探究 5G 資訊安全

國立中山大學資訊工程學系博士研究生 / 施宇澤
國立中山大學工學院院長 / 范俊逸

關鍵字：資訊安全、第五代行動通訊網路、5G 安全、通訊協定、認證機制

前言

隨著時代物換星移，人類的各項科技及通訊技術日新月異，人們身邊攜帶的行動裝置及使用的通訊技術和協定也不斷地改頭換面和創新改革。從西元1938年最早由美國貝爾實驗室第一部行動電話[1]（俗稱黑金剛）開始至目前的智慧型手機、功能面從僅有的接聽電話到現今能運行高畫質遊戲、處理辦公文件以及撰寫程式碼，甚至複雜的金融交易都可以完成的智慧型手機，即可一窺近年來行動裝置發展之迅速。此外，除了硬體的體積縮小以及運算效能突飛猛進外，在軟體端用於支持這些裝置之通訊、網路、視訊等技術亦蓬勃發展。遠從1979年第一代行動通訊技術問世以來[2]，直到2019年4月3日由韓國率先提供第五代行動通訊網路（5th Generation Mobile Networks，5G）[3]的商用服務（以下將簡稱為5G通訊技術）由此可見，行動通訊技術因為世界各國之間的科技競爭而加速改革的腳步。

於2019年全世界各地如，瑞士、英國、義大利、西班牙、德國、中國等也陸續提供5G的服務。2020年，香港及日本也緊跟著這股潮流加入5G的行列。與此同時，臺灣各家電信龍頭也搭上這波最新通訊技術的列車，六月底的中華電信、七月初的台灣大哥大及遠傳電信、以及八月的臺灣之星，最後則是十月的亞太電信。儘管部份電信業者為了顧及市場需求及市占率，將進行合併的考量。然而，這些電信業者對臺灣在5G服務的提供上創下相當重要的關鍵里程碑！

5G 的相關技術和簡介

至此，全世界正式進入第五代行動通訊網路的時代。雖然目前5G的覆蓋率及大眾普

遍的使用率尚無法達成原先規劃中對5G的規模，然而隨著5G基地台的廣佈和各項軟硬體技術的逐漸成熟後，將能真正且確切地體會到5G所帶來的便利和服務！在正式介紹5G之前，我們必須要先來探討一下4G和5G的差異。許多人可能會有疑問，為什麼比起3G升級到4G單就只是網路速度的提升，4G升級到5G卻可以替人們生活帶來全面性的提升和改變，究竟僅僅差這一代為何能夠有如此巨大的革新與變化？

面對傳統的4G，5G中有兩大最為關鍵的網路架構來促成這樣巨大的改變，而這兩項技術分別是軟體定義網路（Software Defined Networking，SDN）以及網路功能虛擬化（Network Function Virtualization，NFV），相信對於有接觸5G新型態網路架構的讀者都有耳聞這兩個名詞，但是對於這兩者之間的分別以及對5G產生的影響可能不甚清楚。因此，以下將會針對5G中這兩大關鍵的網路架構進行介紹，將鉅細靡遺地把軟體定義網路以及網路功能虛擬化這兩者的架構、功能以及之間的差異進行詳細的說明和描述。

首先將從軟體定義網路（Software Defined Networking，SDN）開始介紹，如圖1所示，SDN為一個新型態的網路架構[4]，是利用Openflow將控制平面和資料平

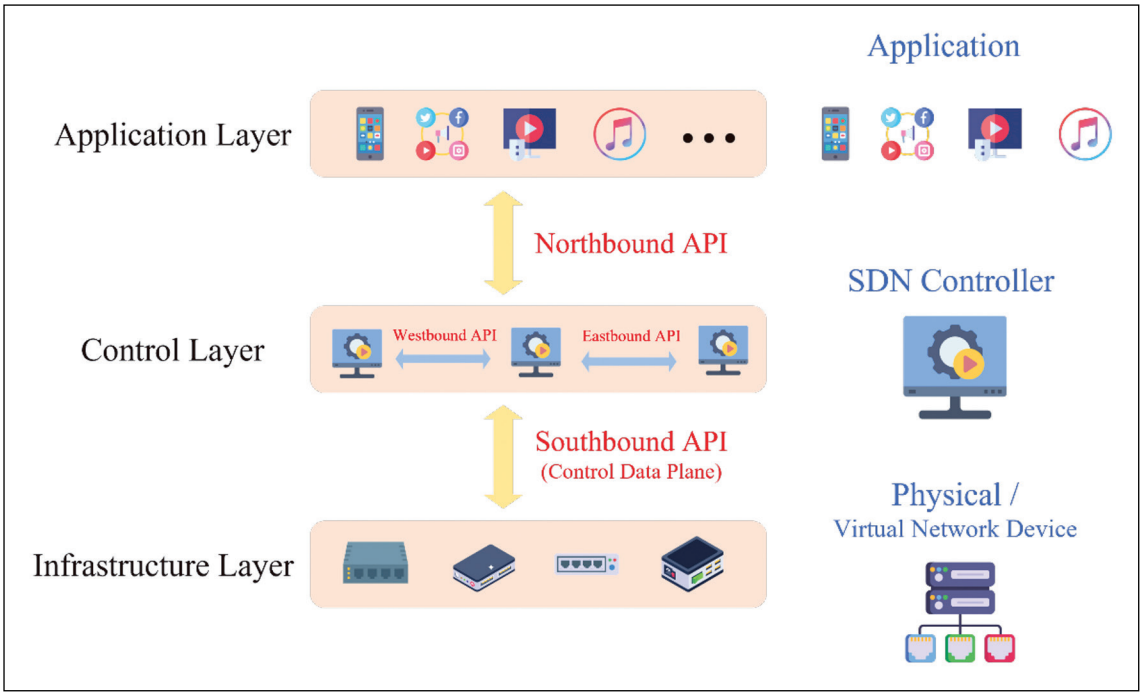

圖 1　SDN 架構圖

面分離。而對比於傳統的網路架構將各種不同的功能和服務集中在交換器也就是俗稱的Switch，SDN將原先包含各種不同服務與應用的應用服務層（Application Layer）、管理底層SDN Switch網路流量且有SDN控制器（SDN Controller）的控制層以及最下層由基礎SDN Switch所組成的基礎設施層（Infrastructure Layer），拆分成三個不同的層，從應用服務層到控制層使用北向接口（Northbound Interface）作為溝通的介面，而控制層到基礎設施層則是由南向接口（Southbound Interface）當作介接的橋樑，南向接口目前主要使用的是REST API。以較容易理解的例子說明如下 [5]，今天一名顧客在咖啡廳向服務生點餐，其中顧客代表使用者而服務生代表的是SDN網路架構，點餐的行為就像是使用者希望使用何種服務。進行點餐之後，代表服務生接收到使用者請求的服務類型，而此時服務生的大腦就像是控制層一樣，會將這個Request（請求）往下發送，並讓身體和四肢來完成，此時該名服務生的身體及四肢就像是基礎設施層接受到大腦的控制來完成顧客的這項服務。而下指令這樣的行為在SDN網路架構中就像是設定封包的轉發路徑，如同大腦的SDN控制器會指示某一個封包的路由規則，也就是該封包將轉發到何處的交換器以達成最終之目的地，並提供使用者應用服務的需求。如此一來，也可以實現對網路設備的集中式控制並大幅增加對網路資源的控管進而提升其效率。

第二部分要介紹的是軟體功能虛擬化 [6]，其實顧名思義，主要的概念為將原本實體設備的網路功能藉由軟體或程式的方式來實現，並達成虛擬化也就是軟體化的網路架構。這樣的改變和突破也顛覆了舊有許多網路功能必須由硬體設備來提供的既有觀念。經過虛擬化或稱作軟體化的網路功能和原本的硬體設備相比能更有擴展性也更能動態彈性地配置各項網路功能，也能夠提升網路部署的效率。當然虛擬化之後更可以減少硬體設備的開銷，進而減少因硬體設備提升或更新而產生的費用。以防火牆為例，不僅可以省下購置硬體設備的開銷，若是隨時需要更新，則直接將新的軟體安裝到設備中即可完成部署。

除了前面介紹的兩大網路架構軟體定義網路以及網路功能虛擬化外，要達成5G中所提及的各項場景及特性還需要一項最為關鍵的技術—網路切片（Network Slicing）[7-8]。而為了實現網路切片這樣的技術，前述所介紹的網路功能虛擬化則是其先決條件。如圖2所示，簡單來說，網路切片的核心概念就是將一個電信業者所提供的物理網路「切」分成多「片」虛擬的網路，而其中每一個虛擬網路根據其不同的服務需求以不同切片的虛擬網路來客製化提供。根據網路速度、時間延遲、安全性、可靠性等各種環境中特殊的需求來滿足每一項服務所具備的要求。而也因為前述提及到「切分虛擬網路」，因此，前面所介紹的能夠將網路中各

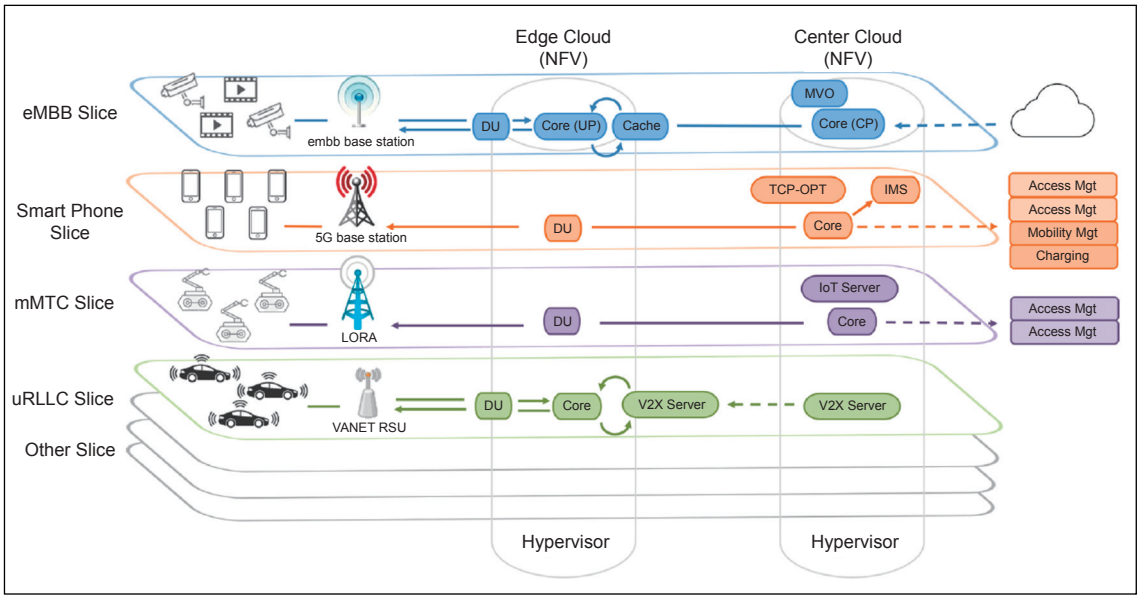

圖 2　網路切片架構

種專用設備的硬體功能，轉移到虛擬主機上之網路功能虛擬化則是實現網路切片技術不可或缺的關鍵網路架構。

介紹完第五代行動通訊網路的前置技術後，將進入5G最重要且關鍵之三大特性或稱三大場景的介紹。5G藉由SDN和NFV為基礎的網路架構並搭配Network Slicing的技術來達成其最為核心的三大特性，分別是增強型行動寬頻（Enhanced Mobile Broadband，eMBB），高可靠度和低時延通訊（Ultra-Reliable and Low-Latency Communication，uRLLC）以及大規模機器類型通訊（Massive Machine Type Communication，mMTC）。如圖3所示，5G能提供的所有服務都是以在這三大特性的不同面向和需求程度來提供。

首先提到增強型行動寬頻，相信這也是當前所有使用5G行動網路的人最有感觸的一項提升。根據國際行動網路調查權威「Opensignal」[9]於2021年2月發表的數據顯示，臺灣的5G下載網速平均為272.2 Mbps。儘管離當初最為理想的每秒10 Gbits有段落差，然而卻是目前對比4G最能感受到的差異，而其中的應用想當然就是需要超高傳輸速率的服務，如4K／8K的超高畫質影片、全像投影技術、增強現實以及虛擬實境等需求都涵蓋在其中。

第二個特性則是高可靠度和低時延通訊，顧名思義就是這類型的服務需要極高的穩定性和極低延遲的傳輸能力，最具代表性的就是自駕車的技術，當然也包括車聯網、

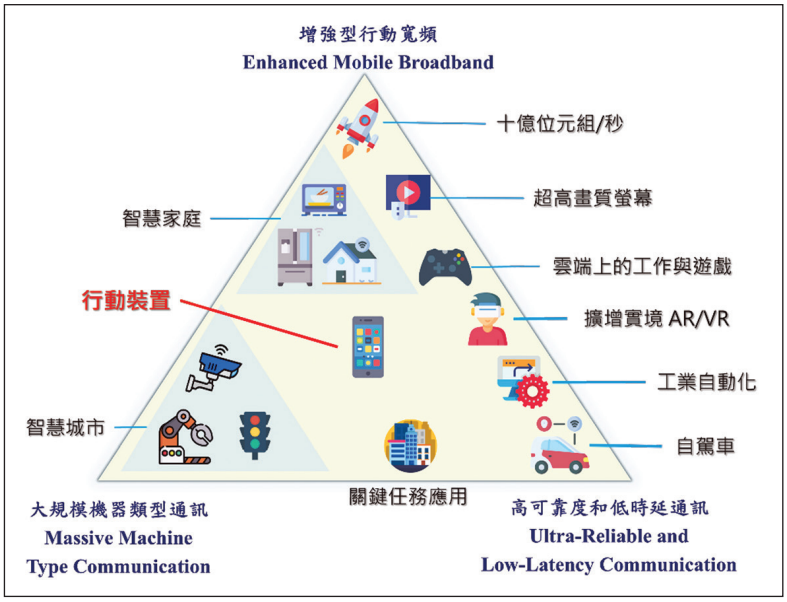

圖 3　5G 三大特性

自動工廠以及遠距醫療等服務。面對瞬息萬變的交通狀況，高可靠和極低延的通訊則變得非常關鍵，在這樣的環境下使用自動駕駛，通訊傳輸必須要具備極低的延遲來應付各種突如其來的特殊情況，進而避免意外或車禍的發生。而醫療環境也是理所當然，若是醫生以遠距方式進行開刀，任何些微不穩定的傳輸或是延遲導致開刀過程中稍有差錯或延誤，都有可能導致病患終身的遺憾甚至喪失性命。

最後第三項特性則是大規模機器類型通訊，此特性顧名思義就是，未來所有裝置都具備連上網路之能力，而這些裝置都將更加便利人們的日常生活並提供更直接適切的服務。從最平常不過的，在家中設置用於監看環境的無線網路監控設備、影音休閒用途的智慧音箱、安全防盜且便利的智慧門鎖到環境調控的智慧冷氣或智慧型除濕機等，到結合上述所建構出的智慧家庭。離開家門後，將進入另一個由智慧交通及車聯網構築而成的智慧城市，以自動駕駛技術且連上車聯網環境的自駕車，僅僅下一個目的地的指令即可讓車輛自動將人載抵特定地點，也能夠在車上藉由資訊的傳遞知悉交通狀況和各地的道路資訊，此場景將是智慧城市結合智慧交通及車聯網所打造的環境。此外，當突然有醫療需求時，可以透過遠距診斷或遠距醫療的方式讓醫生利用全像投影技術來看診，必要或緊急時也能夠在特定場景執行遠距手術，這也是5G中結合各項特性可以達成之智慧醫療目標。最後，將這類技術應用到工廠

或關鍵基礎設施建設等環境時，更可以利用遠端下達指令，讓機器自動生產或製造任何產品，進而減少人力的需求，這也是5G中能夠達成的智慧製造和智慧工廠等應用。

正因為結合多項新型態網路架構以及新興技術，理想的5G能夠完全將人類生活智慧化，從家庭、交通、城市、醫療、工廠以及商務行為都能藉由5G的通訊技術和各式各樣的物聯網裝置來達成，進而建構出一個完整的智慧國家，並讓人們的生活更加便利。然而，隨著技術的日新月異以及人類對網路及各項科技的日漸依賴，無數的資料及各項活動也逐漸線上化及數位化。因此，5G的資訊安全也變得至關重要，任何傳輸協定間的漏洞或是機敏資料的洩漏都可能造成相當嚴重的危害，以下的章節將介紹本團隊在5G環境中針對認證所設計的安全機制及成果。

因應第五代行動通訊技術時代的全面來臨，全世界各國使用5G的用戶也逐年增加。然而，在過去屢見不鮮的案例往往是已經發生資安事件或造成嚴重損害時，人們才開始重視這些資安議題且思考相關的對策以預防下一次相同事件的危害。許多學術研究在技術尚未完全成熟或現階段正在蓬勃發展時，就開始鑽研並提早設計且部署相關的安全機制。本團隊在5G尚未問世前就已經針對通訊及認證的傳輸機制進行研究，並為其設計保護使用者隱私或減少時間延遲之安全機制，下一章節將以淺白的概念來介紹本團隊為5G環境所設計之認證機制。

5G 安全機制成果介紹

在先前的段落中已經介紹了建構5G網路架構的核心，分別是軟體定義網路以及網路功能虛擬化，並搭配網路切片技術來提供5G環境中各式各樣且多元豐富的服務。然而，也因為前面所提及的概念，5G環境下不同類型的服務將會由不同的網路切片來提供。前述所提及的不同網路切片可以簡單理解為每一個網路切片的服務都由一個切片基地台來提供，當用戶想使用該服務的時候將會需要和對應的網路切片基地台進行認證的程序，而認證流程中會需要部分用戶的資訊，主要為該用戶SIM卡裡原先4G的國際行動用戶識別碼（International Mobile Subscriber Identity，IMSI）。在5G環境中為了解決原先存在於4G中IMSI有機會遭到竊取而造成隱私暴露之疑慮，第三代合作夥伴計畫（3rd Generation Partnership Project，3GPP）於5G中引入用戶永久識別碼（Subscriber Permanent Identifier，SUPI）並加密後變成用戶隱藏識別碼（Subscriber Concealed Identifier，SUCI）。而在原先3GPP所發布的標準中，如圖4所示，當用戶要使用不同網路切片的時候將回到核心網路，也就是回到電信業者的伺服器端重新進行認證。然而，在5G的環境中用戶將可能在短時間內有許多使用不同服務的需求，若每一次都回到伺服器端重新認證，將

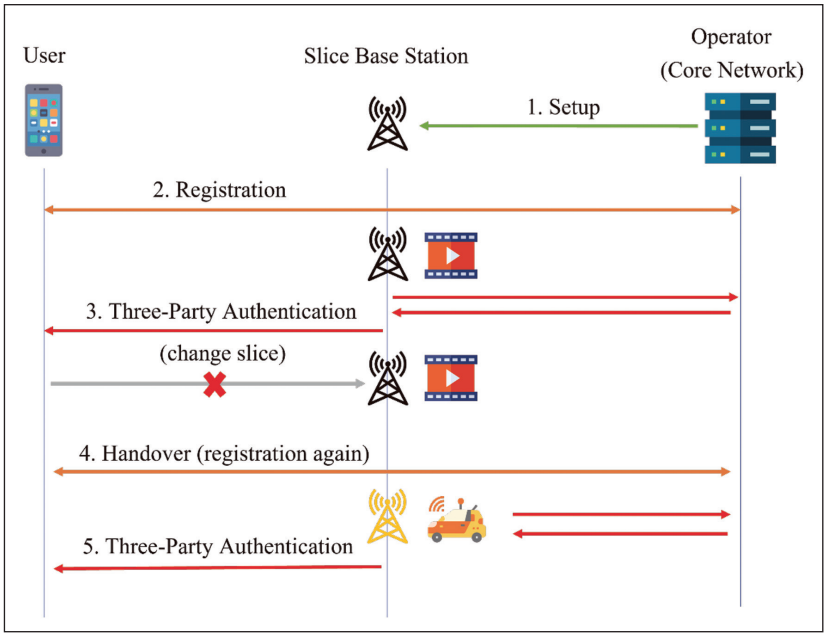

圖 4　3GPP 標準中換網路切片之架構

會產生大量時間上的延遲，且對用戶以及伺服器端也需要進行較多的運算及驗證流程。因此本團隊設計出一個用於網路切片間之切換不須回到伺服器端也可以進行認證的機制“Cross-Network-Slice Authentication Scheme for the 5th Generation Mobile Communication System” [1]。其機制架構如圖5，該安全機制可以大幅地減少認證時使用者端以及網路切片端時間的延遲。當然，在此機制的運作下也能夠保護用戶資訊的隱私並抵擋許多常見的攻擊手法，如重送攻擊。

以簡單的日常行為舉例說明，小明在一個假日裡在家中正欣賞著超高畫質8K的網路電影，突然有朋友打了視訊電話告知有緊急的事情需要到場協助，小明立即掛掉電話、關掉電視，並下達一個目的地的指令給自駕車讓車輛載送小明到朋友所說的地點，這其中光是手機通訊網路、高畫質電視網路以及連接車聯網的自駕車就需要多次的網路切片的交換，使用本團隊所設計之機制可以省下大量的時間延遲以及減少運算需求，將對未來5G服務漸臻完善且關鍵基礎設施更加多元豐富後提供重要且關鍵的技術！

本團隊所介紹的第一項研究成果是考量到跨不同切片間認證之設計，而也因為5G

[1] Chun-I Fan, Yu-Tse Shih, Jheng-Jia Huang*, and Wan-Ru Chiu, ‘Cross-Network-Slice Authentication Scheme for the 5th Generation Mobile Communication System,’ *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 701-712, March 2021.

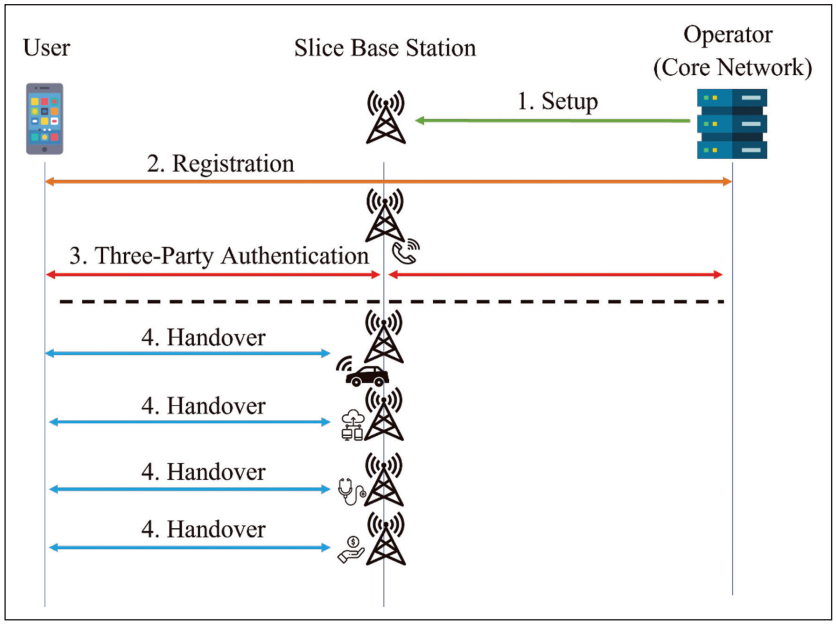

圖 5　跨切片機制之架構圖

的成熟和日漸普及，本團隊成員也持續在該認證領域中找尋符合現行環境和需求的功能進行設計及考量，也確實發現另一項全世界中許多國家都存在的情形，也就是在現行的5G環境中大多數國家都是多家電信業者共同來提供服務的現況。第一篇論文僅考量在相同電信業者間跨網路切片的問題，由於不同電信業者將各自架設其提供不同服務的基地台，且5G因毫米波 [10]的關係導致傳輸距離短且穿透力極低，不僅辦公室的隔間牆可能阻隔其訊號，即使只是窗戶或樹葉都會讓傳輸速度嚴重地降低。因此，各家電信業者都積極地廣佈5G基地台，希望可以增加覆蓋率。這也造成了可能產生原先提供服務的電信業者無5G的訊號而其他電信業者卻可以提供5G服務的情況。以下兩篇發表的論文分別使用不同的方法來達成多電信業者跨網路切片的安全認證機制，首先為“A Fast Authentication Scheme for Cross-Network-Slicing Based on Multiple Operators in 5G Environments”[2]，此項研究成果使用到代理重簽章（Proxy Re-Signature）以及無憑證簽章（Certificateless Signature）的概念，此成果不僅可以滿足3GPP所定義的標準，也可以通過將計算委託給邊緣雲（Edge Cloud）

[2] Jheng-Jia Huang, Chun-I Fan*, Yu-Chen Hsu, and Arijit Karati, ‘A Fast Authentication Scheme for Cross-Network-Slicing Based on Multiple Operators in 5G Environments,’ *The Eighth International Symposium on Security in Computing and Communications*（SSCC’20）, India, Oct. 14-17, 2020.

來實現低時間延遲之特性。即使用戶需要在不同的電信業者中切換使用網路切片的服務，依然可以滿足低時間延遲的認證流程需求。接著下一篇論文為“An Efficient Secure Handover Scheme Supporting Cross-Network Slicing for Multi-Operator Environments”[3]，在該機制中使用了電信業者的簽章並加入了兩階段驗證的概念。在第一階段先驗證用戶持有的電信業者簽章，以過濾掉沒有經過認證或是使用重送攻擊等手段之非法使用者，並且在經過第一階段後先行提供服務給用戶。接著，在第二階段中，此機制會再到網路後端進行二次檢查，以排除簽章遺失或是用戶的服務權限臨時註銷等例外情形。因此，即使用戶需要在不同的電信業者中切換使用網路切片服務，依然可以滿足低時間延遲的認證流程需求。由於本文僅介紹較為概念性的資安知識，若對於機制細節或認證流程有興趣或想了解更為詳細的架構設計，可參考本團隊所發表之論文。希望藉由對本團隊所提出之安全機制進行簡單的介紹，可以讓讀者對於5G環境下資安認證機制能有初步的認識，同時也期許能因應未來5G的發展根據不同的需求持續設計並改善相關的機制及運作流程。

[3] Chun-I Fan, Kai-Yuan Zheng, Yu-Tse Shih, Er-Shuo Zhuang, and Jheng-Jia Huang*, ‘An Efficient Secure Handover Scheme Supporting Cross-Network Slicing for Multi-Operator Environments,’ *The 13th International Conference on Mobile Computing and Ubiquitous Networking*, Japan, Nov. 17-19, 2021.

結論與未來展望

本篇文章內容從第五代行動通訊網路介紹著手，談及架構5G環境所需要之兩大核心技術—軟體定義網路以及網路功能虛擬化，進一步說明如何以網路切片的技術提供5G三大特性—增強型行動寬頻、高可靠度和低時延通訊以及大規模機器類型通訊。接著，說明如何利用以此三大特性構築出5G中各種理想的智慧場景來便利人們的日常生活。然而，隨著新形態網路通訊技術的發明和問世，將產生對應的資安問題及隱私保護之需求。其後也簡短介紹了本團隊於5G環境中提出於多電信業者及跨網路切片之高效且安全的認證機制。

在不遠的將來，5G基地台覆蓋率的提升、通訊及傳輸技術的成熟發展並結合各場景關鍵基礎設施的建置後，世界將迎來全面的大5G時代，儘管目前各國已陸續在探討6G，然而5G終將在6G來臨前遍佈全世界人們日常周遭的一切。從每個人每天早上起床的那一刻起，無數智慧場景將挾帶著高科技裝置席捲而來，目所能及甚至是目不能及之物聯網裝置、傳輸通道乃至通訊協定都可能成為駭客攻擊的目標，人們越依賴5G所提供的服務也同等於將數位資產及自身安全的掌控託付於此，其資安問題也顯得至關重要。希望本團隊之成果可對資安領域挹注新能量，且能夠在未來讓大家在享受5G環境所帶來便利的同時也可保障隱私、生命以及財

產的安全，為臺灣及全世界的資安領域帶來貢獻！

參考文獻

1. “手機演變史,”[線上]. Available: http://yiter1.vexp.idv.tw/~u108029037/f1.html.
2. “維基百科,”[線上]. Available: https://zh.wikipedia.org/wiki/1G.
3. “維基百科,”[線上]. Available: https://zh.wikipedia.org/wiki/5G.
4. “軟體定義網路介紹（SDN）,”[線上]. Available: https://ithelp.ithome.com.tw/articles/10197629.
5. “軟體定義網路（SDN）的定義、架構與實現方案,”[線上]. Available: https://www.uuu.com.tw/Public/content/article/18/20180625.htm.
6. “NFV（Network Functions Virtualization）網路功能虛擬化,”[線上]. Available: https://www.gigabyte.com/tw/Glossary/nfv-network-functions-virtualization.
7. “一篇文章看懂，5G 網路切片是什麼？,”[線上]. Available: https://3smarket-info.blogspot.com/2019/05/5g_6.html.
8. “到底什麼叫 5G 網路切片？,”[線上]. Available: https://zi.media/@twpetsearcharlinksnet/post/amyAw7.
9. “5G 體驗報告,”[線上]. Available: https://www.opensignal.com/zh-hant/reports/2021/12/taiwan/mobile-network-experience-5G.
10. “關於 5G 的錯誤認知,”[線上]. Available: https://www.cio.com.tw/error-perception-about-5g/.
11. “Speedtest 數據揭全球 5G 網速較去年下滑與這些原因有關,”[線上]. Available: https://udn.com/news/story/7088/5991469.