Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

基於卷積神經網路的低速阻斷服務攻擊檢測

蔡旻諺[1]、徐禾瀚[2]、卓信宏[3*]
[1,2,3]國立宜蘭大學資訊工程系
[1]wer9u623@gmail.com、[2]hhann95@gmail.com、[3]hhcho@niu.edu.tw

摘要

低速阻斷服務攻擊(Low-Rate Denial-of-Service, LDoS)是低運算能力的環境中常面臨攻擊手段，在此環境中，攻擊者可以將攻擊封包隱藏在足夠低速率的資料流當中以逃避檢測使得檢測的困難度被大幅提高，使得傳統的方法會因為資料量不夠多元導致無法順利提取特徵而無法精準識別攻擊者，為了改善此問題，本文採用人工智慧的卷積神經網路(Convolutional Neural Network, CNN)以達到更好的全域搜索，實驗結果表明，本文所提之方法可以有效地檢測出 LDoS 攻擊。

關鍵詞：低速阻斷服務攻擊、入侵偵測系統、卷積神經網路

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

Low-Rate Denial-of-Service detection based on Convolutional Neural Network

Min-Yan Tsai[1]、Augustine Sii Ho Hann[2]、Hsin-Hung Cho[3*]
[1,2,3]Department of Computer Science and Information Engineering, National Ilan University
[1]wer9u623@gmail.com、[2]hhann95@gmail.com、[3]hhcho@niu.edu.tw

Abstract

Low-Rate Denial-of-Service (LDoS) is an attack method often faced in environments with low computing power. In this environment, attackers can hide attack packets in sufficiently low-rate data streams to escape detection has greatly increased the difficulty of detection, which makes traditional methods unable to extract features smoothly due to insufficient data and cannot accurately identify attackers. In order to improve this problem, this article uses artificial intelligence convolutional neural networks (CNN) to achieve stronger global search, the experimental results show that the method proposed in this article can effectively detect LDoS attacks.

Keywords: Low-Rate Denial-of-Service, Intrusion Detection System, Convolutional neural networks

壹、前言

隨著移動通信技術的迅猛發展，目前第三代合作夥伴計劃(3rd Generation Partnership Project, 3GPP)已提出了與第五代(5th Generation Mobile Networks, 5G)移動通信技術相關標準，這表明移動通信系統今後將從傳統的 LTE(Long Term Evolution)網路演進到 5G 網路。而在未來的 5G 網路中，會促進許多行業的發展，如物聯網[1]、遠端醫療[2]等應用。而目前低功耗廣域網(Low-Power Wide-Area Network, LPWAN)已被廣泛認為將會是物聯網領域最有前途的技術之一 ,在 IoT Analytics 的報告中表示預計 LPWAN 設備連接數量在 2018-2025 年期間的複合年增長率(Compound Annual Growth Rate, CAGR)將達 81% [3]。據 Machina 比較其他 LPWAN 的情況，到 2025 年，僅窄帶物聯網(Narrow Band Internet of Things, NB-IoT)的份額將達到 48% [4]。根據另一項統計，IHC 建議到 2021 年 NB-IoT 連接的數量將為 1.417 億[5]證明物聯網的應用上有著巨大的潛力，然而物聯網硬體設備計算能力有限，無法防範關於安全性的問題，容易被駭客當成跳板製造惡意攻擊，因此物聯網設備的安全性是一個非常重要的議題[6]。而近年來常見的一種攻擊手段是阻斷服務攻擊(Denial of Service Attack, DoS)，但由於 DoS 的特徵明顯，常常在第一道防火牆就被偵測出來。故低速阻斷服務攻擊(Low-Rate Denial-of-Service, LDoS)則在此種環境中變成主要攻擊手段[7]，在此環境中，攻擊者可以將攻擊封包隱藏在足夠低速率的資料流當中以逃避檢測使得檢測的困難度被大幅提高[8]。

本文的結構如下：第二節將會介紹與本研究背景知識以及簡述相關文獻，第三章則會將會介紹我們使用 CNN 建立攻擊檢測的流程細節，結果分析結論將會在最後兩節進行介紹。

貳、背景介紹及相關文獻

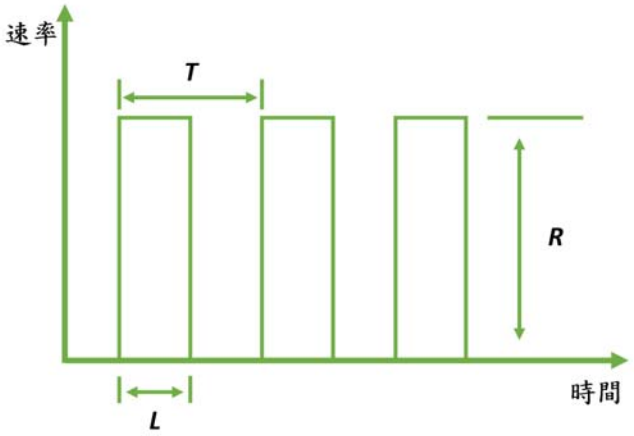
2.1 入侵偵測系統

入侵檢測系統在現代計算機基礎架構中至關重要，是網路管理者檢測網路內部各種安全漏洞的重要且應用非常普遍的工具。目前有許多研究者投入大量精力研究如何建立有效的入侵檢測系統來檢測網路空間安全。而隨著這些年機器學習科技持續的快速成長，研究學者證實使用機器學習算法訓練入侵檢測資料可有效提升準確性能。[9]提出可一種改進的 K-近鄰演算法(TCM-KNN)來訓練，能夠用在少量資料的情況下到達有效的網路入侵資料檢測。[10]提出了一種基於支持向量機(support vector machine, SVM)的入侵檢測技術以達到減少訓練時間的效果，在提供並不多的先驗知識的情況下實現了較高的準確性。為了實現更高的準確率，[11]提出利用 KNN 配合 K 平均演算法(k-means clustering)來進行入侵檢測，在此模型中，網路攻擊的群集中心由 k 均值獲取，並使用 KNN 分類

器進行網路入侵檢測。測試結果顯示，這種方法要比單獨 KNN 的模型優秀，甚至準確率要比 SVM 模型高。[12]提出了一個決策樹的網路入侵檢測模型。在此方法中，由遺傳算法來選擇決策樹模型的特徵子集,最後實驗表明這種方法能夠有效地提高檢測率。

2.2 低速阻斷服務攻擊

傳統的阻斷服務攻擊追求愈來愈高的攻擊速率，透過大流量的封包來引起目標的伺服器癱瘓或是導致該網路之壅塞,，針對這種異常的流量增加，很容易檢測到這些攻擊。低速阻斷服務攻擊(Low-Rate Denial-of-Service, LDoS)攻擊是阻斷服務攻擊的一種特殊形式，其攻擊手段是採取週期性傳送少量封包來消耗目標伺服器的大量資源。所以 LDoS 並不會盲目的追求攻擊速率，因此在滿足一定的破壞性的同時，也盡可能減少被發現的機率。常見的低速阻斷服務攻擊模型如圖一所示，其中 R 為攻擊的脈衝強度，L 表示攻擊持續的時間，T 表示攻擊的週期。



圖一: LDoS 攻擊模型

2.3 卷積神經網路

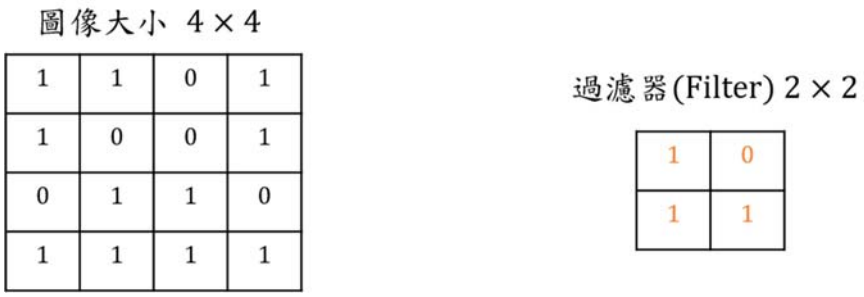
積神經網路(Convolution Neural Network, CNN)是當今深度神經網路(Deep Neural Network, DNN)領域的研究主力，在圖像或者聲音的辨識方面都有較佳的結果。卷積神經網路的結構主要由以下三個主要部分所組成:

卷積層(Convolution Layer): 卷積層運用一個或多個過濾器(Filter)和輸入矩陣來訓練權重，這些過濾器彼此與本層的輸入進行卷積(convolution)計算以萃取特徵。運用卷積層的目的就是萃取輸入的不一樣特徵。下面將簡要介紹卷積層的計算方法，圖二所示為假設有一個 4×4 的圖像大小的輸入矩陣及一個大小為 2 的過濾器，通過對圖片做卷積計算方式的過程如圖三所示。運算方法為將輸入矩陣的值與濾波器值相乘後的結果再相加,相加後的數值會儲存在特徵圖(Feature map) 上。依照步距(stride)為 1 步，會不停往右邊

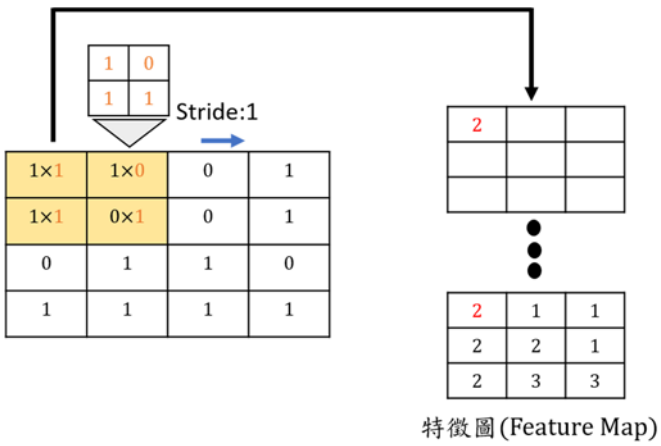
運算特徵值，最後會得到完全的特徵圖，即為該過濾器萃取到的特徵。

池化層(Pooling Layer): 目的是將上述卷積層所輸出的特徵圖縮減，在縮減資料量的同時也保留了主要的特徵，達到加快訓練模型的效果。常用的池化層分為兩種，最大池化(Max Pooling, MP)以及平均池化(Average Pooling, AP)。取樣的方法同樣是使用一個指派大小的過濾器(Filter)，透過如圖四所示最大池化會取出過濾器中最大值而如圖五所示平均池化則會將過濾器中的值加總後取出平均值。

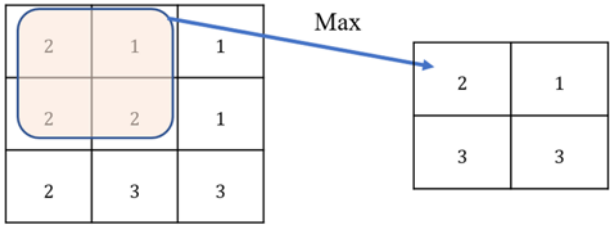
全連接層(Fully Connected Layers, FC): 全連接層是將前一層的輸出去做攤平處理，一般會在卷積神經網路最後的幾層才使用全連接層，可達到學習到更多資訊的效果，與傳統神經網路相同，個個全連接層的神經元都跟前一層全部神經元進行連接。全連接層裡各個鏈接點之間會施加隨機的權重值，透過卷積處理獲得的特徵值跟全連接層進行相乘計算後，會獲得對於預測結果的機率，若是預測錯誤，則會按照誤差以使用反向傳播法去進行參數的修正。



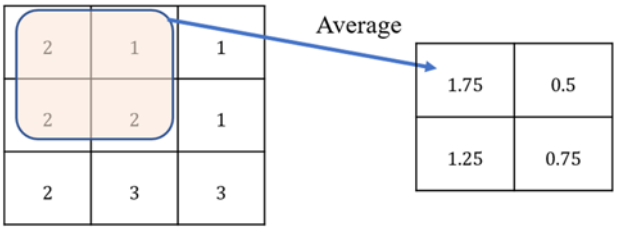
圖二:圖像大小與過濾器矩陣圖



圖三:卷積計算示意圖



圖四:最大池化運算



圖五:平均池化運算

參、卷積神經網路檢測方法

首先我們匯進行資料預處理(Data Preprocessing)，此步驟為機器學習的重要組成部分，同時也是較為耗費時間的任務。為了讓訓練模型可以有效的學習資料集內獨一無二的特徵，以提升在訓練過程的結果，需在模型輸入訓練資料集前仔細檢驗查看資料集內是不是具有不利於模型學習的特徵。最大限度的降低因訓練資料集的缺陷而導致模型在預測或學習階段時的準確率和精確率(Precision)下降。以本論文所使用的 CICIDS2017 資料集為例，該資料集由加拿大網絡安全研究所於 2017 年發布，囊括多種最新的網絡攻擊類型，記錄了 14 類不同的網路攻擊，並且更接近於真實的現代網路流量，此資料集包含包含了 Force Attack、Heartbleed Attack、Botnet、DoS Attack、Web Attack 等攻擊，資料集詳細信息如表一所示，主要來識別序號 6 的 DoS Slow-httptest 以及序號 7 的 DoS slowloris，這兩種攻擊資訊皆為 LDOS。雖然這份資料集已經相當完備，不過在進行資料集的特徵處理時，便會發現到這份資料集內還是有不適合學習的缺值，下邊介紹本論文的解決方式。首先是資料集內的空缺值，空缺值會直接導致模型學習資料特徵的能力下降，為了解決此資料集缺陷問題，我們找出資料集內的空缺值，並將空缺值以 0 補上，表二展示了一筆資料的詳細信息，而訓練資料特徵格式如表三所示。

表一: CICIDS2017 資料集攻擊種類

序號	正常/攻擊標籤	數量	百分比
1	BENIGN	300000	34.97951%
2	Bot	1966	0.229232%
3	DDoS	128027	14.92774%
4	DoS Golden Eye	10293	1.200147%
5	DoS Hulk	231072	26.94262%
6	DoS Slow-httptest	5499	0.641174%
7	DoS slowloris	5796	0.675804%
8	FTP-Patator	7938	0.925558%
9	Heartbleed	11	0.001283%
10	Infiltration	36	0.004198%
11	PortScan	158930	18.53098%
12	SSH-Patator	5897	0.687581%
13	Web Attack-Brute Force	1507	0.175714%
14	Web Attack-Sql Injection	21	0.002449%
15	Web Attack-XSS	652	0.076022%

表二: CICIDS2017 資料示例

49486,1,2,0,12,0,6,6,6,0,0,0,0,0,12,2,1,0,1,1,1,1,0,1,1,0,0,0,0,0,0,0,40,0, 2000000,0,6,6,6,0,0,0,0,0,0,1,1,0,0,0,2326,6,0,40,2,12,0,0,245,-,1,20,0, 0,0,0,0,0,0,0,BENIGN

除此之外，CICIDS2017 資料集還有不少極小值與極大值存在，使得資料集中各個特徵的值差別很大。若模型在訓練時的特徵數值特別大，則會導致模型在訓練時只會學習到值比較大的資料特徵並忽略值比較小的資料特徵，這肯定會導致了大量的特徵缺失，為了促使分類結果越加準確，必須對資料集進行標準化處理，使用的是最小值最大值正規化方法，將資料按比例映射到[0,1]區間中，可利用下面公式進行轉換:

$$x_{new} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

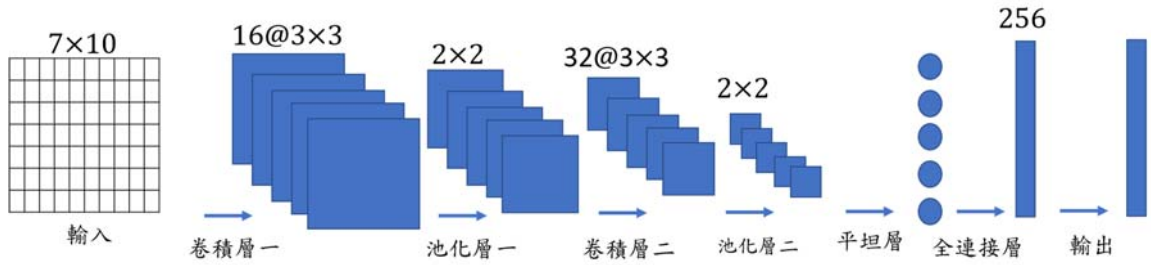
其中 x_max 與 x_min 分別為資料中的特徵最小值與特徵最大值，公式(1)是將所有特徵和特徵最小值之間的差值，其差值除於特徵最大值和特徵最小值的差值，計算出來的數值介於[0,1]。

表三:訓練資料特徵格式

序號	特徵名稱	序號	特徵名稱
1	Destination Port	36	Bwd Packets
2	Flow Duration	37	Min Packet Length
3	Total Fwd Packets	38	Max Packet Length
4	Total Backward Packets	39	Packet Length Mean
5	Total Length of Fwd Packets	40	Packet Length Std
6	Total Length of Bwd Packets	41	Packet Length Variance
7	Fwd Packet Length Max	42	FIN Flag Count
8	Fwd Packet Length Min	43	SYN Flag Count
9	Fwd Packet Length Mean	44	RST Flag Count
10	Fwd Packet Length Std	45	PSH Flag Count
11	Bwd Packet Length Max	46	ACK Flag Count
12	Bwd Packet Length Min	47	URG Flag Count
13	Bwd Packet Length Mean	48	CWE Flag Count
14	Bwd Packet Length Std	49	ECE Flag Count
15	Flow Bytes	50	Down/Up Ratio
16	Flow Packets	51	Source Port
17	Flow IAT Mean	52	Avg Fwd Segment Size
18	Flow IAT Std	53	Avg Bwd Segment Size
19	Flow IAT Max	54	Fwd Header Length
20	Flow IAT Min	55	Subflow Fwd Packets
21	Fwd IAT Total	56	Subflow Fwd Bytes
22	Fwd IAT Mean	57	Subflow Bwd Packets
23	Fwd IAT Std	58	Subflow Bwd Bytes
24	Fwd IAT Max	59	Init_Win_bytes_forward
25	Fwd IAT Min	60	Init_Win_bytes_backward
26	Bwd IAT Total	61	act_data_pkt_fwd
27	Bwd IAT Mean	62	min_seg_size_forward
28	Bwd IAT Std	63	Active Mean
29	Bwd IAT Max	64	Active Std
30	Bwd IAT Min	65	Active Max
31	Fwd PSH Flags	66	Active Min
32	Fwd URG Flags	67	Idle Mean
33	Fwd Header Length	68	Idle Std
34	Bwd Header Length	69	Idle Max
35	Fwd Packets	70	Idle Min

進行資料預處理以及標準化後共有 70 個特徵，資料集匯入卷積網路的時候會把它變成類似圖片的 XY 軸，將 70 個特徵改變成 7x10 的二維規格矩陣作為卷積網路的輸入，模型由兩個卷積層，使用兩層卷積層，卷積核大小均是 3，第一個卷積層的卷積核數量為 16，第二個卷積層的卷積核數量 32，這種加多卷積核數量的方法能夠把輸出特徵值投射到高維度的空間，以讓神經網路學習到更多不一樣的特徵值，從而加強模型的學習能力。兩個池化層，卷積核大小均是 2。池化層主要是為了減少模型的參數量，以達到加快網路訓練的效果，但伴隨來的副作用是局部的特徵丟失。為了提高模型的分類準確度，使用了兩層平均池化(Average Pooling, AP)，使用平均池化是因為不同個的特徵資料點差距很大，就算已經將特徵標準化映射至(0,1)區間中，但對於資料分佈來說，資料內有的元素趨近於 0，一部分趨近於 1，如果使用最大池化的方式會造成趨近於 0 的特徵都會被拋棄，這就會造成分類的誤差從而降低準確度。一個全連接層最後連接輸出層，連接層一般連接在卷積層之後，目的是為了上一層學習到的特徵可以方便做輸出。

可以給予不同的神經元數量做學習，最後連接輸出層做輸出。每一層的激活函數都使用 Relu 函數。圖六所示。



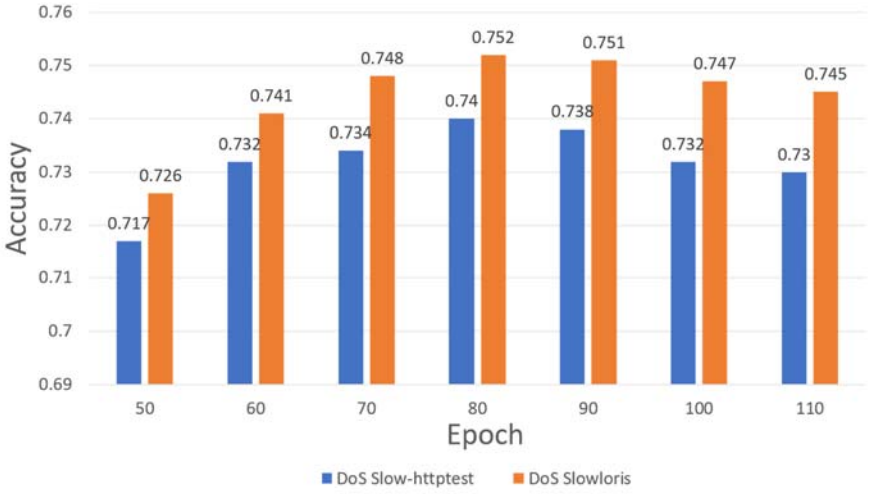
圖六: CNN 模型架構

肆、實驗結果與分析

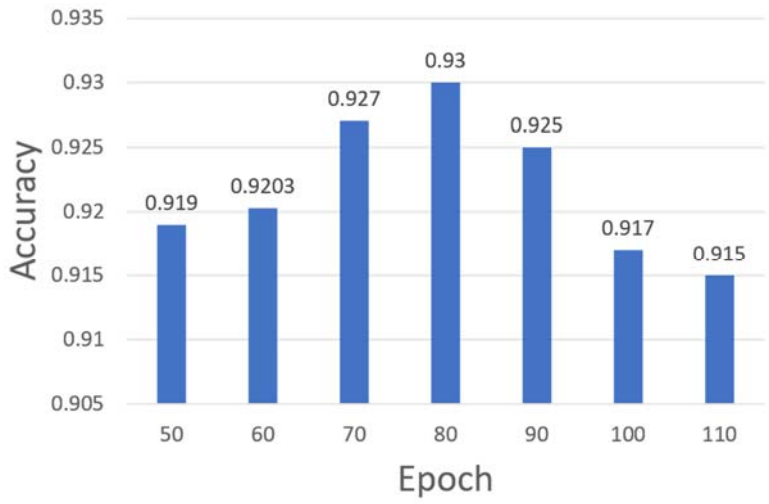
本實驗環境分為硬件環境與軟件環境兩種。其中，硬件環境為 Intel® Core™ i7-8700 處理器並搭載 NVIDIA GeForce GTX 1050 TI 顯示卡，並在 Windows10 作業系統中使用 NVIDIA CUDA 10.1, cuDNN v8.0.2 library 圖像處理器驅動，最後利用 Python 3.7.3 中的神經網路模組進行編程。CICIDS2017 訓練資料以全部資料的 90%進行訓練，剩下的 10%作為測試資料。

圖七顯示了 DoS Slow-httptest 以及 DoS Slowloris 這兩種攻擊在 Epoch 大小變化中的比較，以 50 到 110 遞增來測試結果。Epoch 在 50 以下訓練的次數太少，導致結果太差，在 90 到 110 時，準確度已經開始下降而且需要額外的訓練時間，在結果來說 Epoch 大小在 80 時結果最優。圖八表示在不同的 Epoch 下，分類所有攻擊的準確率，也和 DoS

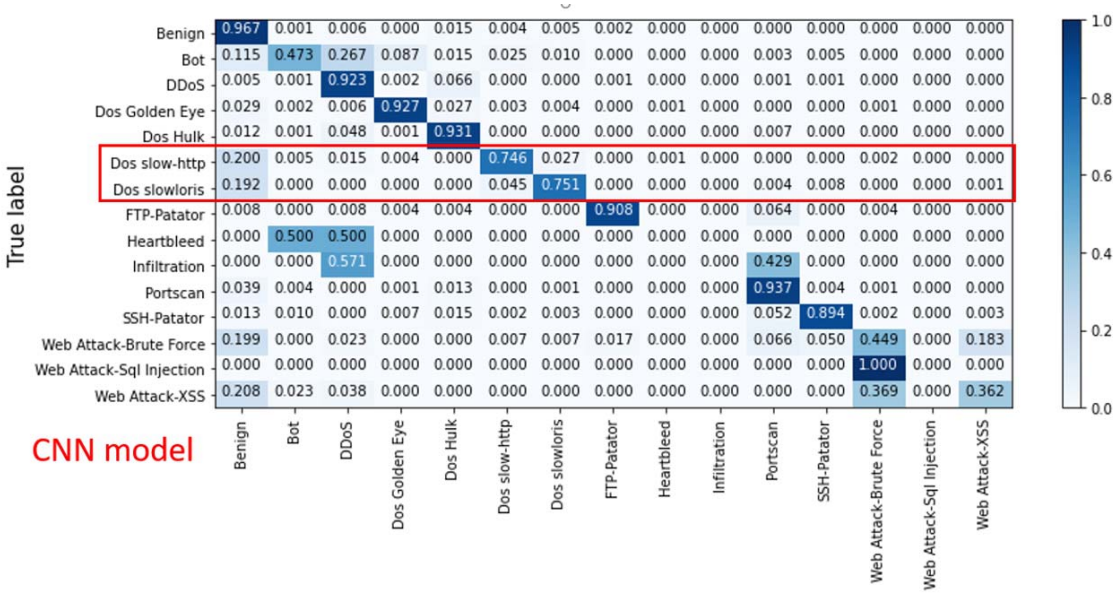
slow 攻擊時候一樣，Epoch 80 的時候準確度比較高。圖九為測試資料進行 CNN 模型分類之後出來的混淆矩陣(confusion matrix)，可以看出模型有著不錯的分類結果，而 Heartbleed，Infiltration 和 Web Attack 由於資料數較少，因為訓練過程中能夠學習的資料太少，間接的造成其分類相較其它攻擊來的更低。因為 LDoS 本身就會隱藏在一般流量中，非常難以識別，故本實驗的結果約為七成五，尚為可接受的範圍。



圖七: LDoS 攻擊獨立準確率



圖八: 全部類別攻擊準確率



圖九:混淆矩陣圖

伍、結論

隨着形形色色的攻擊手段的出现，目前的研究提出許多防禦系統和方法。近年用的防禦系統：入侵偵測系統、密碼學、防火牆等是目前網路安全的代表性技術，其中以入侵偵測系統是網路安全技術中一個熱門的研究領域，在入侵的攻擊中，許多攻擊類別都擁有顯著的特徵，但是 LDoS 可以與一般流量非常接近，故非常難以識別，本研究利用 CNN 作為主要是別技術，可以在 DoS Slow-httptest 以及 DoS Slowloris 攻擊中獲得 75% 的正確率，其餘的攻擊也都能達到不錯的辨識率。

[誌謝]
本研究接受科技部編號：108-2221-E-197-012-MY3 研究計畫經費補助。

參考文獻

[1] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu and X. Du, “From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies,” *IEEE Communications Standards Magazine*, vol. 56, no. 10, pp. 114-120, October 2018.

[2] H. Magsi, A. H. Sodhro, F. A. Chachar and S. A. Abro, "Evolution of 5G in Internet of medical things," *in International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, March 2018.

[3] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B–Market accelerating," 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[4] Babla, C., "Cellular IoT and LPWAN - addressing the industry FUD," 2017. [Online]. Available: https://community.arm.com/iot/b/internet-of-things/posts/cellular-iot-and-lpwan-_2d00_-addressing-the-industry-fud.

[5] L.Ratliff, S.Lucero, "ARM elbows its way into an already crowded NB-IoT semiconductor market," 2017. [Online]. Available: https://technology.ihs.com/589151/arm-elbows-its-way-into-an-already-crowded-nb-iot-semiconductor-market.

[6] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi and Y. Jin, "Security analysis on consumer and industrial IoT devices," *in 21st Asia and South Pacific Design Automation Conference*, pp. 519-524, 2016.

[7] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe and A. Skarmeta, "5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks," *Security and Communication Networks*, vol. 2018, pp. 1-21, December 2018.

[8] J. Brynielsson and R. Sharma, "Detectability of Low-Rate HTTP Server DoS Attacks using Spectral Analysis," *in IEEE Conference on Advances in Social Networks Analysis and Mining*, pp. 954-961, August 2015.

[9] Y. Li and L. Guo, "An active learning based TCM-KNN algorithm for supervised network intrusion detection," *Comput. Secur*, vol. 26, no. 7, pp. 459-467, 2007.

[10] C. Tang, Y. Xiang, Y. Wang, J. Qian and B. Qiang, "Detection and classification of anomaly intrusion using hierarchy clustering and SVM," *Security and Communication Networks*, vol. 9, no. 16, pp. 3401-3411.

[11] C.F. Tsai and C.Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," *Pattern Recognition*, vol. 43, no. 1, pp. 222-229, 2010.

[12] G. Stein, B. Chen, A.S. Wu and K.A. Hua, "Decision Tree Classifier for Network Intrusion Detection with GA-Based Feature Selection," *in 43rd ACM Southeast Conference*, 2005.

[作者簡介]

蔡旻諺及徐禾瀚，現為國立宜蘭大學資訊工程系碩士班學生，其研究領域為：資訊安全、人工智慧。

卓信宏為國立中央大學資訊工程博士，現為國立宜蘭大學資訊工程系助理教授，其研究領域為：行動通訊系統、人工智慧、及資訊安全。