Compte-Rendu Cassiopée

Semaine du 29/01/2018

Tuteur : Gregory Blanc
Membres du projet : Charles Mure, Félix Molina

Projet : **Détection d'intrusion par approche statistique sur un réseau SDN**

1 – Analyse et extraction de données d'articles scientifiques concernant la détection d'intrusion

Analyse des articles :
(A1) A Deep Learning Approch for NIDS
(A2) Deep learning approach for Network Intrusion Detection in Software Defined Networking

Le but est d'obtenir un NIDS à apprentissage supervisé (A2) ou non supervisé (A1), flexible et efficace (taux de détection élevé et faible taux de faux positif).

Attaques testées : DOS, Probe, U2R, R2L.

DataSet utilisés : NSL-KDD dataset – KDD Cup' 99. Les datasets sont non labelisés dans le cas de A1.

Nombres de parametres (features) :
Pour A1 : 121 avant classification ;
Pour A2 : 6 spécifiques (duration, protocole_type, src_bytes, dst_bytes, count, srv_count)

Différents types d'apprentissage : ANN (le plus repondu), SVM, NB, RF (Random Forest), SOM, OPF, CAPSNET.

Aglos de détection : STL (Self-Taught Learning utilisant le SMR) et SMR (Soft Max Regression).

Algos de classification : J48 Decision Tree Classifier, DMNB, SMR.

Etapes d'apprentissage :
Pour A1 :
1 – Unsupervised Feature Learning (UFL) réalisé avec l'algo de Sparse Auto-Encoder
2 – Classification (SMR)

Pour A2 :

Implémentation :
Pour A1 (dans le cas d'apprentissage STL):
1 – Discretisation des valeurs nominales des attributs (1-to-n encoding)
2 – Elimination de l'attribut ayant pour valeur 0
3 – Normalisation des valeurs entre 0 et 1 (max-min normalization)
4 – Sparse Auto-Encoder
5 – Soft Max Regression

Pour A2 :

Resultats :

Pour A1 : taux de détection → 98,84 % (avec STL) et 96,79 % (avec SMR)
Pour A2 : environ 70 % de taud de détection

2 – Pour la semaine du 05/02/2018

→ Récupération des datasets provenant du CIC (Canadian Institute for Cybersecurity)
→ Contacter a.habibi.l@unb.ca pour récupérer des Datasets réels

→ Développement de tests pour différents modèles de réseau de neurones (python Keras module)
→ Choix du modèle du système de réseau de neurones

→ Recherhcer les features accessibles sur OpenFlow

Semaine du 05/02/2018

Tuteur : Gregory Blanc
Membres du projet : Charles Mure, Félix Molina

Projet : **Détection d'intrusion par approche statistique sur un réseau SDN**

1 – Sélection des premiers attributs à utiliser

→ IP source, IP destination
→ Port source, port destination
→ Protocole (type protocole)
→ Date, heure
→ Durée du flux
→ Nombre total de paquets forwardés
→ Nombre total de paquets backwardés
→ Taille moyenne des en-têtes forwardées
→ Taille moyenne des en-têtes backwardées
→ Débit