SmartCAN IDS:智慧 CAN 入侵檢測系統

專題編號：113-CSIE-S021
執行期限：113 年第 1 學期至 114 年第 1 學期
指導教授：張世豪
專題參與人員： 111590025 陳欣霈
111590026 諶予薰

一、 摘要

本研究旨在建構一套基於人工智慧之 CAN bus 攻擊偵測與警示系統，透過 ICSim 平台模擬多種攻擊場景，包括 Fuzzy 與 DoS 攻擊，並蒐集正常與異常封包資料。

本專題 AI 模型導入了擅長處理時序資料的堆疊式長短期記憶網絡 (Stacked LSTM)。我們建構的模型在「正常、DoS、Fuzzy」三元分類任務上，最終達成了 81.4% 的準確率，對正常封包的召回率更高達 98%，展現了極低的誤報率潛力。然而，分析也顯示模型在區分不同攻擊類型上存在挑戰，這為後續的優化提供了明確方向。

未來，我們將在現有模型的基礎上，持續優化其對攻擊的敏感度，並整合警示介面，即時提醒潛在威脅。整體研究成功驗證了一個具備擴充性的 AI 資安防護解決方案。

二、 緣由與目的

近年來車載網路安全議題逐漸受到重視，尤其是多起實際漏洞案例更突顯此問題的嚴重性。例如 CVE-2023-29389 中，攻擊者可在無鑰匙情況下偽造 CAN 訊息並啟動車輛，該漏洞的 CVSS 分數甚至高達 6.8；而在 CVE-2023-28896 中，Škoda Superb III 的資訊娛樂系統透過 CAN Bus 傳送的 UDS 診斷資料並未加密，使攻擊者在實體接觸下能解碼封包並操作診斷功能。

因此，本專題希望導入人工智慧技術，透過資料驅動的異常偵測模型，主動學習 CAN Bus 中封包的行為模式，自動辨識異常通訊並及時回應潛在威脅。透過 AI 模型的資料處理能力，系統可在不依賴嚴格規則設定的情況下完成即時警示，進而建構一套具備學習能力與實務應用的車載資安防護機制。

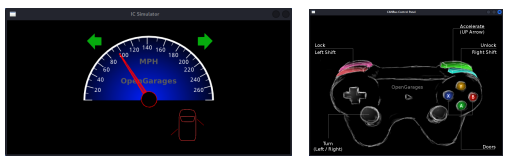
三、 研究報告內容

（一） 研究範圍

本研究聚焦於智慧車輛通訊安全與人工智慧應用的交叉領域，旨在建構一套具即時性與擴充性的 CAN Bus 異常偵測系統。研究範圍涵蓋三個面向：首先，在資安層面針對 CAN 協定之弱點進行模擬與攻擊測試，聚焦於 Fuzzy 與 DoS 攻擊及診斷封包濫用等常見攻擊模式；其次，於模型層面設計分層式 AI 架構，以長短期記憶神經網路(LSTM)作為訓練主要模型；最後，在實作層面，整合 ICSim 模擬平台與 can-utils 工具進行資料收集與驗證，並結合即時推論與視覺化介面，實現異常行為的即時監控與警示回報。

（二） 使用技術方法

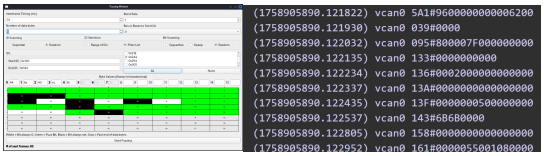
1. ICSim 模擬平台



ICSim(Instrument Cluster Simulator)是一個開源的汽車儀表板模擬平台，主要用於學習與研究 CAN Bus(Controller Area Network)通訊原理。它能在 Linux 環境下透過虛擬 CAN 介面（vcan）模擬車輛的電子控制單元

（ECU）之間的訊息交換，並以圖形化介面呈現車速、方向燈、車門等狀態。使用者可搭配控制程式傳送 CAN 訊息，或使用 can-utils 工具進行封包分析與重放實驗。

2. CAN 攻擊實驗設計



本專題之 CAN 攻擊實驗於 Kali Linux 環境下進行，採用 ICSim 模擬車內 ECU 之實際通訊情境。Fuzzing 部分搭配 SavvyCAN 執行，透過對目標 ID 之 payload 與 DLC 進行隨機與結構化變異、調整封包順序與間隔，並觀察 ECU 的異常回應與錯誤處理行為。DoS 則採資料驅動流程：先截錄 baseline 封包並萃取各 ID 之時序與頻率特徵，將結果標準化為含 timestamp, can_id, dlc, data_hex 欄位的攻擊資料集；再以該資料集為依據，使用 python-can 與 can-utils 產生攻擊計畫並執行。攻擊皆會導致封包遺失、ECU 回應延遲及系統異常。最後再透過 ICSim 提供的儀表板介面觀察攻擊對 ECU 狀態的影響，作為後續 AI 模型訓練與偵測效能評估的依據。

3. 長短期記憶神經網路(LSTM)

長短期記憶網路（Long Short-Term Memory, LSTM）是一種特殊的循環神經網路（RNN）架構，主要用於解決傳統 RNN 在處理長序列資料時容易出現的梯度消失與梯度爆炸問題。LSTM 透過記憶單元（cell state）以及三個控制資訊流動的閘門——輸入閘(Input Gate)、遺忘閘(Forget Gate)與輸出閘(Output Gate)，保留重要訊息並過濾掉不必要的部分，使其能夠在更長的時間段中找出序列的依賴關係。

本專題第二階段導入深度學習方法，建構一個基於堆疊式長短期記憶網路（Stacked LSTM）的入侵偵測模型。模型的輸入資料採用了 10 個關鍵特徵的 CAN 封包序列，涵蓋 CAN ID、資料長度碼（DLC）及 8 位元的 Payload 數據。

模型的核心架構為一個雙層堆疊 LSTM 網路。第一層 LSTM 包含 128 個神經元，並把完整的時序輸出傳遞至下一層；第二層 LSTM 則包含 64 個神經元，負責整合初級特徵並做出高階判斷。為防止模型過擬合並提升泛化能力，每層 LSTM 後均有 Dropout 層（隨機失活率為 0.3），並在 Layer 中加入了 L2 正規化機制。最後數據會送到一個包含 64 個神經元的 Dense 層，並由一個採用 Softmax 激活函數的輸出層進行三元分類（正常、DoS、Fuzzy）。在訓練過程中，我們採用了 Early Stopping 機制，監控驗證集上的損失值，以在最佳時間點自動停止訓練，確保模型達到最佳的泛化表現。

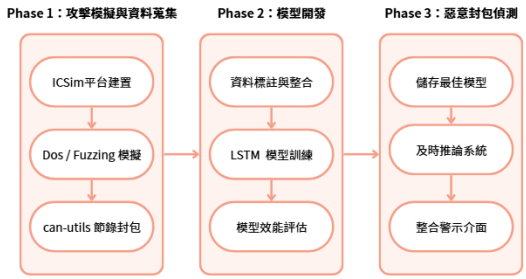
4. GUI

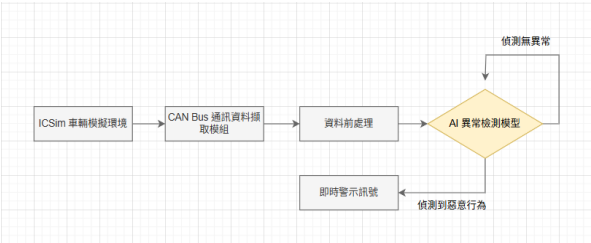
為了將 AI 模型應用於更直觀的場景，我們使用 Streamlit 框架開發了一個圖形使用者介面（GUI）的即時偵測系統。

此系統整合了訓練好的 LSTM 模型與特徵標準化器，並提供檔案上傳功能，讓使用者能上傳 log 日誌檔進行分析。介面採用雙欄式佈局：左側為控制面板與即時封包日誌顯示窗，右側則是攻擊警示牆。當偵測到攻擊時，系統會在警示牆上即時顯示帶有時間戳的警告，讓使用者能追蹤潛在威脅。

透過 Streamlit，我們成功將指令行工具轉化為一個功能完整、使用者友善的視覺化應用，讓專題成果得以具體呈現。

（三） 架構流程





（四） 工具說明

1. can-utils：支援多種 CAN 訊息的傳送、接收、過濾與記錄操作。

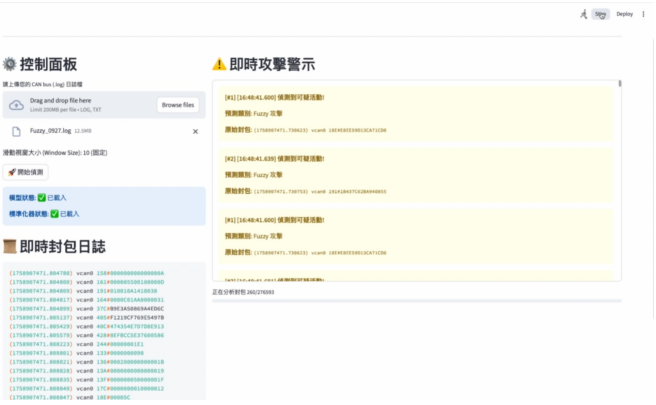
指令	用途
candump	監聽並擷取來自 CAN 的資料，支援過濾與儲存功能。
cansend	傳送自定義 CAN 訊息，模擬惡意攻擊封包。
cansniffer	即時觀察 CAN 訊息的變化。

2. ICSim：ICSim（Instrument Cluster Simulator）為一套模擬現代車輛儀表板與 CAN Bus 訊息傳輸的工具，提供一個可控且真實的車輛通訊環境。
3. SavvyCAN：SavvyCAN 是一套圖形化 CAN Bus 訊息分析工具。主要特色為支援大量訊息的接收與記錄；資料的視覺化過濾、統計分析功能，還可配合 Fuzzing 模組，模擬模糊攻擊，作為異常資料來源。
4. Python（Keras & TensorFlow）– AI 模型開發核心

   Python 是本專題進行資料處理、模型建構與分析的核心語言，主要使用了以下幾個關鍵函式庫：

   - **Pandas & NumPy**：用於高效地讀取、處理及轉換大量的 CAN 封包數據。
   - **Keras / TensorFlow**：我們使用 Keras 提供的 API 來訓練**堆疊式 LSTM 模型**。
   - **Scikit-learn**：用在模型的效能評估。
   - **Matplotlib & Seaborn**：用於將混淆矩陣等評估結果進行視覺化。

（五） 研究成果



本研究最終完成一套名為「SmartCAN IDS」的智慧型 CAN 入侵偵測系統，此系統整合了模擬攻擊、深度學習模型訓練與即時視覺化監控介面，驗證了以人工智慧技術防護車載網路安全的可行性。研究成果主要為攻擊偵測模型與使用者友善的即時監控工具。

（六） 結論

透過本次研究，我們期望能建構一個具實務意義的車輛資安即時偵測系統，提供未來智慧車輛安全監控的重要參考基礎，保障車輛網路通訊的安全性與穩定性。

（七） 參考文獻

[1] D. Olatinwo, R. Joy, A. Roberts, and M. Bawa, “CANGuard: An Enhanced Approach to the Detection of Anomalies in CAN-Enabled Vehicles,” Sensors, vol. 23, no. 15, pp. 6641, 2023.

[2] M. Sabihuddin, Y. Liu, and K. M. Goher, “CAN-Bus Attack Detection With Deep Learning,” IEEE Access, vol. 10, no. 1, pp. 93 – 104, 2022.