於 P4 和 ONOS 實現機器學習的 DDoS 的攻擊偵測

Implementing Machine Learning-based DDoS Attack Detection on P4 and ONOS

指導教授:張燕光

專題成員:江宇浩、林欣誠

開發工具:Python、P4、ONOS、Mininet、Wireshark

測試環境:Ubuntu 18.04

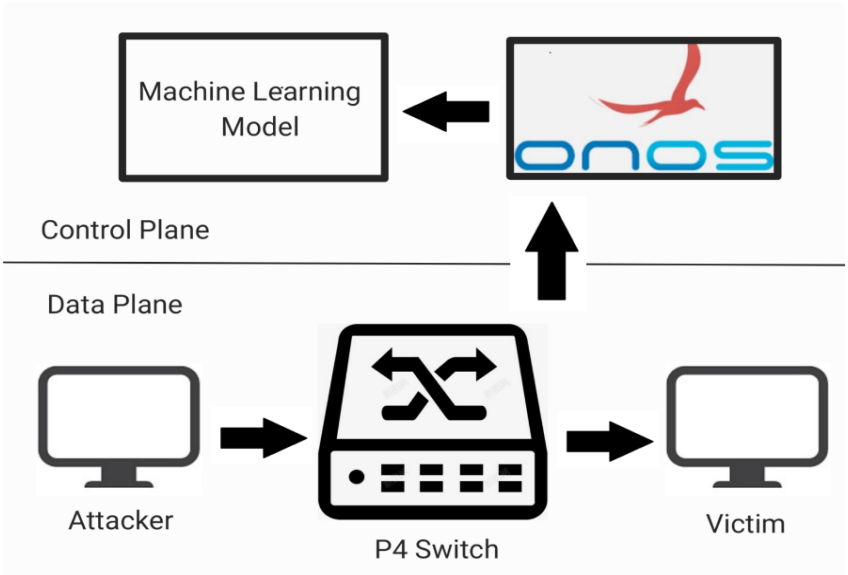
一、簡介:

P4(可程式化協議獨立封包處理器)是一種開源的、專用於網路設備的程式語言，它可以用來設定Data plane設備(交換機、路由器、網路介面卡、過濾器等) 該如何處理封包。

ONOS 提供了 Control plane，負責網路設備的配置、管理和控制。它能夠與各種網路設備和控制器進行通訊，並提供統一的管理介面。

為了解決近年來越來越多的 DDoS 攻擊，我們基於 P4 與 ONOS 來偵測 DDoS 封包，透過 Data plane 擷取封包資訊，並傳送到 Control plane，最後透過 Machine Learning Model 來判斷是否為 DDoS 封包

架構圖:



二、測試結果:

環境都設置好之後，我們在 Attacker 主機上用 Tcpreplay 工具，將入侵檢測評估數據集(CIC-IDS2017)實現網路流量回放。在 Machine Learning Model 我們選用 KNN (K Nearest Neighbor)、RF (Random Forest)來做實驗，並且調整不同大小的 time-window，得到實驗結果。

在同個 Model 下，根據 time-window 設置的不同都會影響到其表現，因此對所有實驗進行觀察後，針對不同 Model 設置其合適的 time-window 是很重要的。對 KNN 來說 time-window 為5秒時，在正確判斷的表現是最好的，而 RF 則是 time-window 為20秒時表現最好。

傳統上機器學習檢測系統全部都在 Control plane執行而導致過載，我們利用Data plane可編程的優點，取出封包資訊，並定期回報給Control plane，減輕Control plane的負擔。