前瞻科技與管理　11 卷 1 期，1-14 頁（2022 年 5 月）
Journal of Advanced Technology and Management Vol. 11, No. 1, pp. 1-14 (May, 2022)
DOI:10.6193/JATM.202205_11(1).0001

5G 專網於 O-RAN 架構下的通訊資安發展趨勢

李大嵩 [1,2,*]　劉恩成 [3]

[1] 國立陽明交通大學電機工程學系教授
[2] 國立陽明交通大學物聯網智慧系統研究中心主任
[3] 國立陽明交通大學電子與資訊研究中心助理研究員

摘 要

政府及業界正積極推動 5th Generation Mobile Networks（5G）專網的發展，並使用 Open Radio Access Network（O-RAN）開放架構來滿足 5G 專網對高品質、低成本的需求，成為客製化情境應用如智慧工廠、智慧醫療、公共設施等廣受關注的解決方案。5G 專網為無線通訊應用帶來了高品質需求的應用情境，但同時其開放架構也對通訊資安帶來新的技術挑戰。本文章分析了 5G 公網與 5G 專網的技術及兩者對於資安需求的差異，針對 5G O-RAN 開放架構與通訊資安風險的關聯性進行討論，並探討 5G O-RAN 架構下的通訊與資訊安全標準的現況發展，另外也介紹 5G 與 Wi-Fi 技術在專網的整合及管理議題對資安帶來的挑戰，在文章最後也介紹人工智慧於 5G、Beyond 5G（B5G）的資安發展趨勢可扮演之角色。本文期能提供產學界在 5G 資訊安全發展趨勢的觀點，鼓勵更多產學合作及通訊技術研發新議題。

關鍵詞：5G 專網、AI 資安、O-RAN、資訊安全、開放架構資安

* 通訊作者：李大嵩
電子郵件：tslee@nycu.edu.tw
（收件日期：2021 年 8 月 16 日；修正日期：2021 年 9 月 22 日；接受日期：2021 年 9 月 24 日）

RECAST　Ainosco Press

Journal of Advanced Technology and Management Vol. 11, No. 1, pp. 1-14 (May, 2022)
DOI:10.6193/JATM.202205_11(1).0001

Trends of Communication Security of 5G Private Networks over O-RAN Architecture

Ta-Sung Lee[1,2,*], En-Cheng Liou[3]

[1]Professor, Department of Electrical and Computer Engineering, National Yang Ming Chiao Tung University
[2]Director, IoT & Intelligent System Research Center, National Yang Ming Chiao Tung University
[3]Assistant Research Fellow, Microelectronics and Information Research Center, National Yang Ming Chiao Tung University

Abstract

Fifth generation mobile networks (5G) private networks are being actively promoted not only by the government but in the industry. The open radio access network (O-RAN) architecture is adopted to meet the demand of providing high-quality and low-cost services, and thus, has become a popular solution for customized application scenarios, such as smart factories, smart hospitals, public utilities, etc. Although the 5G private networks can develop a new wireless scenario providing high-quality applications, the open RAN architecture unavoidably raises new technical challenges on communications security. This article addresses the differences of security requirements between 5G public networks and 5G private networks, meanwhile it discusses the interrelation and trends of the 5G O-RAN architecture, security standards and the risk of communication security. The integration and management issues with corresponding security challenges over 5G/Wi-Fi private networks are elaborated and followed by a discussion on how artificial intelligence (AI) can play a role in the trends of 5G and beyond 5G (B5G) security. This article shares our viewpoints on 5G information security and hopefully can motivate more opportunities for industry-academia cooperation and new research topics.

Keywords: 5G private network, AI security, O-RAN, communication security, security of O-RAN architecture

* Corresponding Author: Ta-Sung Lee
E-mail: tslee@nycu.edu.tw

壹、5th Generation Mobile Networks（5G）專網與 Open Radio Access Network（O-RAN）

一、5G 公網與 5G 專網

無線通訊技術已然成為人類族群的剛性需求，現今有 5G 及 Wi-Fi 無線行動通訊技術能為用戶提供廣域無線通訊的服務。在 5G 通訊技術發展或者是市場應用上，已逐漸的將 5G 公網以及 5G 專網視為兩種不同的面向，其中 5G 專網與 Wi-Fi 專網在無線通訊的市場及技術發展上產生重疊。對 5G 的終端用戶而言，5G 公網以及 5G 專網兩者皆遵循相同的 5G 國際標準並且可以使用相同的 5G 終端裝置進行連線，因此使用者實際感受差異有限，但對管理者或營運者而言，隨著公網與專網執行應用的不同，對覆蓋範圍及控制和管理的要求也會有所差異，因此 5G 公網及 5G 專網在技術的實現以及場域布建的類型上已經可以視為兩個不同的分類。在市場上，在 Gartner 技術成熟度曲線的分析中，5G 公網在 2019 年已從「期望膨脹」階段移至「破滅」階段（Panetta, 2019），然而 5G 專網在 2020 年的技術成熟度仍在「技術萌芽」的階段（Panetta, 2021）；在技術使用上，因 5G 公網對於廣域覆蓋的高度要求，會更加注重相關底層的無線通訊技術，並導入如 Massive Multiple-In Multiple-Out（MIMO）、Beamforming 等多天線控制及訊號集中的方式，達成同時具備高覆蓋率及大流量的傳輸效果，而在探討與 4th Generation Mobile Networks（4G）網路的相容性時，5G 公網選擇使用 Non-Standalone 架構與現有 4G 系統進行介接。在 5G 專網的布建上，為因應特定領域如智慧工廠、智慧醫療、智慧國防等需求，會更加在意其布建成本、資訊安全及特定領域的應用整合與控制上，並探討在單獨採用 5G Standalone 架構下，如何在效能、成本及資安上取得一個有效的平衡點。因此，除了國際標準組織第三代合作夥伴計劃（Third Generation Partnership Project, 3GPP）提供完整的 5G 架構及通訊協定標準外，以 5G 開放式架構設計及應用為目標的國際標準組織 O-RAN，其發展也備受關注。

二、5G O-RAN 開放架構、挑戰及資安風險

國際標準組織 O-RAN 成立的主要目的為推動行動通訊網路架構的開源架構，並以 5G 基地臺的技術發展為核心主軸，專注在連接介面的標準化、功能元件的虛擬化、基地臺設備的自動化、基地臺硬體的白牌化以及基地臺介面的互通性連接上。這樣的推動目標使得未來的基地臺有機會擺脫現行公網架構，減少單一或少數設備供應商鎖定或綁架營運商的機會，並且讓基地臺軟體及硬體進行分離，進而提供更多的選擇及差異化，讓電信商挑選更符合自己需求的基地臺軟硬體組合；對網通設備製造商而言，軟體與硬體的解構也同步的降低了開發技術門檻的需求：設備製造商更可以集中在自己本身的軟體或硬體的優勢，專注在自己擅長的製造流程及製造技術，提供一個較低技術門檻的進入機會。在臺灣，在科技技術發展及網通產業聚落十分完整的環境下，O-RAN 開放架構被許多臺灣製造網通設備、雲端設備等企業視為一個新的藍海市場，並且在近幾年間逐漸的統合天線廠、射頻元件／模組廠商、晶

片廠商、網通設備商、產品測試商、電信服務商、伺服器供應商成為一完整的 5G 基地臺生態系。對專網企業用戶而言，考量到自身智慧工廠、智慧醫療、智慧國防等產業特性、對專網自主性的需求及成本考量下，使用基於 O-RAN 開源架構下的 5G 專網相較於把公網的解決方案直接拿來用或者是使用公網設備以網路切片技術提供專網服務會更具吸引力。對電信商而言，除了有機會切入專網市場外，以 O-RAN 開放架構的成本優勢，在布建上可以先以技術需求較低或使用人數較少的地點探討如何整合或取代現有的公網設備，並在後續提供更多客製化的服務，並逐漸地掌握技術核心及技術研發方向，也驅動著電信業持續關注 O-RAN 標準。以 O-RAN 開放架構導入智慧工廠為例，使用 5G O-RAN 專網來進行工廠內的布建、並導入相關人工智慧圖形辨識技術，進行工業製造流程的資訊搜集及回饋（如自動光學檢查技術 [Automated Optical Inspection, AOI]），並搭配工廠之間的訊息傳遞及遠端或異地工廠的控制管理協助等需求，將促進 O-RAN 開放架構的 5G 專網導入製造業，並進一步的加速智慧工廠的發展。

然而 O-RAN 開放架構在目前的技術成熟度與現行封閉式架構有所落差的情況下，在生態鏈的建立、整體系統的效能，以及系統安全性上仍難與現行的封閉式架構匹敵。在 5G 專網對產業帶來的投資效益有待證明下，現行業界仍在觀望相關技術及市場的發展是否足夠成熟，並期待政府、標竿企業或大型場域的成功案例進行示範，直到在技術逐漸成熟下才有望提升市場的導入意願與速度。在技術與生態鏈的發展上，主要的挑戰來自於電信業的技術要求本身就有別於傳統網通產業，在新的 O-RAN 開放架構生態鏈構建的同時，多個廠商的整合與合作模式仍有待摸索，且急需熟悉網路通訊及行動通訊市場及技術的雙棲高階人才進行管理及整合，為滿足 5G 企業專網的技術需求並有效創造新的技術鏈結；在整體系統的效能發展上，即便 5G 的技術發展主要訴求為大流量、低延遲及高連線數等高服務品質的技術指標，但受限於 O-RAN 開放架構與白牌硬體的成本考量下，通常都會優先考慮將系統效能進行一定程度的控制以降低成本，除了反映在覆蓋率、底層無線技術模組的選擇上，也連帶反映在整體端對端的效能及穩定性上。在系統安全性的發展上更是險峻，除了多個廠商同時合作開發，對資安要求及理解本身就會有認知或習慣上的落差外，也會受限於廠商之間的技術實現細節的交流可能會無法像封閉式廠商一樣的透明。除此之外，來自各個不同專業的製造商對同一份國際標準也可能會因自身的經驗產生實作上的落差。在 O-RAN 開放架構仍在技術萌芽期的階段下，大部分的發展仍注重在功能的完整度以及效能的達標上，對 O-RAN 開放架構下的資訊安全更是難以期待一次到位，導致了現行 O-RAN 開放架構下的基地臺設備仍難以用傳統 5G 電信技術的高品質、高資安、高效能的要求去檢視或整合，並且在效能上與 Wi-Fi 沒有明顯落差。此外，頻譜及基地臺成本仍難以反映出商業效益，也會更進一步降低導入的意願，並且在資安風險仍有疑慮的情況下，更使得 O-RAN 架構的技術的發展速度及投資備受考驗。

為了加速 O-RAN 開放架構的發展並降低上述疑慮，O-RAN 標準組織在 2021 年進行組織的調整及更動，除了強化以往針對互通及功能性的要求外，針對資安面的技術要求以及管理面的流程要求有了更加獨立且完整的規劃及關注。O-RAN 國際標準組織在發展的初期把資安以及管理融入在各個工作小組上，今年則調整為將資安及管理分別獨立為單獨的工作小組（Working Group）及焦點團體（Focus Group）進行獨立的探討，並進一步的去分析如何整合 3GPP 的國際資安標準架構及整個端對端的 5G 系統的資訊安全管理及檢測規範。本文

後續章節將針對 3GPP 的資安標準、核心網路及基地臺的資安架構，以及 5G 專網相關的資訊安全及應用發展進行討論及分析，並圍繞著 5G 專網及 O-RAN 架構下探討可能的技術整合及測試，最後提供 5G 及 Beyond 5G（B5G）專網的資訊安全技術發展趨勢及展望。

貳、5G O-RAN 架構下的通訊與資訊安全標準與現況

一、3GPP 標準的資訊安全標準架構及檢測

無論是 5G 公網還是 5G 專網，最源頭的技術發展都是來自於 3GPP 國際組織，同樣的考慮 5G 資訊安全架構與解析，也是以 3GPP 國際標準做為最根本的考量。跟 5G 有關的資安標準架構最初可追朔到在 4G 時所做的技術報告 TR 33.805（3GPP, 2013），此報告旨在探討針對行動通訊的產品對資安的保證方法以及要求，並且跟 Groupe Speciale Mobile Association（GSMA）、Cellular Telecommunications Industry Association（CTIA）、International Organization for Standardization（ISO）、International Telecommunication Union（ITU）等國際組織進行交流討論，並且探討如何標準化行動通訊的資訊安全所產生的認證及監管需求，並且定義出「3GPP 安全保證框架（Security Assurance Methodology, SECAM）」。此技術報告有別與以往傳統的互通性測試，其定義了不同網路產品的等級並且針對各種不同的等級提供共同可測試的資訊安全品質基準，涵蓋了相關的風險模型以及在各種不同資安等級下所定義的標準內容，後來衍伸成為 Security Assurance Specifications（SCAS）標準，並應用在 5G 行動網路上面。在該技術報告中有明確定義產品的範圍在 4G 的架構下包含基地臺、核心網路的部分包含 Mobility Management Entity（MME）、Serving GPRS Support Node（SGSN）、Serving Gateway（SGW）、Packet Data Network Gateway（PGW）、Home subscriber server（HSS）、Policy and Charging Rules Function（PCRF）、Authentication Authorization Accounting（AAA）伺服器、Operations, Administration, and Maintenance（OAM）系統及應用，以及 Call Session Control Function（CSCF）等功能，因此，在後續探討 5G 網路資訊安全時，相關的功能及介面都應納入 3GPP 的資訊安全架構中。除了明確定義哪些行動網路功能元件應被納入資訊安全架構外，該報告也同時描述了電信商如何確保供應商該如何滿足標準的資訊安全保證的流程，以及對認證機構的角色進行描述，並且說明了相關評估的測試方法之深度、範圍以及嚴謹程度：在合規性測試上主要以黑箱測試為主，但跟密碼學相關的標準可用白箱測試作為補助；在漏洞測試上雖以黑箱進行為原則，但需先根據目標環境及功能進行威脅分析，並定義了在測試的過程中需要提供的文件、操作說明、測試結果的展示及驗證方法等，且根據不同的等級，針對硬體、作業系統以及 5G 標準的合規性進行檢測。

延續 3GPP TR 33.805 提供對 SECAM 的框架及定義、在 TR 33.916（3GPP, 2020a）中明確定義相關的檢測及認證單位是由 GSMA 負責主導，針對行動通訊的相關設備開發、設備生命週期的管理過程、安全合規測試、漏洞分析等進行評估，並且說明所有基於 3GPP SECAM 所規範的行動網路設備該如何定義安全問題、收斂安全需求、完善測試案例的建立流程，最終根據不同的行動網路設備產出相應的 SCAS 標準。在經過 TR 33.926（3GPP, 2021g）定義行動網路設備的通用資安威脅及各設備的關鍵資產、3GPP TR 33.117（3GPP,

2021c）定義行動網路設備針對技術、作業系統、網路伺服器、相關網路設備及網路功能基本資安要求及相關的測試案例後，產生 4G 核網元件 MME 的 SCAS 標準 3GPP TS 33.116（3GPP, 2020c）、4G 核網元件 PGW 的 SCAS 標準 3GPP TS 33.250（3GPP, 2020b）、4G 基地臺的 SCAS 標準 3GPP TS 33.216（3GPP, 2021e）。在行動通訊標準演進至 5G 的過程中，也一併於 3GPP TS 33.501（3GPP, 2021d）標準中探討了整體行動網路的資訊安全架構，並制定 5G 基地臺的 SCAS 標準 3GPP TS 33.511（3GPP, 2021f），而 5G 核網中的 11 個元件分別被定義在 3GPP TS 33.512（3GPP, 2021a）至 3GPP TS 33.522（3GPP, 2021b），另外，針對虛擬化的威脅分析研究在 3GPP TS 33.848 進行討論，最終定義虛擬化行動通訊設備的 SCAS 標準 3GPP TS 33.818。整體基於 3GPP 資訊安全的主要文件分類及 SCAS 標準的整理如表 1 所示。

表 1 SECAM 的框架及 SCAS 系列標準分類盤點

分類	相關標準	說明
通用資安方法	3GPP TS 33.805、3GPP TS 33.916	網路設備的安全確保及評估
通用案例	3GPP TS 33.926、3GPP TS 33.117	通用威脅分析、安全需求與測試案例
虛擬化網路單元	3GPP TS 33.818、3GPP TS 33.848	虛擬化設備安全及衝擊評估
4G 網路單元	3GPP TS 33.116、3GPP TS 33.216、3GPP TS 33.250	4G 核心網路及基地臺元件 SCAS 系列標準
5G 網路單元	3GPP TS 33.511、3GPP TS 33.512、3GPP TS 33.513、3GPP TS 33.514、3GPP TS 33.515、3GPP TS 33.516、3GPP TS 33.517、3GPP TS 33.518、3GPP TS 33.519、3GPP TS 33.520、3GPP TS 33.521、3GPP TS 33.522	5G 核心網路及基地臺元件 SCAS 系列標準

資料來源：作者研究整理。

SCAS 的檢測流程主要可以分成三個階段，在第一階段主要跟據前述標準進行設備的檢測及評估，評估須藉由有公信力的機構，並以 GSMA 為主要執行單位，其檢測實驗室也應包含 ISO/IEC 17025 認證的測試實驗室。廠商藉由測試實驗室的評估取得相關評估報告後即進入第二階段，可自行宣布評估結果或者交由認證方來頒發證書，以此證明此設備產品具備 3GPP 所要求的安全性。在第三階段針對設備的資安弱點則交給資安實驗室，針對相應弱點規範及漏洞檢測進行確認。臺灣資通產業標準協會也針對 5G 基地臺的資安檢測相關流程進行 5G 基地臺資安測試規範的擬定及規劃。3GPP 也與 GSMA 共同主導制定了網路設備的資安確保方案（Network Equipment Security Assurance Scheme, NESAS），並制定網路設備的資安標準認證計畫，若廠商滿足所有的 NESAS 安全要求，其結果就能在 GSMA 相應的網站上公布，作為營運商參考的測試報告。

以 5G 的基地臺 SCAS 標準為例，在本文撰寫的時候最新的版本為基於 3GPP Release 17 所制定的基地臺 SCAS 標準，在安全功能要求上面主要探討基於控制層 Radio Resource Control（RRC）訊令的完整性、資料層數據的完整性、校驗失敗時的反應、加密演算法的

確認、重放行為的保護、密鑰的更新、N2 及 Xn 介面的機密性及完整性保護等確認。在技術的要求下面主要檢查對資料以及訊息的保護，避免未經過授權的檢視，以及在儲存及傳輸過程中的保護及紀錄等，並要求 5G 基地臺的作業系統及網頁伺服器需比照 3GPP TR 33.117 標準所定義的規範。因 5G 基地臺 SCAS 標準主要是針對設備的介面、加密的機制、傳輸的機密性及完整性進行保護，並未針對 5G 公網及 5G 專網的特性差異如不同的覆蓋率、應用及使用者行為進行討論，因此在 5G 公網及 5G 專網的設備上應可使用相同的資安標準流程進行檢測，並根據前述檢測流程取得評估報告及規範，以此來初步證明 O-RAN 開放架構下的基地臺是具備符合 3GPP 資訊安全框架的相應資安等級。

二、O-RAN 標準的資訊安全架構

在 O-RAN 國際組織的推動下，實現基地臺的方式由傳統的封閉式軟硬體整合逐漸走向軟體化及虛擬化，藉由軟體實現 5G 3GPP 的標準通訊流程，且利用開放架構下的硬體及介面進行互通，整合 O-RAN、Multi-access Edge Computing（MEC）、3GPP 之 5G 專網系統架構示意圖如圖 1 所示。在理想的開放架構下，因軟體具有高彈性以及快速更新的特色，可有效率利用以提升軟體的資安品質架構，並且可將軟硬體的漏洞進行獨立考量以及檢測。另外，藉由容器化或者是雲端化的技術，開放架構的基地臺得以進行快速資安偵測、持續性整合或著自動化測試。然而，軟體開發上在 5G 基地臺的高品質效能及資安要求下面臨了難以想像的挑戰，如軟體開發常使用現有的開源工具，因資訊透明化導致駭客有機會利用程式碼開採資安漏洞，最終造成嚴重的零時攻擊。因此，O-RAN 架構下的資訊安全除了傳統電信業所要考量的資安外，對於軟體資安的識別以及防禦上應更加重視，可多參考包含開源專案、虛擬化及容器化專案之資安框架及軟體開發生命週期（System Development Life Cycle, SDLC）的管理等。

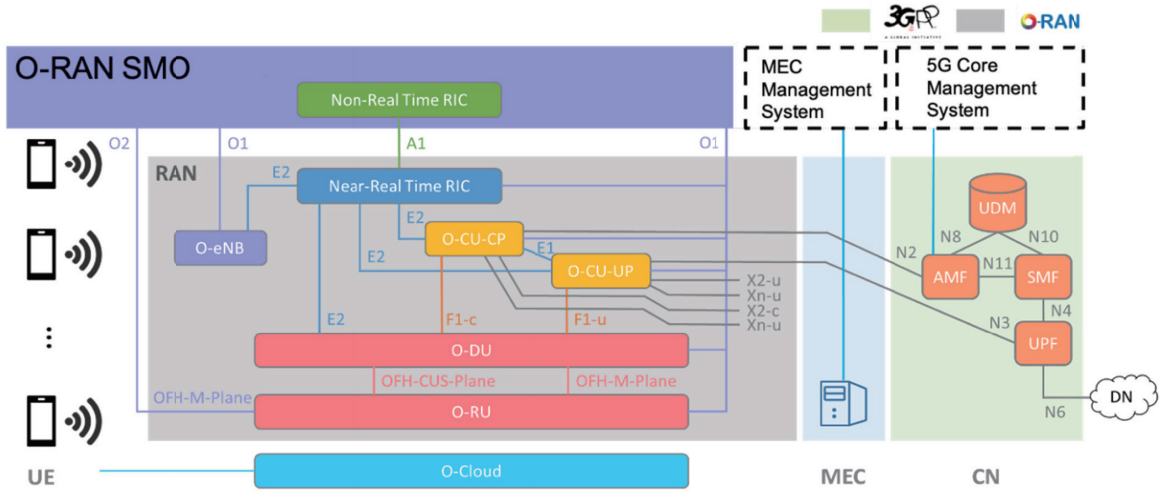

圖 1　整合 ORAN、MEC、3GPP 之 5G 專網系統架構示意圖

資料來源：作者研究整理。

在 O-RAN 開放架構下，若根據不同的資安威脅進行分類及檢視，其管理介面對資訊安全的影響及危害最大。因此，如何以零信任架構為基礎進行相應的資料及服務的保護、訊息與傳輸過程中的加密、連接的完整性、日誌或紀錄的保存等，並加強保護相關介面的資訊安全，包含使用加密傳輸或導入相應資安檢測機制等方式，為 O-RAN 資安小組所發展的重點。在 O-RAN 的資安焦點團體內也針對資安威脅模型進行討論，包含 O-RAN 系統的威脅模型、O-RAN 雲端系統的威脅模型、開源程式碼的威脅模型、物理層的威脅模型、5G 無線網路的威脅模型以及機器學習的威脅模型等。典型的實施範例如使用業界成熟的加密工具如 SSH/TLS 傳輸機制等，並可支援 NETCONF 格式。上述標準協議在 O-RAN 的資安焦點團體內被討論及標準化。預計在 O-RAN 開放架構下的安全傳輸模型其影響介面包含與管理系統連接的 O1 介面、與雲端應用連接的 O2 介面、Non-Real Time RAN Intelligent Controller（RIC）與 Near-Real Time RIC 連接的 A1 介面、基地臺與 Near-Real Time RIC 連接的 E2 等介面等，都是主要應特別考量或需強化資安保護的介面。

三、5G 專網用戶端與應用端的資安議題

在 5G 專網與 O-RAN 架構下，前述 3GPP 標準及 O-RAN 標準的資安架構主要是基於在布建基地臺及核網時，以提供基本服務為假設可能會引發的資安威脅。順帶一提，在 5G 公網下最容易從用戶端引起的資安議題主要為向前相容 4G 或 3th Generation Mobile Networks（3G），因先前標準架構的資安漏洞受限於標準的設計而難以被完全填補，並且在 5G 的 Non-Standalone（NSA）架構或漫遊架構下影響現行的 5G 網路，這方面的問題在一開始即採用獨立組網架構的 5G O-RAN 架構的專網下問題不大。然而，在 5G 專網下，以企業專網為例，針對終端用戶及其他物聯網裝置所引起的資訊安全，包括與智慧工廠應用相互結合時，導入 MEC 並在智慧工廠的布建場景下，也有相應的應用端資安議題需要注意，而應用端引起的資安議題也包含第三方應用程式，在整合時因軟體化及虛擬化的開放架構設計導入至 5G 傳輸標準，導致 5G 協定在進行軟硬體資源配置或網路切片的快速布建（Lai, Lai, and Lai, 2020）及網路設定時，其硬體資源或網路切片的獨立性被攻擊或耗盡資源。5G 協定有關的資安議題已在先前的段落進行相關資安框架的討論，並預期能靠上述的資安框架進行緩解，本段落探討基於物聯網裝置、MEC 及系統整合所引起的資安議題。

物聯網裝置的資安議題在 4G 標準的 NB-IoT 架構下引起了廣泛的討論，這些資安議題在 5G 專網的用戶端主要為物聯網裝置時也仍然存在（Dutta and Hammad, 2020）。在物聯網的資安議題上，主要藉由完整性、保密性、可用性、真實性等進行資安通訊的設計（Chettri and Bera, 2020），但物聯網裝置的資安等級受限於硬體成本考量，在一般情況下不會選擇使用可支援高複雜度的密碼學以及加密通訊等機制，而將寶貴的硬體資源提供給合規的傳輸以及效能的要求上。因此，低價的 5G 物聯網裝置選擇在使用最基本的 5G 通訊模式下，有機會引發相關金鑰管理以及認證的議題，對此有非常多的文獻進行討論與分析（Sanchez-Gomez et al., 2020），值得一提的是，物聯網裝置的資安議題也更為常見在以 Wi-Fi 技術為專網的情境中。

此外，MEC 與 5G 專網的整合應用，也對資安議題帶來雙重的挑戰。邊緣運算主要的功能及特色為建構一低延遲的服務，並以較少的節點數量滿足低延遲需求，以在整體服務流

程中都能獲得保證。然而，若該服務流程涉及核心網路的註冊、認證等機制，若將相關的控制封包直接提供給核心網路，則無法有效的低延遲需求；反之，若相關的註冊、認證及收費機制不被考慮，則該服務的資安風險就會顯著提升，即便部分的服務僅需要在服務開始的前期進行相關註冊、認證、授權等控制訊息的交換，但在部分應用可能為長時間或具備移動性的應用服務，因此仍會產生 MEC 與 5G 專網的整合應用資安議題。雖然（Li et al., 2020）在該文獻中提供了一個兩階段的資安機制可解決的問題，但在標準化未全面強制支援的情況下，是否會有相應或類似的機制全面性的普及在 5G 專網的架構中仍是值得持續觀察及討論的議題。

現行的資安技術在單獨檢視或著是硬體成本足夠的情況下，似乎都有機會解決相應的資安議題，如業界已根據前述問題提供部分的解決方案（Trend Micro, 2021），整合資訊科技（Information Technology, IT）與通訊科技（Communication Technology, CT）的資安議題，並提供相關可視性介面及資安政策的管理。該方案的主要特點為在核心網路提供流量的監控及偵測，在終端裝置以 SIM 卡或應用程式與核心網路的監控系統進行聯防，若是偵測到資安風險的情況下，防護系統可直接進行裝置隔離或流量阻斷。即便完整的布建有機會解決相關的物聯網及 MEC 的資安議題，然而，由於現行 5G 專網的布建規劃及建置仍高度仰賴大量的專業人員以及人員的布建經驗，因此新的風險會在 5G 專網評估及規劃，因高度複雜的技術整合，以及橫跨有線網路的封包及無線網路的資源下將難以以人力進行完整的資安考量。如何以高度自動化或著是智慧化的方式進行高資安的 5G 專網規劃及布建，且根據不同的專網應用情境進行導入測試，並在維運的過程中持續優化並監控相關的資安風險及威脅，將是 5G 專網在資訊安全上一個非常重要的議題。我們將根據此議題於後續段落進行討論。

四、5G 與 Wi-Fi 技術整合之專網資訊安全

專網的需求源自於公用網路沒辦法處理的安全性議題，並且盡力的提供一個具備安全性或是高可靠性的網路環境，隨著無線網路技術的發展，逐漸開始產生高網路連線品質的需求。行動網路技術在控制平面的權限設計以及核心網路路由架構（4G 以 SGW、PGW 為主、5G 以 User Plane Function [UPF] 為主）提供一個較為完整的有線及無線網路安全性的整合，就長期發展和演進而言似乎是一個比較完善的解決方案，相較之下，Wi-Fi 專網雖在無線接入端有相應的 SSID 認證機制，但在缺乏後端路由設計及對用戶端認證的搭配下，其控制的集中性以及全面性仍需要透過額外的系統來進行輔助，如常見的用戶登入畫面等。但 Wi-Fi 網路技術在布建的成本以及用戶端的普及性上具備明顯的優勢，因此在現今 5G 專網的網路安全性及穩定性尚未發展成熟前，5G 技術在專網的效能表現與資安等級和 Wi-Fi 專網相比差異不大，但考量到 5G 與 Wi-Fi 這兩種無線技術在商業布建成本及技術完整度，如何進行兩種無線技術的相互整合及搭配以取得在成本及技術上的平衡點將變得非常重要。因此，5G 專網環境與 Wi-Fi 無線技術的整合議題成為產業界的一個關鍵需求（Naik, Park, Ashdown, and Lehr, 2020）。

在專網的議題上，Wi-Fi 與 5G 兩者競合關係會隨著 5G 技術的發展成熟度的進程而有不同階段的議題需要討論，並探討如何使用前述兩者無線通訊技術滿足專網需提供特定範圍、特定領域、特定應用的高安全性服務模式。使用單一無線通訊技術進行專網的布建都有其限

制，相關無線通訊技術的優勢示意圖如圖 2 所示：5G 行動通訊在提供高品質傳輸服務的同時，高功耗及高布建成本成為他的致命傷；Wi-Fi 技術在提供低成本的布建的同時，受限於共享頻譜及路由器的成本限制，使得傳輸的品質不穩定。兩者若有極低功耗的需求，極有可能搭配藍牙低功耗（Bluetooth Low Energy, BLE）作為最後的解決方案。換言之，受限於各自在技術上及商業上的優勢及劣勢，因此並無單一技術能達成最佳解。回顧無線通訊的落地及演進，在專網的需求及應用導入上，混合型 5G 專網為最可能的實現方向，其主要的模式與現行混合型環境一樣，具有多樣化的通訊技術，手機內也同時具有 5G 以及 Wi-Fi 的傳輸晶片，有高品質需求時使用 5G 專網，有低功耗需求時使用 BLE 通訊，而有低成本需求時則使用 Wi-Fi 網路。

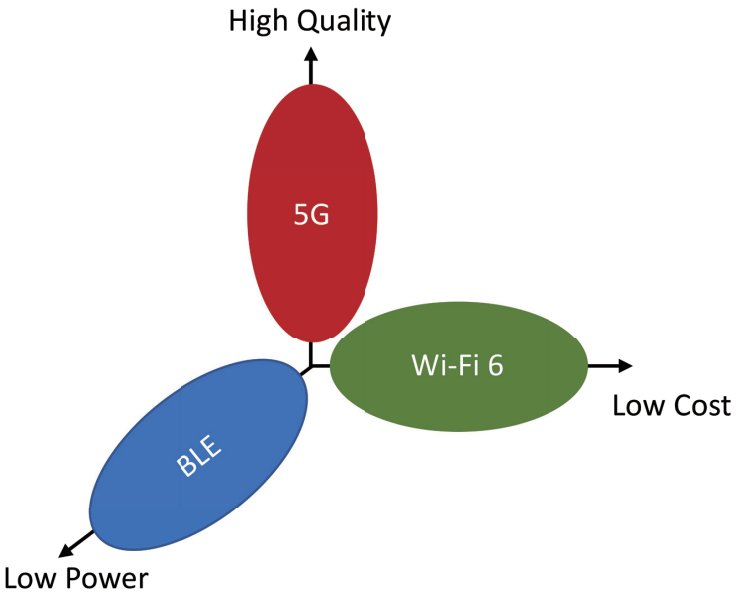

圖 2　現行應用需求及選用之無線網路通訊技術示意圖

資料來源：作者研究整理。

現行整合 5G 及 Wi-Fi 技術的專網，又稱混合型專網，在網路管理的許多方面都仰賴虛擬化技術解決傳統 IT 環境中的固有問題。然而，虛擬化技術受限於不能良好地針對各種服務進行即時性調整，也面臨了許多挑戰。舉例而言，虛擬化技術不能靈活地使用開放的接口進行管理和控制，也無法在共享硬體資源或軟體設備的各種不同使用連線時靈活的變動。

在 5G 技術發展的同時，為了更加強化整合 5G 及 Wi-Fi 技術的專網，其中一個可能的作法為使用網路切片的技術統整混合型專網無線管理系統，通訊方式以 5G 傳輸通道為主，在斷線時以 Wi-Fi 進行輔助，並連接專網的應用服務，以指定流程處理該服務的控制平面和用戶平面。另外一種可能的作法為利用 Wi-Fi 跟 5G 的路由器轉換裝置，將兩種無線傳輸技術同時作為專網的最後一哩。學術界和業界的普遍共識是：網路切片將與雲端伺服器的技術類似，以使用軟體定義網路（Software Deflned Network, SDN）、網路功能虛擬化（Network

Function Virtualization, NFV）、相關 IT 管理協作機制進行開發。預期使用相關網路切片技術來提升運營效率、縮短新服務的上市時間，並為 Over-the-Top（OTT）參與者和垂直行業打開新的商機。混合型專網的管理議題也在國際標準組織的網路切片管理、ETSI NFV 管理以及 3GPP 5G 管理上有相關的介面及設計。在混合型專網環境下的資訊安全管理與測試中，會更加仰賴如何以現行國際組織的資訊安全架構為主，進行端對端的資安檢測流程及服務。以 O-RAN 國際標準組織為例，其 2021 年的 PlugFest 互通大會，其主要的重點項目除了互通之外，也探討如何基於 O-RAN 開放架構下實現 SCAS 資安架構，或針對網路管理的議題進行端對端的驗證或展示。

參、5G、B5G 專網的資訊安全發展趨勢

本段落將針對 5G 及 B5G 時代的專網資訊安全發展趨勢進行探討，並著重探討兩點：一、人工智慧驅動 5G、B5G 專網控制平面的資訊安全，以及二、5G、B5G 專網的資訊安全管理。

人工智慧的相關技術應用在 5G 上已有許多研究（Lin, 2020），如使用人工智慧來控制波束成型（Kao, Zhan, and Lee, 2018）的以人工智慧進行資訊安全的控制及檢查已逐漸變成一個主流的研究趨勢，傳統使用特徵碼來進行資安入侵檢查的方式僅能防堵病毒或惡意程式入侵的一個簡易手段。然而，針對標準或流程上的漏洞，以及具備惡意流程的判定，很難靠著簡單的決策樹邏輯或者是固定的演算法來判定，而是要參考更多相關的參數以及相關過往的數據來輔助判定。此時，使用人工智慧來協助預測相關的流量或判斷操作流程是否為惡意行為成為一個十分合適的選擇。在有線網路的數據傳輸或者是在傳統資料平面上的數據傳輸上，通常只需要檢查用戶的數據，並且及時的去防堵或隔離相關的惡意流量即可。然而，在 5G 專網的環境下，用戶傳送的資料除了資料平面的數據外也包含部分的控制平面數據，如註冊、撥號、換手等行為都跟控制平面的數據有關。因此，考量到控制平面遭受攻擊所造成的衝擊遠高於資料平面，如何判別控制平面的惡意流程以及預測現行 5G 標準控制平面上的潛在漏洞，以及防堵相關惡意行為，或者是如何不要讓人工智慧變成 5G 的威脅（Benzaïd and Taleb, 2020）為現行國際標準組織正在積極討論的議題。

在人工智慧有機會成為 5G 專網的資安技術下，如何在 5G、B5G 專網下引入人工智慧於資訊安全管理成為一個關鍵。在 O-RAN 國際標準組織的推動下，目前已有相關管理系統的架構，針對 Non-RT-RIC 以及 Near-RT-RIC 進行相關人工智慧模組的導入及管理機制，並且成為 Service Management and Orchestration（SMO）的一個參考框架，整合人工智慧與 O-RAN 開放架構的資安數據訓練及管理示意圖如圖 3 所示。以 5G 專網典型的智慧工廠環境為例，其環境會包含感測器、致動器或是其他 M2M/IOT 等設備，而這些 IOT 流量絕大多是未加密流量，易受到中、高度危害的攻擊，此時藉由 5G 開源架構（O-RAN）並結合基於人工智慧的 IOT 攻擊偵測技術（例如入侵偵測系統、DDoS 攻擊偵測等），且同時對專網環境的控制平面及資料平面進行監控及偵測，此外也可依照企業的場域與策略彈性調整人工智慧攻擊檢測應用，可幫助在建置 5G 智慧工廠專網的同時確保其安全性。

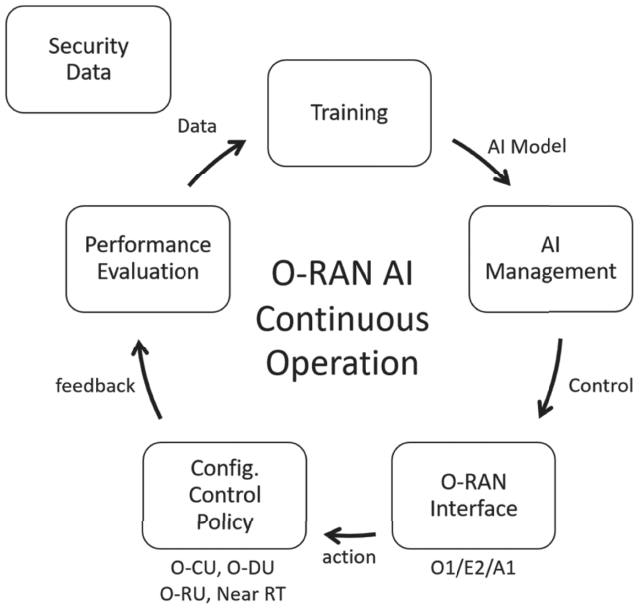

圖 3　整合人工智慧與 O-RAN 開放架構的資安數據訓練及管理示意圖

資料來源：作者研究整理。

肆、結論

5G 專網使用 O-RAN 開放架構並與 Wi-Fi 技術整合是一個加速 5G 專網發展的一個新契機，但在資訊安全的考量及設計上仍是一個充滿挑戰的領域。如何分離 5G 公網和 5G 專網上的資安需求，並且針對 O-RAN 開放架構下的資訊安全進行有效的偵測、管理及營運，將成為 5G O-RAN 專網能否蓬勃發展的一個重要議題。此外，如何整合現有 Wi-Fi 技術並針對特定應用情境進行專網布建，以及在上述整合架構下滿足相應的資安等級，也是本文作者未來所關注的方向。最後，在 5G、B5G 專網的資訊安全發展趨勢中，期待相關的介紹和討論能提供人工智慧驅動專網管理的一個新契機，並讓更多興趣的同業們能加速相關技術及產業的發展。

參考文獻

3GPP, 2013/12, "Study on Security Assurance Methodology for 3GPP Network Products," *TR 33.805*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2304 (accessed January 4, 2022).

3GPP, 2020a/7, "Security Assurance Methodology (SECAM) for 3GPP Network Products," *TR33.916*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx-

?specificationId=2345 (accessed January 4, 2022).

3GPP, 2020b/7, "Security Assurance Specification for the PGW Network Product Class," *TS33.250*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3100 (accessed January 4, 2022).

3GPP, 2020c/7, "Security Assurance Specification (SCAS) for the MME Network Product Class," *TS33.116*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2270 (accessed January 4, 2022).

3GPP, 2021a/12, "5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF)," *TS33.512*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445 (accessed January 4, 2022).

3GPP, 2021b/12, "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)," *TS33.522*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3750 (accessed January 4, 2022).

3GPP, 2021c/6, "Catalogue of General Security Assurance Requirements," *TS33.117*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928 (accessed January 4, 2022).

3GPP, 2021d/6, "Security Architecture and Procedures for 5G System," *TS33.501*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (accessed January 4, 2022).

3GPP, 2021e/6, "Security Assurance Specification (SCAS) for the Evolved Node B (eNB) Network Product Class," *TS33.216*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3129 (accessed January 4, 2022).

3GPP, 2021f/6, "Security Assurance Specification (SCAS) for the Next Generation Node B (gNodeB) Network Product Class," *TS33.511*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3444 (accessed January 4, 2022).

3GPP, 2021g/4, "Security Assurance Specification (SCAS) Threats and Critical Assets in 3GPP Network Product Classes," *TR33.926*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3002 (accessed January 4, 2022).

Benzaïd C., and Taleb T., 2020, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" *IEEE Network*, 34(6), 140-147. doi:10.1109/MNET.011.2000088

Chettri L., and Bera R., 2020, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, 7(1), 16-32. doi:10.1109/JIOT.2019.2948888

Dutta A., and Hammad E., 2020, "5G Security Challenges and Opportunities: A System Approach," in *Proceedings of 2020 IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India: IEEE. doi:10.1109/5GWF49715.2020.9221122

Kao W.-C., Zhan S.-Q., and Lee T.-S., 2018, "AI-Aided 3-D Beamforming for Millimeter Wave

Communications," in *Proceedings of 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Ishigaki, Japan: IEEE. doi:10.1109/ISPACS.2018.8923234

Lai W.-P., Lai H.-L., and Lai M.-J., 2020, "A Design Framework of Automatic Deployment for 5G Network Slicing," in *Proceedings of 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Auckland, New Zealand: IEEE.

Li C.-Y., Lin Y.-D., Lai Y.-C., Chien H.-T., Huang Y.-S., Huang P.-H., and Liu H.-Y., 2020, "Transparent AAA Security Design for Low-Latency MEC-Integrated Cellular Networks," *IEEE Transactions on Vehicular Technology*, 69(3), 3231-3243. doi:10.1109/TVT.2020.2964596

Lin B.-S. P., 2020, "Toward an AI-Enabled SDN-based 5G & IoT Network," *Network and Communication Technologies*, 5(2), 7-14. doi:10.5539/nct.v5n2p7

Naik G., Park J.-M., Ashdown J., and Lehr W., 2020, "Next Generation Wi-Fi and 5G NR-U in the 6 GHz Bands: Opportunities and Challenges," *IEEE Access*, 8, 153027-153056. doi:10.1109/ACCESS.2020.3016036

Panetta K., 2019/8/29, "5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019," *Gartner*, https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019 (accessed January 4, 2022).

Panetta K., 2021/3/8, "5 Trends Drive the Gartner Hype Cycle for Emerging Technologies, 2020," *Gartner*, https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020 (accessed January 4, 2022).

Sanchez-Gomez J., GarcíA Carrillo D., Sanchez-Iborra R., Hernández-Ramos J. S., Granjal J., Marin-Perez R., and Zamora-Izquierdo M. A., 2020, "Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions," *IEEE Access*, 8, 216437-216460. doi:10.1109/ACCESS.2020.3041057

Trend Micro, 2021/8/1, "Mobile Network Security," https://www.trendmicro.com (accessed August 1, 2021).