林文暉、王平、吳保樺、周明勝、蔡東霖、蔡一郎、羅濟群（2020），『一個基於行為分析學習模式之網路入侵偵測分類器』，*中華民國資訊管理學報*，第二十七卷，第四期，頁 465-494。

一個基於行為分析學習模式之網路入侵偵測分類器

林文暉
崑山科技大學資訊管理系

王平*
崑山科技大學資訊管理系

吳保樺
崑山科技大學資訊管理系

周明勝
崑山科技大學資訊管理系

蔡東霖
崑山科技大學資訊管理系

蔡一郎
國立成功大學電腦與通信工程研究所

羅濟群
國立交通大學資訊管理研究所

摘要

資安防護思維模式已逐步朝向整合度高且具有機械學習和認知運算（cognitive computing）技術的資安平台，透過將威脅資料篩濾增加威脅辨識、詮釋及預測精度，並藉由預測性分析（predictive analysis）可視化顯示提高對企業網路的即時安全監控與認知，以期協助企業降低資安管理複雜性和專業人力成本。實務上，個別獨立資安系統的防護裝置已無法有效阻絕來自網路威脅，為了提升網路入侵偵測之威脅辨識確度並降低誤判率，本研究提出一個基於行為分析法（behavior analytics）為基礎之複合型時間卷積神經網路（temporal convolutional network; TCN）及卷積神經網路（convolutional neuron network; CNN）分類器，應

* 本文通訊作者。電子郵件信箱：pingwang@mail.ksu.edu.tw
2020/05/14 投稿；2020/07/07 修訂；2020/09/29 接受

用於網路入侵偵測系統之異常偵測，其整合歷史外地入侵資料庫與近期本地特有資料集的威脅行為特徵，透過擷取完整的行為特徵，以提升模式辨識精確度。實作上，先採用加拿大 New Brunswick 大學建立 CIC-IDS-2017 數據集（外地威脅）之行為特徵先作為模式預訓練（pre-training）學習網路入侵的基本樣態，並搭配蒐集近期本地網路威脅之資訊流特徵，透過 CICFlowMeter-v4.0 工具將資訊流轉化為行為特徵文字檔，加入以墒值為基礎之決策樹 ID3 演算法篩選高頻出現之特徵集，以訓練 TCNs 以提升網路入侵偵測模式之威脅辨識確度並降低誤判率。實驗證明所研提模式可即時辨識出 94.56%五類分散式阻斷式服務的攻擊，協助雲端服務之管理者識別網路威脅。

關鍵詞：網路入侵偵測、時間卷積神經網路、卷積神經網路、行為分析分類器

Lin, W.H., Wang, P., Wu, B.H., Jhou, M.S., Tsai, D.L., Tsai, Y.L. and Lo, C.C. (2020), 'A study on network intrusion detection using behaviorialanalysis-based learning classifier', *Journal of Information Management*, Vol. 27, No. 4, pp. 465-494.

A Study on Network Intrusion Detection Using Behaviorial Analysis-based Learning Classifier

Wen-Hui Lin
Department of Information Management, Kun Shan University

Ping Wang*
Department of Information Management, Kun Shan University

Bao-Hua Wu
Department of Information Management, Kun Shan University

Ming-Sheng Jhou
Department of Information Management, Kun Shan University

Dung-Lin Tsai
Department of Information Management, Kun Shan University

Yi-Lang Tsai
Institute of Computer and Communication Engineering,
National Cheng Kung University

Chi-Chun Lo
Institute of Information Management, National Chiao Tung University

Abstract

Purpose－New ready-made malware on system vulnerability in networks or hosts has been increasing information security risks. Practically, the individual system for security protection has been unable to effectively prevent cyber threats. Thus, the security protection model has gradually moved towards a highly integrated platform with mechanical learning (MA) and cognitive computing technology to assist defenders reduce

* Corresponding author. Email: pingwang@mial.ksu.edu.tw
2020/05/14 received; 2020/07/07 revised; 2020/09/29 accepted

the complexity of security management and cost of professional engineer.

Design/methodology/approach－To improve the classification accuracy of threat detection and reduce its false positive rate for DDoS threats, this study proposes a behavior analysis-based learning classifier for network anomaly detection by training a fused learning classifier aggregating both Temporal Convolutional Network (TCN) and Convolutional Neuron Network (CNN) with ID3-based feature selection algorithm, network flow analyzer, CICFlowMeter-v4.0 on intrusion database generated from an global IDS dataset CIC-IDS-2017 released by the University of New Brunswick and local intrusion dataset to analyze the complete attack features that increase the pattern recognition accuracy and also reduces false negative rate in network intrusion detection.

Findings－The experimental results revealed that the proposed model accuracy is 94.56% in identifying five different types of threats of 94.56% DDoS network intrusion in real time, assisting cloud service managers to recognize network threats.

Research limitations/implications－Although MA techniques for intrusion detection problem have been proposed in this paper. The converge performance of complex networks with new attack types such as APT (advanced persistent threat) will be tackled in future studies.

Practical implications－This paper provides several technical implications in training behavior analysis-based learning classifier for network anomaly detection.

Originality/value－This paper is an empricial analysis report that applies an TCN/CNN architecture with ID3-based feature selection algorithm, to analyze the complete attack features on CIC-IDS-2017 intrusion database and local intrusion patterns in Taiwan. It advances perceptions on the behavior analysis-based learning classifier for network anomaly detection. The paper concludes with performance analysis results in identifying five different types of DDoS threats for enhancing detction accuracy for DDoS attacks.

Keywords: network intrusion detection, temporal convolutional networks, convolutional neuron networks, behavior analysis-based classifier

壹、前言

網路異常偵測精確度的真正挑戰是如何即時正確識別與回應威脅。實務上駭客或惡意網站會使用多種攻擊手段進行交叉攻擊，在面對多樣式威脅行為樣態，如何精確分析網路威脅之多樣化行為特徵，以利正確判斷攻擊型態並作適當回應（response）一直是管理者頭痛的問題。傳統網路威脅分析方法常以行為關聯分析技術，搭配網路資訊流封包蒐集、過濾與精確特徵比對，需要大量資安專家人工作研判，常無法即時判斷或誤認新型態網路威脅，近期網路入侵偵測防護已加入人工智慧（artificial intelligence; AI）之深度學習設計框架，輔助專家準確判斷威脅類別，並推薦對應防護的決策，決策內容包括威脅來自網域對應組織、威脅種類、發生機率與防護方法。

常見深度學習框架包括深度神經網路（deep neural networks; DNN）、卷積神經網路（convolutional neuron networks; CNNs）和深度置信網路（deep belief networks; DBN）和遞迴神經網路（recurrent neural network; RNN）四種，並已被應用電腦影像識別、語音識別、自然語言處理與生物資訊學等領域並取得了良好的辨識效果。其中遞迴神經網路（recurrent neural nets; RNN）（Gupta 2017）節點之間的連接形成沿序列的有向圖，此一序列的有方向性連結架構設計可作為分析時間序列數據（time serial data）的動態行為。近期研究發現深度學習網路（deep learning networks; DLNs）之遞迴神經網路（RNNs）、長短期記憶網路（long short-term memory; LSTM）（Firat et al. 2015; Hochreiter & Schmidhuber 1997; Kandpal 2018; 鍾玉峰等 2018）已在語音、文章識別、機器翻譯、手寫字識別等序列資料分析與預測等領域表現出色，其解決類問題特色是在於識別語意內容之前、後文為有時間順序相關，意思就是待預測的單詞依賴於前面已出現的單詞；網路攻擊行為之實施手法是屬於一種時間序列事件相關的來源識別與行為分類問題，顯然的網路攻擊偵測問題適合應用 RNN 與 LSTM 來解決。故本研究選擇以 RNN 為基礎所創新之時間卷積網路（temporal convolutional network; TCN）來建構新型網路威脅偵測模式，首先須了解現有 RNN、LSTM 及 TCN 之網路架構設計。

長短期記憶網路（LSTM）和門檻遞迴圈單元（gated recurring units; GRU）是改良 RNNs 的長期依賴問題（long-term dependencies），使預測資料可以關聯較遠距離（時間較久遠）的特定詞句，透過關聯與過濾並與判斷那些關鍵資訊能適合決定出現下一個單詞。2017 年初 Google 公司針對時間序列性資料處理翻譯耗時太久問題，提出解決方案叫做 ByteNet，透過在機器翻譯系統導入注意力函數（attention function）與崁入 CNN 並行處理架構，重新設計記憶體儲存方式，將序列數據的關聯運算轉變成大規模並行處理，此種設計有利大規模並行處理，此一改造大幅改善 RNN 運算速度，故基於注意力函數之並行處理架構設計，整個框

架設計上比 LSTM 更為精簡並降低輸入次數與執行時的回饋迴圈，重新命名為時間卷積神經網路（TCNs）。

經研究實證（Ding & Xu 2017; Firat et al. 2015; Hochreiter & Schmidhuber 1997; Kandpal 2018; Kang & Kang 2016; 鍾玉峰等 2018），發現 LSTM 設計架構可以調整記憶門使得應該被記得的詞句永遠留在處理單元內，但實務上 TCN 設計提供一個可調變的認知結構大小（flexible receptive field size），透過彈性調整卷積層的堆疊結構以認知資料的輸入，搭配改變膨脹係數（dilation factors）及濾波器（filter/kernel size）數值的設定，正確的控制模型的記憶層容量來處理輸入資料，此一網路結構設計能留住更長遠先前的記憶資訊，並降低輸入次數與執行時的回饋迴圈，使得 TCN 執行速度較 RNN 與 LSTM 更快速。

綜合上述說明，只使用單一種模型來做入侵偵測訓練及分類，可能無法面面俱到，其中 TCN 擅長於長時間序列數據的建模與特徵擷取，CNN 擅長於並行運算執行複雜影像辨識，故本研究整合 TCN 生成語詞與 CNN 影像辨識兩個深度學習模式成為一個 TCN-CNN 複合型深度網路學習模式；先採用 TCN 以處理方式萃取高頻出現的行為特徵向量，再將多筆特徵向量形成特徵矩陣並轉為圖像供 CNN 做類別映射，求取隱藏層特徵矩陣之最佳化權重，並運用 CNN 強大的圖像辨識能力做分類，以協助網路入侵偵測系統（network intrusion detection system; NIDS）執行網路異常偵測。

為了提升網路入侵偵測之威脅辨識確度並降低誤判率，本研究提出一個基於行為分析法為基礎之異常偵測模式應用於網路入侵偵測系統，整合歷史入侵資料庫與近期本地特有的威脅行為特徵，擷取完整行為特徵作為訓練資料集，以提升 TCN-CNN 為基礎之複合型模式辨識確度。具體目標包括：

1. 以開源碼工具之網路流分析器 CICFlowMeter 工具（Canadian Institute for Cybersecurity 2018）為基礎，設計一個資料預處理程式（data preprocessor），執行網路流即時過濾與格式轉換，轉化網路入侵資料集 CIC-IDS-2017（Canadian Institute for Cybersecurity 2017; Sharafaldin et al. 2018）之分散式阻斷服務攻擊（distributed denial-of-service attack; DDoS）的行為特徵，並蒐集本地即時網路威脅之行為特徵，使模式學習到完整惡意行為特徵。
2. 加入以熵值（entropy）為基礎之決策樹 ID3 演算法（Witten & Frank 2005），計算每一行為特徵權重（weights），篩選出高頻出現異常之行為特徵，作為網路異常偵測之最佳特徵候選集合（best candidates of feature sets）以正確訓練模式，提升網路入侵偵測模式之威脅辨識精確度並降低誤判率。
3. 透過大量惡意時間序列數據來訓練 TCN-CNN 複合型深度網路學習模式，

以提高特徵萃取的質量，搭配逆向傳播演算法修正估算誤差以改善網路架構中各層權重訓練的結果，再依據分類層化權重計算與現有威脅類別的相似度，以量化預測威脅類別，協助管理者評估外部威脅來源之連線風險。

本研究第貳節介紹時間卷積神經網路（TCN）模式，第參節介紹基於行為分析法之異常偵測模式應用於網路入侵偵測系統，第肆節進行實驗網路入侵偵測模式訓練與精度測試，第伍節作出研究結論及提出後續研究方向。

貳、文獻探討

本節將分別探討深度學習之網路威脅偵測發展現況、時間卷積神經網路的發展近況與可能的應用。

一、基於深度學習之網路威脅偵測之研究

由於惡意網路連線與正常網路服務活動，除連線反應速度與間隔時間、固定網域查詢與連線特徵外，兩者工作流程與協定類似，使基本的網路流異常偵測很難察覺偽裝的惡意網路連線。DNN 可應用於網路流之惡意行為特徵學習、識別與威脅分類問題，近期 DNNs 已轉為在新型網路威脅及電腦病毒特徵的識別應用。雖然樣本學習過程耗用較多時間訓練以設定隱藏的參數（卷積核），但完成訓練部署的主機可即時且精確判斷威脅模式，包括威脅種類、發生機率與推薦對應防護方法，表 1 為整理運用深度學習於網路異常監控與偵測之先前研究。

表 1：應用深度學習於網路異常偵測研究

作者	研究貢獻	創新點
Tan（2013）	提出了基於圖像像素矩陣的網路入侵檢測深度學習方法，將網路流通過特徵之間距離轉換為圖像像素矩陣，探討了利用計算機視覺技術處理網路入侵檢測問題的可能性。	提出了基於網路入侵行為特徵作為輸入，並將特徵矩陣轉為圖像像素作為網路入侵檢測深度學習的方法。
Yan 等（2013）	通過結合圖像分析技術與變種惡意程式碼檢測技術，將惡意程式碼映射為無壓縮的灰階圖形，然後根據樣本的紋理指紋，建立紋理索引結構；檢測階段通過惡意程式碼紋理指紋方塊生成策略，採用加權綜合多分段紋理指紋相似性匹配方法，	基於紋理分割演算法對圖片進行分塊，使用灰階共生矩陣演算法提取各個分塊的紋理特徵，並將這些紋理特徵作為惡意程式碼的紋理指紋。

	檢測惡意程式碼變種和未知惡意程式。	
韓曉光等（2014）	將惡意程式的結構進行可視化，再將 JPG 圖片萃取出圖片的紋理（texture），進行惡意程式種類的辨識。	惡意程式的結構進行可視化，再利用深度學習算法以圖像特徵訓練與分類。
Saxe 與 Berlin（2015）	提出了一個深層神經網路惡意程式分類器，整理與運用客戶和內部惡意軟體資料庫的超過 40 萬個二進制軟體程式，提高系統檢測率與降低誤判率。	性能評估結果為 95%正確檢測率與 0.1%的偽陽率（FPR），模式已應用到商品硬體上現實。
Niyaz 等（2015）	提出了一個以深層信念網路（deep belief network; DBN），建立一個之深度學習網路入侵測偵測系統（NIDS），透過實作稀疏性自動編碼器（sparse auto-encoder）和基於 softmax 迴歸的；測試使用網路入侵數據集- NSL-KDD 評估網路異常檢測精度。建議進一步提高無監督特徵學習分類性能，可搭配 NB-Tree，隨機樹或 J48 方法。	通過應用 DBN 作為特徵選擇器，搭配支持向量機（SVM）做為網路入侵偵測精度的驗證，應用於正常/異常檢測在測試數據上，發現所開發的 NIDS 與先前的系統相比設計性能表現更佳。
寇廣等（2016）	利用深度學習算法提取網路資訊流序列中的惡意行為特徵，用以檢測僵屍網路之資訊流序列中的異常事件，探索深度學習在入侵偵測系統之即時檢測中的應用。實驗結果證明，研究演算法之卷積核越大，檢測準確度相對較差，而檢測速度較快。	本文選取的卷積神經網路為最佳卷積核權重，研究成果檢測率、誤報率和漏報率分別為 94.63%、6.57%和 5.71%。
Wang、Cai 與 Wei（2016）	利用深度學習模型和迴歸運算，提出了一個新型檢測惡意 JavaScript 惡意程式碼的學習框架，獲得較高的檢測精度。深度學習算法進行 Java 惡意程式碼檢測，顯著提高檢測正確率。	搭配深度學習模型和迴歸運算，以提高檢測正確度。
Tomiyama 等（2016）	提出一個基於惡意行為的檢測方法，運用深層神經網路來分類威脅。首先，訓練 recurrent neural network（RNN）來淬取程式行為	繪製 ROC 曲線，方法性能評估通過比較 area under the curve（AUC）which 來

	特徵。接下來，訓練卷積神經網路（CNN）對特徵圖像進行分類，由所訓練的 RNN 提取特徵值及權重。	評估幾種圖像大小，最佳情況下獲得 AUC=0.96。
Tang 等（2016）	本文為一個深度學習方法在軟體定義網路（SDN）中基於流量的異常檢測的研究，透過集中邏輯的資安控制器與 DNN 模型，僅使用六個基本的網路流特徵，確認深度學習方法基於流量的異常檢測方法於 SDN 環境中強大的潛力。	在 SDN 環境下使用簡單 DNN 模型搭配 NSL-KDD 訓練模型數據集，選出 SDN 網路流六個基本特徵（共 41 特徵），模型啟動參數訓練資料設置為批量（batch size）大小為 10，訓練 epoch 為 100，透過實驗模式準確性能達到 75.75%。
Kang 與 Kang（2016）	為提高車載網路的安全性，提出了一種基於深度神經網路（DNN）的入侵檢測系統。構建 DNN 結構的參數用基於概率，從車內網路分組中提取特徵向量進行訓練。對於給定的數據包，DNN 提供每個類別識別正常和攻擊數據包的機率，可協助傳感器識別對車輛的惡意攻擊。	通過深度置信網路（DBN）的無監督預訓練來初始化參數，從而提高了檢測精度。實驗結果表明，所提出的技術能夠在控制器局部區域網（CAN）上顯著提高檢測率並對攻擊提供及時反應。
Lea 等（2017）	提出時間卷積網路（TCN），使用時間卷積的層來執行分割或檢測細步動作。TCN 使用編碼器-解碼器和擴張卷積有效地支持長程時間資訊萃取模式，可以應用於網路資訊流的行為特徵的學習。	說明 TCN 能夠捕捉並組合行為特徵，識別分段持續性的序列數據，解決遠程依賴性問題，並且比競爭的基於 LSTM 與 RNN 神經網路更快地完成訓練。
Ding 與 Xu（2017）	提出了一種新穎的混合時間卷積和循環網路的深度學習網路，設計架構為一編碼器-解碼器架構（encoder- decoder）；解碼器是遞歸神經網絡的層次結構，能夠在編碼階段後學習和記憶長期動作。	編碼器由時間卷積核的層次結構組成，捕獲不同動作的局部運動變化;三個行動分割數據集的實驗結果證明，所提出的模型證明優於現有技術的優越性能。
Sharafaldin 等（2018）	產生 CIC-IDS-2017 數據集是公開可用且合乎標準的網路入侵（IDS）	本文運用學習算法完整篩選網路流量特徵並進行綜合評估，指出檢測某些攻

	數據集，包含七種網路常見的攻擊和正常連線樣態行為。	擊類別的最佳網路行為特徵集合。
Bai、Kolter 與 Koltun（2018）	基於 TCN 基礎，搭配多隱藏層（卷積層與池化層）以進行大規模並行處理，驗證各類時間序列數據應用，發現模式訓練和驗證的時間都會較 RNN 短。	研究結果證明，TCN 網路訓練和驗證的時間都會較 RNN 及 LSTM 短，同時展示了更長時間的有效資訊儲存，測試模式精確度卻能保持相同或更佳。

二、時間卷積神經網路

TCN 設計的目標是用來加速時間序列數據處理，卷積神經網路（TCNs）透過擴張卷積（dilated casual convolutions）結構設計，改進 RNNs 的只能關聯前一級序列數據的限制，擴大認知區域架構，已在即時序列數據的辨識科學領域表現出色，尤其對於文字和語音識別性能表現優異。基本上，TCN 隱藏層架構通常由由多個時間卷積（temporal convolutions）、空間池化層（spatial pooling layer）和連接輸出的全連通層（fully connected layer）所組成。而全連通層內容包括特徵權重（weights）和 SoftMax 分類層，如圖 1 所示。

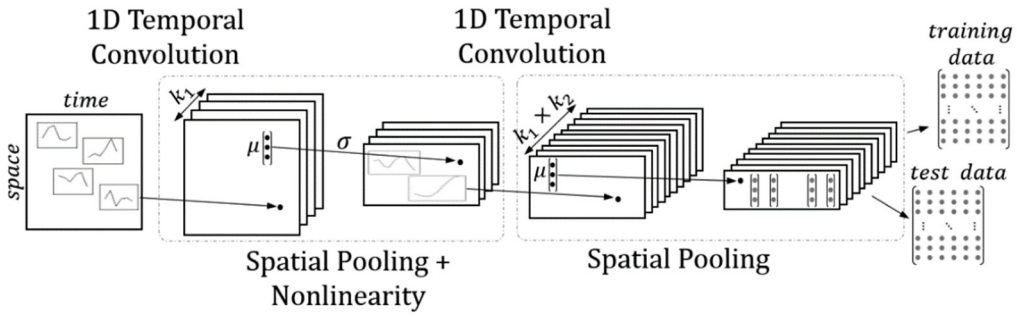

圖 1：基本時間卷積網路架構圖（Firat et al. 2015）

由圖 1 可知，當輸入為一大型且複雜多空間/時間序列數據，模式則增加擴張因果捲積的堆疊以放大認知區域，以容納 1~多維序列數據。整理 TCNs 的特色：(1)可以接受任意長度的時間序列輸入，通過滑動視窗（sliding windows）並將動態數據映射到與輸入相同長度的序列數據的輸出；(2)隱藏層架構的捲積是將輸出與先前資料互為因果關係（casual effects），以利並行計算架構處理先前相關資訊做預測；(3)使用組合深度的網路，增加因果卷積層及擴張卷積，擴大記憶歷史資料的容量並能確保持模式性能。

綜整上述說明，TCN 架構設計具有以下五項主要特點（Firat et al. 2015; Ding & Xu 2017; Lea et al. 2017; Bai et al. 2018; Yu & Koltun 2016）：

（一）序列建模（sequence modeling）（Bai et al. 2018）

假設給定輸入序列 $x_0,\ldots,x_T$，期望每次預測相應的輸出序列$\widehat{y_0},\ldots,\widehat{y_T}$，該關鍵限制條件是一段時間 t 預測輸出$\widehat{y_T}$，限制為使用輸入的先前觀察的歷史資料：$x_0,\ldots,x_T$。形式上，序列建模是任何即生成函數 $f: X_{T+1} \rightarrow Y_{T+1}$ 執行輸入序列與輸出序列間的映射如式(1)

$$\widehat{y_0},\ldots,\widehat{y_T} = \mathrm{f}(x_0,\ldots,x_T) \tag{1}$$

假設式(1)滿足因果限制，就是$\widehat{y_T}$取決於先前序列資料 $x_0,\ldots,x_T$，而不是未來輸入 $x_{t+1},\ldots,x_T$。在序列建模設置f學習的目標是找到一個最小化函數，降低預期實際產出與預測序列間的損失，$L(y_0,\ldots,y_T, f(x_0,\ldots,x_T))$，其中序列輸出序列會滿足某種分佈型態。常見序列建模函數形式，以自我迴歸預測為例，給定先前資訊序列，通過目標函數映射，輸出為簡單的輸入資訊平移以預測可能的輸出。

（二）因果卷積（casual convolution）（Bai et al. 2018）

如上所述，TCN 資訊處理基於兩個原則：產生與輸入相同序列長度的輸出序列，時間 t 的元素輸出與先前歷史資訊完全相關，不能遺漏任何的先前過程中的任何資訊。要滿足第一點需求，TCN 使用一維完全卷積網絡（full convolutional network; FCN）架構，其中每個隱藏層長度都是與輸入層長度相同，長度為核長度 k-1（kernel size-1），以保持後續層與以前輸入資訊相同的長度。這種基本設計的主要缺點是會保存過多長期的歷史資訊，以滿足未來的輸出估算，但造成一個極端深度的網路架構（長度非常大的卷積過濾器）。為了要滿足第二點需求，TCN 使用因果卷積，卷積在時間 t 的輸出僅與來自時間 t 的元素和前一層中的(0,...,t-1)先前歷史資訊進行卷積運算萃取特徵運算 r 如圖 2 所示。

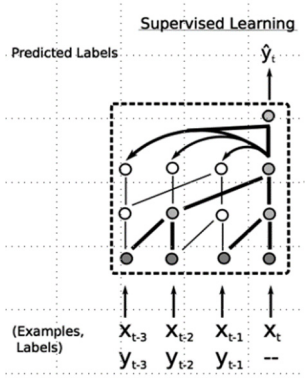

圖 2：因果卷積之基本架構（Firat et al. 2015）

（三）擴張卷積（dilated convolutions）（Bai et al. 2018）

擴張運算是在每兩相鄰濾波器引入一個固定的跳躍。基本上，一個簡單的因果卷積只能關聯前一級深度的歷史資訊，因果卷積應用實務時，須關聯更長時間歷史序列資訊的挑戰，此時可採用擴張卷積使擴大認知區域來因應。以公式表示，對於 1-*D* 序列輸入 $x \in R^{n}$ 和過濾器 $f: \{0,...,k\text{-}1\} \rightarrow R$，擴張卷積對序列的元素 *s* 的操作 *F* 定義為

$$F(s) = (x *_d f)(s) = \sum_{i=0}^{k-1} f(i).\, x_{s-d.i} \quad (2)$$

其中 d 是擴張因子，k 是濾波器大小，$s\text{-}d{\cdot}i$ 解釋了過去資料搜尋的方向。當跳躍步數為 1($d = 1$)時，擴張卷積成為一般正規卷積運算，當 $d \geq 2$ 有效地擴大輸入 ConvNet 的認知區域，因此使用較大的 d 值可以擴張輸出長度；由於 TCN 的感知區域大小取決於網路深度 n、濾波器大小 k 和擴張係數 d，選擇更大的濾波器長度 k 與擴張因子 d 可為 TCN 提供了兩個擴大認知區域因子的方法，此時卷積層的有效歷史資料維度增加為$(k\text{-}1)d$。此設計提供了兩種擴增認知區的方法：選擇更大的濾波器尺寸 k 並增加擴張因子 d，其中一個這樣的層的有效歷史是$(k–1)d$。使用擴張捲積關聯運算區域，能隨著網路的深度呈指數增長，意思即為，$d = 0^{(2i)}$，i 表示在網路的第 i 層，這確保過濾器可以處理到在有效範圍內命中每個輸入歷史資料，同時也允許極大的有效使用深度網路內的歷史資料（Firat et al. 2015）。

以圖 3 舉例說明，在圖 3(a)中，$F(1)$使用 1-dilated convolutions 認知區域為 3×3，在圖 3(b)中，$F(2)$使用 2-dilated convolutions 將原來認知區域擴大為 7×7，在圖 3(c)中，$F(3)$使用 4-dilated convolutions 將原來認知區域擴大為 15×15，認知區域面積呈現指數上升，可彈性處理不定長度的序列數據輸入。

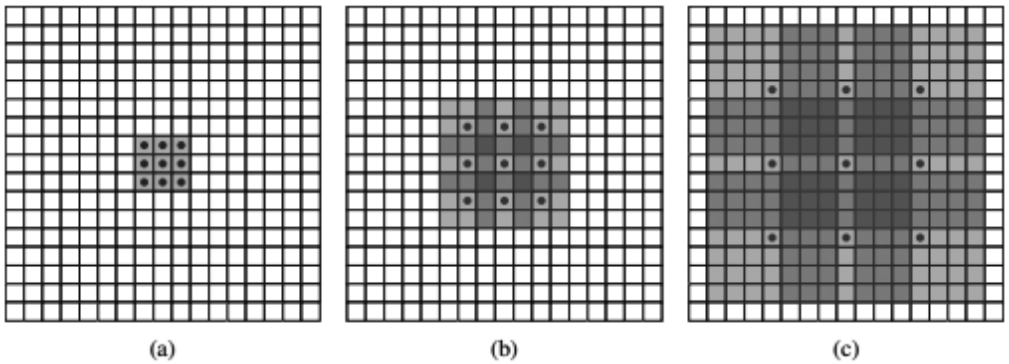

圖 3：時間卷積網路之擴張因果卷積運算（Yu & Koltun 2016）

（四）殘差連接（residual connections）（Bai et al. 2018）

殘差區塊（residual block）設計是屬於一回饋設計（feedback design），包含一個分支連接到一序列 $F(s)$轉換，如圖 4，其輸出 o 回饋至輸入序列 x 區塊

$$o = \sigma(x + F(s)) \tag{3}$$

如此連接設計將允許修正隱藏層之學習映射，而不是整個網路結構作轉換，已被證明有利於深層網路殘差的修正。

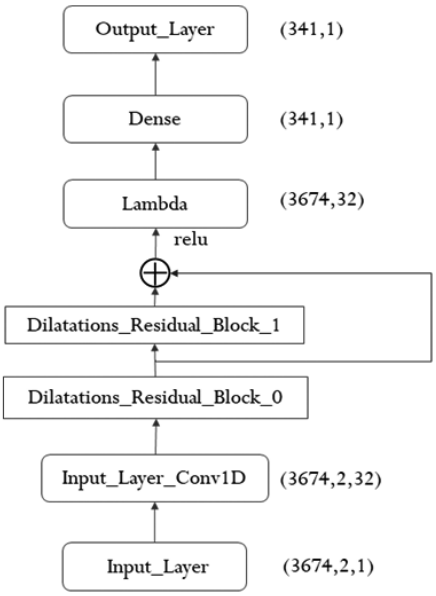

圖 4：時間卷積網路之殘差區塊設計

（五）注意力（attention model）（Mishra et al. 2018; Lea et al. 2017）

深度學習的注意力模型是模擬人腦的注意力行為，可從眾多資訊中過濾並擷取個人認為重要的資訊並加以記住，注意力函數之輸入資訊過濾擴張示意圖如圖注意力函數有兩個獨特的特徵：

1. 多次跳躍：不同於傳統 RNN 方法的每個句子只有一次讀取、解析輸入本文，多次跳躍讓系統可多次讀取、解析輸入句子，每次可能會關注某個名詞或動詞，在每一次反覆運算中可以更深入解析其含義。
2. 門檻控制：用來控制各隱藏層之間的資訊流，以控制過度訓練。在上下文解析過程中，通過對尺度控制篩選機制以記取重要資訊，以判斷那些先前重要資訊能用以預測下一個出現的詞句。

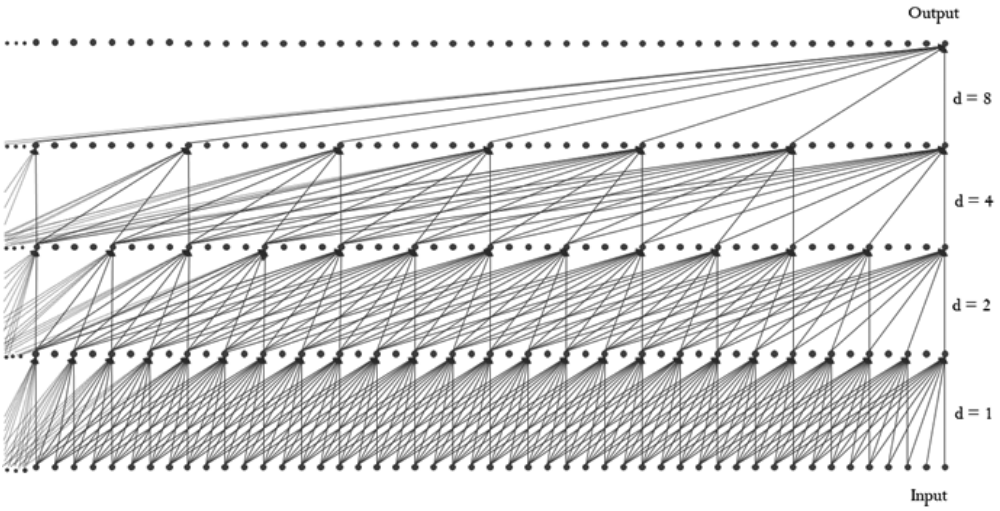

圖 5：時間卷積網路之輸入擴張過濾示意圖（Bai et al. 2018）

TCN 繼承注意力函數（attention function）處理技術，已成功加速機器翻譯為主的任務並被應用在大量序列資訊處理的問題上，成功解決長時間序列的特徵擷取問題。因此，長時間序列之特徵擷取問題不再是先前研發 RNN 的專屬領域，TCN 已成為未來專案的優先選項。

整理 TCN 優點與限制說明如下:（Bai et al. 2018）

三、TCN 優點

1. parallelism：在 TCN 中可進行大規模並行處理，網路訓練和驗證的時間都會較 RNN 短。
2. flexible receptive field size：TCN 設計提供一個可調變的感知區域（receptive field）大小，透過更多卷積層的堆疊、使用更大的膨脹係數（dilation factors）d 及增大濾波器大小（filter/kernel size）k，此一彈性設計可更容易來控制模型的記憶層長短，一般能使網路回饋環更短，故網路執行速度較 RNN 更快。
3. stable gradients：此外 TCN 的反向傳播路徑和序列的時間方向不同。這避免了 RNN 中經常出現的梯度爆炸或梯度消失（exploding/vanishing gradients）問題。
4. low memory requirement for training：訓練時需要的記憶體更少，尤其是對於長輸入序列處理。
5. variable length inputs：類似 RNN 輸入結構一樣，透過可循環多次輸入的方式對可變長度的輸入資料進行建模，TCN 也可以通過滑動一維卷積核來獲

取任意長度的輸入。這意味著可以採用 TCN 替換 RNN，應用於任意長度的順序數據的輸入與處理。

四、TCN 限制

TCN 在遷移學習方面可能沒有以影像處理專長的 CNN 適應能力那麼強。因為在不同的領域，模型預測所需要的歷史資訊量是不相同。因此，當將一個模型從一個對記憶資訊需求量少的問題，遷移到一個需要更長記憶的問題時，例如大量影像的處理，若硬體記憶體不足，則 TCN 可能會表現得很差，因為認知區域空間不夠大。

1. data storage during evaluation：在評估 / 測試中，RNN 僅需要維持隱藏狀態並接收當前輸入 x_t 以便生成預測；換句話說，整個歷史資料的摘要是由固定長度的向量集合 h_t 提供，並且可以丟棄過多觀察的序列資料。相反，TCN 需要將原始序列接收並儲存一定歷史長度的資料，故評估期間可能需要更多的儲存空間。
2. potential parameter change for a transfer of domain：不同的處理問題對模型所需的歷史記錄量會有不同的需求。因此，當僅需要很少儲存空間（即，較小 k 和 d 值）轉移到需要更大儲存空間（即，更大的 k 和 d 值），TCN 因可能因硬體限制，缺乏足夠大的感知區域空間，性能可能表現不佳。

參、研究方法

為能檢測複雜網路入侵攻擊，本研究針對時間序列性網路威脅資訊提出一個基於複合式深度學習為基礎之網路異常偵測模式，整合時間卷積神經網路（TCN）和卷積神經網路（CNN）兩種複合框架，強化網路入侵偵測辨識精確度。

一、架構設計

本研究究假設的模型是整合兩個深度學習框架與演算法（TCN 及 CNN），首先以 TCN 以萃取長時間序列資料之高頻出現的行為特徵，將多筆特徵向量形成特徵矩陣並轉會為圖像供 CNN 卷積學習，求取隱藏層特徵矩陣之最佳化權重，再運用 CNN 強大的圖像辨識能力執行類別映射，以協助 NIDS 落實自動化網路異常偵測。

參考 Google Brain 團隊的 RNN encoder-decoder 設計理念與 Lea 等（2017）建立的編碼 / 解碼為基礎之時間卷積網路（encoder-decoder temporal convolutional

network; ED-TCN)，本研究設定複合深度學習神經網路模型架構如圖 6 所示。特徵萃取主要由兩個 TCN 單元組成，第一層用於將輸入特徵數據進行編碼（encoding)，第二層是將經過編碼的序列數據透過訓練與比對，再將對應特徵向量轉變為一個固定大小的向量特徵值，經多次訓練後，將各類威脅行為特徵向量值組成一系列的特徵矩陣，透過數據轉圖像（B2M）演算法（韓曉光等 2014）輸出其特徵矩陣影像，以做為後續 CNN 影像辨識輸入。設計方法構想如下：

1. 加入 CICFlowMeter 協助工程師過濾可疑資訊流並即時過濾出對應 84 個重要欄位，外加上標記（label)，作為候選特徵集合（feature candidates）並自動轉換成文字 csv 格式，可大幅降低人力的負擔。
2. 再透過 TCN 執行特徵向量值計算可有效萃取出關鍵特徵做為 CNN 模式輸入，可降低人工方式誤判的機率。

經資料處理後的資料集分為訓練資料集與驗證資料集，訓練資料先由兩層 TCN 模型預訓練，再加入 CNN 模型四層隱藏層（二層時間卷積層、二層空間池化層）與分類層，最後由 Softmax 演算法區分出不同種類網路威脅與正常連線的機率。值得注意在 TCN 單元的輸出層適度控制資料遺棄比率（dropout)，可避免模型出現過度擬合（overfitting）問題，TCN-CNN 架構設計如圖 6 所示。

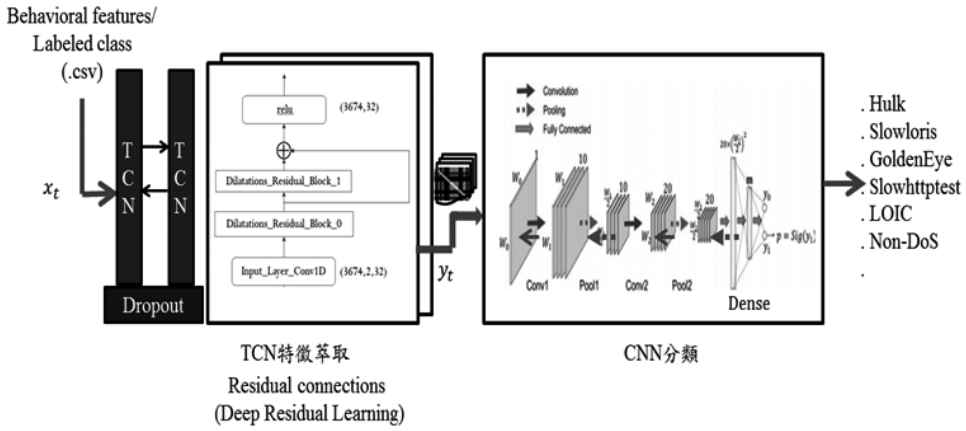

圖 6：TCN-CNN 架構設計

以 TCN-CNN 為基礎之網路入侵偵測的作業流程示意圖如圖 7 所示，模式設計是考量以下兩個因素：

第一行為特徵萃取：考量 TCN 處理輸入時間序列數據能力，但缺乏特徵分類處理能力，可作為前端處理器；第二影像分類：採用 CNN 的原因是考量 TCN 在遷移學習（transfer learning）上缺乏類似 CNN 同時輸入調適應與並行分類處理能

力，因為在不同的應用領域，模型預測所需要的歷史時間序列數據量可能不同，故不易彈性調整輸入認知區域，無法確保記憶所有相關的歷史資料做推論。

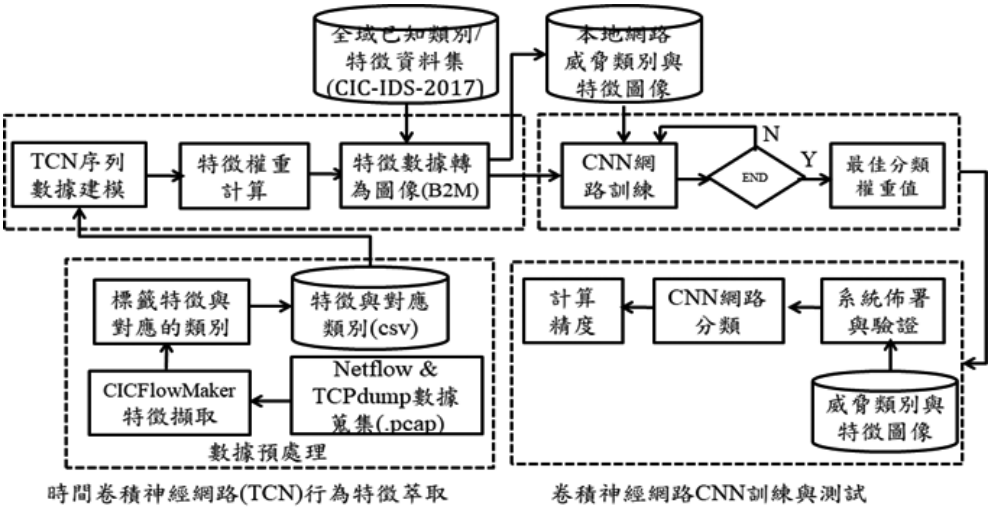

圖 7：應用 TCN-CNN 架構於網路異常行為特徵的萃取與辨識流程

由圖 7 可知，TCN-CNN 模式透過輸入不同時間 / 空間之特徵集合（temporal/spatialfeatures of malicious connections），透過 ED-TCN 的模型建構特徵萃取器以學習惡意連線重要欄位紀錄，針對時間序列數據透過因果卷積運算整理獲得對應的行為特徵向量，再將各類威脅行為特徵向量值組成特徵矩陣，以利 CNN 模式影像辨識出不同種類的威脅。

二、研究步驟

本研究過程將分為以下四個階段，詳如圖 7 所示。

（一）資料預處理（data preprocessing）

將國外全域威脅數據集 CIC-IDS-2017 及本地 DDoS 威脅數據集，運用資訊流的特徵提取器 CICFlowMeter 工具（Canadian Institute for Cybersecurity 2018）針對惡意連線資訊流取出資訊流重要欄位並做標記。

實作上，將採用加拿大 University of New Brunswick 提供網路開放資源 CIC-IDS-2017 數據集（廣域威脅）（Canadian Institute for Cybersecurity 2017; Sharafaldin et al. 2018）之行為特徵先作為模式預訓練（pre-training）學習歷史網路入侵的行為樣態，並搭配由國家南部高速網路中心取得本地網路入侵之惡意資訊流，透過 CICFlowMeter 工具轉化，訓練 TCN 以提升行為特徵網路入侵偵測模式之威脅辨

識，故規劃之實驗資料集來源包括 global intrusion dataset 及 local intrusion dataset 兩項：

1. global intrusion dataset：使用先前研究 CIC-IDS-2017 資料集，以預訓練方式（pre-training）學習先前廣域網路攻擊的入侵偵測行為特徵，找出網路入侵測的基本共同特徵。CIC-IDS-2017 數據集由 University of New Brunswick 建立，數據集包括多樣性攻擊，包括 2016 McAfee report 最常見的 13 種攻擊類別，此數據集中涵蓋的 web 攻擊、DoS、DDoS、infiltration、heart-bleed、bot 與 port scan 84 項網路行為特徵。
2. local intrusion dataset：與國家高速網路中心（國網中心）南區分院合作，於線上將本地網路連線威脅源之取樣的行為序列記錄下來，運用 tcpdump 工具對網路資訊流採用分散取樣及主機 port 下載 pcap 檔案，再運用 cfm 轉換 csv 格式（如圖 6），再運用資訊流的特徵提取器 CICFlowMeter 工具針對惡意連線資訊流取出資訊流重要欄位+標記，做為特徵候選集，特徵候選集為一個包括 84 個特徵的檔案（csv 格式）作為 TCN 模式訓練輸入，如圖 8 所示。

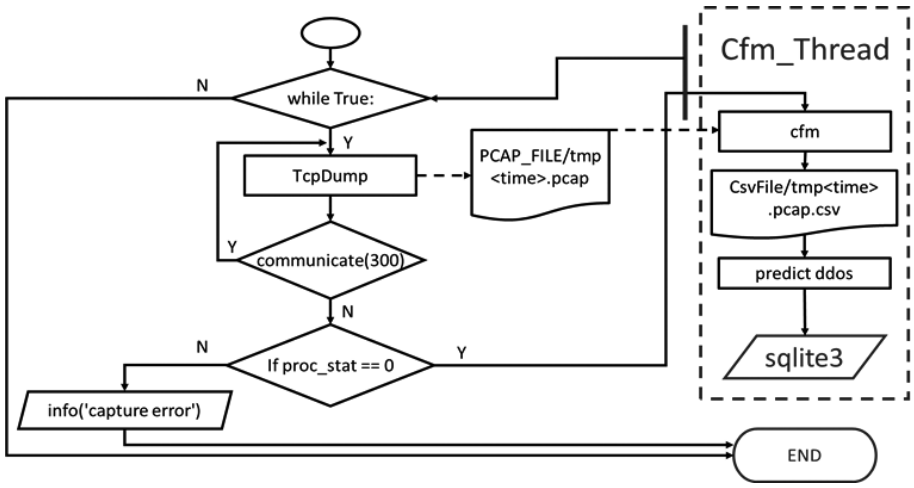

圖 8：程式 dataoreprocess：整合 tcpdump 工具蒐集資訊流 Pcap 與產出 csv 檔案特徵集

（二）特徵集篩選（feature selection）

透過決策樹 ID3 來輔助選擇資料集中候選的特徵（feature alternatives）的最佳子集。

基本上，應用較少威脅特徵允許更快的攻擊檢測，但亦可能會增加偽陽率（FPR）。為建立一個入侵預測模型，找到一組精簡的行為特徵（reduced

features）需要搭配在網路流檢測問題領域之相關實務知識與經驗。在構建模型時，資料集中候選的特徵（feature alternatives）的最佳子集可由決策樹 ID3 演算法（Witten & Frank 2005）來輔助選擇，屬性節點與分支透過在決策樹學習中對數據進行特徵分類與排列；ID3 算法以原始集合 S 作為根節點開始，在解決過程的每一此迭代中，演算法將重複加總集合 S 的每個特徵 A，的信息增益 $IG(A, S)$，並針對增益值大小進行排序。最後，集合 S 然後被所選擇的特徵屬性 A 分割以產生數據的子集。設定特徵屬性 A 的信息增益表示為 $IG(A, S)$，代表度量從集合 S 依據特定屬性 A 分割前後熵的差值。

$$IG(A,S) = H(S) - \sum_{t \in T} p(t)H(t)$$
$$H(S) = -\sum_{t \in T} p(t)\log_2 p(t) \tag{4}$$

其中熵 $H(S)$是資料集 S 中出現機率的度量，$p(t)$代表中單一特徵 t 在整個資訊流出現相對機率。

（三）模式訓練（model training）

降低萃取特徵誤差，TCN 模式訓練使用雙向學習方式，包括前饋傳播與逆向傳播雙向學習（back propagation Through Time; BPTT）。

假設給定 m 筆訓練輸入序列數據x_i={x_1,x_2,...,x_T}與輸出y_i={y_1,y_2,...,y_T}，若模型總體成本函數 C 為交叉熵（cross-entropy）函式，網路學習一個輸入到輸出的映射，映射函數 f_θ 被定義為 $\widehat{y_0}, \dots, \widehat{y_T} = f_\theta(x_0, \dots, x_T)$，$f_\theta = \sigma(W_o s_t + b_o) = \sigma(W_o[h_{t-1}, x_t] + b_o)$，$s_t$代表隱藏層，演算法目標要極小化輸入到輸出間估算誤差，以交叉熵損失的最小化作為成本函數

$$\text{Min } C = -\sum_{i=1}^{T} (\widehat{y_i} log \widehat{y_i} + (1 - \widehat{y_i}) \log(1 - \widehat{y_i})) \tag{5}$$

其中$\widehat{y_i}$為模式生成輸出的估計值。透過最大似然估計（maximun likelihood method），透過目標模型訓練使輸出估計值與疊代過程的輸出值誤差達到最小，以生成輸出$\widehat{y_0}, \dots, \widehat{y_T}$，從數學觀點，在 TCN模式參數 θ的所有可能值中尋找一個適合值，使得似然函數f_θ為最大值

$$\widehat{y_i} = \max_y f_\theta(y_t | y_{t-1}, s_t) \tag{6}$$

搜尋過程可透過逆向時間傳播演算法（BPTT）的疊代運算來獲得模式參數θ。為降低萃取特徵誤差，TCN 使用類似 LSTM 雙向學習方式，區分前饋傳播與逆向傳播雙向學習（back propagation Through Time; BPTT），透過

BPTT 雙向學習以防止誤差消失或爆炸，逆向傳播採用 BPTT 演算法採取以下三個步驟：

1. 前向傳播：前向傳播計算每個神經元的輸出值。
2. 逆向傳播：反向傳播計算每個神經元的誤差值，它是誤差函數 E 對每一神經元的加權輸入的偏導數。
3. 計算每個權重的梯度：最後再用隨機梯度下降演算法更新權重。

使用惡意連線或正常連線（良性）產生的靜態特徵圖像以訓練 TCN-CNN 分類模式精確度。

（四）性能評估（performance evaluation）

透過交叉驗證方法（cross validation scheme）搭配測試資料集，運用已訓練複合型時間卷積神經網路（trainedTCN-CNN）進行模式精度與誤判率評估。

肆、研究成果

本節使用 Python 語言發展環境，以人工智慧發展系統 TensorFlow 數值計算函式庫為平台，搭配 Keras、Anaconda 及 Numpy 深度學習函式庫來實現 TCN/CNN 神經網路模型。

一、資料前處理

本實驗環境架構如圖 9，攻擊主機為樹莓派 Pi3B+，網址為 10.10.0.10，路由器採用 Ubuntu 16.04 主機，網址為 10.10.0.1 及 192.168.2.1，受害主機為 Ubuntu 16.04 主機，網址為 192.168.2.201，映射主機為 Ubuntu 16.04 主機，網址為 192.168.2.203，入侵偵測主機為 Ubuntu 16.04 主機，網址為 192.168.200.1，整理本研究實驗使用軟硬體如表 2，實驗步驟分述如下：

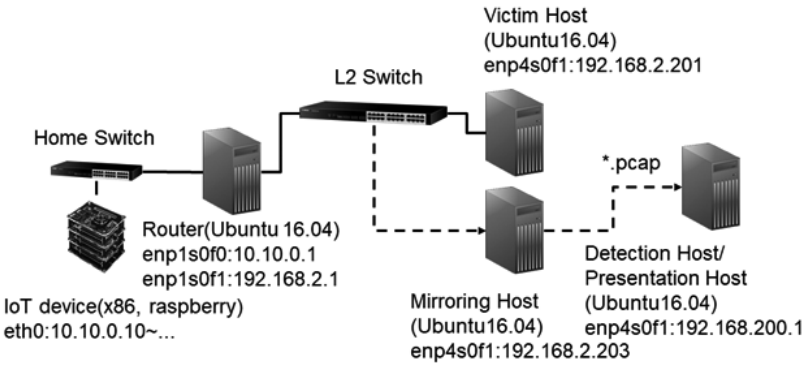

圖 9：攻擊網路資訊流分析環境

表 2：網路入侵偵測之偵測主機特徵分析軟體環境

	Processor	Model	Generation
CPU	AMD Ryzen Threaddripper (3.4GHz)	1920X	第一代
GPU	NVIDIA GTX-2080Ti		
OS	Ubuntu 14.04 LTS 64 位元		
RAM	32GB RAM DDR4		
Language	Python 3.5		
Libraries	TensorFlow-gpu 1.13、Keras 2.2.4、Numpy 1.18、Pandas 0.23.4、Openjdk-1.8、Bazel、Nvidia-driver 375.66、Nvidia-cuda 8.0、Nvidia-cudnn 5.1		
IDE	Anaconda Spyder		

（一）廣域網路入侵樣本

先應用已知網路威脅之共同特徵來執行網路威脅模式預訓練（pre-training）。本研究應用網路公開廣域網路威脅資料集 CIC-IDS-2017 的 84 個重要的候選行為特徵來預訓練模式，透過 TCN 學習廣域網路威脅的行為特徵，並調適 CNN 模式隱藏層的權重。接下來，以國家高速網路中心的骨幹網路獲得的本地惡意資訊流的行為進行分析與分類。

（二）本地網路入侵樣本

樣本來源主要由「國家網路高速中心」、「國家資通安全會報技術服務中心」之交流平台所提供惡意網路資訊流，實驗環境架構如圖 9。樣本取得日期：2018 年 12 月。本研究使用 tcodump 工具錄製惡意網路流資訊，再以 Tcpreplay（http://tcpreplay.appneta.com/）重放與確認攻擊者的攻擊情境及路徑，解析源端及目的端 IP、port、協定等，並錄製成 pcap 檔案（1Gbyte 切割為一單位，以利資料分批次處理），運用 CICFlowMeter-V4.0 工具（Canadian Institute for Cybersecurity 2018）進一步篩選出本地威脅重要的行為特徵，並標示攻擊類別與對應特徵欄位（csv 檔案），以利 TCN 輸入本地威脅特徵集合，以降低訓練複雜度。接下來，運用樹莓派 Pi3B+依序進行 DoS 及 DDoS 混合攻擊，攻擊類型包括 Hulk、Slowloris、GoldenEye、Slowhttptest、LOIC 交互攻擊，攻擊時每 3 分鐘收集一次攻擊流，在 mirror 主機搭配使用 tcpdump 與 libpcap-dev 將即時網路流進行錄製，待錄製時間成功後搭配 Pandas 函式庫進行型態轉換，區分三次實驗，每次約偵測到 30 萬筆 DDoS 攻擊結果如表 3，再將偵測攻擊依據攻擊行為分成四大

類，其中 GoldenEye、Slowhttptest 被歸類到 DDoS 攻擊，其餘 DoS 攻擊被正確分類，整理如圖 10，完成資料格式轉換成.csv 後，作為入侵偵測實驗的輸入。

表 3：DDoS 攻擊資料流之蒐集

資料流（pcap 格式）	資料流（csv 格式）	攻擊偵測到筆數	csv 轉換資料筆數	Tcpdump 接收筆數
2018-12-27 04:06:14.pcap	2018-12-27 04:06:14.pcap_Flow.csv	303,844	3,030,058	16,579,258
2018-12-27 04:10:14.pcap	2018-12-27 04:10:14.pcap_Flow.csv	309,789	2,607,136	14,502,914
2018-12-27 04:14:14.pcap	2018-12-27 04:14:14.pcap_Flow.csv	291,604	2,600,716	14,409,525

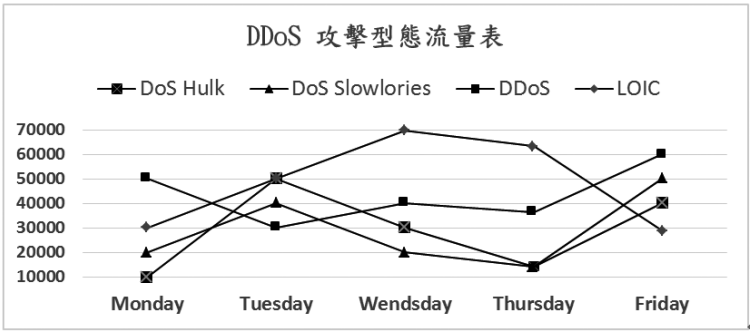

圖 10：攻擊網路流資訊之呈現（國網中心）

二、特徵萃取（feature extraction）

本研究應用與本地 DDoS 攻擊資料蒐集，根據決策樹 ID3 演算法信息增益（IG）度量正規化的評分進行特徵重要性的排序。依據方程式(4)的資訊增益方法的運算，從行為特徵後選集如表 4，比對本地的威脅特徵權重排序與 CIC-IDS-2017 的共同特徵，選出 16 個與 DDoS 威脅直接相關的特徵，代表應用 16 個行為特徵可區別出 DDoS 攻擊，故輸入層的特徵矩陣設計為 16×16 大小圖像矩陣。

表 4：實驗網路入侵之特徵子集評選

威脅特徵	權重
B.Packet Len Std	0.2028
B.Packet Len Min	0.0479

Flow Duration	0.0443
F.IAT Min	0.0378
Flow IAT Min	0.0317
B.IAT Mean	0.03
F.IAT Mean	0.0265
Fwd IAT Min	0.0257
Active Min	0.0228
Flow IAT Std	0.0227
Active Mean	0.0219
Flow IAT Mean	0.0214
Avg Packet Size	0.0162
SubflowF.Bytes	0.0007
Total Len F.Packets	0.0004
F.Packet Len Mean	0.0002

三、模式訓練與測試

（一）模式訓練

模式訓練過程最佳化成本函數經評估 Adamfunction（預設）、SGD 及 RMSprop，其中成本函數收斂誤差以 Adamfunction（預設）最佳，故選擇則 Adam 函數，架構參數之選定以 50 萬筆訓練資料和 10 萬筆測試資料在 kernel_size 為 10、疊代參數 batch_size 為 64、epoch 為 100，濾波器（types of filter）有 4 個選項 [16, 32, 64, 128]、擴張卷積（dilatations）有 3 個選項[d_0, d_1, d_2] 其中 d_0=[1, 2, 4] d_1 = [1, 2, 4, 8] d_2 = [1, 2, 4, 8, 16]、擴張卷積殘差（dilations-residual block）有 4 個選項 [6, 7, 8, 9]。

測試採用不同模式參數進行實驗，整理實驗訓練與測試的結果之精準度平均值如表 5，表 5 數據顯示，因成本函數的誤差收斂狀況佳，模式準確度達 95%以上，不同參數組合影響模式準確度不大，最後選定模式濾波器數目設定為 16，dilatations 設定為 d_0=[1, 2, 4]，擴張卷積殘差設定為 6。

在監督的機器學習算法中，期望在學習過程中最小化訓練樣本的誤差，通常是透過對成本函數的梯度下降來完成優化，並以損失函數（loss function）評估誤差下降速度與大小來判斷選擇參數是否朝向正確的方向，若誤差收斂不佳或有彈跳的現象，則須修改成本函數或模式參數，本實驗訓練過程之成本函數誤差下降如圖 11 所示，在 epoch 疊代 45 次後誤差下降達到穩定，故選定訓練模式參數如表 6。

表 5：TCN 模式參數實驗精度分析

	最大值	最小值	平均
訓練精準度	98.2%	97.1%	97.8%
測試精準度	96.7%	92.9%	95.1%
（訓練精準度+測試精準度）/2	97.45%	95.0%	96.4%

表 6：訓練模式架構的參數

algorithm	layers	neurons/ kernel	AF/LF	optimizer	epochs	batch-size
TCN-CNN 為基礎之網路入侵	TCN（2）	(18×16×176)	norm_Relu	*Adam*	100	64
	Dropout layer		-			
	Conv Layer	(10, 16, 16)	Relu/ CC-E			
	Conv Layer	(20, 8, 8)	Relu/ CC-E			
	Merge layer		-			
	Dense Layer	32	-			
	Output layer	2	Softmax			

AF=activation function, LF=loss function, CC-E=categoticalcross-entropy

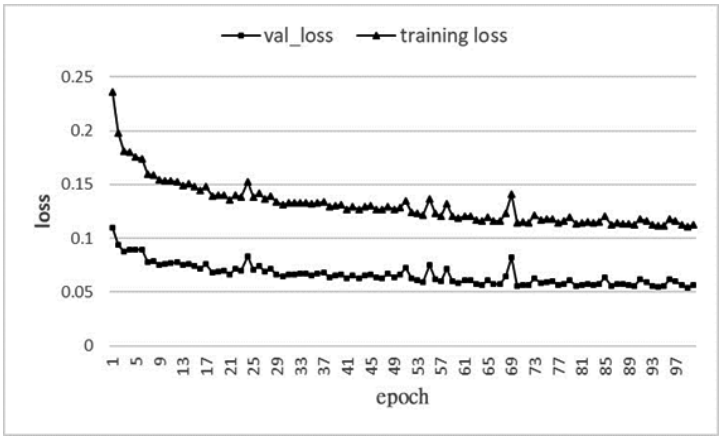

圖 11：TCN 模型訓練的誤差收斂

（二）模式測試

將測試資料輸入執行卷積神經網路模型測試進行威脅分類，判斷成本函數值是否低於設定下限，如果成本函數誤差值高於下限，則保存參數後微調重複進行疊代，直到低於下限或到達最大迭代次數。

四、模式性能評估與比較

（一）性能評估

為測試 DoS 威脅模型分類的性能，訓練階段必須包括 DoS 威脅與非 DoS 兩類型態資料，其中 DoS 攻擊資料集進一步在細分成五個子類，分類樣本及數量詳如表 7，以利機器學習不同特徵。模式訓練採用 500,000 筆（5/6）DoS 威脅與非 DoS 兩類交錯資料，模式訓練準確度達到 97.8%，再運用 100,000 筆（1/6）進行測試，模式測試準確度達到 95.1%，實驗結果詳如表 8。

值得注意，若測試資料中去除 Non-DoS 資料，只剩 DoS 威脅單一類資料進行模式訓練，因缺乏正常資訊流的行為特徵，容易將正常資訊流誤判為惡意資訊流，故模式訓練準確度降為 73.37%，測試損失誤差提高至 1.1257，故確認模式訓練資料須加交叉使用 DoS 與非 DoS 兩類威脅型態數據，模式才能學習不同特徵，在入侵偵測時才能正確辨識。

表 7：CIC-IDS-2017 DoS 五類網路威脅之訓練與測試資料

records / attacktypes	no of records in CIC-IDS-2017	training data	testing data
non-DoS	2,449,646	196,209	24,052
DoS hulk	230,124	184,099	46,025
DoSslowloris	5,796	4,637	1,159
DoSslowhttptest	5,499	4,399	1,100
DDoS	128,027	102,422	25,605
DoSGoldenEye	10,293	8,234	2,059

表 8：CIC-IDS-2017 資料集分類於實驗精確度統計

階段	資料量（筆）	損失值（loss）	準確度（%）
模式訓練	500,000	0.064	97.8
模式測試	100,000	0.349	95.1
模式交叉驗證	500,000	0.327	94.6

完成系統測試後，為避免模式過度訓練（over-fitting），將訓練資料進行 *k*-fold 交叉驗證，其中 *k* 值為 2~6 進行驗證，並將結果依照各 *k* 值成功率高低進行比較，驗證準確度如表 9，測試驗證準度為 94.56%。

表 9：各 k-fold 平均驗證準度

k-fold	Epoch	損失值（loss）	準確度（%）
2	100	0.3055	94.20
3	100	0.3142	94.50
4	100	0.3113	94.80
5	100	0.3168	94.90
6	100	0.3893	94.40
平均	100	0.32742	94.56

（二）模式架構的選擇

以下比較現有的時間序列處理的深度學習模式，包括遞迴神經網路（RNNs）、長短期記憶網路（LSTM）、門檻遞迴圈單元（GRU），以確認所研提的 TCN 性能較先前三類時間序列處理模型較佳，首先整理先前研究心得如下：

1. GNN 對序列性資料處理架構是採用循環一維輸入架構，不適採用並行處理架構與導入注意力函數，無法處理本案大量時間序列性資料（每次約 30 萬筆數據），經實驗無法使成本函數模型的訓練誤差收斂，故不適用於本案例。
2. Lea 等（2017）提出時間卷積網路模型（TCN）模型，使用時間卷積層來執行分割或檢測細步動作，搭配使用編碼器-解碼器（encoder-decoder）模式和擴張卷積機制有效地支持長程時間資訊萃取，使用時間卷積的層次結構來處理輸入資料細部的動作分割或識別，實驗證明 ED-TCN 能夠捕捉細部動作特徵與解決遠程依賴問題，並且比 LSTM 與 RNN 更快速的訓練神經網路。
3. Bai 等（2018）提出 TCN 搭配多隱藏層（卷積層與池化層）以進行大規模資料的並行處理架構，研究結果證明 TCN 網路訓練和測試的收斂時間均較 RNN 及 LSTM 短，同時展示了更長時間的有效資訊儲存與特徵記憶，同時保持與 LSTM 模式相同精確度。

以下以本案例資料，分析與比較 TCN/CNN 與 LSTM/CNN 及 GRU/CNN 三個混合模式性能。依據混淆矩陣定義，模型的性能期望是高精確度（accuracy）、低錯誤率與快速的收斂速度，錯誤率包括偽陽率（false positive rate; FPR）與偽陰率

（false negative rate; FNR）兩項，其中偽陽率 FPR=1-Specificity，偽陰率 FNR=1-Sensitivity，整理三個混合模式實驗結果如表 10。

表 10：時間序列資料之深度學習模式性能比較分析

指標模式參數	Precision（%）	Sensitivity（%）	Specificity（%）	Accuracy（%）	FPR/FNR（%）
LSTM/CNN（optimizer=RMSporp、學習率ξ=0.002）	86.9%	87.8%	98.0%	96.7%	2.0%/ 12.2%
GRU/CNN（optimizer=RMSporp、學習率ξ=0.01）	76.4%	75.1 %	96.4%	93.5%	3.60%/ 24.90%
TCN/CNN（optimizer=Adm）	95.0%	85.4 %	99.2%	97.2%	0.80%/ 14.60%

由表 10 可知，模式精確度以 TCN/CNN 最佳，LSTM/CNN 次之，GRU/CNN 最差；模式誤差（包括偽陽率及偽陰率）以 LSTM/CNN 最低，TCN/CNN 次之，GRU/CNN 表現最差；收斂速度則參考圖 12，觀察損失函數收斂過程，發現 TCN/CNN 收斂速度最快，LSTM/CNN 收斂過程產生震盪，GRU/CNN 震盪幅度更大且無法收斂，綜合表 10 與圖 12 結果，比較模式精確度、錯誤率與收斂速度，TCN/CNN 模式仍是時間序列資料之深度學習模式的最佳選擇，實驗結果與 Lea 等（2017）與 Bai 等（2018）研究結論相似。

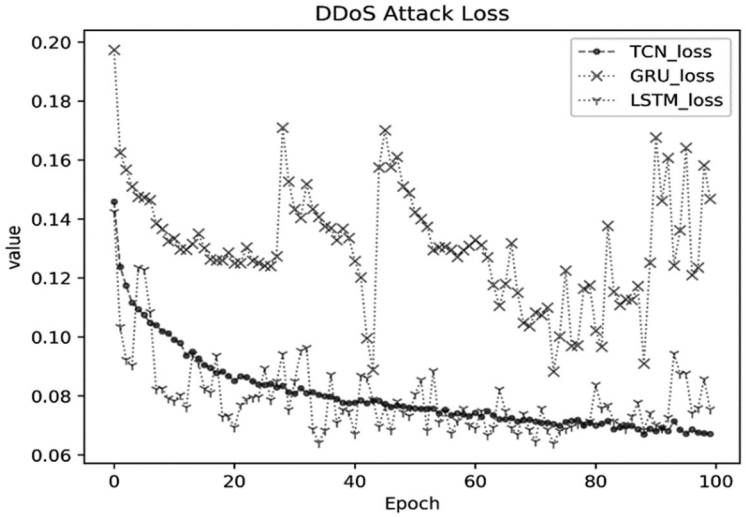

圖 12：三種模型訓練的損失函數收斂

伍、結論

本研究設計一個複合型 TCN-CNN 神經網路架構，應用 CIC-IDS-2017 與本地 DDoS 攻擊資料，搭配 CICFlowMaker 工具與決策樹 ID3 演算法分析網路流樣本中 DDoS 的攻擊行為特徵，實驗結果可即時辨識出網路入侵 94.56%DDoS 五類不同的威脅，協助雲端服務之管理者識別網路威脅。

本研究目前已完成部分深度學習網路環境建立與獲得初期研究成果，以機器學習方式來辨識已知 DDoS 威脅行為特徵，未來研究將朝向歸納共同行為特徵方式，運用正規化概念分析（formal concept analysis; FCA）建構網路威脅之知識本體模型（ontological model），並將其轉化為規則可應用於網路入侵偵測系統之威脅即時偵測，以機率顯示偵測多元混合型態攻擊及未知的攻擊，並提高入侵偵測偵測的精確度並降低誤判率。

誌謝

本研究承蒙行政院科技部計畫（編號：MOST 108-3116-F-168-001-CC2、MOST 108-2410-H-168-003）經費補助，謹此致謝。

參考文獻

鍾玉峰、張文鎰、蔡惠峰、蘇威智（2018），『基於深度學習之環境空污智能預測』，TANET 2018 臺灣網際網路研討會，頁 1185-1190，https://doi.org/10.6861/TANET.201810.0220。

韓曉光、曲武、姚宣霞、郭長友，周芳（2014），『基於紋理指紋的惡意程式碼變種檢測方法研究』，*通信學報*，第三十五卷，第八期，頁 125-136。

寇廣、湯光明、王碩、宋海濤、邊媛（2016），『深度學習在僵屍雲檢測中的應用研究』，*通信學報*，第三十七卷，第十一期，頁 114-128。

Bai, S., Kolter, J.Z. and Koltun, V. (2018), 'An empirical evaluation of generic convolutional and recurrent networks for sequence modeling', https://arxiv.org/abs/1803.01271.

Ding, L. and Xu, C. (2017), 'TricorNet: A hybrid temporal convolutional and recurrent network for video action segmentation', https://arxiv.org/abs/1705.07818.

Firat, O., Aksan, E., Oztekin, I. and Vural, F.T.Y. (2015), 'Learning deep temporal representations for brain decoding', *Proceedings of the First International Workshop on Machine Learning in Medical Imaging (MLMMI 2015)*, Lille, France, July 11,

pp. 25-34, https://doi.org/10.1007/978-3-319-27929-9_3.

Gupta, D. (2017), 'Fundamentals of deep learning – Introduction to recurrent neural networks', *Analytics Vidhya (2107)*, https://www.analyticsvidhya.com/blog/2017/12/introduction-to-recurrent-neural-networks/.

Hochreiter, S. and Schmidhuber, J. (1997), 'Long-short term memory', *Neural Computation*, Vol. 9, No. 8, pp. 1735-1780.

Kandpal, A. (2018), 'Generating text using an LSTM network', https://codeburst.io/generating-text-using-an-lstm-network-no-libraries-2dff88a3968.

Kang, M.-J. and Kang, J.-W. (2016), 'Intrusion detection system using deep neural network for in-vehicle network security', *PLoS ONE*, Vol. 11, No. 6, pp. e0155781, https://doi.org/10.1371/journal.pone.0155781.

Lea, C., Flynn, M.D., Vidal, R., Reiter, A. and Hager, G.D. (2017), 'Temporal convolutional networks for action segmentation and detection', *Proceedings of the 30th IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2017)*, Honolulu, HI, USA, July 21-26, pp. 1003-1012.

Mishra, N., Rohaninejad, M., Chen, X. and Abbeel, P. (2018), 'A simple neural attentive meta-learner', *Proceedings of the 6th International Conference on Learning Representations (ICLR 2018)*, Vancouver, BC, Canada, April 30-May 3, https://arxiv.org/abs/1707.03141.

Niyaz, Q., Sun, W., Javaid, A.Y. and Alam, M. (2015), 'A deep learning approach for network intrusion detection system', *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, New York, NY, USA, December 3-5, pp. 21-26.

Canadian Institute for Cybersecurity (2017), 'Intrusion detection evaluation dataset CSE-CIC-IDS2017', University of New Brunswick, NB, Canada, https://www.unb.ca/cic/datasets/ids-2017.html.

Canadian Institute for Cybersecurity (2018), 'CICFlowMeter', University of New Brunswick, NB, Canada, https://github.com/ahlashkari/CICFlowMeter.

Saxe, J. and Berlin, K. (2015), 'Deep neural network based malware detection using two dimensional binary program features', *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE 2015)*, Fajardo, PR, USA, October 20-22, pp. 11-20, https://arxiv.org/abs/1508.03096v2.

Sharafaldin, I., Lashkari, A. and Ghorbani, A. (2018), 'Toward gnerating a new intrusion detection dataset and intrusion traffic characterization', *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP*

2018), Funchal, Portugal, January 22-24, pp. 108-116.

Tan, Z.Y. (2013), 'Detection of denial-of-service attacks based on computer vision techniques', Unpublished Ph.D. dissertation, University of Technology, Sydney, Australia.

Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R. and Ghogho, M. (2016), 'Deep learning approach for network intrusion detection in software defined networking', *Proceedings of the International Conference on Wireless Networks and Mobile Communications* (*WINCOM '16*), Fez, Morocco, October 26-29, pp. 258-263, https://doi.org/10.1109/WINCOM.2016.7777224.

Tomiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T. and Yagi, T. (2016), 'Malware detection with deep neural network using process behavior', *Proceedings of the 40th IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016)*, Atlanta, GA, USA, June 10-14, pp. 577-582.

Wang, Y., Cai, W.-D. and Wei, P.-C. (2016), 'A deep learning approach for detecting malicious JavaScript code', *Security and Communication Networks*, Vol. 9, No. 11, pp. 1520-1534.

Witten, I.H., Frank, E. and Hall, M.A. (2011), *Data Mining: Practical Machine Learning Tools and Techniques (3rdedition)*, Morgan Kaufmann, Burlington, Massachusetts, USA.

Yan, J.-E., Yuan, C.-Y., Xu, H.-Y. and Zhang, Z.-X. (2013), 'Method of detecting IRC botnet based on the multi- features of traffic flow', *Journal on Communications*, Vol. 34, No. 10, pp. 49-64, https://doi.org/10.3969/j.issn.1000-436x.2013.10.006.

Yu, F. and Koltun, V. (2016), 'Multi-scale context aggregation by dilated convolutions', *Proceedings of the 4th International Conference on Learning Representations (ICLR 2016)*, San Juan, PR, USA, May 2-4, pp. 1-13, https://arxiv.org/abs/1511.07122.