基於聯邦學習之 ROS2 零信任協同防禦系統

專題編號：114-2-CSIE-S003
執行期限：114 年第 1 學期至 114 年第 2 學期
指導教授：陳昱圻
專題參與人員：　112590022　陳駿逸
112820022　周佩樺
112820024　陳仕龍
112590052　謝博任

一、摘要

機器人作業系統（ROS2）廣泛應用於資訊物理系統中，但其原生架構缺乏完善安全防護，易受阻斷服務與網路探索等攻擊。為此，本專題開發一套基於 ROS2 的零信任入侵偵測系統。我們採用 ROSPaCe 資料集，擷取系統資源與網路流量特徵，並建構機器學習防禦模型。方法上，結合非監督式的「孤立森林」捕捉未知威脅，以及監督式的「XGBoost」進行精準分類。此外，我們引入時間序列區塊技術模擬真實情境，並透過 GPU 加速優化訓練效能。實驗結果顯示，本系統不僅在極低假警報率下維持高召回率，更在偵測延遲時間（TTD）表現優異，能於攻擊發動瞬間成功觸發警報，大幅提升 ROS2 系統的即時預警與實戰防禦能力。

關鍵詞： ROS2、零信任架構、機器學習、XGBoost、入侵偵測系統、偵測延遲時間（TTD）

二、緣由與目的

機器人作業系統（ROS2）廣泛應用於資訊物理系統（Cyber-Physical System, CPS）中，但其原生架構缺乏完善的安全認證與防護機制，極易遭受阻斷服務（DoS）與網路探索等惡意攻擊。一旦系統遭到入侵，不僅將導致服務中斷，更可能引發嚴重的實體安全威脅。

為了解決上述安全痛點，本專題旨在導入「零信任架構」理念，開發一套基於機器學習的入侵偵測系統（IDS）。本計畫的核心目的在於建構雙層防禦模型，在不干擾 ROS2 機器人正常運作的前提下，精準辨識系統異常，並實現即時的威脅預警 。

三、 研究範圍

本研究聚焦於 ROS2 環境下的系統安全監控 。實作上採用專為 ROS2 設計的 ROSPaCe 資訊安全資料集，針對 Linux 作業系統資源、網路流量與 ROS2 服務層，萃取 60 個核心特徵作為模型訓練與測試的基準。研究範圍涵蓋特徵資料的前處理、機器學習模型（XGBoost 與 Isolation Forest）的訓練與 GPU 效能優化，以及在時間序列環境下對偵測延遲時間（TTD）的量化評估 。

四、 使用技術方法

本專題設計了結合「廣度」與「精度」的雙層機器學習防禦策略 ：

（一）孤立森林（Isolation Forest）

利用非監督式學習特性，建立正常系統行為輪廓，負責捕捉偏離常態的未知零時差攻擊 。

（二）XGBoost（極限梯度提升）

採用監督式學習，針對已知攻擊特徵進行高精度分類，並結合時間序列區塊**技術，最小化系統反應時間** 。

五、架構流程

本系統架構透過區域網路（LAN）串接邊緣節點與伺服器。Raspberry Pi 節點負責運行 ROS2 服務並即時收集系統特徵，資料隨後回傳至 Demo 後端 。後端模型在接收到監控特徵後，會將其對齊並打包為時間序列緩衝區塊，即時進行推論與攻擊阻擋。

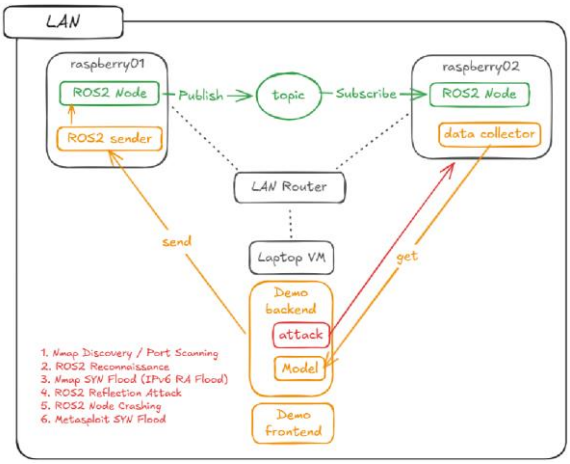

圖 1. ROS2 零信任監控系統實體架構圖

六、工具說明

（一）邊緣運算與收集設備

採用樹莓派作為 ROS2 的實體運作節點。在區域網路環境中，樹莓派分別扮演訊息 Publisher 與 Subscriber，負責在邊緣端即時擷取系統特徵與網路流量，並回傳至後端伺服器。

（二）硬體加速與優化工具(NVIDIA RTX 4060 GPU)

針對後端龐大的機器學習訓練與即時推論需求，於模型中啟動 GPU 加速參數（tree_method='hist'），並實作資料型態降轉（轉為 float32）。此舉有效解決了 8GB VRAM 的記憶體不足（OOM）瓶頸，確保系統能達到極低延遲（TTD）的防禦要求。

七、實驗結果

本系統針對 ROSPaCe 資料集進行了靜態分類與動態時間序列測試。

（一）靜態防禦表現

在單點分類測試中，XGBoost 模型展現出極高的鑑別度。在極嚴苛的防護標準下（鎖定假警報率 FPR = 0.0001），模型依然能維持極高的精準度與召回率，證明其能有效避免資安系統中常見的「狼來了」誤報困境 。

（二）動態實戰反應（TTD）

在連續時間序列的區塊測試中，系統整體的偵測延遲時間統計分佈呈現極度右偏。這代表絕大多數的網路攻擊與節點異常，模型皆能在攻擊發動的瞬間（約 0~5 個數據點內）成功觸發警報，具備極佳的即時預警能力。

八、結論

本專題成功將「零信任架構」概念落地於 ROS2 機器人系統中。透過結合非監督式的「孤立森林」以防範未知零時差攻擊，以及監督式的「XGBoost」精準攔截已知威脅，本系統建構了完善的雙層防禦網。此外，實驗證實本模型在時間序列下的極低延遲特性，能大幅縮短 ROS2 遭受破壞前的黃金救援時間，具備高度的實務部署價值 。

九、參考文獻

[1] T. Puccetti, S. Nardi, C. Cinquilli, T. Zoppi, and A. Ceccarelli, "ROSPaCe: Intrusion Detection Dataset for a ROS2-Based Cyber-Physical System and IoT Networks," *Scientific Data*, vol. 11, no. 1, p. 481, 2024.

[2] T. Puccetti, "rospace_dataset," GitHub repository, 2024. [Online]. Available: https://github.com/TommasoPuccetti/rospace_dataset