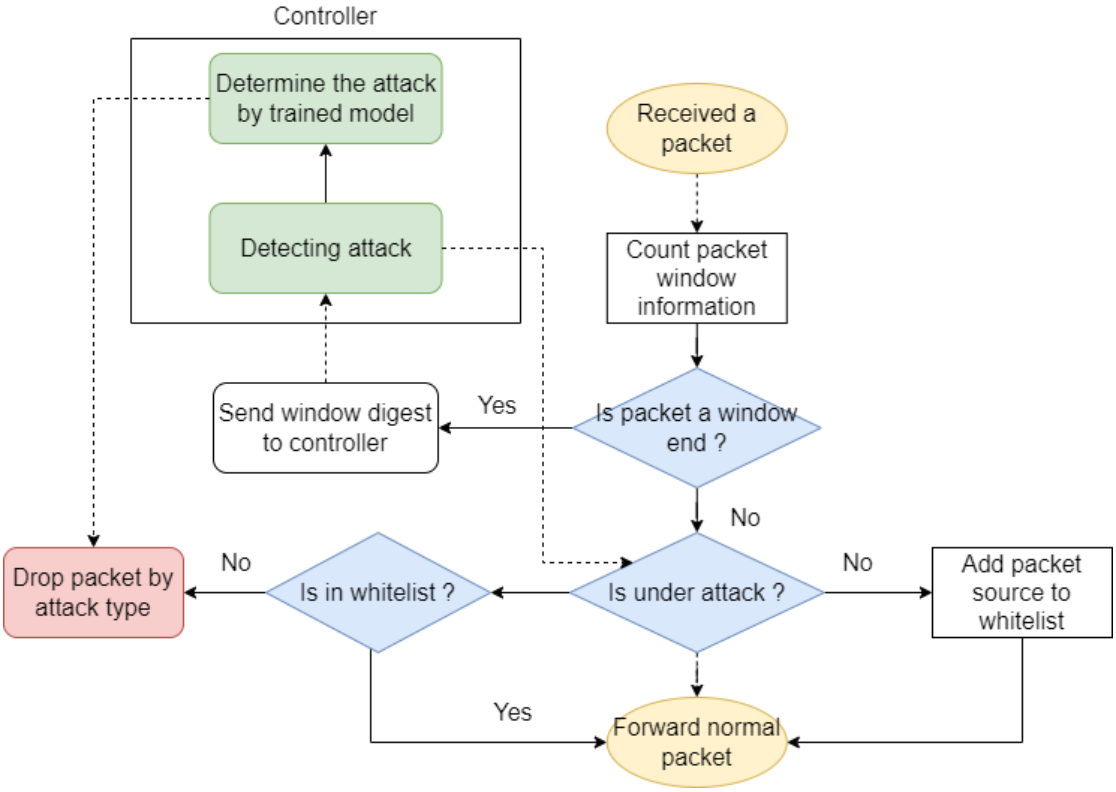
基於 P4交換機實現機器學習的 DDoS 偵測及攻擊緩解

指導教授：張燕光
專題成員：林禹圻、江少謙
開發工具：Python , BMv2 , Mininet
測試環境：Ubuntu-20.04

一、簡介：

為了應對日漸嚴重且多變的 DDoS 攻擊，基於 P4 在 Data plane 的靈活性及 Machine Learning 的準確性，我們設想若在 Switch 就提前進行防禦，可以有效減少被攻擊的影響。因此設計了一套用於 DDoS 防禦的框架，包含偵測與減緩兩個區塊，使用 P4 Switch 負責特徵擷取與減緩機制，及 Controller 負責利用機器學習模型進行攻擊偵測。
以下為系統架構與流程圖：



二、測試結果：

透過實驗結果我們可以發現在 TPR 時，表現通常都非常良好接近99%，這是因為我們的模型能夠去判斷不同種類的攻擊，所以在判斷丟包時能設定非常嚴格的條件，能準確丟棄有該攻擊特徵的封包。

而在 FPR 時能發現在 ICMP flood 以及 TCP flag flood 時幾乎沒有正常封包被丟棄，這是因為在我們嚴格的丟包條件，原本正常的流量會繼續通過，新連線幾乎不會有 ICMP 或 Fault flag 所以不會被丟棄。在 SYN flood 以及 UDP flood 時，表現較差，則是因為新的正常連線通常都是 TCP SYN 或是 UDP ，在我們的丟包判斷下，有極高的機率被丟棄。

我們成功實現利用機器學習的方式偵測 DDoS，與傳統的統計方法不同，機器學習更容易發現人類無法發現的特徵隱藏價值。P4 方面我們活用了其對於 data plane 的可編成性，直接利用交換機收集特徵，相比於傳統 SDN 交換機需要透過來回與 controller 溝通，節省許多時間成本。