於 P4 實現基於 SpreadSketch 的 DDoS 偵測

DDoS detection based on SpreadSketch and implementation with P4

指導教授：張燕光
專題成員：李昆翰、李育丞
開發工具：Python、P4 BMv2
測試環境：Ubuntu 22.04 LTS

一、簡介：

DDoS 攻擊，又稱分散式阻斷服務攻擊，主要的概念是攻擊者會控制多部殭屍主機，對受害者的系統或網路進行大量的訪問或請求，導致其無法正常運作或服務中斷。這不管是在過去還是現在，都依然存在著，也都不敢說有一個明確的偵測方式。

我們這組於本次專題中實現的 DDoS 偵測方法是參考自此篇論文:【SpreadSketch: Toward Invertible and Network-Wide Detection of Superspreaders】。這篇論文的作者創造了一個名為 SpreadSketch 的 Sketch 資料結構，用來偵測網路環境中哪些主機是 ”superspreader”，以捕捉哪些主機擁有大量和不同主機的網路連結數。在網路世界中，不管是蠕蟲攻擊，還是 DDoS 攻擊等攻擊型態，都會有一個共通的特點 – 那就是會有主機會在一段時間突然擁有很多不同的連線。因此，偵測網路中的 ”superspreader” 也可說是相當重要的研究課題。

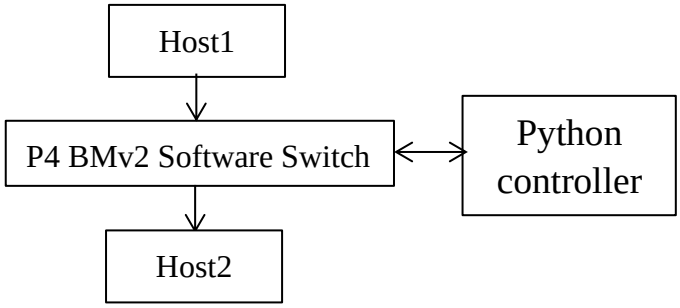
我們將此資料結構實現及架設在 P4 BMv2 虛擬交換機中。P4 是一種實現軟體自定義網路 (SDN) 的程式語言，主要是編譯及執行在網路的 data plane 中，也就是交換機內。這使得開發者可以不須直接由 control plane 來去對 data plane 去做操作外，P4 也擁有了 Protocol Independent、Target Independent、Field Reconfigurable 的特性，解決傳統交換機，以及舊型的 SDN 交換機無法隨時更新協議及跨平台集中控管的問題，降低了網路的研究和管理成本，讓其成為了眾多的網路研究的實驗平台，如 DDoS、QoS 等。

二、實驗方法：

我們的系統架構是由兩個虛擬主機、一個虛擬 P4 BMv2 交換機、以及一個在 control plane 的 controller 所組成，且都運行在 Ubuntu 22.04 作業系統。其中，虛擬 P4 BMv2 交換機部屬了 SpreadSketch 資料結構在其中。

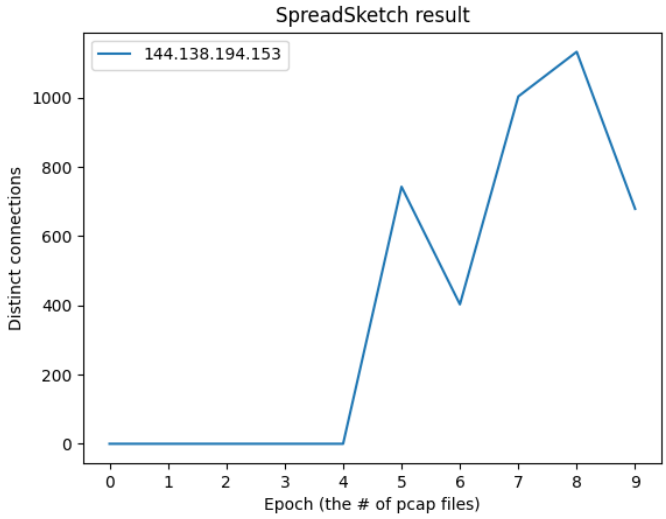
在設定且部屬完實驗環境後，我們會用 Python 中的 Scapy 套件，將 10 組打包成 pcap 檔案的攻擊封包 (在第五個 pcap 檔會有攻擊封包出現，其餘的都是混和了正常封包內容將其擴充。攻擊封包的來源為 L.F. Haaijer, DDoS Packet Capture Collection, (2022).。) 由 host1 傳送到 host2，並於每個封包檔傳送完的當下，由 controller 呼叫及分析交換機內 SpreadSketch 資料結構的數據。

以下為系統架構圖：



三、測試結果：

在本次展示的測試中，我們設定的非重複連線數量 (distinct connections) 的閾值為 350。



圖二：實驗結果圖

藉由上圖中的測試結果，我們可以發現到，在 epoch >= 5 以後，IP 位置為 144.138.194.153 的主機的非重複連線數量開始急遽增加，成為 “superspreader”。

而在我們製作的 pcap 封包檔中，攻擊封包是都安排在 epoch >= 5 的封包，因此可以觀察且推斷出該 IP 位置有極大的機率正在承受 DDoS 的攻擊，從而發出了如此多的回應訊息給殭屍主機。