於 P4 實現基於 CountMin 和 Hyperloglog 的 DDoS 攻擊偵測

DDoS Detection by using Hyperloglog and Count-Min Sketch on P4 Switch

指導教授：洪昌鈺; 專題成員：吳驊明、陳柏佑

開發工具：Python、P4、Mininet; 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，它可以用來自定 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。

為了方便偵測 DDoS 攻擊，我們在 P4 Switch 上蒐集封包的資訊，用佔空間極少的 Sketch 儲存它們。在達到設定的警示時，通知 Controller[1][2]來判斷是否為 DDoS 攻擊。(見圖 1)

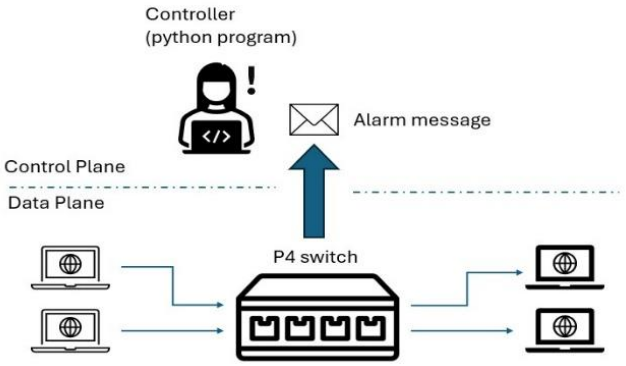

圖 1 專題的整體架構

實務方面，參考論文[3]在 P4 Switch 上透過 CountMin Sketch 來統計「每一個 destination 分別收到了幾個封包」，另一方面，假如某一個特定的 destination 收到過多封包時，再啟動 Hyperloglog 來估計「這個 destination 收到的封包大約來自幾個不同的 source」。(見圖 2)

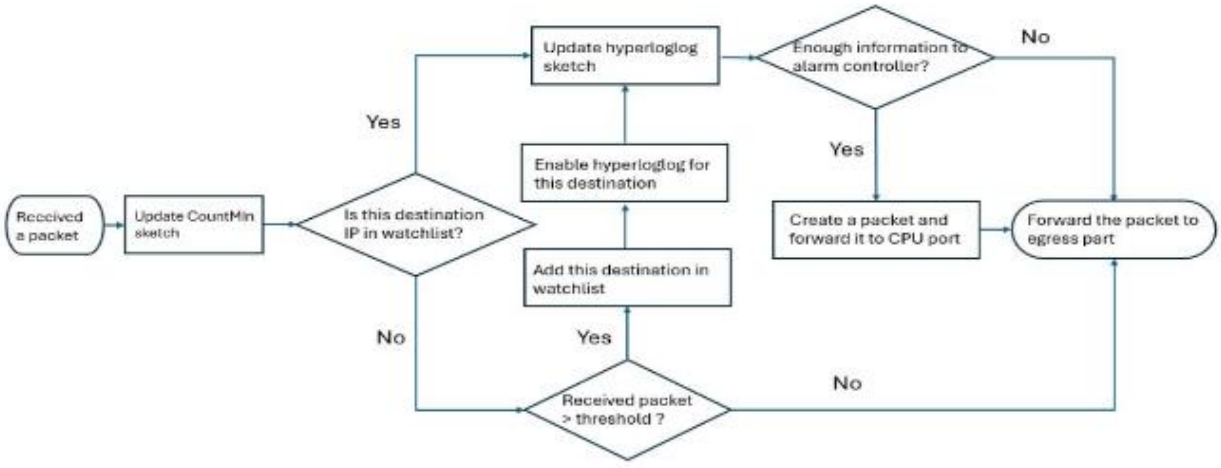

圖 2 P4 Switch 上的大致流程圖

CountMin 類似於多個 Hash Table，但是它的 Hash Function 不只一個。可以想像，一個 key 會因為多個 Hash Function 得到不同的 index，在每個 hash table 的不同 index 處加一，方便我們多重確認。與傳統的 Hash Table 相比，大幅避免了發生 Collision 可能造成的誤判。(見圖 3)

Hyperloglog Sketch 是統計「在集合中有多少相異的元素」的方法，將 Hash 的結果(bits)依照 bucket 數量來擷取後 n 位，代表它屬於哪個 bucket，並記錄最先出現 1 的位置(應用 Bernoulli trial)，同時搭配 Harmonic Average 來將誤差值降低。(見圖 4)

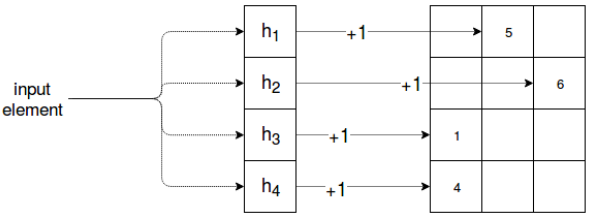

圖 4 CountMin Sketch 示意圖

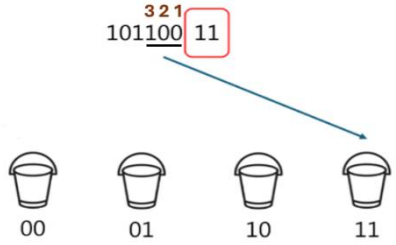

圖 3 Hyperloglog Sketch 示意圖

二、測試結果：

測試前，先決定 Hyperloglog 中適合的 Bucket 數量，估計值才會準確。圖 5 和圖 6 是在一個集合中放入 1000 個和 100000 個 source IP，並用 Hyperloglog 估計的結果，在我們的實驗(source 數量在 1000~100000 之間)中，我們設定2^8個 bucket。

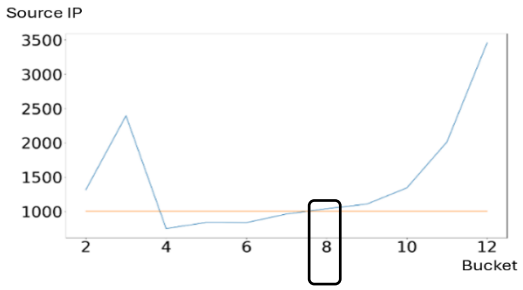

圖 5 1000 個不同元素的估計結果

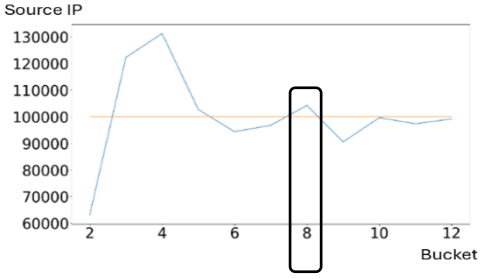

圖 6 100000 個不同元素的估計結果

最後的結果如圖 7.所示，我們對 5 個 destination 寄送封包，其中兩個(10.0.0.2 和 10.0.0.3)為高流量(其餘都沒有大於我們設定的 CountMin 標準值)。

可以看到 P4 Switch 在面對其中兩個高流量的 destination 都有將它們放進 watchlist 估計，也分別得到相對準確的估計值，這樣的結果可以幫助 Controller 判斷是否為 DDoS 攻擊。

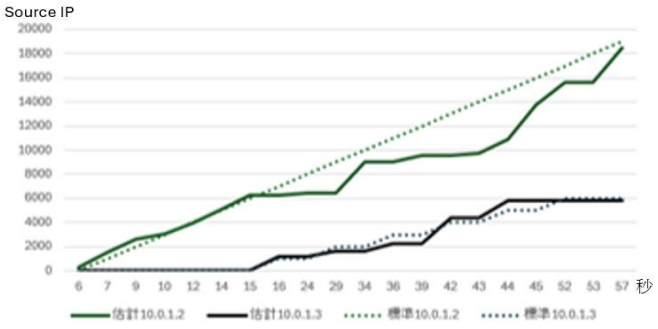

圖 7 結果

三、參考文獻：

[1] “網路模擬與分析”， https://hackmd.io/@110510549/ByyNkAasu , 2021

[2] “第十六周 P4 筆記”, https://hackmd.io/qRKNdQLaSVmQjorzJbeUNw , 2022

[3] “DDoS Detection in P4 Using HYPERLOGLOG and COUNTMIN Sketches”, Vera Clemens, IEEE Symposium on Network Operations and Management , May 2023