SDN 網路下基於 AutoEncoder 的 DDoS 偵測方法

AutoEncoder Based DDoS Attack detection in SDN network

指導教授：蔡孟勳
專題成員：李廷偉
開發工具：Keras
測試環境：Google CoLab

一. 簡介

分散式阻斷服務（DDoS）攻擊是一種惡意嘗試，它利用大量的網路流量使目標主機或其周圍的基礎設施不堪重負，從而阻斷目標伺服器、服務或網路的正常流量。DDoS 一直是資安的一大隱憂，因為任何人都可以輕易使用 open source 的工具達到。

SDN (Software Defined Network) 將傳統網路的 Control Plane 和 Data Plane 分離,由控制器統一控制交換器。這樣的架構，讓控制器可以取得網路中每一個交換器的資訊，達到更全面的防護。

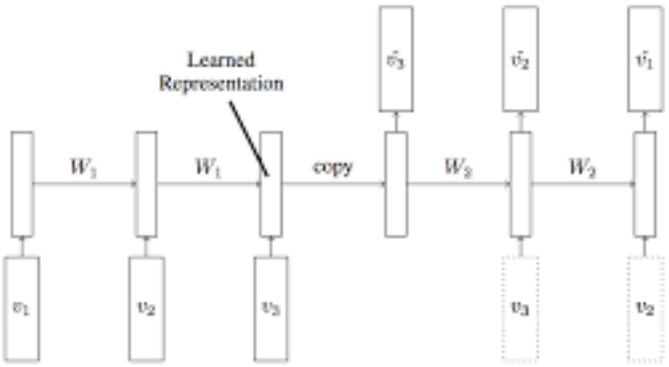
而近年常見用於偵測 DDoS 的方法之一，就是使用 Control Plane 蒐集每一個交換器的封包相關資訊，再經由訓練好的監督式機器學習模型辨別是否為惡意封包，這類方法的原理是將惡意封包的偵測當作一個二元分類的問題處理。

在這些方法中，訓練模型的資料集中，惡意封包的數目通常和正常封包的數目相差不多。但這正常網路的封包蒐集中，很有可能正常封包的數量遠超過惡意封包的數量，造成『imbalance dataset』，而『imbalance dataset 』通常會讓在『 balance dataset 』下表現良好的模型表現下滑 (https://arxiv.org/pdf/2107.01777.pdf)。所以這個專題試著在『imbalance dataset 』下訓練出一個相對精準的模型。

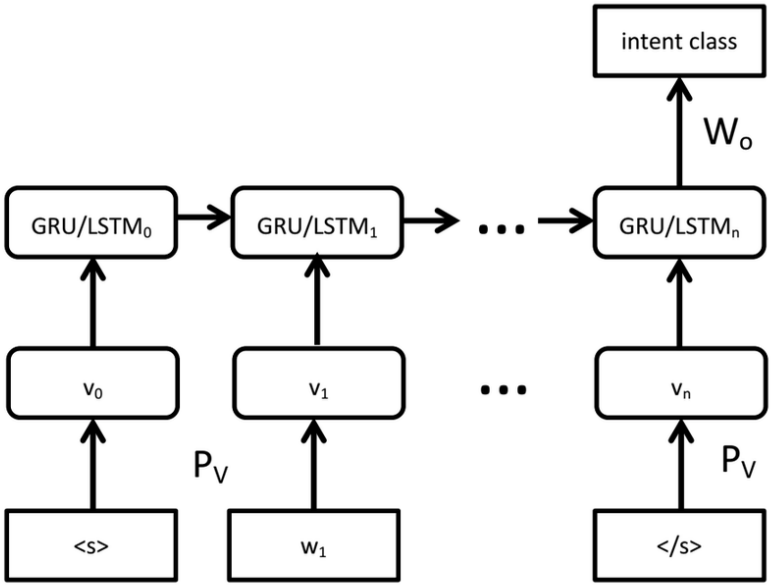
二. 方法

訓練的資料集使用 UNSW-NB15 Dataset ，這個是由澳大利亞國防大學 (UNSW Canberra at the Australian Defence Force Academy) 經由 IXIA PerfectStorm 這個工具去模擬真實世界的網路流量。其中有多種的惡意封包，我們只選擇 DoS 的惡意封包與所有的正常封包。

訓練的模型分成兩個部分，第一個部分先經由一個 GRU 的 AutoEncoder 和正常的封包資料進行訓練，這個階段 GRU-AutoEncoder 會找到正常封包的 Hidden Information。不加入惡意封包的原因想要讓惡意封包經過 GRU-AutoEncoder 後，會產生數據分佈與正常封包相差很大的 Hidden Information，接下來的模型可以分辨。



接下來經過訓練模型的第二層，取出第一部分的 Encoder 並連上，一個 SoftMax 的 Classifier 進行訓練。使用全部的資料，讓模型可以分辨正常與惡意的封包。



三. 結果

最終訓練出來得模型，經由混淆矩陣算出模型的分數，其中 positive 為有惡意封包。可以看到經由長度 15 的 window分割後，有 3454 個 window 含有惡意封包，而 141012 個 window 沒有，惡意封包只占去整體 window 的 2.3 % 。

```
TP: 3182, TN: 140740, FP: 272, Fn:259
[[140740    272]
 [   259   3182]]
Auccracy: 0.99632406388237
Precision: 0.9212507237984945
Recall: 0.9247311827956989
F1: 0.9573178275873826
```