SpreadSketch 結合 P4 於多交換器架構下之 Superspreader 偵測機制

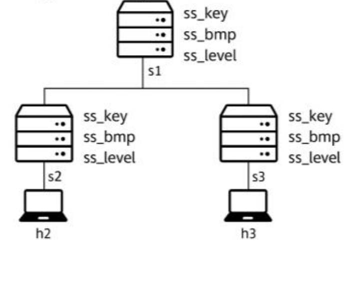
Distributed Superspreader Detection using SpreadSketch on a Multi-Switch P4 Architecture

指導教授：張燕光
專題成員：洪恩佳、蔡亦琁
開發工具：bmv2, p4c
測試環境：Ubuntu 20.04

一、簡介：

我們的專題動機源於`SpreadSketch_Toward_Invertible_and_Network-Wide_Detection_of_Superspreaders`這篇論文，其中的 Spreadsketch 即是用來偵測 DDoS 攻擊中的 superspreader，但論文提供的 SpreadSketch 架構僅適用於單一 switch，尚未擴展至多個 switch 的環境。而在目前的資料中心、IoT 架構或大型骨幹網路中，流量會經多個 router/switch，若只仰賴單個 switch 紀錄 superspreader 資料，一旦網路中出現瞬間高流量的 packet flow（例如 : IoT DDoS 攻擊中的 burst traffic 或 fast-flux 攻擊策略），很可能會因 register table 來不及被更新、尚未輪到該封包進行處理 （pipeline lag）、bitmap 未累積足夠資訊，進而錯過該 superspreader 的識別。此外，single switch 架構下的 Spreadsketch 也可能因 switch 本身的硬體故障或記憶體溢位（register overflow）而失效，導致監控紀錄完全遺失而無法回溯先前的封包行為（packet flow pattern）以及 switch 內存的 register table 回溯 sperspreader IP。

由此可見單點監控不具擴展性與容錯能力，因此我們將 SpreadSketch 分散部署到多個 switch，避免瞬間高流量 packet flow 導致 register 紀錄不完整，以及藉由 redundancy of register table 的特性解決 switch 單點失敗（Single Point of Failure, SPOF）的損失，透過跨 switch 的 bitmap 合併（bitmap fusion），還原可能遺失的 spread 訊息。以下為系統架構圖（圖一）：



➢ sender： h1 負責執行 send.py 發送 packet

➢ receiver： h2, h3 為接收封包的終端設備

➢ switch：s1, s2, s3

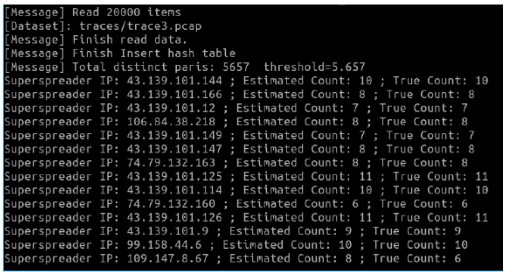
■ s1 為所有 packet 會經過的 switch

■ s2 和 s3為 packet 經 s1 forward 到的 switch

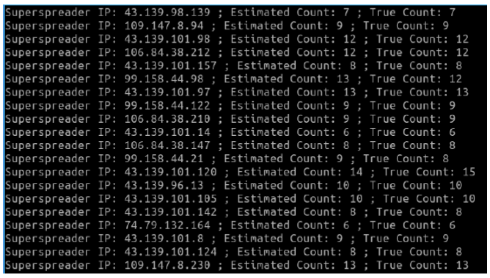
➢ s1 forwarding rule：依 source ip address 的 hash value (8-bit)，偶數者 forward 到 s2，奇數者到 s2

二、測試結果：

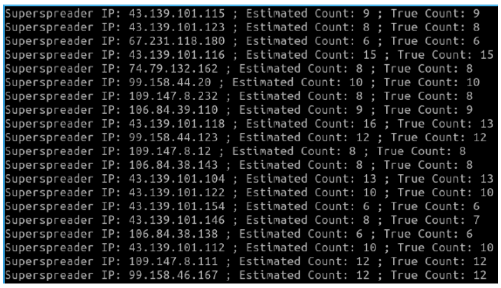
Spreadsketch Implementation 有兩個版本：c++和 p4，其中 c++版本是用來驗證我們寫的 p4版本 superspreader IP 還原結果是否正確。Spreadsketch 採用 multi-resolution bitmap 記錄 packet flow 分佈和 source IP 的 key value，在（圖一）中，每個 switch 都存有獨立的 register table，其中 ss_key, ss_bmp, ss_level 三者構成一層 Spreadsketch，而每個 switch 都有三層 Spreadsketch，目的在於減少 hash collision 和比較各個 bucket 在三層 Spreadsketch 中的 level 最大值並選定該層 bucket 對應到的 source IP key value 作為 candidate superspreader （即 Merge Operation）。



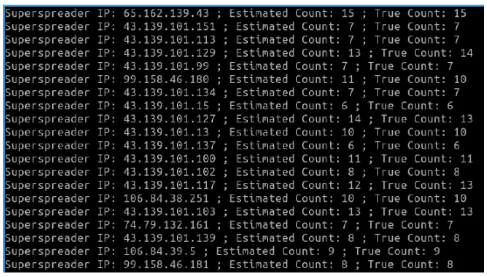
```
[Message] Read 20000 items
[Dataset]: traces/trace3.pcap
[Message] Finish read data.
[Message] Finish Insert hash table
[Message] Total distinct paris: 5657  threshold=5.657
Superspreader IP: 43.139.101.144 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.166 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.12 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 106.84.38.218 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.149 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.147 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 74.79.132.163 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.125 ; Estimated Count: 11 ; True Count: 11
Superspreader IP: 43.139.101.114 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 74.79.132.160 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.126 ; Estimated Count: 11 ; True Count: 11
Superspreader IP: 43.139.101.9 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 99.158.44.6 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 109.147.8.67 ; Estimated Count: 8 ; True Count: 6
```



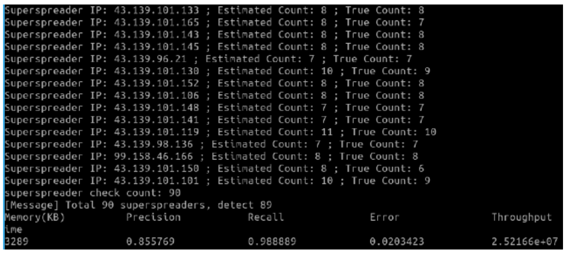
```
Superspreader IP: 43.139.98.139 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 109.147.8.94 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 43.139.101.98 ; Estimated Count: 12 ; True Count: 12
Superspreader IP: 106.84.38.212 ; Estimated Count: 12 ; True Count: 12
Superspreader IP: 43.139.101.157 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 99.158.44.98 ; Estimated Count: 13 ; True Count: 12
Superspreader IP: 43.139.101.97 ; Estimated Count: 13 ; True Count: 13
Superspreader IP: 99.158.44.122 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 106.84.38.210 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 43.139.101.14 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 106.84.38.147 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 99.158.44.21 ; Estimated Count: 9 ; True Count: 8
Superspreader IP: 43.139.101.120 ; Estimated Count: 14 ; True Count: 15
Superspreader IP: 43.139.96.13 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.105 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.142 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 74.79.132.164 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.8 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 43.139.101.124 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 109.147.8.230 ; Estimated Count: 13 ; True Count: 13
```



```
Superspreader IP: 43.139.101.115 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 43.139.101.123 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 67.231.118.180 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.116 ; Estimated Count: 15 ; True Count: 15
Superspreader IP: 74.79.132.162 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 99.158.44.20 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 109.147.8.232 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 106.84.39.110 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 43.139.101.118 ; Estimated Count: 16 ; True Count: 13
Superspreader IP: 99.158.44.123 ; Estimated Count: 12 ; True Count: 12
Superspreader IP: 109.147.8.12 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 106.84.38.143 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.104 ; Estimated Count: 13 ; True Count: 13
Superspreader IP: 43.139.101.122 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.154 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.146 ; Estimated Count: 8 ; True Count: 7
Superspreader IP: 106.84.38.138 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.112 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 109.147.8.111 ; Estimated Count: 12 ; True Count: 12
Superspreader IP: 99.158.46.167 ; Estimated Count: 12 ; True Count: 12
```

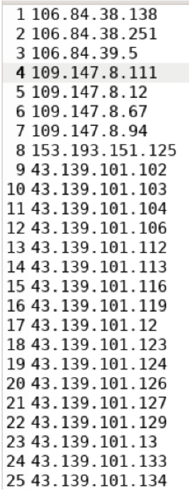


```
Superspreader IP: 65.162.139.43 ; Estimated Count: 15 ; True Count: 15
Superspreader IP: 43.139.101.151 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.113 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.129 ; Estimated Count: 13 ; True Count: 14
Superspreader IP: 43.139.101.99 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 99.158.46.180 ; Estimated Count: 11 ; True Count: 10
Superspreader IP: 43.139.101.134 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.15 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.127 ; Estimated Count: 14 ; True Count: 13
Superspreader IP: 43.139.101.13 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.137 ; Estimated Count: 6 ; True Count: 6
Superspreader IP: 43.139.101.100 ; Estimated Count: 11 ; True Count: 11
Superspreader IP: 43.139.101.102 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.117 ; Estimated Count: 12 ; True Count: 13
Superspreader IP: 106.84.38.251 ; Estimated Count: 10 ; True Count: 10
Superspreader IP: 43.139.101.103 ; Estimated Count: 13 ; True Count: 13
Superspreader IP: 74.79.132.161 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.139 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 106.84.39.5 ; Estimated Count: 9 ; True Count: 9
Superspreader IP: 99.158.46.181 ; Estimated Count: 8 ; True Count: 8
```

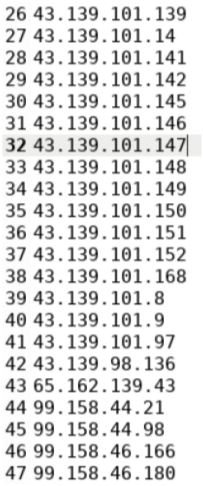


```
Superspreader IP: 43.139.101.133 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.165 ; Estimated Count: 8 ; True Count: 7
Superspreader IP: 43.139.101.143 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.145 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.96.21 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.130 ; Estimated Count: 10 ; True Count: 9
Superspreader IP: 43.139.101.152 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.106 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.148 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.141 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 43.139.101.119 ; Estimated Count: 11 ; True Count: 10
Superspreader IP: 43.139.98.136 ; Estimated Count: 7 ; True Count: 7
Superspreader IP: 99.158.46.166 ; Estimated Count: 8 ; True Count: 8
Superspreader IP: 43.139.101.150 ; Estimated Count: 8 ; True Count: 6
Superspreader IP: 43.139.101.101 ; Estimated Count: 10 ; True Count: 9
superspreader check count: 90
[Message] Total 90 superspreaders, detect 89
Memory(KB)        Precision        Recall        Error        Throughput
ime
3289              0.855769         0.988889      0.0203423    2.52166e+07
```

左到右、上到下依序為（圖二）、（圖三）、（圖四）、（圖五）、（圖六），為 c++版本 Spreadsketch 得出的 superspreader list



```
106.84.38.138
106.84.38.251
106.84.39.5
109.147.8.111
109.147.8.12
109.147.8.67
109.147.8.94
153.193.151.125
43.139.101.102
43.139.101.103
43.139.101.104
43.139.101.106
43.139.101.112
43.139.101.113
43.139.101.116
43.139.101.119
43.139.101.12
43.139.101.123
43.139.101.124
43.139.101.126
43.139.101.127
43.139.101.129
43.139.101.13
43.139.101.133
43.139.101.134
```



```
43.139.101.139
43.139.101.14
43.139.101.141
43.139.101.142
43.139.101.145
43.139.101.146
43.139.101.147
43.139.101.148
43.139.101.149
43.139.101.150
43.139.101.151
43.139.101.152
43.139.101.168
43.139.101.8
43.139.101.9
43.139.101.97
43.139.98.136
65.162.139.43
99.158.44.21
99.158.44.98
99.158.46.166
99.158.46.180
```

左起依序為（圖七）、（圖八）：P4 受限於無法進行浮點數運算及 register 的長度限制

Register_name	Data type	Length
ss_bmp	1-bit	262144
ss_key	32-bit	2048
ss_level	8-bit	2048

因此只能還原出一部分，（圖七）、（圖八）為 packet 分流至 s2, s2 後經 merge operation 得出的 superspreader IP list，所有 IP 皆能從 c++版本的結果找到對應值。