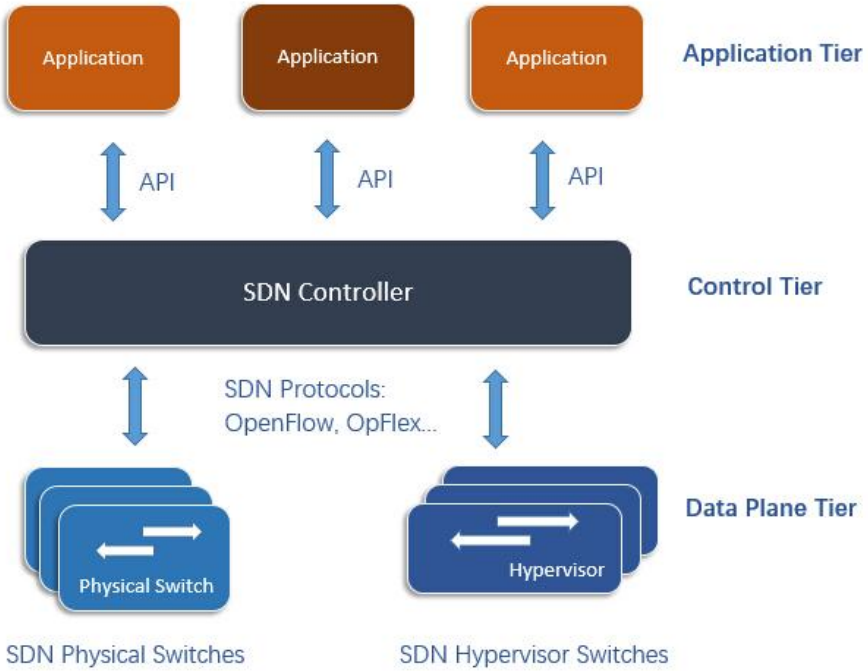
AutoEncoder Based DDoS Attack detection in SDN network

資訊 112 李廷偉
指導教授 蔡孟勳教授

大綱

1. 簡介
2. 使用的模型
3. 測試成果

簡介 - SDN 網路



sdn 網路是一個新型態的網路拓撲可以將 data plane 和 control plane 分離。經由 controller 統一集中管理 control plane，讓開發者可以在 control plane 上開發更有彈性的 application。

簡介 - DDoS

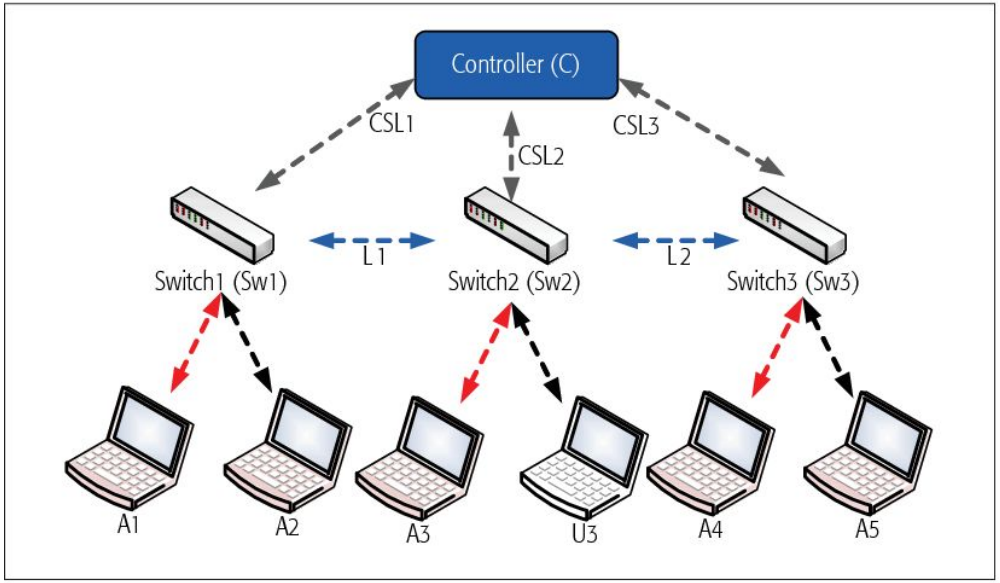


Figure 1. A sample SDN topology with DDoS attackers

DDoS 全名為 Distributed Denial of Service,是一種網路攻擊手法,其目的在於使目標電腦的網路或系統資源耗盡,使服務暫時中斷或停止,導致其正常使用者無法存取。

簡介 - 機器學習應用於 SDN DDoS 防禦的常見方法

近年來，機器學習常見用於 SDN 中防範 DDoS 的方法，常見的方法有 SVM , MLP, Decision tree 等等的方法, 這些方法大多將偵測DDoS 的行為視為一個『binary classification』即一個監督式的二元分類的問題進行訓練。

簡介 - 方法與現實資料取得的差異

在監督式的二元學習下，通常要兩個分類的資料數量一樣，才會有良好的結果，但在現實情況下，異常的資料相比正常資料通常很少。而常見的方法如 SVM 或是 MLP 的方法如果在正反資料集數量差距很大的情況，這些模型的表現通常不會很好。

1 INTRODUCTION

Many binary classification problems exhibit class imbalance, in which one of the two classes vastly outnumbers the other. Classifiers that perform well with balanced classes routinely fail for imbalanced classes, and developing reliable techniques for classification in the presence of severe class imbalance remains a challenging area of research (He and Ma, 2013; Krawczyk, 2016; Fernández et al., 2018). Many practical approaches

reference : https://arxiv.org/pdf/2107.01777.pdf

簡介 - Dataset 與 Data Processing

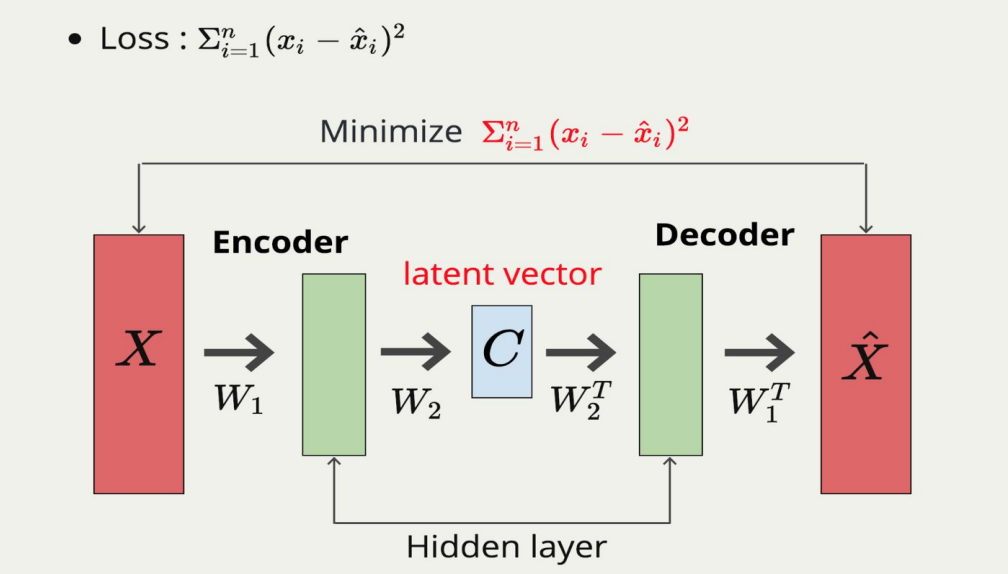
UNSW-NB15 是由位於澳洲的新南威爾斯大學使用工具模擬出來接近真實的資料集，已經被學界許多論文引用。

資料集之中含有 2百多萬筆 flow 的資料，並經由時間的 sorting 後，依照長度為 15 的 window size 進行切分，最後得到下面的資料，可以看到 Normal window 的數量明顯大於 Anomal window 的數量。(normal 有 14多萬筆，anomal只有 3441 筆)。

```
Data Shape: (144453, 15, 34)
Label Shape: (144453, 2)
Anomal Shape: (3441, 15, 34),
Normal Shape: (141012, 15, 34)
```

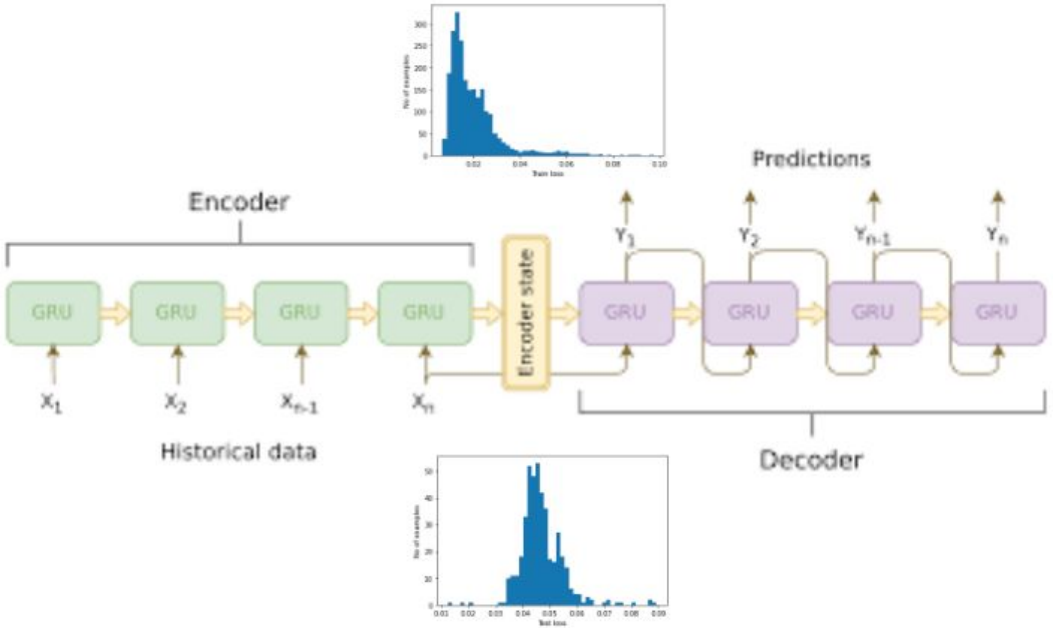
模型設計 - GRU AutoEncoder

AutoEncoder 是一種無監督式學習的方法，可以使用兩個 networks 將輸入的 vector embedding 成一個 Latent vector, 再經由 Latent vector 轉換回來原來的 vector。



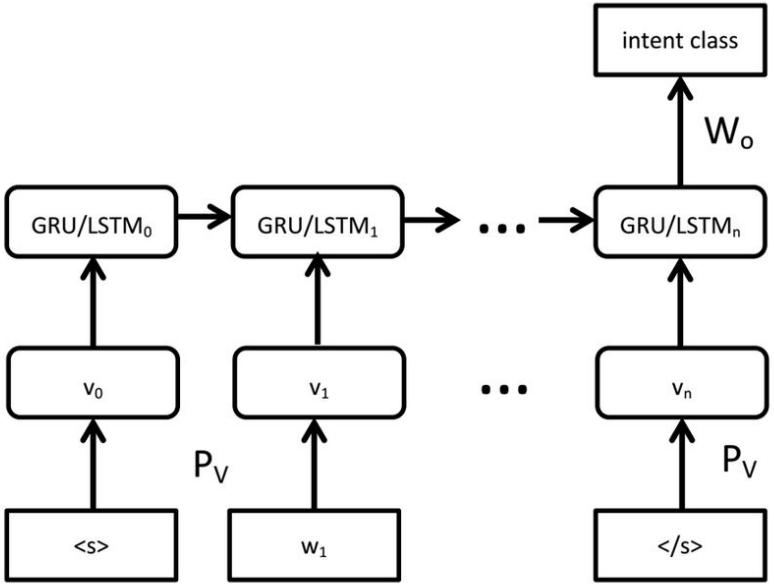
模型設計 - GRU AutoEncoder

這裡的模型使用 AutoEncoder 作為 dimension reduction 的工作。



模型設計 - Softmax Classifier

經由 Encoder 和 Decoder 的訓練後，將 Encoder 取出，並連上一個 Softmax 的二元分類 Layer。再使用 Normal 和 Anomal Data 進行 Training。



訓練成果

```
TP: 3182, TN: 140740, FP: 272, Fn:259
[[140740    272]
 [   259   3182]]
Auccracy: 0.996324063882237
Precision: 0.9212507237984945
Recall: 0.9247311827956989
F1: 0.9573178275873826
```