我們的工作目標是為開發一種基於機器學習的網路流量控制系統。該系統旨在定位、分類和建模。我們對過去文獻進行了研究，並得出結論，使用GRU(CNN)進行網路流量檢測將是構建自動化ddos檢測技術的(最佳)方法。

在本方法中我們使用軟體定義網路(SDN)來達成及時流量控制系統，switch負責資料的轉送，controller負責對switch下達資料的轉送規則和蒐集流量資訊。資料的轉送規則是利用flow table來達成，switch藉由查看flow table來決定資料的流向。

我們提出的方法分階段進行：擷取數據、計算特徵、使用深度學習模型進行分類以及控制流量。週期性的擷取流量數據用以計算特徵組成特徵值矩陣。使用GRU模型對特徵進行分類以區分流量。(以下小節詳細介紹了每個階段。)

A 擷取數據

週期性的從controller請求流量狀態並記錄到記憶體中，再利用這些數據去訓練模型和預測流量種類，其中重要的流量數據為來源位置、目的位置、封包數量和封包大小。

B 計算特徵

解析流量的資訊，如封包目的位置、封包個數和封包大小，計算要提供給機器學習模型的特徵。根據[https://www.hindawi.com/journals/scn/2018/9804061/]分析，ddos攻擊與以下五種特徵相關。

1. 來源IP速度(SSIP)是單位時間內來源IP位址的數量：

|  |  |  |
| --- | --- | --- |
|  |  | (1) |

Sum\_IPsrc是來源位址的數量，T是取樣間隔。因為攻擊時會產生大量偽造封包使位址數量增加。

1. 流資料包標準差(SDFP)，即一段時間內資料包數量的標準差，如下

|  |  |  |
| --- | --- | --- |
|  |  | (2) |

Mean\_packets表示一段時間內的平均資料包數量，N是flow entry數量

1. 串流位元組偏差(SDFB)，即週期內位元數的標準差，如下

|  |  |  |
| --- | --- | --- |
|  |  | (3) |

Mean\_bytes表示一段時間內的平均位元數

1. 流表項速度(SFE)，即單位時間內流表項的數量，如下：

|  |  |  |
| --- | --- | --- |
|  |  | (4) |

1. Pair-Flow比率(RPF)，即交互流表項與總流表項的比率，如下：

|  |  |  |
| --- | --- | --- |
|  |  | (5) |

Pair\_Sum是interactive flow entries數量。

C 流量分類

我們訓練了GRU(CNN)模型進行分類，判斷流量是否為正常流量。GRU是 RNN的變體，簡化了LSTM閥的數目已加快執行速度及減少記憶體用量。利用先前計算的特徵進行學習，分辨流量是否為攻擊。

D 控制流量

利用controller對switch下封包轉送規則，並將結果顯示於視窗中。依造模型分類的結過執行不同的行為，當模型將流量識別為正常流量時不對封包的轉送做任何的變更，而當模型將流量判斷為異常時利用controller對switch新增拋棄封包轉送規則，使攻擊失效。

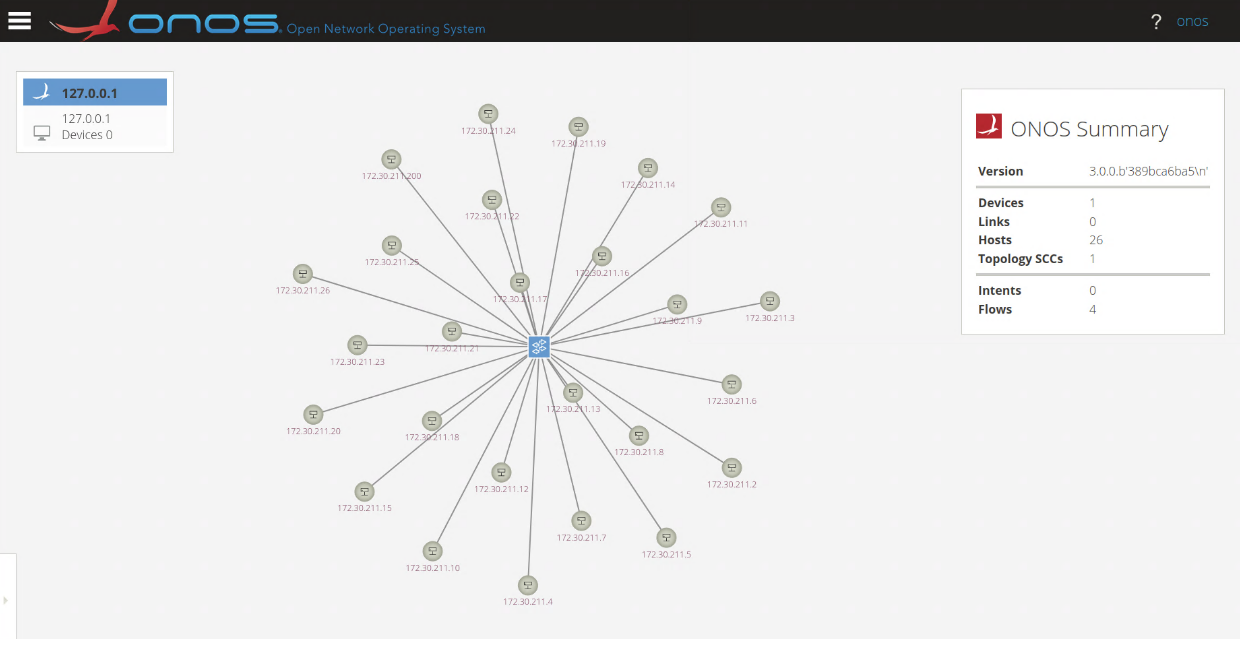
設置

Mininet

Ryu controller

運行機器學習的主機

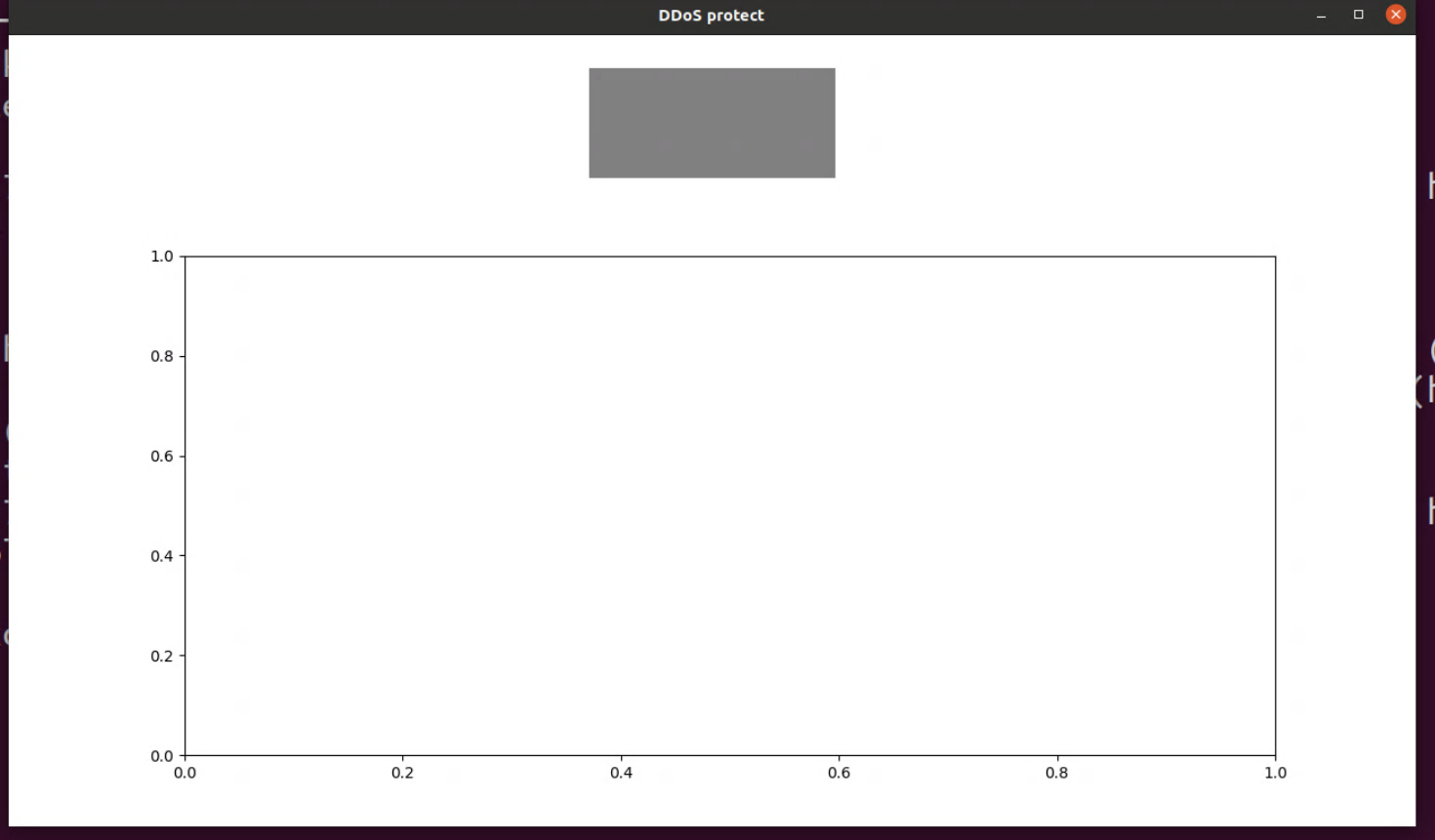
利用mininet 建立虛擬網路，組成為一台switch 和 26台主機，由兩台controller c1 c2控制switch，c1負責封包的傳送規則設定，c2負責接收指令及時控制switch。整體拓譜如下圖，因ryu controller無法使用圖形介面故使用onos controller讀取網路拓譜

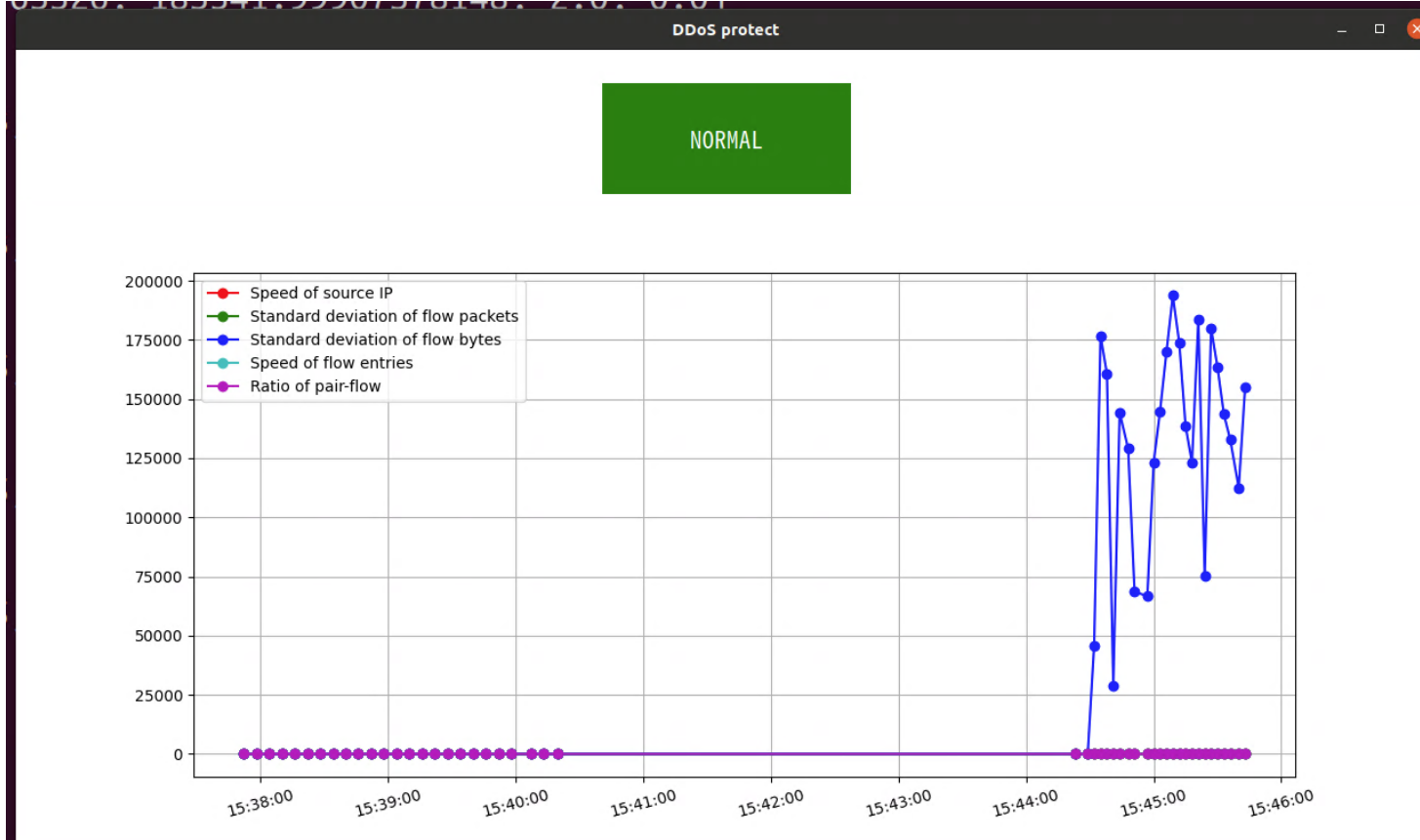


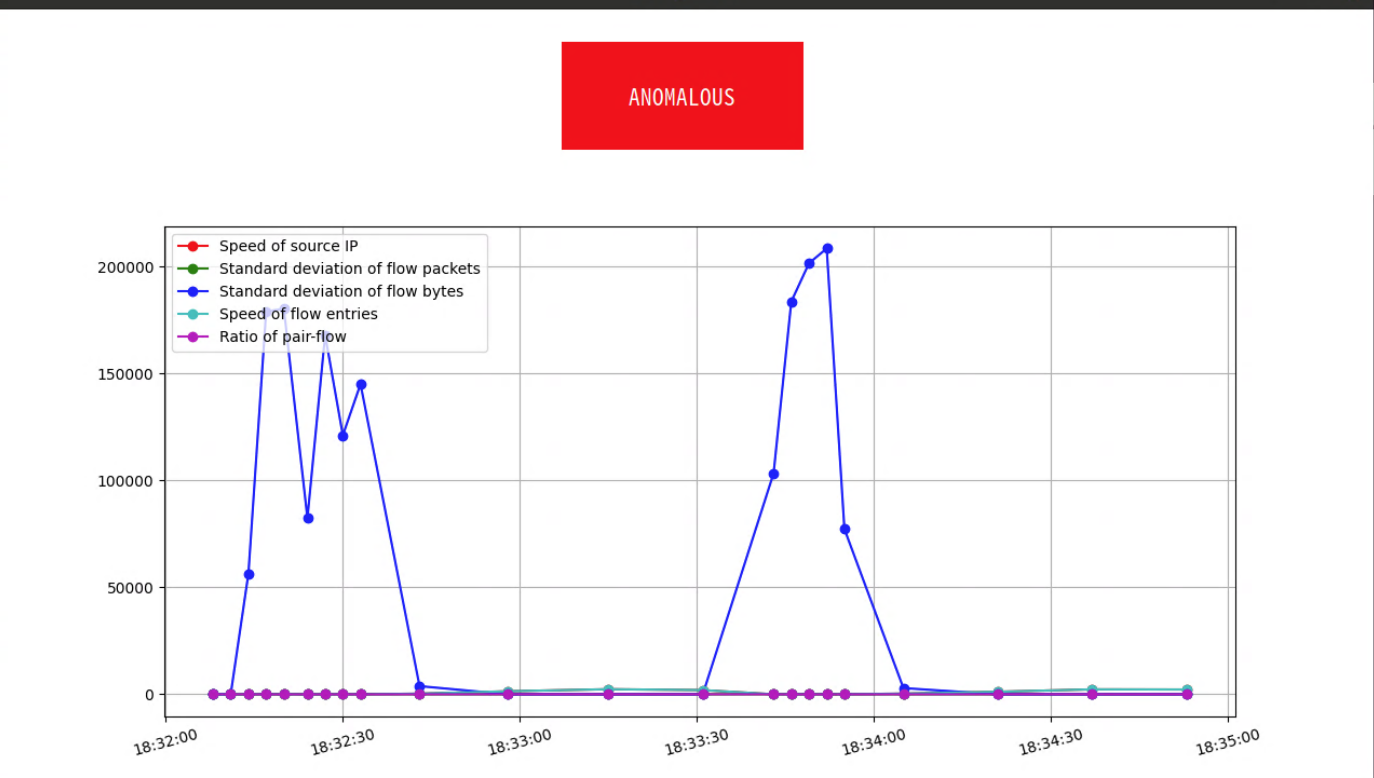
選定目標主機作為攻擊目標其ip 位置為172.30.211.200。運行腳本製造大量流量至目標主機，利用c2蒐集流量資料送至GRU模型中，模型將會判斷此流量是否為攻擊，如果不是攻擊則不做行動繼續判斷下次資料是否為攻擊，若為公及則會利用c2下規則至switch使此攻擊流量不會進到目標主機。

流量製造腳本分為兩部分，第一部分為正常流量將傳送隨機封包個數至目標主機，第二部分為攻擊流量將會對目標主機進行隨機次數的攻擊，兩種部分將會交叉進行以模擬真實情況。

將會利用圖形視窗顯示目標主機封包接收狀況，當流量為正常時標示正常，異常時標示異常。如圖顯示。







在訓練階段，正常流量通過設定隨機的封包數量和間隔時間以模擬真實網路連線的不穩定狀態。異常網路流量通過攻擊工具hping3來產生。hping3是一款免費的資料包產生器和分析器。 可用於防火牆規則測試、網路測試、效能測試，壓力測試(DOS)，幾乎可以傳送任意類型的TCP/IP封包。其優點在於能夠自訂封包的各個部分，因此使用者可以靈活地對目標進行細緻地探測。基於以上特點，我們使用hping3產稱不同類型的攻擊資料，用以模擬TCP SYN Flood、UDP Flood和ICMP Flood等網路流量攻擊。

結果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表 1 | | | | |
|  | precision | recall | f1-score | support |
| 正常流量 | 0.75 | 0.9 | 0.82 | 1202 |
| 異常流量 | 0.96 | 0.9 | 0.93 | 3370 |
| accuracy |  |  | 0.9 | 4572 |

在實驗中我們使用1202筆正常流量和3370筆異常流量進行測試。攻擊檢測的性能透過一般機器學習性能指標表示，結果如表1顯示。我們訓練的GRU模型測得90%的準確率，正常流量與異常流量的召回率皆有90%。雖然正常流量的精確率只有0.75，但我們的應用在於異常流量的檢測，因此較低的正常流量精確率不影響真實使用場景，符合阻止異常流量的應用。

結論

本實驗透過controller從switch擷取網路流量狀態，計算與ddos攻擊相關的特徵，然後用GRU模型對流量進行分類，最後使用controller向switch下達應對的轉送規則，達成阻止攻擊的目的。我們透過SDN部屬實驗環境來驗證。攻擊檢測的準確率足夠用於阻止異常流量，雖然正常流量的精確率較低，但在阻止攻擊的應用尚不構成影響。在未來我們應該全面模擬真實正常流量以提高正常流量精確率的表現。