後量子密碼與視覺定位之 ROS 安全通訊架構分析與整合

Integrated Analysis of Post-Quantum Secure ROS Communication with Visual Localization

林昱翔[1]、王敦瑞[2]、董一志[1,3]、柯沛岑[1]、李孟修[1]

1. 明志科技大學電子工程系

2. 工程學院創新科技應用於生物醫學暨醫療照護產品研發國際系

3. 通訊作者：iggy@mail.mcut.edu.tw

摘要

隨著智慧城市快速發展與自主移動機器人(AMR)多方應用需求，使得機器人作業系統（ROS）已成為關鍵基礎架構[1]。然而，傳統公鑰密碼（RSA、ECC）於量子運算環境下將面臨失效風險，衍生通訊安全威脅[2][3]。本研究整合視覺定位（VSLAM）與後量子密碼學（PQC），提出分層式安全通訊架構，並於嵌入式平台驗證 ML-KEM 與 ML-DSA 效能，同時結合 WireGuard 建立混合式後量子安全隧道。實驗結果顯示，在 MPU 和 MCU(NVIDIA NANO, Raspberry Pi and Pico, ESP32, STM32) 等資源受限環境中，ML-KEM-768 握手效能優於傳統 ECC，且 ORB-SLAM3 仍可維持 14–22 Hz 即時定位頻率。所提架構採非侵入式部署模式，並可應用於高頻影像辨識與 5G FWA 傳輸場景，提供透明式安全覆蓋機制。研究證實，在高頻資料環境下兼顧抗量子安全與即時導航具實務可行性。

關鍵詞： 後量子密碼學、機器人作業系統、視覺定位、WireGuard、5G FWA

Abstract

With the rapid development of smart cities and the increasing demand for Autonomous Mobile Robot (AMR) applications, the Robot Operating System (ROS) has become a critical infrastructure platform. However, traditional public-key cryptographic schemes such as RSA and ECC are vulnerable in the era of quantum computing, posing significant communication security risks. This study integrates Visual Simultaneous Localization and Mapping (VSLAM) with Post-Quantum Cryptography (PQC) and proposes a layered secure communication architecture for ROS-based systems. The performance of ML-KEM and ML-DSA is evaluated on embedded platforms, and a hybrid post-quantum secure tunnel is implemented using WireGuard. Experimental results demonstrate that in resource-constrained environments—including both MPUs and MCUs such as NVIDIA Jetson Nano, Raspberry Pi, Raspberry Pi Pico, ESP32, and STM32—ML-KEM-768 achieves superior handshake performance compared to conventional ECC. Meanwhile, ORB-SLAM3 maintains a stable real-time localization frequency of 14–22 Hz. The proposed architecture adopts a non-intrusive deployment strategy and can be extended to high-frequency image processing and 5G Fixed Wireless Access (FWA) transmission scenarios, providing transparent quantum-resistant protection. The results confirm the practical feasibility of achieving both quantum-resilient security and real-time navigation performance in data-intensive robotic environments.

Keywords: Post-Quantum Cryptography, ROS, VSLAM, WireGuard

1.緒論

1.1 研究背景與動機

隨著人工智慧與邊緣運算技術的快速發展，自主移動機器人（Autonomous Mobile Robots, AMR）已成為智慧城市、工業 4.0 基礎設施及自動化物流的核心元件。在此發展趨勢下，機器人作業系統（Robot Operating System, ROS）因具備高度模組化與開源特性，已成為全球最廣泛使用的機器人軟體開發框架 [4]。ROS 採用發布／訂閱（Publish/Subscribe）的通訊模型，使得不同感測器與控制節點能有效率地進行資料交換 [5]。

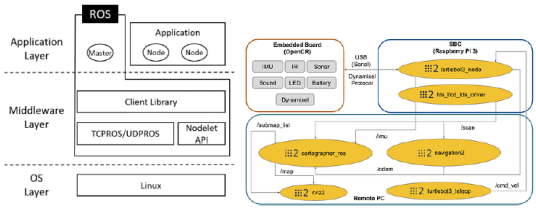

圖 1 ROS 架構圖

然而，ROS 1 的原生架構在設計初期主要考量通訊效能與封包傳輸的即時性，並未將資訊安全防護機制納入核心規範 [6][7]。其底層依賴 TCPROS 或 UDPROS 中介層，預設以明文形式傳輸所有感測器數據與控制指令。在複雜的智慧城市網路或開放式 SD-WAN 架構中，這種未加密的通訊協定存在極大的安全隱患，使得機器人系統極易遭受中間人攻擊、訊息竄改與重放攻擊 [8]。

為解決上述安全漏洞，傳統的網路防禦機制多依賴虛擬私人網路（VPN）或傳輸層安全性協定（TLS），這些技術的核心建立在 RSA 或橢圓曲線密碼學（Elliptic-Curve Cryptography, ECC）等公鑰加密演算法上。RSA 的安全性奠基於大整數分解難題，而 ECC 則依賴於橢圓曲線上的離散對數難題。

此外在智慧醫療等高密度物聯網場域中，機器人系統除需具備自主導航能力外，亦須承載高頻影像資料流與即時控制訊號交換。例如於智慧醫院應用情境中，TurtleBot3 可搭載攝影機模組進行視覺特徵萃取與標誌辨識，並透過 5G Fixed Wireless Access（FWA）進行資料回傳與遠端監控。在此類場景中，網路廣播頻繁且影像資料流量高，若缺乏適當之通訊加密與驗證機制，將可能面臨封包竊聽、訊息竄改與控制指令注入等風險。因此建立一套可於高頻資料流環境下穩定運作之後量子安全通訊架構，具有實際部署價值與延伸應用潛力。

1.2量子運算威脅

近年來，量子運算技術取得突破性進展。根據 Shor 演算法的理論模型，具備足夠邏輯量子位元的量子電腦，能在多項式時間內解決大整數分解與離散對數難題 [4][5]。這意味著現有的非對稱加密防護將完全失效。並衍生出「現在截獲，稍後解密」（Harvest Now, Decrypt Later）的嚴重國安與工控威脅。儘管美國國家標準暨技術研究院（NIST）已積極推動後量子密碼學（Post-Quantum Cryptography, PQC）標準化，選定 ML-KEM（原 Kyber）與 ML-DSA（原 Dilithium）作為新一代防護標準[6]，但這些演算法通常伴隨著較大的金鑰尺寸與運算開銷。

1.3 研究目的與貢獻

在 AMR 的實際應用中，機器人高度依賴視覺即時定位與建圖（Visual Simultaneous Localization and Mapping, VSLAM）技術來實現自主導航。VSLAM（如 ORB-SLAM3）需要持續處理高解析度影像特徵，對邊緣設備（如 Raspberry Pi 4 或各類嵌入式開發板）的 CPU/GPU 資源消耗極大。

若直接將高運算複雜度的 PQC 演算法強加於機器人通訊鏈路中，極易引發嚴重的網路延遲與運算資源排擠效應，導致 VSLAM 模組出現影像幀丟失（Frame Drop），進而使定位頻率大幅下降，嚴重影響機器人的即時避障與導航安全性。因此，如何在資源受限的嵌入式平台上，同時達成抗量子通訊安全與即時視覺導航，是當前學術界與產業界亟待克服的技術瓶頸。

基於上述挑戰，本研究旨在提出一套整合

VSLAM 與後量子密碼學的分層式安全架構，以確保 AMR 在智慧城市網路中的通訊機密性與完整性。本研究之具體貢獻包含以下三項： (1) 完成資源受限平台之 PQC 效能驗證：針對 NIST 標準之 ML-KEM-768 進行嵌入式裝置上的效能分析，證實其握手與封裝效率在特定場景下可優於傳統 ECC 演算法。(2)提出一種基於 WireGuard 的混合式後量子握手機制：透過整合原生 ECC 與 ML-KEM，建立抗量子安全 VPN 隧道，提供 ROS 系統「非侵入式」的安全覆蓋，無須大幅修改現有機器人應用程式碼。(3) 實證即時定位系統之相容性：建立實驗場域，評估在後量子加密傳輸環境下，ORB-SLAM3 視覺定位模組的即時效能，並證實其可穩定維持 14–22 Hz 之運行頻率，滿足 AMR 即時導航之需求。

2. 嵌入式後量子密碼驗證成果

後量子密碼學（Post-Quantum Cryptography, PQC）為因應量子計算可能對現行公鑰密碼系統造成之影響而發展之新一代加密技術。在智慧城市與物聯網環境中，大多數為資源受限的微控制器（Microcontroller Unit, MCU），因此評估 PQC 在嵌入式平台上的可行性成為重要課題。

2.1 micro-ROS 應用之實驗架構設計

本研究架構採用 micro-ROS Client-Agent 模型 [12]，以模擬 IoT 裝置與後端系統之真實互動情境，透過 DDS-XRCE 協定與 ROS2 進行通訊 [13]，並在此標準化架構上進行 PQC 替換與效能評估，如圖 2所示，使測試結果能直接反映對 ROS2 Topic 發布／訂閱機制的實際影響，而非僅限於網路延遲量測。系統包含三個核心組成：

(1) micro-ROS Client：部署於 ESP32，作為感測或控制節點，透過 DDS-XRCE 與 ROS2 通訊。

(2) micro-ROS Agent：運行於 PC，負責橋接 Client 與 ROS2 DDS 網路，並確保代理端不成為效能瓶頸。

(3) 安全通道：Client 與 Agent 之間透過基於 TCP/IP 的 TLS 1.3 加密通道通訊，本研究比較傳統加密與 PQC 加密套件之效能差異。

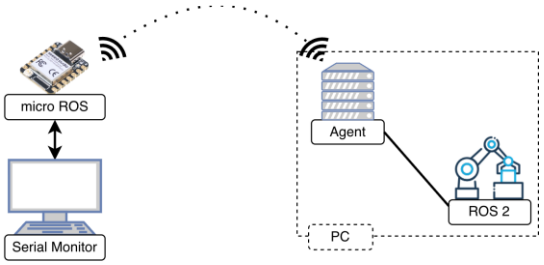

圖 2 micro-ROS 應用框架之實驗架構

2.2 TLS 握手效能比較

如表 1 及表 2 所示，在 ESP32-C3 與 ESP32-S3 平台上，整合 ML-KEM 之 TLS 1.3 握手效能已由既有研究完成量測與驗證。若以本文後續分析採用之 ESP32-S3 平台為例，換算方式為表中 μs 數值除以 1,000，表 2 顯示 ECC 之 TLS 交握時間經換算後為 2,260.824 ms；ML-KEM-768 之 TLS 交握時間經換算後為 1,539.408 ms。

表 1 不同 TLS 組態在 ESP32-C3 上的效能表現

指標	ECC	ML-KEM-512	ML-KEM-768	ML-KEM-1024
TLS 交握時間	1,782,971 µs	1,193,142 µs	1,491,035µs	1,767,625 µs
CPU 使用量	122,095,789 週期	83,877,488 週期	85,218,751 週期	87,122,689 週期
記憶體使用峰值	24,729 Bytes	22,415 Bytes	22,329 Bytes	30,152 Bytes
總傳輸吞吐量	0.044 Mbps	0.044 Mbps	0.046 Mbps	0.048 Mbps

表 2不同 TLS 組態在 ESP32-S3 上的效能表現

指標	ECC	ML-KEM-512	ML-KEM-768	ML-KEM-1024
TLS 交握時間	2,260,824 µs	1,637,636 µs	1,539,408 µs	1,852,759 µs
CPU 使用量	542,724,833 週期	393,156,077 週期	370,776,185 週期	447,176,567 週期
記憶體使用峰值	24,756 Bytes	21,928 Bytes	21,143 Bytes	28,992 Bytes
總傳輸吞吐量	0.048 Mbps	0.053 Mbps	0.049 Mbps	0.051 Mbps

此結果顯示 ML-KEM-768 在嵌入式微控制

器上，握手效率約為 ECC 的 3.5 倍。儘管 ML-KEM 金鑰與密文尺寸較大，但其數學運算特性在通用 MCU 上具有較高計算效率，使整體握手時間反而縮短。

2.3 記憶體使用量分析

在嵌入式環境中，記憶體資源為關鍵限制因素。測試結果顯示，如

指標	ECC	ML-KEM-512	ML-KEM-768	ML-KEM-1024
TLS 交握時間	1,782,971 µs	1,193,142 µs	1,491,035µs	1,767,625 µs
CPU 使用量	122,095,789 週期	83,877,488 週期	85,218,751 週期	87,122,689 週期
記憶體使用峰值	24,729 Bytes	22,415 Bytes	22,329 Bytes	30,152 Bytes
總傳輸吞吐量	0.044 Mbps	0.044 Mbps	0.046 Mbps	0.048 Mbps

及表 2，ML-KEM-512 與 ML-KEM-768 之記憶體需求與傳統 ECC 相近。 ML-KEM-1024 峰值記憶體使用量約為 30 KB。

此結果表示，在安全等級 512 與 768 下，ML-KEM 具備良好部署潛力。然而，在 1024 等級下，對極低資源裝置而言可能構成挑戰。

因此在嵌入式應用中，ML-KEM-768 被視為兼顧安全性與效能之較佳選擇。

2.4 即時通訊影響評估

除握手效能外，研究亦評估 PQC 對應用層即時通訊之影響。測試結果指出，PQC 主要影響初始連線建立階段，對後續資料傳輸之延遲與吞吐量未產生顯著負面影響。

2.5 嵌入式可行性綜合說明

綜合上述測試成果，ML-KEM-768 於嵌入式平台上具備實際可行性， 握手效能優於傳統 ECC，記憶體需求在 512 與 768 等級下可接受且不會對即時資料傳輸造成顯著影響。

此結果為後續將 ML-KEM 整合至 ROS 通訊架構奠定基礎，顯示在嵌入式機器人系統中導入後量子安全機制具有實務可行性。

3. ROS 安全覆蓋架構設計

3.1 ROS 安全威脅

在封閉式實驗環境中，明文傳輸可能不構成即時威脅；然而當機器人系統部署於開放式網路或跨站點環境時，可能面臨以下風險[6][8]：

(1) 中間人攻擊（Man-in-the-Middle Attack）：攻擊者於通訊雙方之間攔截並轉發封包，使雙方誤以為通訊正常進行，實際上所有資料皆可被監控或修改。於機器人系統中，此類攻擊可能導致控制指令遭竄改，影響導航與任務執行安全性。

(2) 封包竊聽：攻擊者透過被動監聽網路流量取得未加密之感測資料與控制訊號。在高頻影像傳輸或狀態回報場景下，若資料未經加密，可能洩漏環境資訊與系統運作細節，造成隱私與安全風險。

(3) 訊息竄改：攻擊者於傳輸過程中修改封包內容，使接收端取得錯誤或惡意資料。於 ROS 系統中，若 Topic 訊息遭竄改，可能導致定位誤判、速度異常或行為決策錯誤，進而影響整體系統穩定性。

(4) 重放攻擊：攻擊者重複傳送先前合法封包，使系統誤判為新的有效指令。此類攻擊可能造成機器人重複執行舊指令或錯誤觸發控制流程，對即時控制與安全機制構成潛在威脅。

同時若通訊安全機制仍依賴傳統公鑰密碼，未來在量子計算環境下可能面臨破解風險。因此在既有 ROS 架構中導入後量子安全通訊機制，成為必要議題。

3.2 基於 WireGuard 之後量子安全隧道設計

如圖 3，為確保 ROS 系統於未來量子運算環境下仍具備通訊機密性，本研究採用混合式金鑰交換設計，將 NIST FIPS 203 標準之 ML-KEM-768 演算法整合至 WireGuard 原生握手流程中。WireGuard 原始設計基於 Noise Protocol Framework，其握手階段使用 Curve25519 進行 Diffie-Hellman 金鑰交換 [14]。本研究並未完全取代原有機制，

而是在既有握手流程中同步執行 ML-KEM 金鑰封裝程序，使傳統橢圓曲線共享金鑰與後量子共享金鑰共同參與最終會話金鑰之派生。

圖 3 WireGuard 密鑰路由

在實作層面上，混合式握手機制保留原有 Noise 協定之流程結構，同時於握手階段加入 ML-KEM 封裝與解封裝程序，並將兩組共享金鑰結果透過金鑰派生函式（KDF）整合為最終 Session Key。此設計確保在傳統攻擊模型下仍維持原有 WireGuard 之安全性，而在未來量子攻擊情境下，即使橢圓曲線機制失效，ML-KEM 所提供之安全性仍可保障通訊機密性

本研究所提出之安全架構採取非侵入式部署模式，安全模組僅部署於網路閘道器層，並透過系統路由設定與 VPN 隧道機制對 ROS 通訊進行透明式保護，而無須修改既有 ROS 節點或應用程式碼 。此種設計降低了系統整合複雜度，亦使既有 ROS1 或 ROS2 系統得以在不變動應用層邏輯之情況下完成安全升級。

3.3 混合式縱深防禦架構

在 ROS2 環境中，雖可透過 SROS2 建立應用層安全機制[15] ， DDS Security 機制亦提供中介層保護能力 [16]，但全面加密高頻寬資料流（例如影像串流或雷射掃描資料）可能增加系統負擔。因此本研究提出混合式縱深防禦架構，如圖 4。

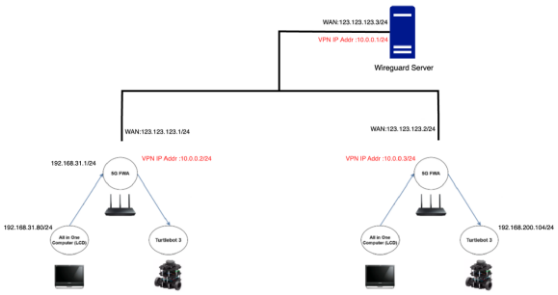

圖 4 PQC-WireGuard 架構圖

本架構之核心設計理念如下：

(1) 傳輸層安全強化：於網路傳輸層建立 PQC-WireGuard 加密隧道，確保所有跨站點與跨網域資料傳輸具備抗量子安全能力。

(2) 應用層選擇性保護：僅針對關鍵控制指令於應用層進行數位簽章與驗證，而非對所有資料流進行額外加密處理，以降低系統運算負擔。

在應用層機制上，本研究採用 ML-DSA 對重要控制訊息進行數位簽章與驗證，以確保指令之完整性與來源可驗證性。同時，大量感測資料仍維持於傳輸層加密保護之下，避免因重複加密導致延遲與效能下降。

在整合後之 ROS 安全架構中，系統運作流程可概述為：

(1) 機器人節點於本地端透過 ROS Topic 完成資料發布與訂閱。

(2) 跨站點或跨網域通訊經由 PQC-WireGuard 隧道進行加密傳輸。

(3) 關鍵控制指令於應用層進行 ML-DSA 簽章與驗證，確保控制鏈路之安全性與可信度。

本架構具備以下特性：

- 抗量子通訊安全能力
- 低延遲與高效能傳輸特性
- 非侵入式部署模式（不修改既有 ROS Topic 機制）
- 可與既有 ROS 系統架構無縫整合

3.4 應用層簽章效能測試結果

為了驗證在不同環境特徵下的防禦效能，本研究選用 TUM Visual-Inertial Dataset 作為標準測試資料 [17]，並定義了以下兩種測試場景：

場景一為室內環境，採用 dataset-room4_512 序列，模擬空間狹小、紋理豐富的辦公室環境。此場景主要用於驗證在發生被動式竊聽 (Passive Eavesdropping) 威脅時，系統對室內地圖與影像隱私的保護能力。

場景二為廣域環境，採用 dataset-magistrale4_512 序列，模擬空間開闊的大型廳堂環境。此場景用於驗證在面臨主動式注入 (Active Injection)攻擊時，系統維持長距離巡檢控制指令完整性的能力。

我們量測了兩個不同的ROS使用場景的有效數據傳輸速率（Goodput），以評估實際數據承載能力。

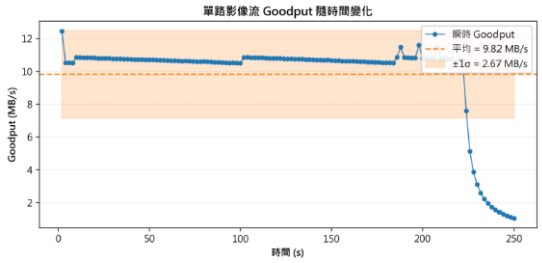

圖 5 場景一數據集在 PQC-WireGuard 下的 Goodput 變化

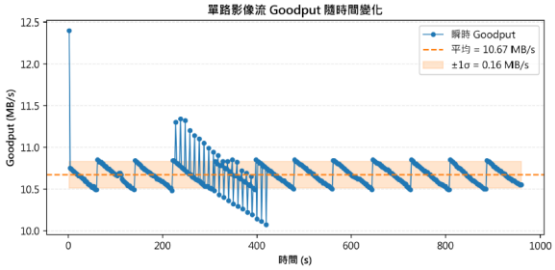

圖 6 場景二數據集在 PQC-WireGuard 下的 Goodput 變化

如圖 5在場景一中，平均 Goodput 穩定維持於 9.82 MB/s（約 78.56 Mbps）；而圖 6於場景二中，平均 Goodput 提升至 10.67 MB/s（約 85.36 Mbps）。

實驗結果顯示，本 PQC 安全框架可穩定承載高流量之即時影像資料傳輸，且應用層資料流量尚未逼近通道容量上限。整體通訊頻寬仍保有餘裕，可同時支援其他 ROS 控制指令與狀態回報訊息之傳輸，而不致造成顯著效能瓶頸。

在高頻影像資料流場景下，傳輸層加密機制之效能表現尤為關鍵。由於影像串流資料量遠高於一般控制訊號，若於應用層進行全面加密，將可能造成額外運算負擔與延遲累積。本研究所採之分層式設計，將高流量影像資料維持於傳輸層加密保護之下，而僅對關鍵控制指令進行數位簽章與驗證，避免重複加密造成效能下降。此種設計策略，使系統於高頻影像流場景中仍可維持穩定傳輸效率，同時兼顧通訊機密性與完整性需求。

3.5 應用層安全效能評估

為量化本細顆粒度安全方案於實際機器人情境下之效能表現，本研究設計混合負載實驗：系統持續接收高頻寬影像資料，同時周期性接收控制指令。

實驗分為三種情境：

- 情境 A（基準組）：ROS2 Humble，所有 topics 明文傳輸，未啟用安全機制。
- 情境 B（SROS2）：啟用 SROS2，對影像與控制 topics 進行身份驗證與加密。
- 情境 C（本研究方案）：影像 /camera/image_raw 維持明文；控制指令 /cmd_vel 經 ML-DSA（FIPS 204）簽章後，由 PQC-Verify 節點驗章並發布至 /cmd_vel/verified。

量測指標包括：

- /cmd_vel 端到端延遲（遙控端至 verified topic 被訂閱之時間差）。
- 簽章與驗章處理時間（PQC-Sign 與 PQC-Verify 節點運算耗時）。

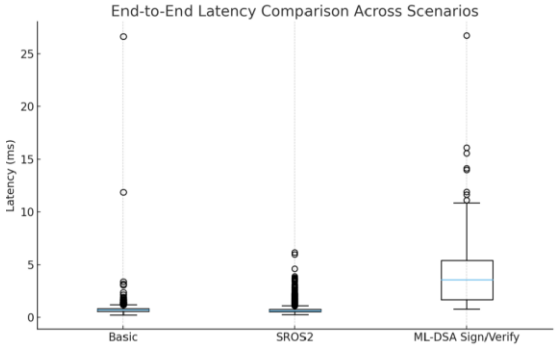

圖 7 詳細測試結果圖

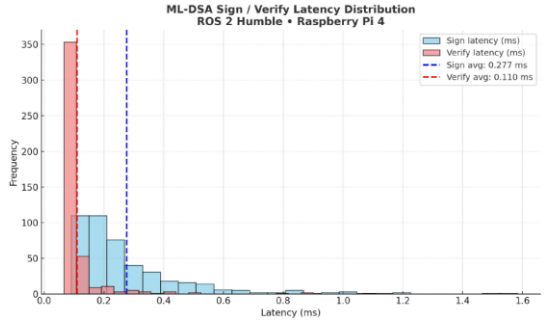

圖 8 ML-DSA Sign/Verify 測試結果

如圖 7及圖 8顯示，基準組與 SROS2 組之端到端延遲皆低於 1 ms，顯示 DDS 在小封包加密下具高度效率。本研究方案因採用應用層服務呼叫與簽章驗證流程，延遲分佈落於 2 – 5 ms，平均約 3.5 ms。雖然延遲略高於 SROS2，但對於 10 Hz 或 50 Hz 控制頻率之移動機器人而言，此 3 – 4 ms 延遲仍屬可接受範圍。

本研究以極小延遲成本換取細顆粒度安全控制，使高流量影像維持明文傳輸，避免全面加密造成之運算競爭與掉幀風險，在系統效能與關鍵指令安全性之間取得較佳平衡。

3.6 智慧醫療高頻影像場域之應用

為進一步驗證本研究所提出之後量子安全架構於高頻資料傳輸環境下之適用性，可將其延伸至智慧醫療場域進行應用情境分析。在該場景中，以移動式機器人（如 TurtleBot3）作為教育與研究平台之代表 [18]。搭載攝影機模組進行影像擷取與特徵萃取，並透過無線網路將辨識結果與狀態資訊即時回傳至後端控制中心。於高頻影像流傳輸與多節點廣播環境下，網路負載與通訊安全需求同步提升，對通訊協定之延遲與穩定性提出更高要求。

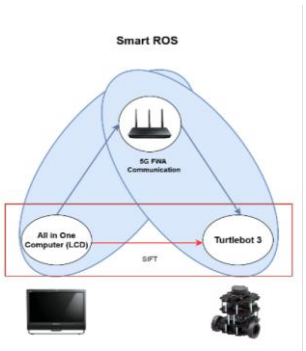

圖 9 基於網路的影像處理方法

如圖 9所示，在高頻影像處理與網路傳輸並存之應用情境中，移動式機器人透過攝影機模組進行影像擷取與特徵分析，並將辨識結果與狀態資訊透過無線網路回傳至後端控制節點。於此架構下，影像資料流與控制訊號同時存在於通訊通道中，使整體網路負載與即時性需求顯著提升。若缺乏適當之傳輸層安全機制，資料於傳輸過程中可能面臨竊聽與竄改風險。因此，本研究所提出之 PQC-WireGuard 架構可於既有應用流程外層建立透明式安全覆蓋機制，在不改動 ROS 節點程式碼之情況下，提供抗量子安全保護能力。在高頻影像資料流與多節點網路廣播並存之智慧醫療場域中，本研究之分層式安全設計可維持系統即時性與資料完整性，顯示其除城市級 AMR 應用外，亦具備延伸部署潛力。

4.視覺定位與通訊模組整合

4.1 驗證平台架構說明

為驗證在導入後量子安全通訊架構後，機器人系統是否仍能維持穩定定位能力，本研究整合 VSLAM 模組與安全通訊架構，並依據表 3及表 4 所列之硬體與軟體配置進行實驗測試。驗證平台以 TurtleBot3 為基礎，並使用 Raspberry Pi 4 (8GB) 作為主控單元。

本實驗架構硬體配置如表 3：

表 3VSLAM 模組與安全通訊硬體配置表

類別	設備名稱	說明
主控運算單元	Raspberry Pi 4 (8GB)	系統主要運算平台
影像感測模組	Pi Camera v2.1	即時影像擷取
光達感測器	360 LDS LiDAR	環境距離量測與定位輔助
運動控制板	OpenCR	馬達控制與底層驅動
慣性量測單元	外接 IMU 感測器	姿態與加速度量測

表 4 VSLAM 模組與安全通訊軟體配置表

類別	平台／模組	說明
作業系統	Ubuntu 22.04 LTS	系統執行環境
機器人中介層	ROS2 Humble	節點通訊與控制架構
視覺定位模組	ORB-SLAM3	視覺式定位與地圖建構

此平台用於評估在嵌入式硬體環境中，同時運行視覺定位與安全通訊架構之整體系統效能。

4.2 VSLAM 定位效能驗證結果

在測試環境中，機器人於室內場域進行自主移動與建圖任務，並記錄定位誤差與系統運行狀態。

如圖 10 ，VSLAM 軌跡估算結果與 ATE 分析圖。藍線為系統估算軌跡，黑線為地面真實軌跡（Ground Truth），紅線表示兩者誤差距離。實驗結果顯示平均絕對軌跡誤差 (ATE) 約為 18 – 21 公分。

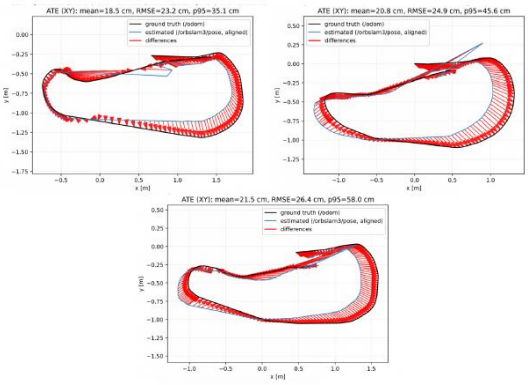

圖 10 VSLAM 軌跡誤差

如圖 11，mono_node 即時處理幀率變化圖。灰線為攝影機輸入幀率，藍線為 VSLAM 模組實際處理幀率。儘管輸入影像幀率存在波動，系統仍穩定維持在 14 – 22 Hz 之處理效能，顯示 Raspberry Pi 4 平台具備足夠之即時運算能力。

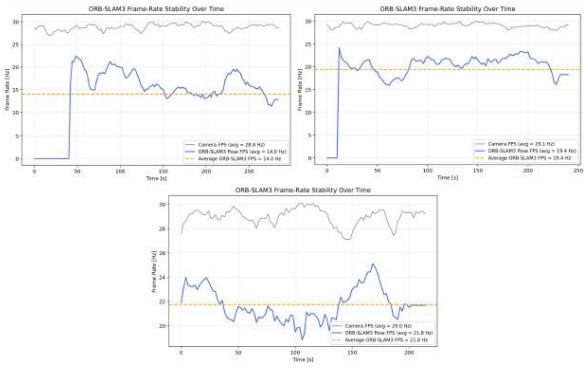

圖 11 VSLAM 的 FPS 穩定性

如圖 12所示， mono_node 執行期間之系統資源使用率。上圖為 CPU 使用率變化曲線，下圖為記憶體使用量變化曲線。實驗結果顯示平均 CPU 佔用率為 25.1%，平均記憶體使用量為 626 MB，證實 VSLAM 模組在 Raspberry Pi 4 平台上具備良好的資源效率。

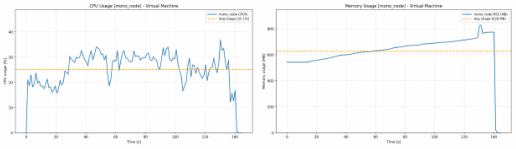

圖 12 VSLAM 模組系統資源佔用率

上述數據顯示，在 Raspberry Pi 4 平台上，ORB-SLAM3 模組可穩定維持即時定位能力，並未因嵌入式硬體限制而顯著下降。

4.3 安全通訊架構對定位模組影響評估

根據驗證平台測試結果顯示，在 Raspberry Pi 4（8GB）環境下，VSLAM 模組之平均絕對軌跡誤差（ATE）維持於約 18–21 公分範圍內，處理幀率穩定維持於 14–22 Hz，CPU 平均使用率約為 25.1%，記憶體使用量約為 626 MB 。上述數據顯示，在安全模組部署於網路層之架構下，視覺定位效能並未出現顯著下降，系統仍可滿足低速自主移動機器人之即時建圖與導航需求。

4.4 整合測試結果整理

綜合 VSLAM 模組與安全通訊架構整合後之實驗結果，可歸納如下表 5：

表 5 VSLAM 驗證結果摘要

指標	實測結果	結論
定位精準度 (ATE)	平均絕對軌跡誤差約 18–21 cm	定位穩定且一致，與地面真實軌跡高度吻合
即時處理效能 (FPS)	穩定維持約 14–22 Hz	滿足低速自主導航之即時建圖需求
系統資源占用 (RPi4)	CPU 約 25.1% / 記憶體約 626 MB	輕量化設計，保留充足資源供 PQC 模組使用

此結果證明，在既有 ROS 架構下導入後量子安全通訊後，機器人系統仍可維持原有即時定位與導航能力。

5. 綜合討論

本研究針對後量子密碼（PQC）整合至機器

人作業系統（ROS）之架構進行了全方位驗證，並從嵌入式裝置效能、系統層非侵入式保護及視覺定位穩定性三個維度展開深度討論。

5.1 後量子密碼於嵌入式平台之可行性與效能分析

根據第 2 章之實驗數據顯示，後量子演算法在資源受限裝置上展現出優異的運算效率，直接挑戰了過往認為 PQC 運算複雜度過高而難以部署於微型裝置的刻板印象。以 NIST 標準之 ML-KEM-768 為例，其在 ESP32-S3 平台上的 TLS 握手時間約為 310 ms，相較於傳統 ECC 演算法所需的 1088 ms，效能提升了約 3.5 倍。

這種高效能表現主要源於 ML-KEM 基於格（Lattice-based）的數學運算特性，其在通用型 MCU 上執行多項式運算的速度優於 ECC 的橢圓曲線點乘運算。此外，在記憶體資源極度受限的環境下，ML-KEM-512 與 768 等級的記憶體需求均能維持在 21–25 KB 左右，與傳統加密方案相近，僅有 1024 等級（約 30 KB）可能對極低階設備構成挑戰。由於 PQC 運算主要集中於初始連線建立階段，對後續資料傳輸的延遲與吞吐量未產生顯著負面影響，證實了在資源受限的物聯網環境中導入抗量子安全機制具有高度的實務可行性。

5.2 分層式安全架構之設計哲學與非侵入式特點

本研究提出的分層式安全架構，核心在於將 ML-KEM 整合至網路傳輸層的 WireGuard 隧道中，結合應用層的驗證。這種設計在系統層級體現了兩大關鍵價值：

1. 非侵入式部署（Non-intrusive Deployment）：由於安全模組部署於網路閘道器層，透過 VPN 隧道機制對 ROS 通訊進行透明保護，這意味著現有的 ROS1 或 ROS2 節點無須修改任何應用層程式碼即可完成量子安全升級，大幅降低了系統整合的複雜度與維護成本。

2. 混合式防禦策略（Hybrid Defense Strategy）：針對高頻寬、高流量的感測資料（如影像串流），系統維持在傳輸層進行加密保護，以避免重複加密造成的效能損耗。而針對關鍵的控制指令（如 /cmd_vel），則額外在應用層進行基於 ML-DSA 的數位簽章驗證。

實驗結果指出，雖然應用層驗證使端到端延遲增加約 3.5 ms（從低於 1 ms 提升至約 2–5 ms），但對於一般運行頻率在 10 Hz 至 50 Hz 的移動機器人而言，此延遲對即時控制的影響幾乎可以忽略不計，成功在安全性與系統負擔之間取得了平衡點。

5.3 視覺定位模組在加密環境下的穩健性實證

機器人的即時定位精度是衡量安全架構是否會干擾核心任務的最終標準。整合 PQC-WireGuard 隧道後，VSLAM 模組在 Raspberry Pi 4 上展現了極佳的運作韌性：

- 定位精確度保持：平均絕對軌跡誤差（ATE）穩定維持於 18–21 cm，且定位軌跡與地面真實值（Ground Truth）高度吻合，顯示底層加密處理並未導致感測數據封包的時序錯位或嚴重遺失。

- 導航即時性：系統處理幀率維持在 14–22 Hz，滿足低速自主移動機器人對於避障與建圖的即時性需求。

- 資源效率最優化：在執行高負載視覺運算的同時，CPU 平均佔用率僅約 25.1%，記憶體約占用 626 MB。

上述數據證明，分層式架構能有效隔絕「通訊安全運算」與「導航定位運算」間的資源競爭。即使在計算資源有限的嵌入式主機上，系統仍保有充足的運算餘裕，確保安全機制不會成為影響機器人行動安全的效能瓶頸。

5.4 應用場景延伸與未來擴展分析

綜合本研究成果，所提出之後量子安全架構展現了極強的適配性，不僅可應用於智慧城市級的 AMR 導航，亦具備延伸至智慧醫療、工業 4.0 等高密度物聯網場域的潛力。在 5G FWA 傳輸環境中，本架構能穩定承載平均 9.82 至 10.67 MB/s 的影像流量，顯示其具備支援高頻資料傳輸的能力。

未來研究可進一步結合 SD-WAN 技術與 FogROS2 雲霧協同架構，透過動態路由與鏈路品質監測，強化跨站點通訊的韌性。這種將後量子安全機制與彈性資源調度結合的趨勢，將為未來量子威脅環境下的智慧機器人系統提供更完整的防禦藍圖。

6. 結論與未來展望

6.1 結論

本研究針對智慧城市與物聯網環境下面臨的量子運算威脅，探討了後量子密碼（PQC）於嵌入式裝置與 ROS 通訊架構中的實作可行性。透過將 ML-KEM 整合至 TLS 1.3 協定堆疊，並於網路層導入混合式 PQC-WireGuard 安全隧道，我們成功建立了一套兼具抗量子安全性與即時通訊能力的防護架構。回顧本研究之實驗與系統驗證，具體貢獻可歸納為以下三點：

(1) 破除 PQC 於邊緣裝置的硬體效能迷思：過去常認為後量子演算法因運算負擔過大，難以部署於微型裝置。然而本研究實測證明，在 ESP32-S3 平台上執行 ML-KEM-768，其 TLS 握手時間僅需約 310 ms，計算效率反而比傳統 ECC 機制（約 1088 ms）提升了近 3.5 倍。這證實了金鑰封裝機制在資源受限的物聯網設備上的可行性甚至具備優勢。

(2) 提出「非侵入式」安全通訊架構：我們所設計的分層式架構，將加密隧道部署於網路閘道器層，並在應用層僅對關鍵指令進行選擇性數位簽章。這種設計使得既有的 ROS 系統不需要修改任何底層的 Topic 傳輸程式碼，即可獲得透明的安全覆蓋，大幅降低了大規模機器人系統升級量子安全的整合成本。

(3) 確保即時視覺定位（VSLAM）的穩健性：在導入混合式加密通訊後，實驗證實系統的導航核心並未受到拖累。ORB-SLAM3 在 Raspberry Pi 4 平台上依然能穩定維持 14–22 Hz 的即時影像處理幀率，且平均絕對軌跡誤差（ATE）控制在 18–21 cm 範圍內。這項數據充分表明，本架構成功在「高強度資安防護」與「即時導航效能」之間取得了最佳平衡。

6.2 未來展望

雖然本研究已初步驗證了後量子安全架構在單一與區域網路環境下的可行性，但面對未來更複雜的智慧場域，仍有以下幾個值得深入探討的研究方向：

首先是網路拓撲與硬體的廣泛擴展。目前架構主要針對點對點隧道進行驗證，未來計畫將此方案導入跨廠區、多節點的分散式網路中。若能進一步結合軟體定義廣域網路（SD-WAN）的動態路由與 FogROS2 雲霧協同技術，將能有效改善大範圍通訊的封包重組與延遲問題。同時，我們也將著手評估具備硬體加速指令（如 ARMv8 密碼學擴展）的處理器，以進一步探索 PQC 演算法的效能極限。

其次是進階應用場景的壓力測試。現階段系統已能滿足低速自主移動機器人的需求，但在無人機高速飛行或多台機器人密集協作的情境下，系統對通訊延遲與丟包的容忍度將更為嚴苛。面對攻擊者「現在截獲，稍後解密（Harvest Now, Decrypt Later）」的長期威脅，未來應建立一套涵蓋應用層至網路層的綜合資安評估框架，以確保 ROS 系統在未來的複雜實務場域中，能持續維持高度的安全韌性與運作穩定性。

7. 致謝

本研究之順利完成，首先誠摯感謝通訊作者董一志教授的悉心指導，以及其帶領之研究團隊所提供的全力支援。本文之核心實驗數據與系統架構，部分淬鍊自其實驗室所指導之優秀研究生李孟修與柯沛岑的碩士學位論文，兩位研究員在系統實作與數據收集上貢獻卓著，特此申謝。

8.參考文獻

1. Diputra, I. G. N. A. S.（2025）, “Performance Evaluation of Post-Quantum Cryptography on Resource-Constrained IoT Devices: A Case Study of Smart City Communication Security and ML-KEM/Kyber.” Master Thesis, Ming Chi University of Technology.
2. 李孟修（2025），後量子密碼學在機器人作業系統中的應用：基於 WireGuard 的安全通訊架構設計與效能評估，明志科技大學電子工程系碩士論文。
3. 柯沛岑（2025），後量子密碼學於資源受限物聯網裝置之效能評估：以智慧城市通訊安全與 ML-KEM/Kyber 為例，明志科技大學電子工程系碩士論文。
4. Shor, P.（1994）, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.”
5. Shor, P.（1997）, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.”
6. National Institute of Standards and Technology (NIST)（2024）, “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.”
7. Quigley, M., et al.（2015）, “Programming Robots with ROS.” O'Reilly Media.
8. Macenski, S., et al.（2022）, “Robot Operating System 2: Design, Architecture, and Uses in the Wild.”
9. micro-ROS Project（2023）, “micro-ROS: ROS 2 on Microcontrollers.” Official Documentation.
10. Object Management Group (OMG)（2019）, “DDS for Extremely Resource Constrained Environments (DDS-XRCE) Specification.”
11. White, R., et al.（2016）, “SROS: Securing ROS over the Wire, in the Graph, and through the Kernel.”
12. Mayoral-Vilches, V., et al.（2022）, “SROS2: Usable Cyber Security Tools for ROS 2.”
13. “About the DDS Security Specification Version 1.1.”
14. Donenfeld, J. A.（2017）, “WireGuard: Next Generation Kernel Network Tunnel.”
15. Amsters, R. and Slaets, P.（2020）, “TurtleBot 3 as a Robotics Education Platform.”
16. Zhu, J., et al.（2021）, “A Survey of Robotics Cybersecurity: From Single Robots to Multi-Robot Systems.”
17. Computer Vision Group（2014）, “TUM Visual-Inertial Dataset.”
18. Timperley, B., et al.（2022）, “A Systematic Assessment of Software Defects in ROS1.”