# 於 P4 實現基於 Euclid 的 DDoS 防禦策略

# DDoS mitigation strategy based on Euclid and implemented with P4

指導教授：張燕光
專題成員：余紹桓、陳明閎
開發工具：P4、Scapy、Wireshark
測試環境：Debian GNU/Linux 11

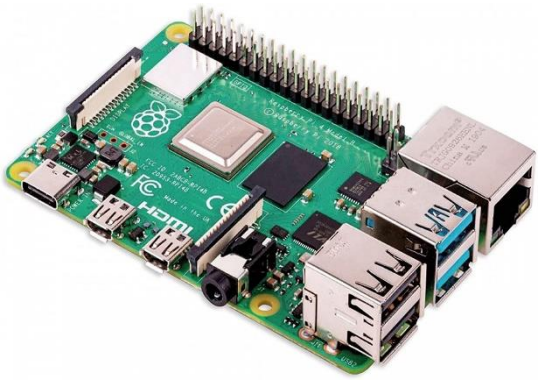
## 一、簡介：

DDoS(Distributed Denial of Service)攻擊，又稱分散式阻斷服務攻擊，利用傳送大量偽造的封包到目標電腦的網路，使其系統資源耗盡，造成服務中斷，來達到攻擊的目的。

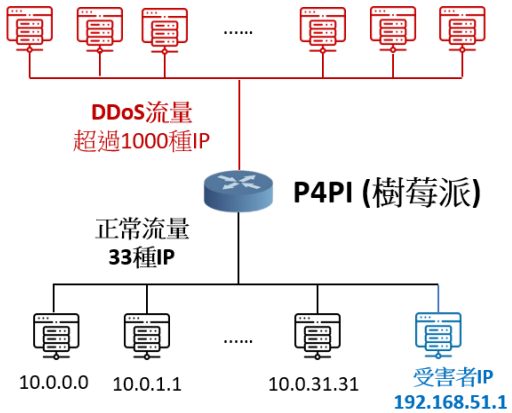
而近年來興起的 SDN(Software Defined Network)，也就是軟體定義網路，將交換器的 Control Plane 與 Data Plane 分離，解決了傳統交換機無法隨時更新與集中控管的困境，降低了時間與金錢成本，適合用來研究 DDoS 解決方法。

P4 正是一種能夠實現 SDN 的程式語言，不過他還多了 PDP (Programmable Data Plane)，他的特點還有 Protocol Independent （可相容任何通訊協議）、Target Independent （支援任何平台）、Field Reconfigurable （隨時都能修改）。

這次特別的地方是，我們實現防禦策略的裝置是在 **P4PI** 上，P4PI 就是將 P4 實現在 **Raspberry Pi**（俗稱的**樹莓派**）：



（圖一）樹莓派(Raspberry Pi)




（圖二）P4PI網路拓樸示意圖

我們選擇在 P4PI 上實現的 DDoS 防禦策略是參考【Euclid: A Fully In-Network, P4-Based Approach for Real-Time DDoS Attack Detection and Mitigation】的論文，該策略是使用 IP Entropy 方法來偵測 DDoS 的，內容會在簡報中出現。

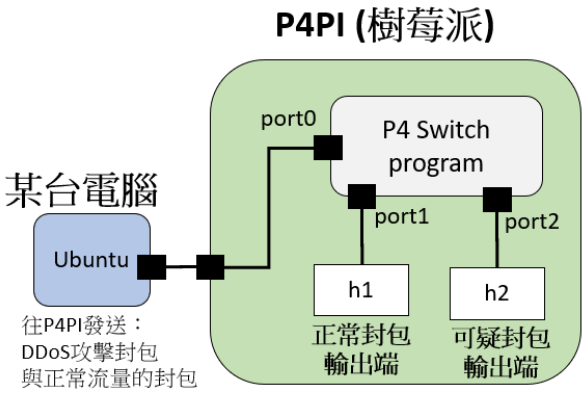
## 二、方法：

在 P4PI 上使用 P4 部屬好交換機策略後，我們會從另一台電腦利用 **Tcpreplay** 套件，將 DDoS 攻擊封包數據集 (CAIDA DDoS 2007 Attack Dataset) 與正常流量數據集同時發送給 P4PI，並將封包轉送狀況記錄成 Pcap 檔，再從本地端用 wireshark 觀察結果。

首先會從連接 P4PI 的電腦，透過預先製作的 pcap 檔，來發送正常流量以及 DDoS 攻擊流量，最後 P4PI 裡的 P4 switch 會將處理後的封包丟往 port1 與 port2 出口，我們就可以從這兩個 port 去分析 TPR 和 FPR。

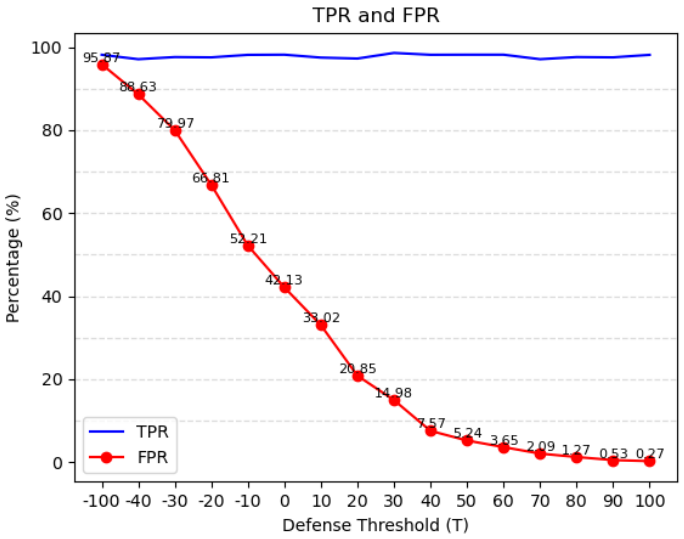
(TPR：**攻擊流量**成功阻擋的百分比)

(FPR：**正常流量**錯誤阻擋的百分比)

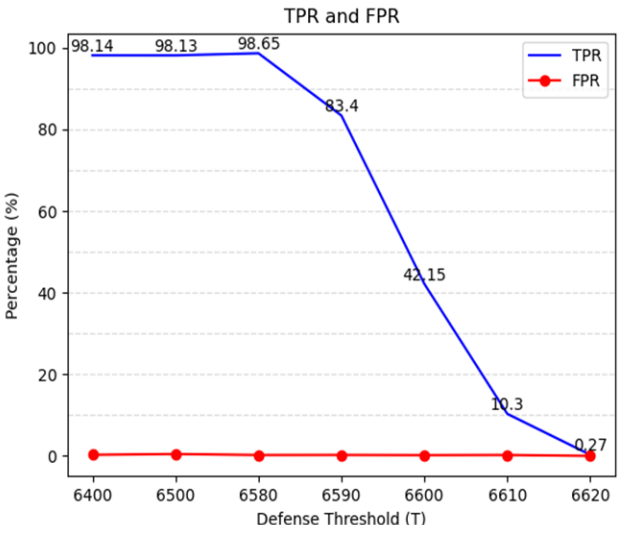



（圖三）實際環境示意圖

## 三、測試結果：




（圖四）不同閥值T的影響




（圖五）T值過高時的情況

在這次的 DDoS 防禦策略中，會有**閥值 T** 與 **Window Size** 可自行調整，閥值 T 會影響到 **TPR(True Positive Rate)**和 **FPR(False Positive Rate)**的表現，調太低會導致正常流量被誤判成攻擊而被阻擋，導致 FPR 上升，若閥值 T 調太高也會導致 TPR 下降，因此必須將 T 設成適當的值，才能有效阻擋攻擊。

(TPR：**攻擊流量**成功阻擋的百分比)

(FPR：**正常流量**被阻擋的百分比)

Euclid 策略使用較大量的計算，使得 switch 效能可能成為瓶頸，但其 TPR 與 FPR 表現良好，當未來 switch 效能日漸提升，這種策略就有更高的價值。