應用 BERT 模型於加密網路流量之行為特徵提取與分類識別研究

Analysis and Classification of Encrypted Network Traffic via BERT-based Behavioral Feature Extraction

指導教授:楊中平教授 | 專題成員:李宗翰、簡翊恩 | 國立成功大學 資訊工程學系

研究動機與目的

研究背景

- 隨著 VPN、Tor、TLS 等加密通訊普及，封包內容難以直接解析。
- 傳統依賴 Port 或 DPI 的流量辨識方式，在加密環境下效果逐漸下降。
- 深度學習可直接由封包序列中學習流量行為特徵。
- Transformer / BERT 具備 Self-Attention 機制，可捕捉封包間的長距離關聯。

研究目的

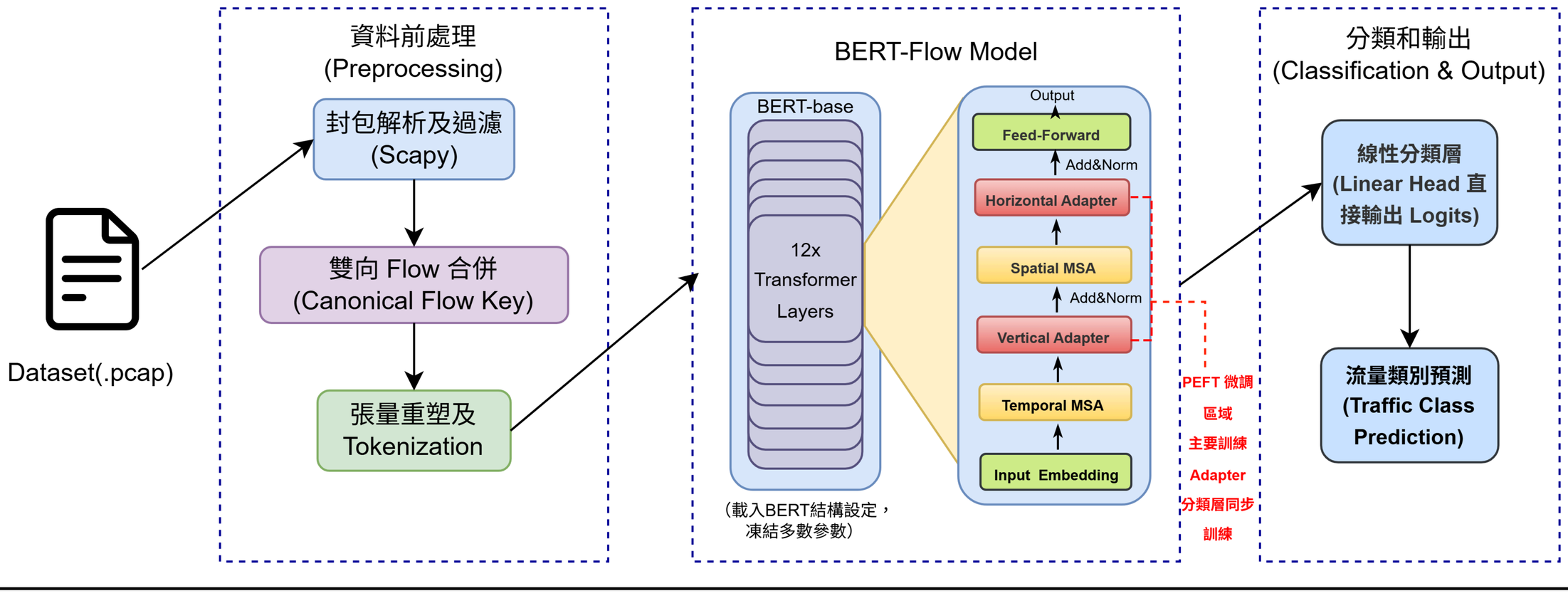
- 建立加密流量資料前處理流程。
- 復現並優化 BERT-Flow 架構。
- 分析模型在惡意/正常流量分類與 VPN 服務分類上的表現。

研究方法流程

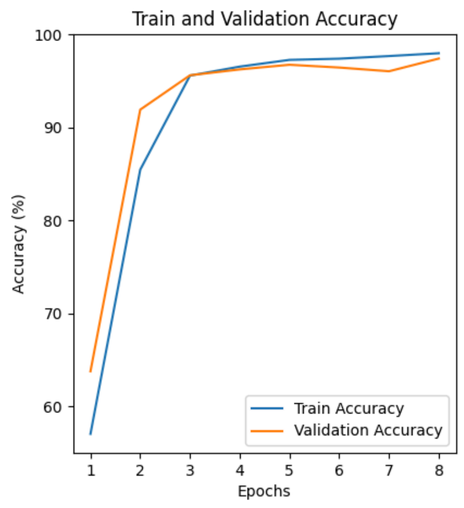
研究方法流程

1. 資料集選用
   USTC-TFC2016、ISCX-VPN-Service
2. 封包前處理
   以 Scapy 讀取 .pcap，擷取 TCP/UDP 封包
3. Flow 樣本建立
   使用 Canonical Flow Key 合併雙向封包
4. 張量轉換
   Byte-to-ID、Padding、截斷為 [N, 32, 128]
5. 模型訓練
   以 BERT-Flow 進行 Adapter Fine-tuning
6. 效能評估
   使用 Accuracy 與 Confusion Matrix 分析分類結果

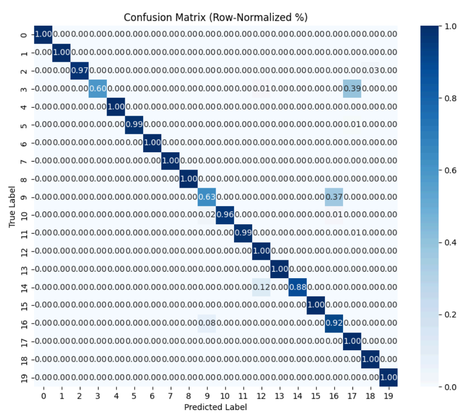
系統核心架構圖



實驗成果與數據分析



圖一、USTC-TFC2016 Training / Validation Accuracy Curve



圖二、USTC-TFC2016 Confusion Matrix

表一、不同資料集之分類準確率比較

資料集	分類任務	類別數	準確度
USTC-TFC2016	正常 / 惡意流量分類	20類	95.5%
ISCX-VPN-Service	VPN 服務類別分類	11 類	96.4%

- Training Accuracy 顯示模型在前幾個 Epoch 快速上升，後期逐漸趨於穩定，表示模型已完成主要特徵學習。
- Validation Accuracy 與 Train Accuracy 差距不大，代表模型沒有出現明顯過擬合。
- Confusion Matrix 中多數預測集中於對角線，表示大部分類別能被正確辨識。
- 兩組資料集皆達 95% 以上準確率，顯示 BERT-Flow 對不同加密流量分類任務具有穩定表現。

結論

本專題完成 BERT-Flow 加密流量分類系統之建置與測試，並透過資料前處理與模型微調策略，提升模型對加密流量行為特徵的辨識能力。

在資料端，本系統利用 Canonical Flow Key 將雙向封包合併為同一連線樣本，並透過 Byte-to-ID、Padding 與張量重塑，將原始 .pcap 封包轉換為固定長度模型輸入。

在模型端，BERT-Flow 結合 Temporal MSA、Spatial MSA 與 Adapter 微調機制，使模型能同時學習封包間時序關係與封包內部特徵。實驗結果顯示，本系統於不同加密流量資料集皆能達到 95% 以上準確率，具備良好的分類效果與後續延伸潛力。