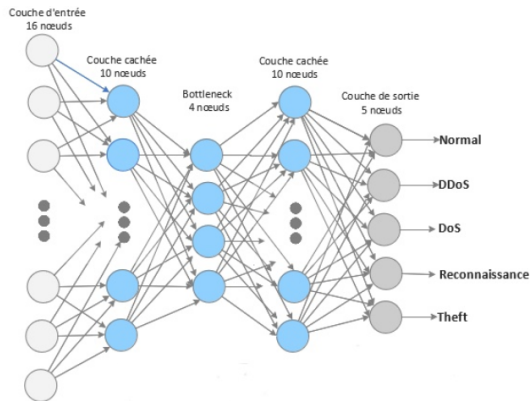
Définition du modèle Auto Encodeur(AE)



```
public void createModelAE(int numInputs){
    // Setup network configuration
    // 16 -> 10 -> 4 -> 10 -> 16 (nodes)
    MultiLayerConfiguration configurationAE =
        new NeuralNetConfiguration.Builder()
            .seed(1234)
            .weightInit(WeightInit.XAVIER)
            .optimizationAlgo(OptimizationAlgorithm
                .STOCHASTIC_GRADIENT_DESCENT)
            .updater(new Adam(0.001))
            .l2(0.00005)
            .activation(Activation.TANH)
            .list()
            .layer(0, new DenseLayer.Builder()
                .nIn(numInputs)
                .nOut(10)
                .build())
            .layer(1, new DenseLayer.Builder()
                .nIn(10)
                .nOut(4)
                .build())
            .layer(2, new DenseLayer.Builder()
                .nIn(4)
                .nOut(10)
                .build())
            .layer(3, new OutputLayer.Builder()
                .nIn(10)
                .nOut(numInputs)
                .lossFunction(LossFunctions.LossFunction
                    .MEAN_SQUARED_LOGARITHMIC_ERROR)
                .build())
            .build();
    this.modelAE = new MultiLayerNetwork(configurationAE);
    modelAE.init();
}
```

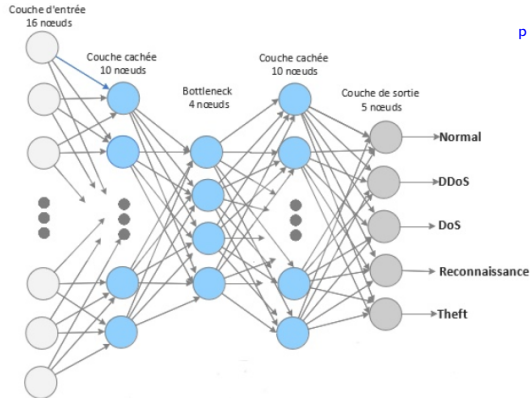
Approche proposée

Définition du modèle du réseau de neurone profond(DNN)



Approche proposée

Définition du modèle du réseau de neurone profond(DNN)

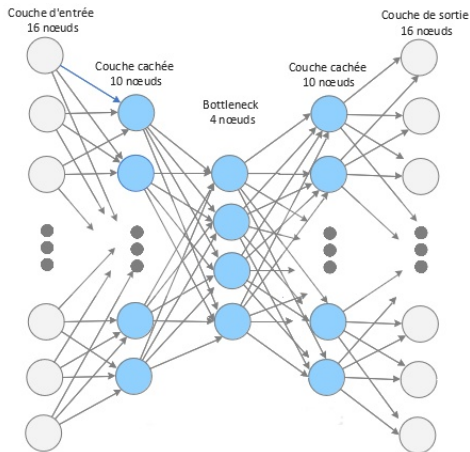


```
public void createModelFFNN(MultiLayerNetwork modelAE){
    FineTuneConfiguration fineTuneConf =
        new FineTuneConfiguration.Builder()
            .updater(new Adam(0.01))
            .build();

    this.modelFFNN = new TransferLearning.Builder(modelAE)
        .fineTuneConfiguration(fineTuneConf)
        .removeOutputLayer()
        .addLayer(new OutputLayer.Builder()
            .nIn(10)
            .nOut(this.numClasses)
            .activation(Activation.SOFTMAX)
            .lossFunction(new LossMCXENT())
            .build())
        .build();
    modelFFNN.init();
}
```

Approche proposée

Fonction d'activation du modèle Auto Encodeur(AE)



Fonctions d'activation

1

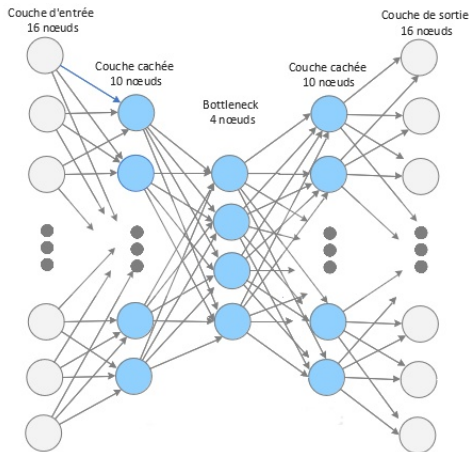
$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

2

$$\text{Softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^k e^{x_j}}$$

Approche proposée

Fonction d'activation du modèle Auto Encodeur(AE)



Fonctions d'activation

1

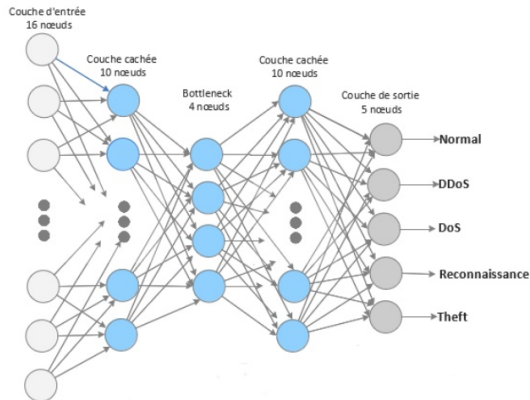
$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

2

$$\text{Softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^k e^{x_j}}$$

Approche proposée

Fonction d'activation du modèle du réseau de neurone profond (DNN)



Fonctions d'activations

1

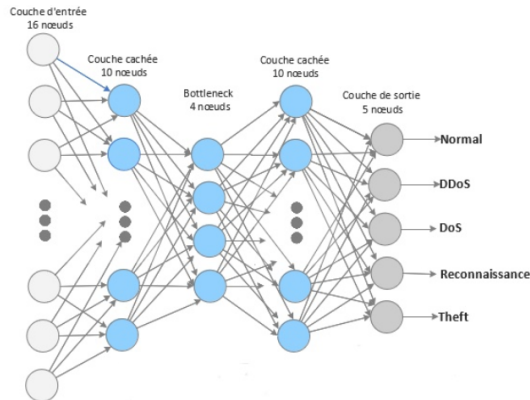
$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

2

$$\text{Softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^k e^{x_j}}$$

Approche proposée

Fonction d'activation du modèle du réseau de neurone profond (DNN)



Fonctions d'activations

1

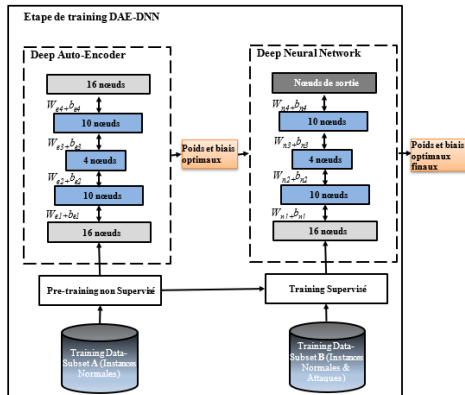
$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

2

$$\text{Softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^k e^{x_j}}$$

Approche proposée

Entraînement du modèle



Somme pondérée

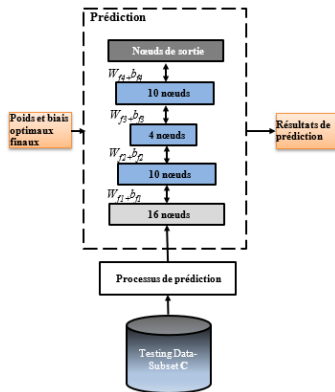
$$z = \sum_{i=1}^n (X_i \times W_i) + bias$$

$$y = \varphi(z)$$

FIGURE – Entraînement du modèle

Approche proposée

Phase de test du modèle



Somme pondérée

$$z = \sum_{i=1}^n (X_i \times W_i) + bias$$

$$y = \varphi(z)$$

Approche proposée

Entraînement et test du modèle

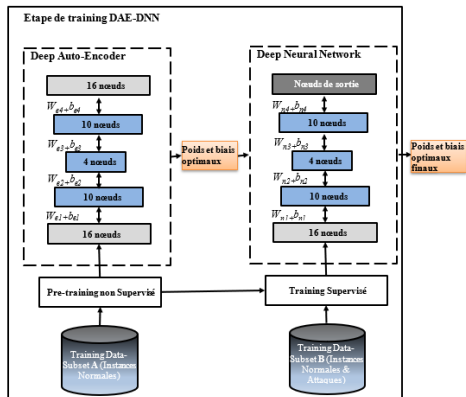


FIGURE – Entraînement du modèle

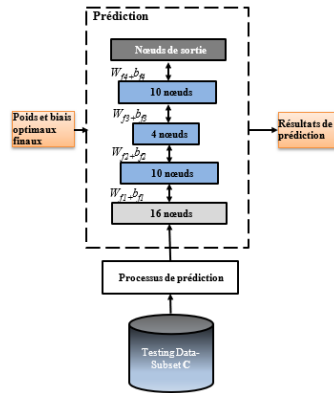


FIGURE – Phase de test du modèle

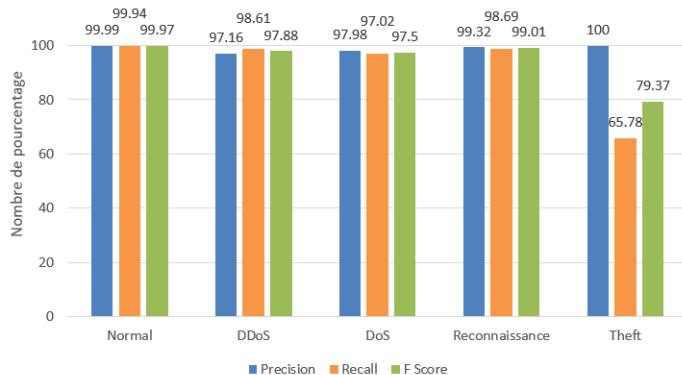
Résultats

Matrice de confusion

		Classe prédite					
		Classifié →	Normal	DDoS	DoS	Reconn	Theft
Classe réelle	Normal		29238	1	4	11	0
	DDOS		0	26684	357	19	0
	DOS		0	718	26033	79	0
	Reconn		2	59	175	17909	0
	Theft		0	0	0	13	25

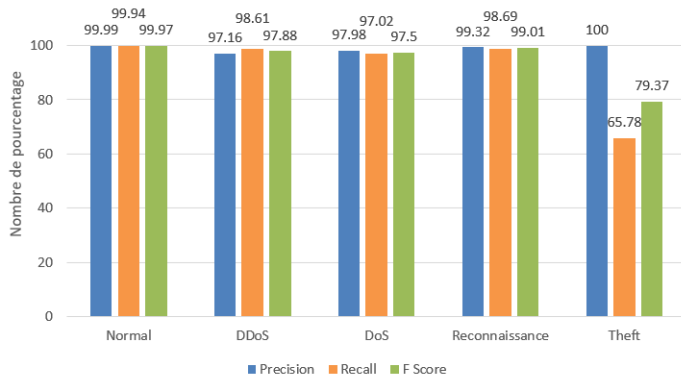
Résultats

Métriques d'évaluation



Résultats

Métriques d'évaluation



moyennes des résultats obtenues

Accuracy = 98.58%

Precision = 98.89%

Recall = 92.01%

F Score = 94.74%

FPR = 0.38%

Comparaison

Comparaison avec d'autres Travaux

Méthodes & Auteurs	L'année	Dataset	Accuracy(taux de réussite)
CNN par B.Susilo et R.Sari	2020	Bot IoT	91.27%
FNN par O.Ibitoye et O.Safig	2019	Bot IoT	95.1%
CNN par Y.Zheng, Y.Xin et Y.Zhao	2020	NSLKDD	86.95%
MLP par MOKHTARI Sidi	2018	NSL-KDD	93.57%
Notre Approche	2020	Bot IoT	98.58%
		NSL-KDD	99.12%

1. INTRODUCTION

Contexte
Problématique
Objectif

2. APERÇU SUR L'ÉTAT DE L'ART

IoT
DDoS
IDS

3. CONTRIBUTIONS

Deep Learning
Approche proposée
Résultats
Comparaison

4. CONCLUSION GÉNÉRALE

Conclusion
Perspectives

Conclusion

conclusion

Notre approche a été testée et validée sur les datasets IoT Botnet et NSL-KDD pour l'apprentissage et le test. Les résultats obtenus sont très satisfaisants et prouvent l'efficacité de notre approche avec un taux de réussite (Accuracy) de **98.58%** et un taux de faux positifs de **0.38%**

Perspectives

- ▶ IDS mode online
- ▶ Gestion multi tâches des alertes dans l'IDS
- ▶ Générer et Tester avec son propre dataset

Merci pour votre attention !