基於深度強化學習之行動邊緣計算異常的偵測

指導老師：張保榮1

隊員：陳冠儒2、謝佳衛3、莫翔宇4、梁耿成5

1, 2, 3, 4, 5國立高雄大學資訊工程學系

競賽組別: 智慧視覺組

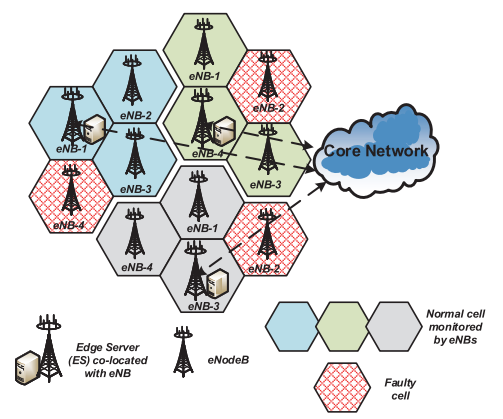
# 摘要

隨著5G與行動邊緣計算技術的快速發展，行動邊緣裝置如手機、無人機、感測器等裝置成倍數增長，形成高度複雜的網路。當一個區域的網路發生壅塞或中斷時，容易導致該區網速變慢，甚至是終止服務而降低QoS，因此維持一個網路服務的問題至關重要。深度強化學習大程度的提升了異常檢測的準確度，透過代理與環境多次的互動修正模型參數，讓模型具有泛化能力且能動態適應快速變化的環境。本作品使用深度強化學習方法，針對一個蜂窩網路基站的行動邊緣計算情境執行異常檢測，並利用真實的CDR資料集做實驗，驗證深度強化學習的可行性。

**關鍵字：**5G、行動邊緣計算、QoS、異常檢測、深度強化學習、CDR

# 一、作品構想

隨著行動裝置數量不斷的增加，每人對行動裝置需求的推動下，造成行動網路流量龐大且複雜。蜂窩網路為現今行動網路的主要架構，它使用多個基站組成，訊號範圍呈蜂窩狀以及使用不同頻率進行傳輸，確保彼此互不干擾，如圖一所示。但隨著流量增加，一般架構也很難維持穩定的服務品質(QoS)。近年來行動邊緣運算技術將邊緣伺服器安裝在基站附近，減少核心網路壓力提升服務品質。若能夠將深度學習技術佈署至邊緣伺服器，並接收來自地台蒐集的呼叫詳細記錄(CDR)即時檢測網路異常，有助於減少因為意外導致的經濟損失。



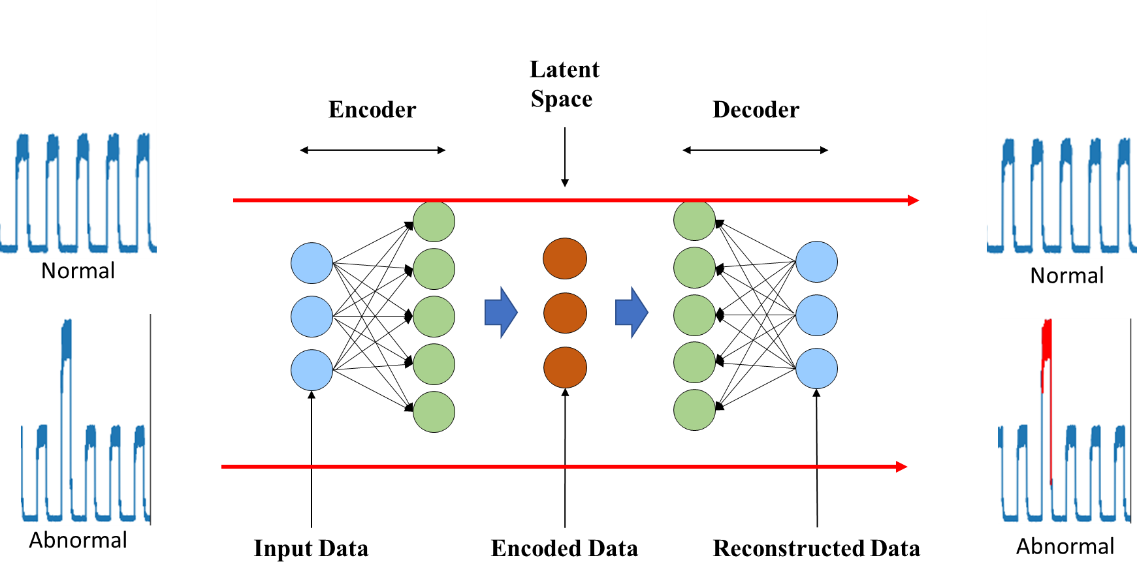
圖一、邊緣計算伺服器的蜂窩網路架構[1]

時間序列異常檢測在許多領域都很重要。資料中心監控系統、感測器、物聯網和金融等等。一般異常檢測任務使用無監督學習或半監督學習，較常見的做法為編碼器與解碼器的神經網路架構，在隱含向量中會對資料分布做先驗假設，當資料違反資料分布則會出現迴歸誤差，系統可以以此機制判定為異常。該方法在資料分布發生變化時容易失準，需要頻繁更新在線預測模型適應。

# 二、原理與方法

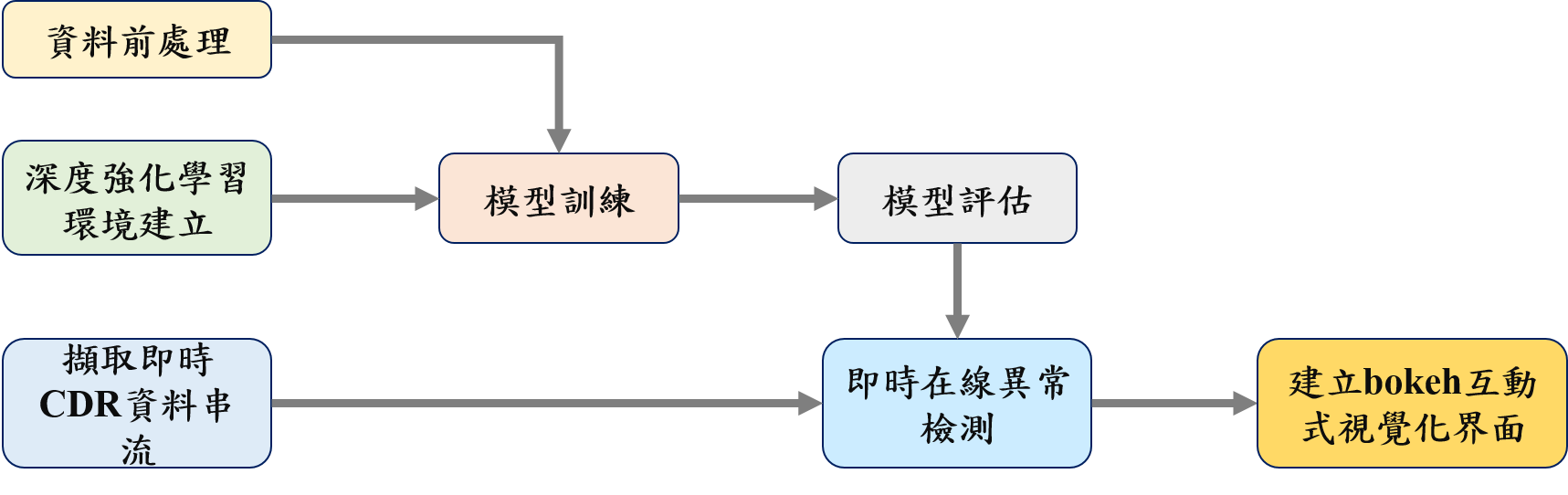
(一) 創意的內容與特色說明:

一般的異常檢測任務使用半監督學習，較常見的做法為編碼器與解碼器的神經網路架構，在隱含向量中會資料分布做先驗假設，當資料違反資料分布則會出現誤差並以此判定為異常。此方法在資料分布發生變化時容易失準，需要更新再現預測模型適應。



圖二、自編碼器架構之異常檢測流程圖

本研究使用深度強化學習結合時間序列異常檢測。首先，我們將時間序列使用固定的滑動窗口擷取資料作為環境狀態(State)，並將動作空間(Action Space)限制為兩個離散狀態:0(正常)、1(異常)。再來，我們透過模型不斷的與不同資料中與環境互動得到不同回饋更新網路，使得模型能適應不同分布的環境。最後，我們會模擬即時擷取CDR資料串流即時檢測異常，並使用一個視覺化界面監測系統狀態，整體流程如圖三所示。



圖三、實驗流程圖

(二) 應用範圍

本作品可以應用於分布急遽變換之異常檢測任務，例如:伺服器使用率、網路需求等。

# 三、軟硬體系統

1.說明本系統使用之開源軟體:

1. Tensorflow
2. Keras
3. Bokeh
4. Pandas

2. 描述本系統其它採用之軟硬體:

1. Cuda

# 四、實作成果

**1. 執行環境之硬體設備規格**

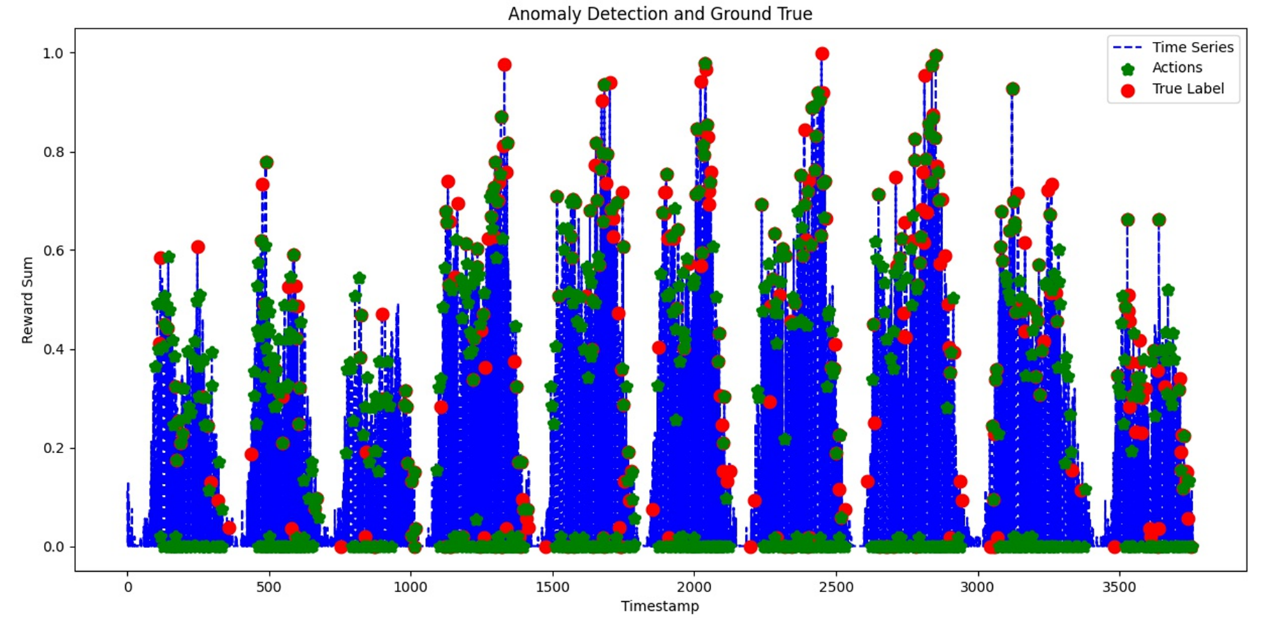
訓練環境主要在Workstation進行，如表一所示。

表一 硬體規格

|  |  |
| --- | --- |
| Resource | Workstation |
| GPU | NVIDIA GeForce RTX 3070 |
| CPU | Intel (R) Core(TM) i5-9500 CPU @ 3.00GHz |
| Memory | 64GB |
| Storage | 512GB\*1(SSD)  2TB\*1(HDD) |

**2. 模型評估結果**

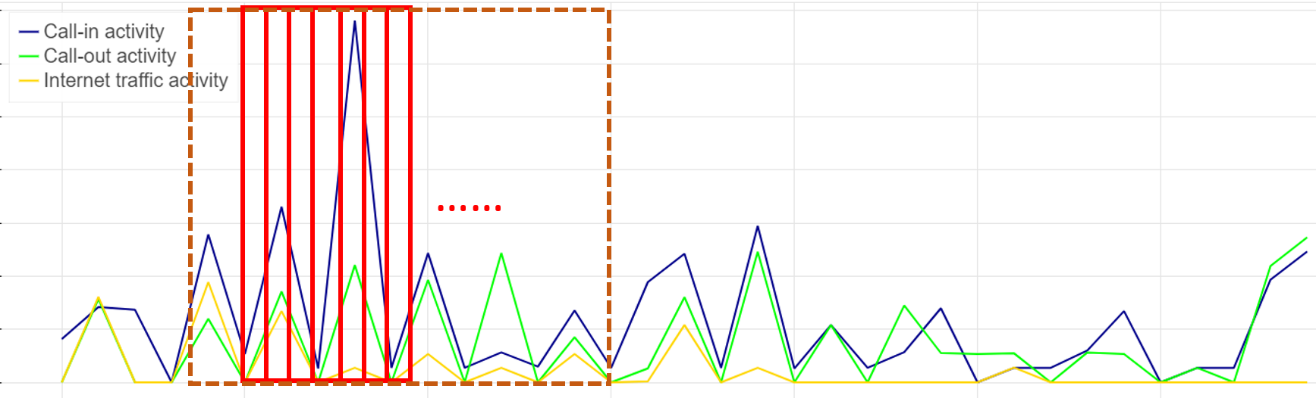
透過視覺化套件觀察檢測結果，我們發現系統對於資料內的點異常過於敏感，因此改為基於窗口的異常閥值，預測成果如圖四所示。

****

圖四、異常檢測結果

**3. 基於窗口異常閥值評估結果**

我們對一個固定長度的區間擷取多個滑動窗口，藉由判定為異常的窗口數量來判定異常區間，如圖五所示。



圖五、基於窗口異常閥值方法

最後，我們透過不同蜂窩小區的資料做評估，計算出修正前與修正後的平均檢測結果，如表二所示。

表二 評估結果

|  |  |  |
| --- | --- | --- |
| Metric | Point anomaly | Window anomaly |
| Precision | 0.018 | 0.894 |
| Recall | 0.483 | 0.983 |
| F1\_score | 0.263 | 0.937 |

**4. 討論**

實驗後得到的實驗結果表明，深度強化學習與異常檢測結合有助於判定行動網路基站的異常。對於不同蜂窩小區也能克服不同資料分布的問題實現精確的檢測結果。本研究使用滑動窗口數量異常大大增加了模型的準確性，應用於真實情境可以減少過多的假警報發生，也幫助系統準確判定連續時間的異常。

# 五、結論

本作品提出一個基於深度強化學習的異常檢測方法，解決在5G蜂巢網路下的異常，提升QoS。

# 六、參考文獻

1. H. Muosa and A. H. Ali, "Internet Routing Anomaly Detection Using LSTM Based Autoencoder," *2022 International Conference on Computer Science and Software Engineering (CSASE)*, 2022, pp. 319-324
2. Bilal Hussain, Qinghe Du, Ali Imran, Muhammad Ali, “Artificial Intelligence-powered Mobile Edge Computing-based Anomaly Detection in Cellular Networks,”, *IEEE Transactions on Industrial Informatics*. 1551-3203. 10.1109/TII.2019.2953201.
3. K. Sultan, H. Ali and Z. Zhang, "Call Detail Records Driven Anomaly Detection and Traffic Prediction in Mobile Cellular Networks," *in IEEE Access*, vol. 6, pp. 41728-41737, 2018
4. Mengran Yu, Shiliang Sun, “Policy-based reinforcement learning for time series anomaly detection,” *Engineering Applications of Artificial Intelligence*, Volume 95, 2020
5. Meng, X. S. Jiang, X. M. Wei, and T. Wei, “A Time Convolutional Network Based Outlier Detection for Multidimensional Time Series in Cyber-Physical-Social Systems,” *IEEE Access*, vol. 8, pp. 74933–74942, 2020.
6. Zhou and R. C. Paffenroth, “Anomaly Detection with Robust Deep Autoencoders,” *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017.
7. C.-W. Tien, T.-Y. Huang, P.-C. Chen, and J.-H. Wang, “Using Autoencoders for Anomaly Detection and Transfer Learning in IoT,” *Computers*, vol. 10, no. 7, p. 88, Jul. 2021.
8. Lunga, J. Gerrand, L. Yang, C. Layton and R. Stewart, "Apache Spark Accelerated Deep Learning Inference for Large Scale Satellite Image Analytics," *in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 13, pp. 271-283, 2020.
9. Z. Zou and J. Ai, "Online Prediction of Server Crash Based on Running Data," *2020 IEEE 20th International Conference on Software Quality*, Reliability and Security Companion (QRS-C), 2020, pp. 7-14.
10. T. Wu en J. Ortiz, “RLAD: Time Series Anomaly Detection through Reinforcement Learning and Active Learning”, *CoRR,* vol abs/2104.00543, 2021.
11. DQN-Timeseries-Anomaly-Detection (https://github.com/jorekai/DQN-Timeseries-Anomaly-Detection)
12. S. Kumar, L. Hussain, S. Banarjee and M. Reza, "Energy Load Forecasting using Deep Learning Approach-LSTM and GRU in Spark Cluster," *2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT)*, Kolkata, India, 2018, pp. 1-4, doi: 10.1109/EAIT.2018.8470406.
13. S. Gupta and D. A. Dinesh, "Resource usage prediction of cloud workloads using deep bidirectional long short term memory networks," *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bhubaneswar, India, 2017, pp. 1-6, doi: 10.1109/ANTS.2017.8384098.