前瞻科技與管理　11 卷 2 期，1-27 頁（2023 年 5 月）
Journal of Advanced Technology and Management Vol. 11, No. 2, pp. 1-27 (May, 2023)
DOI:10.6193/JATM.202305_11(2).0001

應用於智慧家庭之物聯網身分驗證機制

陳昱仁 [1,*]　廖耕億 [2]　邱珮瑜 [3]

[1] 長庚大學資訊管理學系助理教授
[2] 長庚大學資訊管理學系副教授
[3] 長庚大學資訊管理學系碩士生

摘 要

隨著網際網路以及硬體設備的發展，生活中到處都能看見物聯網（Internet of Things, IoT）的影子。2005 年國際電信聯盟（International Telecommunication Union, ITU）便指出「物聯網」的時代來臨，物聯網可以應用在生活各處，不管是城市、工業或是小至一個家庭，都能用物聯網將環境中的設備串聯在一起。另外，有報導指出全球的智慧家庭裝置數量也不斷在增加，愈來愈多人選擇用智慧家庭來管理自己家中的設備。但隨著使用智慧家庭的人數增加，對於智慧家庭的疑慮也愈來愈多。智慧家庭中充斥著家中各種設備的資訊，這些資訊都與家中所有人的隱私息息相關，如果沒有善加保護這些資訊，很有可能會對於家中成員的安全造成威脅。但在保護這些資訊的過程中，必須對於設備的計算能力加以考慮，因為家中設備的運算能力通常較為受限以降低成本，所以本論文提出一個設備身分和封包驗證機制，給智慧家庭一個運算負擔輕且安全的環境。

關鍵詞：物聯網、智慧家庭、身分驗證、封包驗證、金鑰管理

[*] 通訊作者：陳昱仁
電子郵件：cyr@mail.cgu.edu.tw
（收件日期：2022 年 2 月 9 日；修正日期：2022 年 9 月 25 日；接受日期：2022 年 10 月 4 日）

Journal of Advanced Technology and Management Vol. 11, No. 2, pp. 1-27 (May, 2023)
DOI:10.6193/JATM.202305_11(2).0001

Identity Authentication Mechanism in the Internet of Things at Smart Home Applications

Yu-Jen Chen[1,*], Gen-Yih Liao[2], Pei-Yu Chiu[3]

[1]Assistant Professor, Department of Information Management, Chang Gung University
[2]Associate Professor, Department of Information Management, Chang Gung University
[3]Master Student, Department of Information Management, Chang Gung University

Abstract

With the development of the Internet and hardware equipment, the Internet of Things (IoT) can be seen everywhere in our life. In 2005, the International Telecommunication Union (ITU) pointed out that the era of the "Internet of Things" is coming. Whether in a city, an industry, or a home, we can use the IoT to connect devices in everywhere. In addition, there are reports indicated that the number of smart home devices increased, and more and more people choose to use smart homes to manage their home devices. However, with the increase in the number of people using smart homes, there are more and more doubts about smart homes. Smart homes are full of information about various devices in the house. These data are closely related to the privacy of everyone in the home. However, in the process of protecting these data, the computing power of the device must be considered. Because the computing power of the devices in the home is usually limited, this thesis proposes an identity and packet verification mechanism that gives the smart home a lightweight computing and secure environment.

Keywords: Internet of Things (IoT), smart home, identity authentication, packet verification, key management

* Corresponding Author: Yu-Jen Chen
E-mail: cyr@mail.cgu.edu.tw

壹、緒論

一、研究背景

2005 年 11 月 17 日，世界資訊峰會上，國際電信聯盟（International Telecommunication Union, ITU）發布了《ITU 網際網路報告 2005：物聯網》，其中指出「物聯網」（Internet of Things, IoT）時代的來臨，隨著網際網路以及硬體設備的蓬勃發展，物聯網已成為生活中不可或缺的技術。在物聯網中，一個完整的智慧家庭方案，包含了燈光照明、門窗和窗簾的控制、環境感測、防盜與攝影設備的整合等，在使用者（User）外出時，只要把門鎖上後，智慧鎖會直接通知恆溫器，讓恆溫器自動進入「離家」模式；當使用者開門，就可以切換至「居家」模式，並將室內調節至舒適的溫度。

物聯網為實體物品被嵌入電子軟體或感測器（Sensor），並與網路連接所組成的網路系統，隨著智能設備以及高速網路的發展，物聯網在生活中愈來愈普及，也被大家接受。物聯網代表了一個網路，其中的「事物」為遍布在生活中的感測裝置或嵌入式設備利用網路互相連接溝通著，來達到資料蒐集或是交換的功能，人們可以遠程控制這些物聯網的設備，自動化監控、管理以及蒐集資料來增進執行效率與提供方便性（Khan and Salah, 2018; Wu et al., 2017）。物聯網架構中總共可以分為三層（Li, 2012），包括感知層（Perception Layer）、網路層（Network Layer）和應用層（Application Layer）。

二、研究動機

物聯網即時感測環境並傳送數據給人們做參考，提供了人們極大的方便，但漸漸地因為數據涉及私人的資訊，例如：心跳、脈搏、飲食習慣，甚至所在位置等，都在物聯網大數據裡面，如讓惡意人士竊取資料，可能會危害到個人的隱私或人身安全（Salami, Baek, Salah, and Damiani, 2016）。整個物聯網為一個異質網路架構，牽涉到網路、手機網路及感測器網路等，這樣的架構增加了驗證或是訪問機制設計的困難度，連帶著出現更多的安全問題（Zhao and Ge, 2013）。另外，物聯網裝置還有著電力以及運算能力的限制，不能因為限制而降低安全性，也不能設計太複雜的運算，導致要製造更大的電池而增加物聯網裝置的大小。因為物聯網的發展，愈來愈多人將家裡改造成智慧家庭，很多家用電器都能用一支手機操控，用手機就能夠開燈開門，就算是出門在外也可以監控家裡的情況。此時如果家裡的智能設備被入侵，就可能對人身安全造成威脅，或是受到金錢上的損失。

三、研究目的

智慧家庭愈來愈受重視，但是現有的安全架構並不一定能夠對資料提供足夠的安全性。智慧家庭共分為三個部分，家庭中的物聯網設備、儲存數據的雲端平臺以及手機的管理介面。本研究主要解決的問題有兩個：

（一）假冒物聯網裝置節點（Node）：預防他人假造物聯網裝置節點，利用竊取的資訊（例

如：IP 位址、MAC 地址等）來假冒自己為整個架構中的成員，進而取得物聯網環境內的相關數據。

（二）非法成員控制或取得系統訊息：防止沒有經過註冊的使用者操控智慧家庭的介面來竊取資料或是發送訊息給不明的成員。

根據以上的問題，本研究針對智慧家庭中智慧型裝置（Device）的身分驗證以及物聯網封包的來源驗證提出一個安全架構，基於身分加密來減少智慧裝置身分驗證的複雜性（Salami et al., 2016），封包部分則參考 DeCusatis, Liengtiraphan, Sager, and Pinelli（2016）所提到驗證第一個欄位的方法來驗證封包來源是否合法，以降低整體驗證負擔。

貳、文獻探討

一、物聯網通用架構與安全現況

物聯網最普遍的架構包含儲存資料的雲端伺服器（Cloud Server）、使用者、感測環境數據的感測器，以及具有較強計算能力的閘道（Gateway），閘道也會管理著底下相對應的感測器。這個架構中的所有角色會使用 4G、5G、無線網路、ZigBee、藍芽（Bluetooth）等網路技術做連接（Chuang, Lo, Yang, and Tang, 2018）。閘道是相較於感測器運算能力較好的處理器，在物聯網中會跟感測器在同一個網域下工作。閘道的用途如下：第一，在目前的物聯網市場上各家廠商都使用著不同的網路技術，即便到了現在仍然沒有一個通用的物聯網網路標準（Uviase and Kotonya, 2018），要讓感測器達到可以與現在所有的協定通訊難度也較高，為了克服這個問題，物聯網中常會使用計算能力較高且記憶體較大的閘道去做中心管理，來支援物聯網的異質網路架構；第二，感測器在運作過程中會產生大量數據，這時閘道可以當作感測器以及雲端伺服器之間的橋樑；第三，因為有較好的計算能力以及較豐富的記憶體資源，閘道還可以作為集中管理使用者權限與訪問紀錄，避免非法使用者入侵的一道關卡（Lin and Bergmann, 2016）。

物聯網的特徵包含全面感知、可靠傳輸以及智能處理，全面感知外在實體世界並隨時隨地獲取目標訊息，透過有線或無線的網路將數據在節點中完整的傳輸到資料中心，最後再對這些數據做更進一步的分析及運算（Zhao and Ge, 2013）。物聯網常見的安全問題有以下幾點：

（一）數據收集及傳遞因為物聯網結構簡單、設備運算能力較差，所以無法建構較複雜的安全架構。

（二）傳統的網路安全議題，因為網路層仰賴著現有的 IPv4、IPv6 等技術，所以物聯網會因為原本這些技術的漏洞而造成相同的威脅。

（三）安全性與成本上的考量，如果想要降低成本勢必會降低節點的安全性，相同的如果想要高保護性的安全策略就要提升不少成本，兩邊權衡也是物聯網在設計上會遇到的困難。

（四）物聯網設備計算能力相對較差，所以無法執行過於繁複的運算或是負擔太重的身分驗證機制。

（一）感知層安全問題

感知層會偵測是否有節點出現異常以及是否受到攻擊，它們要即時監控來避免攻擊的範圍擴大。如果一個節點被惡意人士控制，惡意人士就可以從此節點去探知整個系統的其他資訊，對整個物聯網系統產生更大的威脅。惡意攻擊者也可能會重送一個已經驗證通過的封包來取得系統的信任。最後，在龐大的節點中，要如何在節點與節點之間有效率地做身分驗證以及存取控制，是此層最棘手的問題。感知層的安全問題包括節點擷取、節點捕獲及惡意資料、阻斷服務（Denial-of-Service, DoS）攻擊、重送攻擊、旁通道攻擊（Side Channel Attack）和大量節點的驗證等（Zhao and Ge, 2013）。

（二）網路層安全問題

網路層會用到的技術有 IPv4、IPv6 和 6LoWPAN 等，雖然這些協定都有各自完善的安全機制，但還是存在著中間人攻擊或是 DoS 攻擊等威脅，這些技術用在物聯網自然還是可能會受到這些攻擊。另外，這些協定設計的角度為人，但用在物聯網則是要處理機器與機器之間的溝通，在存取控制上可能就會產生不同的差異，異質性的架構對這些網路協定的整合產生了更多阻礙。如果使用現有的身分驗證識別技術，大量的數據可能會造成網路壅塞。現在的 IP 技術並不適合用於大量節點間的識別，設備之間互相的驗證還可能會造成關鍵資源的浪費。網路層的安全問題包括傳統網路安全問題、相容性問題和群集安全問題等（Zhao and Ge, 2013）。

（三）應用層安全問題

應用層會遇到的安全問題是因為這些裝置都由網路去做連結，所以可能會因此而感染到木馬病毒造成設備癱瘓。另外，物聯網中數量龐大的節點也提供了惡意攻擊者一個範圍大且可以執行殭屍網路的新環境（Zhao and Ge, 2013）。應用層還牽涉到資料的使用，要管理取得資料的權限以及身分驗證也是此層重要的安全議題。應用層的安全問題包括資料取得權限及身分驗證、資料的保護及復原和處理大量資料的能力等。

（四）傳統安全問題於物聯網的影響

雖然說網路技術已經相當成熟，但也無法安全且適用地用於物聯網，因為物聯網的規模龐大，許多感測節點的資源也是受限制的，整個物聯網也屬於異質性架構。傳統網路技術用於物聯網常發生的問題包括金鑰管理（Key Management）、DoS 攻擊和身分驗證及存取控制（Authentication and Access Control）等。

二、智慧家庭與其相關研究

家庭中的建築自動化、家庭自動化系統能夠控制燈光、溫濕度、影音設備以及家電等，也可能同時包含家庭保全，例如出入控制或者警報器。根據國際數據資訊公司（International Data Corporation, IDC）研究，2017 年全球的智慧家庭裝置超過 4 億臺，比起 2016 年成長了 27.6%，他們預測在 2022 年智慧家庭市場的出貨量可高達 9 億臺（科技政策研究與資訊中心，2018），智慧家庭的產品市值在 2022 年都有一定的成長，雖然智慧家庭還在起步階

段，但是在 Siri 或 Google 語音助理的輔助下，使用者對於智慧家庭的控制更為自然方便。在智慧家庭系統中，用戶可以透過自己的手機來控制家中的電器設備，例如空調設備、警報器、門禁系統等。這些智能設備會將所收集到的數據傳送至使用者的手機，讓用戶的生活更加便利，但也因此增加了用戶隱私以及安全上的疑慮。如果家中的門禁系統顯示大門為開啟狀態，而這個狀態又被惡意人士探知，這樣可能會對用戶造成安全上的威脅，或是任何狀態被竄改都有可能造成無法挽回的事故（Salami et al., 2016）。另外，因為智慧家庭的裝置或設定皆為動態的，並且是異質網路架構，增加了安全的弱點，加深了建立完善安全策略的困難度（Salami et al., 2016）。

Salami et al.（2016）提出了一個智慧家庭的輕量化加解密方案，設計一個有效率且靈活的運算來降低智慧家庭中裝置的計算負擔。他們提出的方法有兩個，基於身分加密以及有狀態的公鑰加密過程。基於身分加密代表公鑰只是身分的字串不須額外做認證，另外有狀態的意思是將加密計算中的參數預先做好計算並儲存，如此一來就能提高計算的效率。在他們的實驗分析中，這樣的方法確實提高了計算的效率，但是如此的做法還是存在著疑慮，將一些數值預先計算好並儲存，如果被有心人士得知這些數值，也許就能事先破解往後的加密結果，提高了計算效率但也增加了安全性的疑慮。

Liu, Xiao, and Chen（2012）分析了現有的身分驗證和存取控制的方法並且提出了一個用於物聯網的方案，整個驗證協定有多個任務，包括識別密鑰建立或是密鑰切換等，他們利用橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）簡單有效率的產生密鑰，在存取控制的部分則是採用以角色為基礎的存取控制（Role-Based Access Control, RBAC）來定義物聯網中的各個角色和應用。

DeCusatis et al.（2016）提出雲端網路上的存取控制，其中提到的零信任以及第一個封包驗證概念也可以運用於物聯網上。零信任的模式中，無法相信網路內外的任何事物，以資料為中心的邊界強化加密技術來保護這些資料，要通過身分驗證、裝置驗證後才能看到資料內容。這樣的概念也適用於物聯網中，提升每個封包傳遞的機密性。但在物聯網中有許多受限的設備，無法承受太複雜的計算，此篇提到的第一個封包驗證，只對於封包第一個欄位做驗證，不檢查封包內容，就不會占用到其他數據的頻寬。

Khemissa and Tandjaoui（2015）提到在智慧醫療中非常看重數據的即時傳輸以及數據的安全性，因為病患有任何狀況時必須即時回報，也要確保數據在傳輸的過程中不被竄改導致醫生誤判等情況。但是因為這些貼在患者身上的感測器的運算能力都較弱，所以必須設計一套輕量化的驗證機制給智慧醫療使用。他們用到 Nonce 以及金鑰雜湊訊息驗證碼（Keyed-Hash Message Authentication Code, HMAC）兩概念。Nonce 指的是在整個通訊過程中，只會出現一次的隨機數，以避免被截取利用產生重送攻擊。HMAC 則是利用特別的演算法來計算出一個訊息驗證碼，並將此訊息以及加密金鑰一起做雜湊，可以確保資料的完整性，也可以作為驗證訊息的來源。但是這樣的架構僅限於物聯網感測器與後端設備在進行數據傳輸前的雙向驗證，除了驗證時間過期後會再重新做一次設備之間的雙向驗證，驗證通過之後的每一次資料傳輸是沒有經過驗證的。如此一來，會造成在傳輸資訊的過程中以及到下一個身分驗證週期之前是不安全的。

Chuang et al.（2018）提到在物聯網設備傳輸數據到後端的過程中，重複驗證用戶的合

法性，他們稱為「連續驗證」。但是連續驗證之前還是必須進行靜態驗證，事先驗證雙方的身分。他們利用存取感測設備的電量來驗證一次的溝通之後所損耗的電量是否合理，是否被秘密進行著非法的動作。另外，他們一樣利用 HMAC 的概念並在每一個階段每個角色上判斷所得到的資訊是否被竄改，也利用掩蔽值避免資訊直接在通道上傳遞，被有心人士擷取並且假冒節點。這樣的構想提高了物聯網的安全性，避免通過靜態驗證後在傳遞資料時遭受攻擊進而失去初始驗證的意義。但是他們的構想中，要求感測器必須要有一定的記憶體容量來記住所有的資訊，這樣也許會造成感測器一遭受攻擊就威脅到整個物聯網網路。

Wu et al.（2017）提出一個基於多閘道的物聯網驗證方案，他們提及在無線環境中，當參與者與整個網路之間的距離增加時，發送和接收訊息的成本會跟著增加，所以提出利用閘道來跟較遠的使用者或節點溝通，以避免物聯網的效率降低。他們將閘道分為內部閘道以及外部閘道，使用者可以存取各閘道管理的節點。整個過程中他們運用了雜湊以及互斥或的運算來降低運算的負擔，並且運作流程分為兩個情境，一是使用者透過內部閘道向該閘道管理的節點溝通，二是使用者向內部閘道請求資料，內部閘道再作為橋樑向外部閘道去取得該節點的資訊。但在整個運作流程中，節點的運算量以及所需記憶的資料量龐大，需要利用記憶體中的資訊去計算出各種不同的驗證資訊來做訊息驗證，如此一來，若節點遭受攻擊可能會被取得重要資料或者是增加節點負擔。

參、物聯網身分驗證機制設計

一、研究問題與需求

物聯網應用層負責管理以及存取資料的身分驗證，本研究針對身分以及封包的驗證提出一個安全機制，考量到物聯網設備的資源有限無法負擔過於繁複的驗證過程，所以提出的機制中所用到的加密方法及驗證方法都不可太複雜。本研究將以下特性作為安全機制設計的需求：

（一）機密性：物聯網中連結了非常多的物件，物件中又透過不同網路去連結，整體為異質性架構，又因為智慧家庭中的不同裝置間傳遞了各種跟個人隱私有關的資料，如果被惡意人士攻擊取得這些資料，很可能威脅到當事人的人身安全及造成財產損失，因此必須提供智慧家庭環境中傳遞資料的機密性。

（二）身分驗證：在整個物聯網架構中出現的閘道以及所有的裝置節點都需要事先對註冊機構（Registration Authority）做註冊動作，以利於後續收送封包前必須先通過身分驗證才能對資料做存取。另外，物聯網的應用層中牽涉資料的存取及使用，需要讓使用者通過身分驗證才能取得權限來存取所需的資料。

（三）設備、使用者新增／註銷：整個物聯網中隨時會有不同的設備或是新的使用者加入感測及監控，也會有設備以及使用者離開此物聯網環境。必須要有一套彈性的新增及註銷機制，才可以讓設備及使用者動態新增，在移除時也可以確保移除了原物聯網環境的相關設定，避免到了其他環境中，讓非法使用者取得相關資訊。

（四）封包來源驗證：感知層中包含了眾多物聯網感測裝置，每個裝置都會在特定管轄範圍中，感知層的裝置可能被偽造，所以需要驗證封包來源來驗證封包的合法性。

（五）執行效率：智慧家庭網路中有許多裝置的計算能力有限，所以本研究利用身分驗證加密以及降低資料傳遞次數來提供一個有效率的身分驗證機制。

二、研究架構與假設

本研究方法假設智慧家庭裝置的供應商在儲存資料還有執行加解密上具有可靠性、可用性的基本要求，對於物聯網裝置給予基本的信任。但是智慧家庭中充斥著個人隱私的資訊，在存取的過程中還是可能會被非法人士竊取來做惡意使用，所以必須對於資料的存取做身分驗證。

為了要建構出前一小節提到的身分驗證機制，此部分定義在驗證機制中會出現的各種角色內容、特色及負責工作，各個參與流程的角色與單位如圖 1 所示。

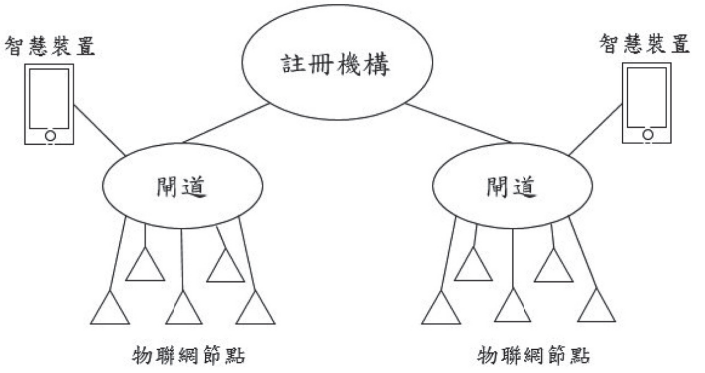

圖 1　研究角色架構圖

資料來源：作者自行研究整理。

（一）註冊機構：可信任機構，可以抵擋中間人攻擊以及 DoS 攻擊，有較大資料儲存能力，記錄所有物聯網裝置節點註冊以及訪問紀錄，也有較大的運算能力。在初始註冊階段，RA 擔任金鑰分發中心的角色，物聯網節點、閘道以及智慧型裝置都必須向註冊機構進行身分註冊。註冊機構會利用自己的私密金鑰來產生驗證訊息，讓節點、閘道以及智慧裝置能夠在驗證階段（Authentication Phase）證明自己的身分。在註冊階段，節點以及閘道會透過離線註冊來進行，智慧裝置則會透過其他管道傳遞重要資訊，例如：簡訊等方式，透過這樣的模式來降低線上作業可能面臨的網路攻擊。這個角色最主要會遇到身分管理的問題，因為要掌握眾多的節點，在這裡我們使用基於身分的存取控制，降低身分識別的負擔，也可以利用此唯一識別來針對特定對象做裝置的移入或移出，更動態性的做裝置的擴增移除。

（二）閘道：作為註冊機構以及各種物聯網節點的中間人，在初始註冊階段要使用自己的 ID 向註冊機構做註冊，在未來才能驗證自己的身分。計算能力較佳，驗證封包來源是否屬於自己管轄範圍的節點，以防止有惡意人士偽造節點。因為閘道在一開始註

冊時使用離線註冊，防止他人取得重要參數，所以就算惡意人士取得封包，也沒有閘道的參數可以進行解密取得封包內容。

（三）智慧型裝置：智慧居家的使用者，他們可以利用行動裝置遠端操控家中設備以及取得設備所感測到的數據。在初始階段，這些行動裝置也必須向註冊節點做註冊，以利於後續請求資料以及控制節點。當遭受攻擊，家中資訊被傳遞到惡意人士手中時，因為惡意人士的裝置未經註冊，無法得知封包內容，由此來增強訊息的機密性。

（四）物聯網裝置節點：智慧家庭中的所有感測裝置，負責感測家中環境數據，例如：溫溼度、空調控制、瓦斯感測、門禁管理等相關數據。節點的資料儲存空間較小，計算能力也較低，在節點中只儲存最基本的參數，主要工作為傳遞資訊，驗證的工作由閘道代為處理，如此便能適用於更彈性的智慧家庭環境中。

三、機制設計

本研究透過以上各角色進行身分及封包驗證的流程設計，整個流程設計分為「初始化」、「驗證」、「封包傳遞」、「會話金鑰更新」和「節點以及使用者註銷」等五個階段。在物聯網感測節點以及使用者的智慧裝置要加入物聯網環境時必須先初始化，向註冊機構請求註冊來取得自身的公私鑰以及後續驗證需要的秘密資訊。初始化階段結束後，在感測節點與閘道或是閘道與智慧裝置之間要開始進行通訊前，要經過驗證階段，雙方進行雙向驗證，確認雙方身分並取得會話金鑰來進行後續的溝通。一段的對話結束過後，如果要開始下一段的對話，就必須先更新會話金鑰，雙方取得新的金鑰才可開始傳遞封包。若有物聯網感測裝置或是智慧裝置要離開當下的物聯網環境時，傳遞註銷訊息向註冊機構下達指令，即可完成節點以及使用者註銷的流程。此研究設計會使用到的符號以及函式定義表，如表 1 和表 2 所示。

（一）初始化階段

在此階段，註冊機構作為金鑰分發中心，要加入此物聯網環境中的各角色，閘道、節點、智慧裝置都必須跟註冊機構進行離線註冊，註冊機構會執行 ECC 來產生該角色相對應的公私鑰以及利用自身的公鑰來計算出秘密資訊。一開始，註冊機構執行 ECC 產生自身的公私鑰 *RPU* 以及 *RPR* 以利後續驗證使用，以下將介紹不同角色註冊時詳細步驟。

1. 閘道註冊

閘道 j 在加入環境時，將自己的唯一識別碼 GID_j 向註冊機構下達註冊指令，註冊機構執行演算法 3-1，詳細閘道註冊運作流程如圖 2。

演算法 3-1：

(1) Start。

(2) 產生閘道 j 的公鑰 GPU_j 以及私鑰 GPR_j。

(3) 產生一隨機數 R_{Gj}。

(4) 利用自己的公鑰 *RPU* 產生秘密資訊 G_j。

(5) $G_j = EP\left(RPU, GID_j \middle|\middle| R_{Gj}\right)$。

表 1 符號定義表

符號	說明
RPU	註冊機構公開金鑰
RPR	註冊機構私密金鑰
GID_j	閘道 j 識別 ID
GPU_j	閘道 j 公開金鑰
GPR_j	閘道 j 私密金鑰
G_j	閘道 j 註冊後，註冊機構回傳之秘密資訊
NID_i	節點 i 識別 ID
NPU_i	節點 i 公開金鑰
NPR_i	節點 i 私密金鑰
N_i	節點 i 註冊後，註冊機構回傳之秘密資訊
DID_k	智慧裝置 k 識別 ID
DPU_k	智慧裝置 k 公開金鑰
DPR_k	智慧裝置 k 私密金鑰
D_k	智慧裝置 k 註冊後，註冊機構回傳之秘密資訊
X	節點與閘道之間的會話金鑰
Z	閘道與智慧裝置間的會話金鑰
T	時間戳記
R	隨機產生的亂數
NIP_i	節點 i 的 IP 位址
GIP_j	閘道 j 的 IP 位址
DIP_k	智慧裝置 k 的 IP 位址

資料來源：作者自行研究整理。

表 2 函式定義表

符號	說明
$EP(PU, M)$	用公鑰 PU 對明文 M 做 ECC 加密
$DP(PR, C)$	用私鑰 PR 對密文 C 做 ECC 解密
$E(K, M)$	用金鑰 K 對明文 M 做對稱式加密
$D(K, C)$	用金鑰 K 對密文 C 做對稱式解密
$H(M)$	對訊息 M 做雜湊運算

資料來源：作者自行研究整理。

(6) 將閘道 j 的 ID、公鑰、私鑰以及秘密資訊 $\{GID_j, GPU_j, GPR_j, G_j\}$ 傳送給閘道 j 保存。

(7) 在自己的資料庫中存入閘道 j 的相關資訊 $\{GID_j, GPU_j, R_{Gj}\}$。

(8) End。

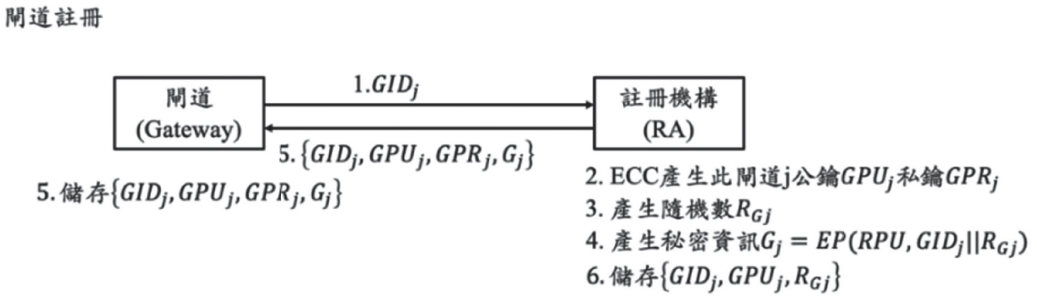

圖 2　閘道註冊流程圖

資料來源：作者自行研究整理。

2. 節點註冊

節點 i 在加入環境時，將自己的唯一識別碼 NID_i 給予註冊機構，註冊機構執行演算法 3-2，詳細節點註冊運作流程如圖 3。

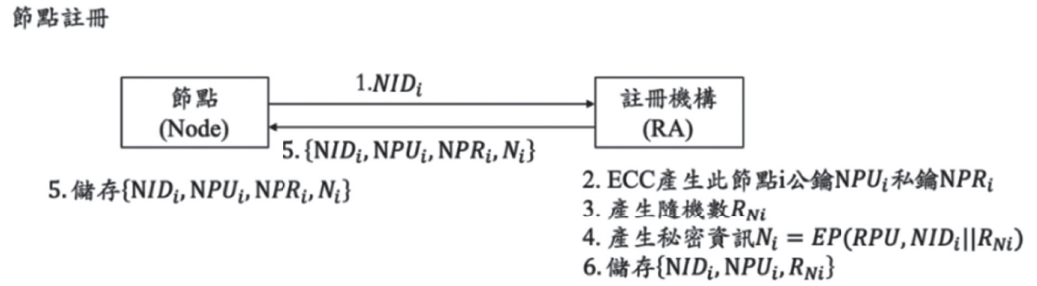

圖 3　節點註冊流程圖

資料來源：作者自行研究整理。

演算法 3-2：

(1) Start。

(2) 產生節點 i 的公鑰 NPU_i 以及私鑰 NPR_i。

(3) 產生一隨機數 R_{Ni}。

(4) 用自己的公鑰 RPU 產生秘密資訊 N_i。

(5) $N_i = EP\left(RPU, NID_i \middle|\middle| RN_i\right)$。

(6) 將節點 i 的 ID、公鑰、私鑰以及秘密資訊 $\{NID_i, NPU_i, NPR_i, N_i\}$ 傳送給節點 i 保存。

(7) 存入節點 i 的 $\{NID_i, NPU_i, R_{Ni}\}$。

(8) End。

3. 智慧裝置註冊

智慧裝置 k 在加入物聯網環境時，將裝置的唯一識別碼 DID_k 給予註冊機構請求註冊，註冊機構執行演算法 3-3，詳細智慧裝置註冊運作流程如圖 4。

演算法 3-3：

(1) Start。

(2) 產生智慧裝置 k 的公鑰 DPU_k 以及私鑰 DPR_k。

(3) 產生一隨機數 R_{Dk}。

(4) 利用自己的公鑰 RPU 產生秘密資訊 D_k。

(5) $D_k = EP\left(RPU, DID_k \middle|\middle| R_{Dk}\right)$。

(6) 將智慧裝置 k 的 ID、公鑰、私鑰以及秘密資訊 $\{DID_k, DPU_k, DPR_k, D_k\}$ 利用加密安全通道（Secure Sockets Layer）或簡訊傳送給智慧裝置保存（使用者取得簡訊後在 App 所設計的產品驗證畫面中貼入訊息內容來做帳號開通）。

(7) 將智慧裝置 k 的資訊 $\{DID_k, DPU_k, RD_k\}$ 存入資料庫中。

(8) End。

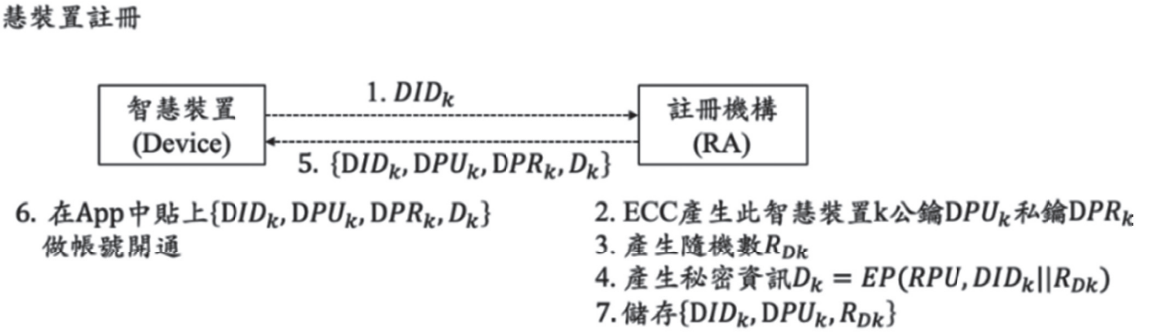

圖 4　智慧裝置註冊流程圖

資料來源：作者自行研究整理。

（二）驗證階段

在驗證階段時分為兩個部分，一個為節點與閘道間做雙向驗證，驗證對方身分後雙方取得會話金鑰，才可繼續後續的封包傳遞；第二個部分為智慧裝置與閘道間的雙向驗證，智慧裝置需要先與閘道做驗證，雙方拿到會話金鑰以利於後續對閘道下指令取得所需資料，以下詳細介紹這兩種的運作流程。

1. 節點與閘道雙向驗證

節點 i 向閘道 j 發出驗證請求 A 並記下時戳 T_n 傳送到閘道 j，閘道 j 確認來源封包的 ID，接受請求後記下時戳 T_g，將節點 i 的驗證請求 A 連同自己的驗證資訊 B，$\{A + B\}$ 一起

傳送到註冊機構做驗證。註冊機構執行演算法 3-4，詳細節點與閘道雙向驗證運作流程如圖 5。在演算法 3-4 中，行號 (2) 至行號 (5) 為註冊機構驗證閘道是否合法，行號 (6) 至行號 (9) 為註冊機構驗證節點是否合法，而行號 (10) 至行號 (11) 為註冊機構將秘密資訊（驗證結果）回傳給閘道和節點的做法。

$$A = \left\{ NID_i,\ GID_j,\ EP\left(NPR_i,\ T_n \,||\, GID_j \,||\, NID_i \,||\, N_i\right) \right\} \quad (1)$$

$$B = \left\{ GID_j,\ NID_i,\ EP\left(GPR_j,\ T_g \,||\, GID_j \,||\, NID_i \,||\, G_j\right) \right\} \quad (2)$$

演算法 3-4：

(1) Start。

(2) 用 GID_j 到資料庫提取相對的閘道公鑰 GPU_j，解密閘道 j 的驗證資訊 B，$DP(GPU_j, B)$ 並檢查驗證資訊 B 中以及外部的 GID_j、NID_i 是否相符。

(3) 檢查時戳 T_g 是否在合理範圍內。

(4) 利用自身的私鑰 RPR 解密 G_j，$DP(RPR, G_j)$ 取得 GID_j 以及 R_{Gj}。

(5) 利用 GID_j 到資料庫搜尋相對應的 R_{Gj}，驗證此閘道 j 的身分是否合法。

(6) 用 NID_i 到資料庫提取相對應的節點公鑰 NPU_i，解密節點 i 的驗證資訊 A，$DP(NPU_i, A)$ 並檢查驗證資訊 A 中以及外部的 GID_j、NID_i 是否相符。

(7) 檢查時戳 T_n 是否在合理範圍內。

(8) 利用自身的私鑰 RPR 解密 N_i，$DP(RPR, N_i)$ 取得 NID_i 以及 R_{Ni}。

(9) 用 NID_i 到資料庫搜尋相對應的 R_{Ni}，驗證此節點 i 的身分是否合法。

(10) 閘道 j 與節點 i 皆通過驗證後註冊機構會記下時戳 T_r，產生一會話金鑰 X。

(11) 利用會話金鑰 X 形成秘密資訊 NG_i，並用閘道 j 以及節點 i 各自的公開金鑰將秘密資訊 NG_i 以及會話金鑰 X 加密形成驗證資訊 C、D 並與節點 i 及閘道 j 的 ID 將 $\{NID_i, GID_j, C, D\}$ 傳送回閘道 j。

(12) $NG_i = E\left(X,\ T_r \,||\, NID_i \,||\, GID_j\right)$。

(13) $C = EP\left(NPU_i, NID_i \,||\, GID_j \,||\, NG_i \,||\, X\right)$。

(14) $D = EP\left(GPU_j, GID_j \,||\, NID_i \,||\, NG_i \,||\, X\right)$。

(15) End。

閘道 j 接收到註冊機構傳送的訊息後，利用自身的私密金鑰 GPR_j 解密訊息，$DP(GPR_j, D)$，取得秘密資訊 NG_i 以及會話金鑰 X，解密 NG_i，$D(X, NG_i)$ 取得 T_r，將 $\{NID_i, GID_j, C\}$ 傳送至請求驗證的節點 i。節點 i 取得回覆後，利用自身的私密金鑰 NPR_i 解密訊息，$DP(NPR_i, C)$，取得秘密資訊 NG_i 以及會話金鑰 X，解密 NG_i，$\mathrm{D}(\mathrm{X}, NG_i)$ 取得 T_r。以上的任一步驟皆在驗證失敗時即丟棄該封包，如驗證通過才進行下一步驟。

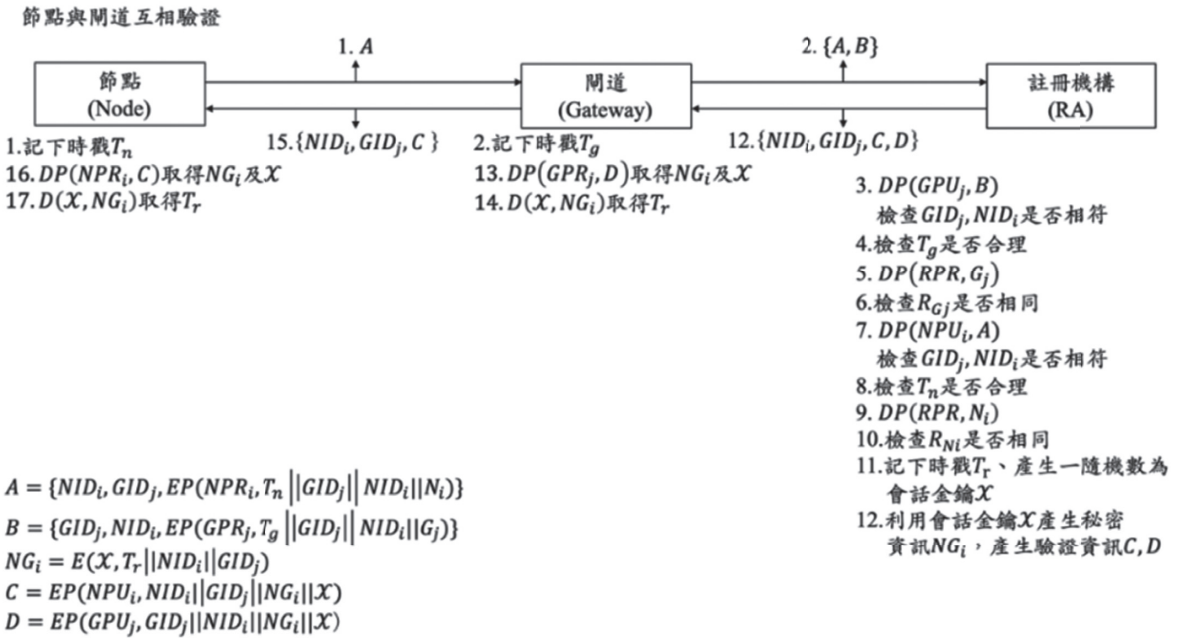

圖 5　節點與閘道雙向驗證流程圖

資料來源：作者自行研究整理。

2. 智慧裝置與閘道雙向驗證

智慧裝置在取得感測設備所感測到的環境數據前，必須先與閘道做雙向驗證。智慧裝置 k 提出驗證請求 Q 並記下時戳 T_d，傳送到閘道 j。閘道 j 確認來源封包的 ID 後接受請求，記下時戳 T_{gd}，將智慧裝置 k 的驗證資訊 Q 連同自己的驗證資訊 B，$\{Q + B\}$ 一起傳送到註冊機構做驗證。註冊機構執行演算法 3-5，詳細運作流程如圖 6。在演算法 3-5 中，行號 (2) 至行號 (5) 為註冊機構驗證閘道是否合法，行號 (6) 至行號 (9) 為註冊機構驗證智慧裝置是否合法，而行號 (10) 至行號 (11) 為註冊機構將秘密資訊（驗證結果）回傳給閘道和智慧裝置的做法。

$$Q = \left\{ GID_j,\ DID_k,\ EP\left(DPR_k,\ T_d \,||\, GID_j \,||\, DID_k \,||\, D_k\right) \right\} \tag{3}$$

$$B = \left\{ GID_j,\ DID_k,\ EP\left(GPR_j,\ T_{gd} \,||\, GID_j \,||\, DID_k \,||\, G_j\right) \right\} \tag{4}$$

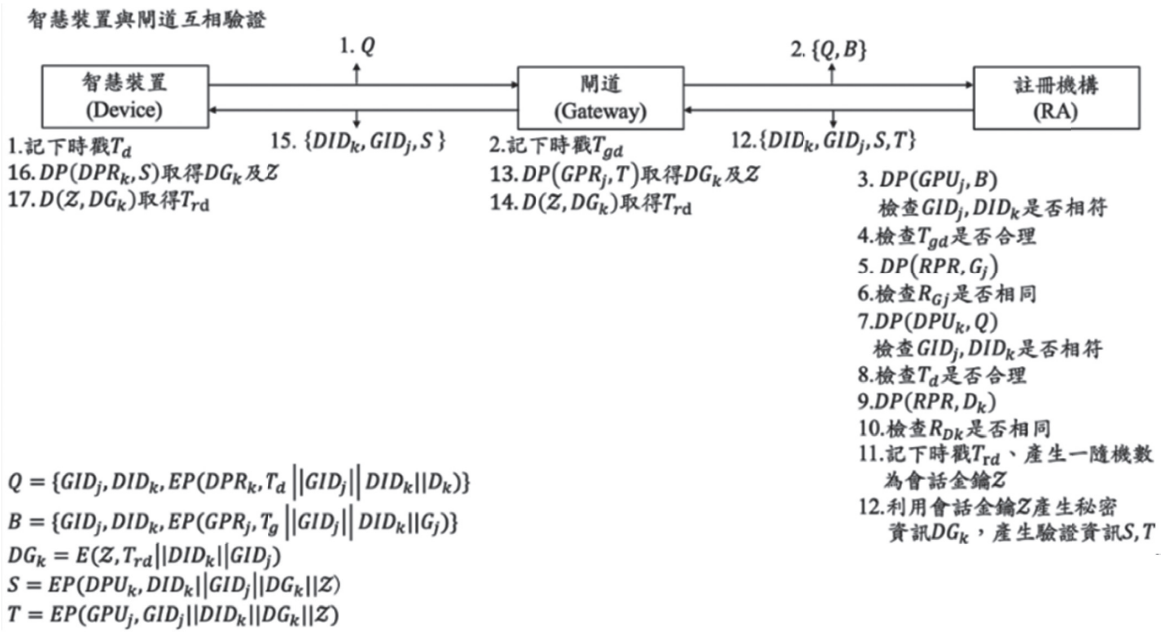

圖 6　智慧裝置與閘道雙向驗證流程圖

資料來源：作者自行研究整理。

演算法 3-5：

(1) Start。

(2) 用 GID_j 到資料庫找相對應的閘道公鑰 GPU_j，解密閘道 j 的驗證資訊 B，$DP(GPU_j, B)$ 並檢查驗證資訊 B 中以及外部的 GID_j、DID_k 是否相符。

(3) 檢查時戳 T_{gd} 是否在合理範圍內。

(4) 利用自身的私鑰 RPR 來解密 G_j，$DP(RPR, G_j)$ 取得 GID_j 以及 R_{Gj}。

(5) 用 GID_j 到資料庫搜尋相對應的 R_{Gj}，驗證此閘道 j 的身分是否合法。

(6) 用 DID_k 到資料庫找相對應的智慧裝置公鑰 DPU_k，解密智慧裝置 k 的驗證資訊 Q，$DP(DPU_k, Q)$ 並檢查驗證資訊 Q 中以及外部的 GID_j、DID_k 是否相符。

(7) 檢查時戳 T_d 是否合理。

(8) 利用自身的私鑰 RPR 解密 D_k，$DP(RPR, D_k)$ 取得 DID_k 以及 R_{Dk}。

(9) 用 DID_k 到資料庫搜尋相對應的 R_{Dk}，驗證此智慧裝置 k 身分是否合法。

(10) 閘道 j 與智慧裝置 k 皆通過驗證後註冊機構會記下時戳 T_{rd}、產生一會話金鑰 Z。

(11) 利用會話金鑰 Z 形成秘密資訊 DG_k，並用閘道 j 以及智慧裝置 k 各自的公開金鑰將此秘密資訊 DG_k 以及會話金鑰 Z 加密，形成驗證資訊 S、T 並連同智慧裝置 k 與閘道 j 的 ID 將 $\{DID_k, GID_j, S, T\}$ 傳送回閘道 j。

(12) $DG_k = E(Z, T_{rd} \| DID_k \| GID_j)$。

(13) $S = EP(DPU_k, DID_k \| GID_j \| DG_k \| Z)$。

(14) $T = EP(GPU_j, GID_j \| DID_k \| DG_k \| Z)$。

(15) End。

閘道 j 接收到註冊機構的訊息後，利用自身的私密金鑰 GPR_j 解密訊息 $DP(GPR_j, T)$，取得秘密資訊 DG_k 以及會話金鑰 Z，解密 DG_k，$D(Z, DG_k)$ 取得 T_{rd}，將 $\{DID_k, GID_j, S\}$ 傳送至請求驗證的智慧裝置 k。智慧裝置 k 取得回覆後，利用自身的私密金鑰 DPR_k 解密訊息，$DP(DPR_k, S)$，取得秘密資訊 DG_k 以及會話金鑰 Z，解密 DG_k，$D(Z, DG_k)$ 取得 T_{rd}。以上有任一步驟驗證失敗則立即丟棄該封包，如驗證通過才進行下一步驟。

（三）封包傳遞階段

封包傳遞階段分為三個部分，一個部分為節點傳送封包給閘道做儲存，第二個部分為使用者利用智慧裝置來向閘道取得所需資訊，第三個部分為智慧裝置可以直接向節點要求取得即時資訊。三個部分做封包傳遞前都必須經過前述的驗證階段來取得會話金鑰，以下敘述封包傳遞時的詳細步驟。

1. 節點向閘道傳送封包

閘道 j 與節點 i 取得會話金鑰 X 後開始進行封包傳遞，節點 i 利用會話金鑰 X 來加密訊息內容，並記下時戳 T_m。節點 i 每次送出封包時將 T_r 與自己的 IP 位址做雜湊後形成訊息 $Auth$，送出封包前將秘密資訊 $Auth$ 放置於 IP 標頭，將 T_r 加一，利用 T_m 與感測訊息（$Message$）用會話金鑰 X 加密形成訊息 U，並連同節點 i 及閘道 j 的 ID 一起將 $\{NID_i, GID_j, U\}$ 傳送至閘道 j。

$$Auth = H(T_r \| NIP_i) \tag{5}$$

$$U = E(X, T_m \| Message) \tag{6}$$

封包在網路層中會先在系統取得 T_r 和 NIP_i 雜湊並和 IP 標頭的雜湊值做比對，比對相符代表為同一網域來源，如果雜湊值有誤，可能遭到有心人士重送攻擊。閘道 j 將 T_r 加一，封包傳送到所屬的閘道 j 後，閘道 j 運用對稱式會話金鑰 X 來解密訊息 U，$D(X, U)$，驗證時戳 T_m 合法則取得該訊息（$Message$）。詳細節點向閘道傳送封包運作流程如圖 7，以上有任一步驟驗證失敗則立即丟棄該封包，如驗證通過才進行下一步驟。

2. 智慧裝置向閘道請求資料

智慧裝置 k 與閘道 j 取得會話金鑰 Z 後就會開始進行封包傳遞，智慧裝置 k 利用會話金鑰 Z 來加密請求數據的指令，並記下時戳 T_{md}。智慧裝置 k 每次送出指令時將 T_{rd} 與自己的 IP 位址做雜湊形成訊息 $Auth$，將指令送出前將秘密資訊 $Auth$ 放置於 IP 標頭，將 T_{rd} 加一，利用 T_{md} 與命令（$Command$）用會話金鑰 Z 加密形成訊息 V，並連同智慧裝置 k 及閘道 j 的 ID 一起將 $\{DID_k, GID_j, V\}$ 傳送至閘道 j。

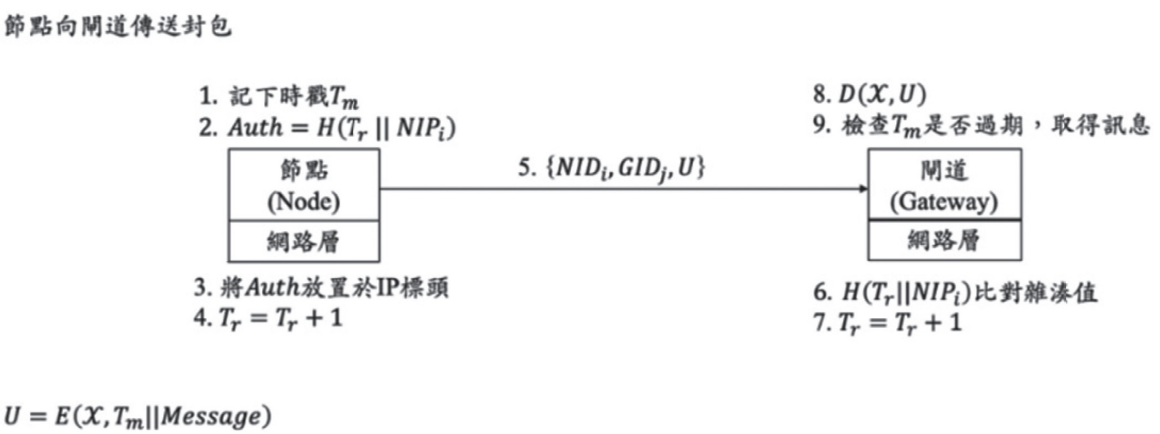

圖 7　節點向閘道傳送封包流程圖

資料來源：作者自行研究整理。

$$Auth = H\left(T_{rd} \,||\, DIP_k\right) \tag{7}$$

$$V = E\left(Z,\, T_{md} \,||\, Command\right) \tag{8}$$

封包在網路層中會先將 T_{rd} 和 DIP_k 做雜湊並和 IP 標頭的雜湊值做比對，比對相符代表為同一網域來源，如果雜湊值有誤，可能遭到有心人士重送攻擊。閘道 j 將 T_{rd} 加一，封包傳送到所屬的閘道 j 後，閘道 j 會運用會話金鑰 Z 來解密訊息 V，$D(Z, V)$，驗證時戳 T_{md} 合法則取得該指令（$Command$）。閘道 j 取得指令後，記下時戳 T_{mg}，每次送出訊息時將 T_{rd} 自己的 IP 位址做雜湊形成訊息 $Auth$，將訊息送出前將秘密資訊 $Auth$ 放置於 IP 標頭，利用 T_{mg} 與感測訊息用會話金鑰 Z 加密形成訊息 W，並連同智慧裝置 k 及閘道 j 的 ID 一起將 $\{DID_k, GID_j, W\}$ 傳送至智慧裝置 k。

$$Auth = H\left(T_{rd} \,||\, GIP_j\right) \tag{9}$$

$$W = E\left(Z,\, T_{mg} \,||\, Message\right) \tag{10}$$

封包在網路層中會先將 T_{rd} 和 GIP_j 做雜湊並與 IP 標頭的雜湊值做比對，比對相符代表為同一網域來源，如果雜湊值有誤，可能遭到有心人士重送攻擊。智慧裝置 k 取得封包後利用會話金鑰 Z 解密訊息 W，$D(Z, W)$，驗證時戳 T_{mg}，成功則取得感測訊息。詳細智慧裝置向閘道請求資料流程如圖 8，以上有任一步驟驗證失敗則立即丟棄該封包，如驗證通過才進行下一步驟。

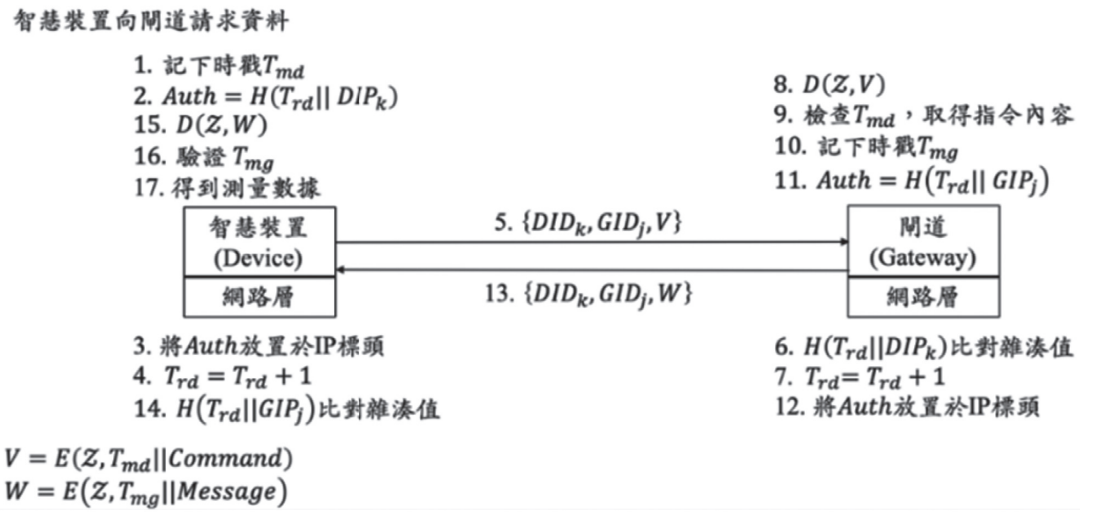

圖 8 智慧裝置向閘道請求資料流程圖

資料來源：作者自行研究整理。

3. 智慧裝置向節點下達指令

在訊息傳遞過程中，各角色均會產生秘密資訊 *Auth* 放置於 IP 標頭，以作為網路層的封包來源驗證，此做法和前面兩個小節的敘述相似，本小節中將省略此部分，著重在傳遞的訊息本身。

智慧裝置 k 向特定節點 i 取得即時資料或是下達指令時記下時戳 T_{md}，利用 T_{md} 與命令（*Command*）用會話金鑰 Z 加密形成訊息 Y，並連同智慧裝置 k、閘道 j 以及節點 i 的 ID 一起將 $\{DID_k, GID_j, NID_i, Y\}$ 傳送至閘道 j。

$$Auth = H\left(T_{rd} \,||\, DIP_k\right) \tag{11}$$

$$Y = E\left(Z,\, T_{md} \,||\, Command\right) \tag{12}$$

閘道 j 取得封包後利用會話金鑰 Z 解密訊息 Y，$D(Z, Y)$，確認 T_{md} 是否過期，取得指令，記下時戳 T_{mg}，利用 T_{mg} 與命令（*Command*）用會話金鑰 X 加密形成訊息 F，並連同閘道 j 與節點 i 的 ID 一起將 $\{GID_j, NID_i, F\}$ 傳送至節點 i。

$$Auth = H\left(T_r \,||\, GIP_j\right) \tag{13}$$

$$F = E\left(X,\, T_{mg} \,||\, Command\right) \tag{14}$$

節點 i 將 T_r 加一，取得封包後利用會話金鑰 X 解密訊息 F，$D(X, F)$，確認 T_{mg} 是否過期。節點 i 確認指令來源合法後開始傳送資料給閘道 j，記下時戳 T_{mn}，利用 T_{mn} 與訊息用會話金鑰 X 加密形成訊息 H，並連同節點 i 及閘道 j 的 ID 一起將 $\{NID_i, GID_j, H\}$ 傳送至閘道 j。

$$Auth = H\left(T_r \,||\, NIP_i\right) \tag{15}$$

$$H = E\left(X, T_{mn} \,||\, Message\right) \tag{16}$$

閘道 j 將 T_{rd} 加一，利用會話金鑰 X 解密出訊息，$D(X, H)$，記下時戳 T_{mgd}，利用 T_{mgd} 與訊息用會話金鑰 Z 加密形成訊息 K，並連同閘道 j 及智慧裝置 k 的 ID 一起將 $\{GID_j, DID_k, K\}$ 傳送至智慧裝置 k。

$$Auth = H\left(T_{rd} \,||\, GIP_j\right) \tag{17}$$

$$K = E\left(Z, T_{mgd} \,||\, Message\right) \tag{18}$$

智慧裝置 k 利用會話金鑰 Z 解密訊息，$D(Z, K)$，確認時戳 T_{mgd} 是否過期，取得所需資料。詳細智慧裝置向節點下達指令流程如圖 9，以上有任一步驟驗證失敗則立即丟棄該封包，如驗證通過才進行下一步驟。

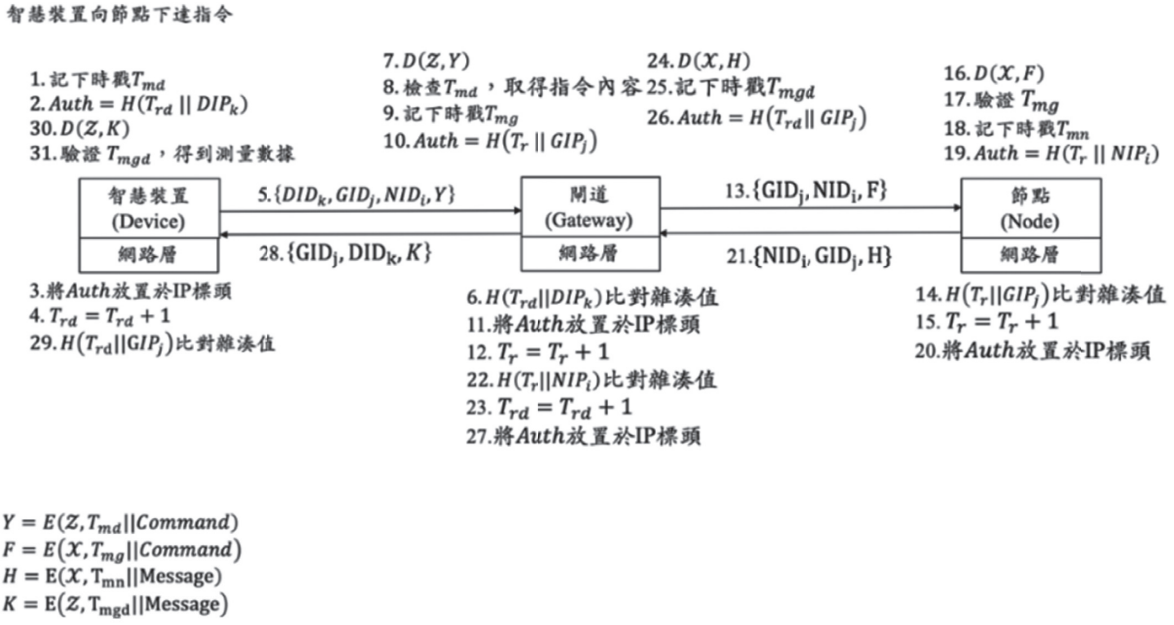

圖 9　智慧裝置向節點下達指令流程圖

資料來源：作者自行研究整理。

（四）會話金鑰更新

在會話金鑰過期之後，要開始下一段的對話前要更新會話金鑰，才能開始進行對話。

1. 節點 i 產生一個新的隨機數 X'。
2. 節點 i 記下新的時戳 T_r'。
3. 節點 i 用舊的會話金鑰 X 來加密新的金鑰 X' 以及新的時戳 T_r' 形成訊息 $Renew$，並連同節點 i 及閘道 k 的 ID 傳送給閘道 j。
4. $Renew = E\left(X, X' \middle|\middle| T_r'\right)$。
5. 閘道 j 利用舊的會話金鑰 X 來解出新的金鑰，$D(X, Renew)$。
6. 閘道 j 取得新的會話金鑰 X' 以及驗證時戳 T_r'。

以上皆驗證通過後才開始新的通訊，圖 10 為會話金鑰更新流程圖。

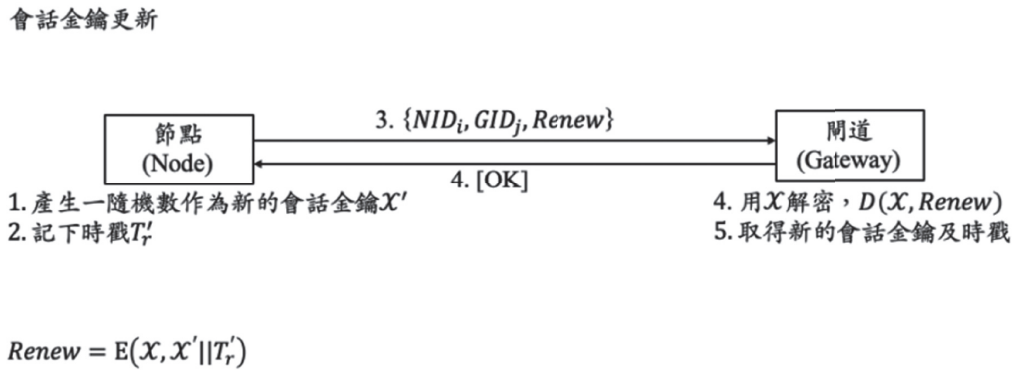

圖 10　會話金鑰更新流程圖

資料來源：作者自行研究整理。

（五）節點以及使用者註銷

當有節點或是智慧裝置要離開此物聯網環境時，必須向註冊機構提出註銷請求，由註冊機構來驗證註銷請求，驗證通過後刪除該角色的相關資料，圖 11 為節點以及智慧裝置註銷的流程圖。節點 i 設下時戳 T_{Revoke} 並提出 $\{NID_i, Revoke_{node}\}$ 或智慧裝置 k 提出 $\{DID_k, Revoke_{device}\}$ 註銷請求，註冊機構執行演算法 3-6，最後節點刪除資料庫中相關的秘密資訊 NPU_i、NPR_i、N_i 或智慧裝置移除 DPU_k、DPR_k、D_k。

$$Revoke_{node} = EP\left(NPR_i, NID_i \middle|\middle| T_{Revoke} \middle|\middle| N_i\right) \tag{19}$$

$$Revoke_{device} = EP\left(DPR_k, DID_k \middle|\middle| T_{Revoke} \middle|\middle| D_k\right) \tag{20}$$

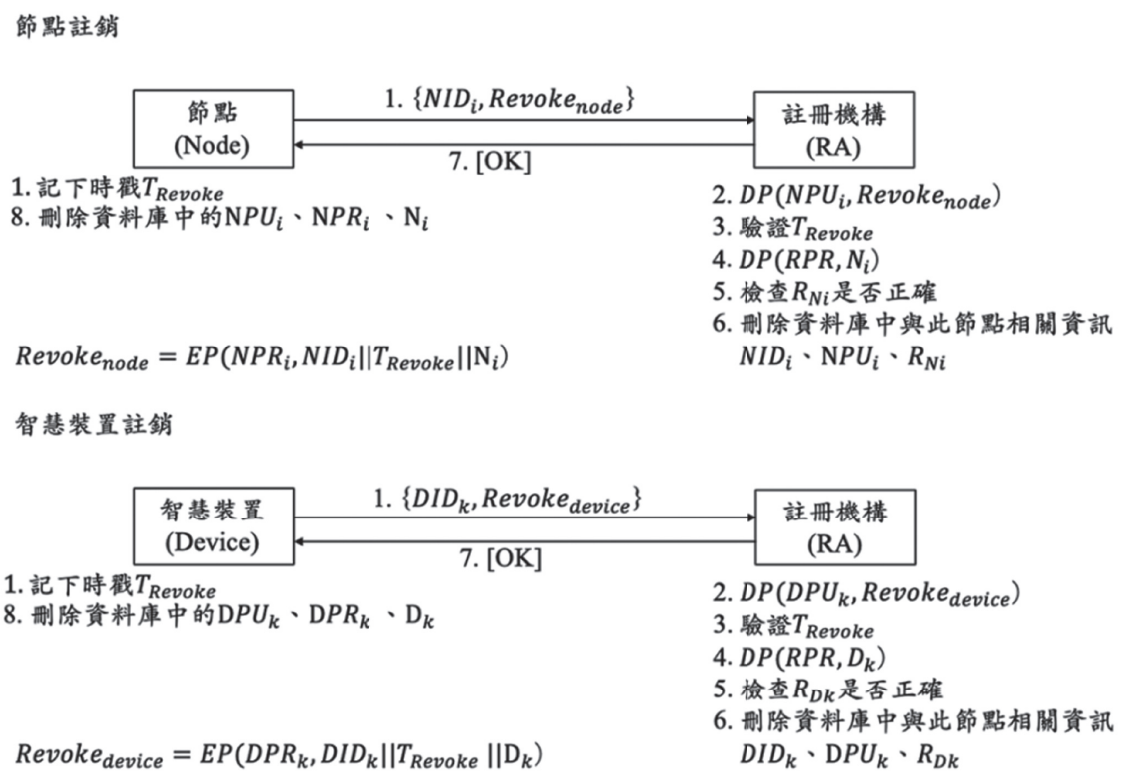

圖 11　節點以及智慧裝置註銷的流程圖

資料來源：作者自行研究整理。

演算法 3-6：

1. Start。
2. 用 NID_i 或裝置 DID_k 查詢資料庫中有關此節點或智慧裝置的相關資訊，並用該角色的公開金鑰解密註銷請求，$DP(NPU_i, Revoke_{node})$ 或 $DP(DPUk, Revoke_{device})$。
3. 驗證時戳 T_{Revoke}。
4. 利用自身的私鑰 RPR 解密 N_i 或 D_k，$DP(RPR, N_i)$ 或 $DP(RPR, D_k)$ 取得 R_{Ni} 或 R_{Dk}。
5. 檢查 R_{Ni} 或 R_{Dk} 是否正確。
6. 刪除儲存在資料庫中的 NID_i、NPU_i、RN_i 或智慧裝置的 DID_k、DPU_k、R_{Dk}。
7. 驗證成功後回傳成功訊息給註銷請求方。
8. End。

（六）驗證資訊置於 IP 標頭

在封包傳遞階段，傳送端會先將驗證資訊 *Auth* 放置於 IP 標頭中，以利於接收端在網路層中可以用標頭中的驗證資訊來做封包來源端驗證。在 IPv4 標頭中 Options 為非必要且長度不固定的欄位，通常可以用來記錄時戳或路由的相關資訊，所以本研究設計的機制為達成在網路層做封包來源驗證的目的，將驗證資訊放置於 IPv4 標頭的 Options 欄位中。另外，IPv6 的 Next Header 表示 Extended Header 的代碼，可以插入不同長度的 Extended Header，

每個 Extended Header 可以分別記錄路由、TCP、UDP 和身分驗證資訊等內容，所以本研究新增一個 Extended Header 放置驗證資訊 *Auth*。

肆、安全與效率分析

一、安全特性分析

（一）機密性：在物聯網環境中充斥著許多感測數據，為了避免這些數據洩漏導致威脅到當事人的人身安全及造成財產損失，因此這些數據的傳遞都必須經過加密處理，在解密這些數據的重要金鑰也不能落入他人手中，所以本研究方法的機密性可以兩個方面進行分析，分別為金鑰機密性和封包內容機密性。

1. 金鑰機密性：在封包傳遞開始之前，雙方進行身分驗證，註冊機構會產生一個隨機數作為會話金鑰並用請求驗證的兩方的公鑰進行加密，因此只有擁有相對應的私密金鑰的角色才能有權利取得會話金鑰。在後續的會話金鑰更新，新的會話金鑰也會利用舊的會話金鑰加密，所以一樣只有原來符合權限的角色可以取得新的金鑰。
2. 封包內容機密性：許多物聯網的感測數據在網路中流傳著，為了避免數據遭到有心人士竊取，本篇論文的封包傳遞流程設計在數據傳遞之前，傳送端與接收端會在驗證階段中進行雙向驗證產生會話金鑰，並且只有用自己的私鑰才能解出會話金鑰，進而用會話金鑰取得時戳，後續才能利用此時戳來產生驗證資訊。因此如果不是符合權限的使用者便無法順利的取得會話金鑰進而取得後續驗證所需資訊，也無法取得封包內容。

（二）身分驗證：本機制在各角色一開始進入物聯網環境時就先跟註冊機構做註冊，註冊機構驗證角色通過後，會針對該角色產生一個隨機數並且利用自身的私密金鑰來產生一個秘密資訊，以利於後續各角色在進行驗證階段時可以向註冊機構表明合法身分。

（三）設備、使用者註銷：當有感測裝置或是智慧裝置要離開此物聯網環境時，必須要撤銷這些角色能夠在此環境中傳送、存取資料的權限。本機制的註銷機制是由要離開的該角色向註冊機構提出註銷請求，註冊機構驗證過註銷請求後，利用該角色的 ID 到資料庫查詢，將該角色的相關資料刪除，刪除過後這些角色就無法在物聯網環境中傳送封包以及存取資料。

（四）封包來源驗證：在本機制中，封包傳遞的驗證是由閘道負責的，閘道必須確保所取得的封包來源要為合法節點所傳送的，所以封包在網路層時先進行封包標頭的驗證，驗證時戳是否合法、來源 IP 位址是否正確，先確認封包來源才在應用層進行封包解密，如此一來，可以避免遭到 DoS 攻擊，也避免沒有確認封包來源就解密封包內容可能會釋放出惡意程式到該物聯網環境中。

（五）執行效率：在物聯網環境中充斥著各種的物聯網數據，閘道要負責處理大量的封包驗證，負擔較大。為了避免因為大量封包影響到驗證時間過長，造成系統負荷太重，閘道在網路層取得封包時會先驗證封包標頭的驗證資訊，只要有一個步驟驗證失敗

立即丟棄該封包，驗證通過後才開始解密封包內容，如此一來可以降低閘道在驗證以及加解密上的負擔，避免遭大量封包攻擊而導致系統當機。

二、效率分析

此小節整理本研究設計的機制中每個流程的加解密運算次數、隨機數以及雜湊值產生的次數，再以本機制的流程為主軸，針對機制中各個角色，包括註冊機構、閘道、節點以及智慧裝置來進行分析，各流程的各角色不同運算種類的運算次數如表 3。

表 3　各角色在各流程中不同運算種類的運算次數

角色	運算種類	初始化階段	驗證階段	封包傳遞階段	會話金鑰更新階段	註銷階段	總和
註冊機構	非對稱式加密	3	4	0	0	0	7
	非對稱式解密	0	8	0	0	2	10
	對稱式加密	0	2	0	0	0	2
	對稱式解密	0	0	0	0	0	0
	隨機數	6	2	0	0	0	8
閘道	非對稱式加密	0	2	0	0	0	2
	非對稱式解密	0	2	0	0	0	2
	對稱式加密	0	0	3	0	0	3
	對稱式解密	0	2	4	1	0	7
	隨機數	0	0	0	0	0	0
	雜湊函數	0	0	7	0	0	7
智慧裝置	非對稱式加密	0	1	0	0	1	2
	非對稱式解密	0	1	0	0	0	1
	對稱式加密	0	0	2	0	0	2
	對稱式解密	0	1	2	0	0	3
	隨機數	0	0	0	0	0	0
	雜湊函數	0	0	4	0	0	4
節點	非對稱式加密	0	1	0	0	1	2
	非對稱式解密	0	1	0	0	0	1
	對稱式加密	0	0	2	1	0	3
	對稱式解密	0	1	1	0	0	2
	隨機數	0	0	0	1	0	1
	雜湊函數	0	0	3	0	0	3

資料來源：作者自行研究整理。

根據各流程的運算次數來分析各項運算需要的時間，本機制將大部分的運算集中在註冊機構，其次則是閘道。節點的非對稱式運算三次發生在封包傳遞前的驗證階段以及節點註銷階段，在封包傳遞時則做了兩次以下的對稱式加解密運算，如此一來可以有效的降低封包傳遞時所需要的運算成本，降低節點負擔。

三、方法比較

本小節將本機制與其他相關文獻做安全特性的比較，比較結果如表 4。Chuang et al.（2018）提出物聯網的輕量化驗證，著重於連續驗證的輕量化驗證。在一段會話的開始時先進行靜態驗證，會話進行階段也進行著連續驗證，並利用動態的電量來當作驗證的因素。其運算模式較為不適合應用於智慧家庭，不斷的進行驗證身分並讓閘道去提取節點的電量來做驗證，來回多次的運算可能對於此環境較為不友善。另外，此篇也未完整考量設備以及使用者的新增／註銷。Wu et al.（2017）在物聯網環境中設計內部閘道以及外部閘道的架構，利用這樣的架構較遠的節點也可以容易的與閘道溝通，節點可以跟自己最近的閘道溝通，避免太遠的節點跟閘道接觸消耗太多資源。這樣的架構並無考慮到來源驗證來抵擋 DoS 攻擊，以及使用者的新增／註銷。

表 4　安全特性比較

機制	特性				
	機密性	身分驗證	設備、使用者新增／註銷	封包來源驗證	執行效率
Chuang et al.（2018）	O	O	n/a	O	O
Wu et al.（2017）	O	O	n/a	n/a	O
本方法	O	O	O	O	Δ

註：O：有做到；Δ：部分做到；n/a：未考慮此特性。
資料來源：作者自行研究整理。

表 5 為 Dai（2009）提出的 Crypto++ Benchmark，在處理器 1.83 GHz 且作業系統為 Windows Vista 32 位元的環境中執行相關的運算項目和相對應的運算時間。產生一次 128 位元的隨機數約為 0.0002 毫秒，產生一次雜湊的時間為 0.00006 毫秒，做一次 256 位元的對稱式加、解密時間約為 0.0003 毫秒，做一次的非對稱式加密時間為 0.08 毫秒，非對稱式解密的時間則為 1.46 毫秒。本研究各流程之運算時間以及各角色運算時間如表 6 及表 7，其中 T_r 為產生隨機數的時間，T_{ae} 代表 RSA 非對稱式加密時間，T_{ad} 代表 RSA 非對稱式解密時間，T_{se} 代表 AES 對稱式加密時間，T_{sd} 代表 AES 對稱式解密時間，T_h 為產生雜湊值的時間，以及 n/a 代表該文獻無此值。

表 5　相關演算法運算時間

演算法	產生隨機數（128 位元）	雜湊函數	AES 加密（256 位元）	AES 解密（256 位元）	RSA 加密	RSA 解密
運算時間	0.0002 ms	0.00006 ms	0.0003 ms	0.0003 ms	0.08 ms	1.46 ms

資料來源：Dai（2009）。

表 6　各流程運算時間

	流程				
機制	初始化	驗證階段	封包傳遞	會話金鑰更新	節點以及使用者註銷
Chuang et al.（2018）	$1T_r \approx 0.0002$ ms	$20T_h \approx 0.0012$ ms	$14T_h \approx 0.00084$ ms	n/a	n/a
Wu et al.（2017）	$5T_h \approx 0.0003$ ms	$35T_h \approx 0.0021$ ms	n/a	n/a	n/a
本方法	$3T_{ae} + 6T_r \approx 0.2412$ ms	$8T_{ae} + 12T_{ad} + 2T_{se} + 4T_{sd} + 2T_r \approx 18.16$ ms	$7T_{se} + 7T_{sd} + 14T_h \approx 0.00504$ ms	$1T_{se} + 1T_{sd} + 1T_r \approx 0.0008$ ms	$2T_{ae} + 2T_{ad} \approx 3.08$ ms

資料來源：作者自行研究整理。

表 7　各角色運算時間

	角色				
機制	註冊機構	閘道	節點	智慧裝置	總和
Chuang et al.（2018）	n/a	$1T_r + 18T_h \approx 0.00128$ ms	$16T_h \approx 0.00096$ ms	n/a	$1T_r + 34T_h \approx 0.00224$ ms
Wu et al.（2017）	n/a	$24T_h \approx 0.0014$ ms	$3T_h \approx 0.00018$ ms	$13T_h \approx 0.00078$ ms	$40T_h \approx 0.0024$ ms
本方法	$7T_{ae} + 10T_{ad} + 2T_{se} + 8T_r \approx 15.1$ ms	$2T_{ae} + 2T_{ad} + 3T_{se} + 7T_{sd} + 7T_h \approx 3.08$ ms	$2T_{ae} + 1T_{ad} + 3T_{se} + 2T_{sd} + 1T_r + 3T_h \approx 1.65$ ms	$2T_{ae} + 1T_{ad} + 2T_{se} + 3T_{sd} + 4T_h \approx 1.62$ ms	$13T_{ae} + 14T_{ad} + 10T_{se} + 12T_{sd} + 9T_r + 14T_h \approx 21.48$ ms

資料來源：作者自行研究整理。

根據表 6 和表 7 的比較結果，Chuang et al.（2018）以及 Wu et al.（2017）提出的方法大多使用雜湊值的計算並進行比對，Chuang et al.（2018）在每個階段的流程中，各角色都必須要向設備提取電池壽命等資訊，並與時戳等數值做計算與比對。Wu et al.（2017）則是在驗證過程中大量使用雜湊值以及互斥或的觀念來做數值的比對。在兩個文獻中皆無註冊機構的角色，所有驗證工作都由閘道執行，可能會因為閘道掌握了所有的運算資源而被惡意人士攻擊，進而取得系統的相關資訊。在 Chuang et al.（2018）提出的文獻中，閘道與節點在

進行封包傳遞時會同時執行連續驗證，節點在封包傳遞時皆要進行約十次左右的雜湊計算並且比對，可能會使節點所需要的資源較多且需要較多的記憶體而導致負擔較大。本文封包傳遞的三種狀態中，封包在各角色的傳遞次數最少為一次，最多為智慧裝置向節點下達指令時的四次。雖然本機制在計算時間上較為弱勢，但封包的來回傳遞也會增加運算的時間，本文在封包來回傳遞的次數以及驗證資訊複雜度相較於兩篇參考文獻有較多優勢。

伍、結論與未來研究方向

本研究設計一個智慧家庭的身分驗證機制，適用於智慧家庭中的資料保護並輕量化驗證的過程。本研究在開始封包傳遞前，各角色間會先進行雙向驗證取得會話金鑰，以及取得註冊機構提供的時戳。開始進行封包傳遞時，各角色會在 IP 標頭中先放入驗證資料讓封包在網路層時可以先做來源驗證，如驗證不符即丟棄該封包，驗證通過才將封包送往應用層，如此可以減少在應用層中大量驗證的工作，提升驗證效率並且保護資料安全。本研究機制在驗證階段時，會由註冊機構產生隨機數作為會話金鑰，並且利用各角色的公開金鑰加密，所以只有合法角色才能取得會話金鑰，取得會話金鑰後才能取得註冊機構提供的時戳，作為後續封包傳遞時所需要的驗證資訊。因為以上的金鑰機密性，在會話金鑰更新時，直接由節點產生一隨機數作為新的會話金鑰，並且利用舊的會話金鑰加密新的會話金鑰，如此就不用時常重複進行較為複雜的驗證階段，讓雙方最快速的取得新的會話金鑰進行下一次對話。

本研究是適用於智慧家庭，有鑑於智慧家庭中不會有過多的感測裝置，所以在架構中只有一個註冊機構。未來可以在這樣的驗證機制中修改架構，增加多個註冊機構，讓更大量的節點以及使用者可以向不同的註冊機構進行註冊，避免註冊機構負擔過大。另外，增設不同的閘道，讓節點的設置範圍可以無限擴大，讓使用者也可以取得遠方目標節點的感測數據。這樣的改變能讓該機制更為彈性，以適用於更大型的物聯網環境，例如智慧城市或者智慧醫院等。

參考文獻

科技政策研究與資訊中心，2018 年 4 月 2 日，〈智慧家庭裝置於 2022 年出貨量接近 10 億〉，《科技產業資訊室》http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=14315（瀏覽日期：2018 年 10 月 1 日）。

Chuang Y.-H., Lo N.-W., Yang C.-Y., and Tang S.-W., 2018, “A Lightweight Continuous Authentication Protocol for the Internet of Things,” *Sensors*, 18(4), 1104. doi:10.3390/s18041104

Dai W., 2009, “Crypto++ 5.6.0 Benchmarks,” https://www.cryptopp.com/benchmarks.html (accessed January 1, 2020).

DeCusatis C., Liengtiraphan P., Sager A., and Pinelli M., 2016, “Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication,” paper presented

at *the IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY. doi:10.1109/SmartCloud.2016.22

Khan M. A., and Salah K., 2018, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, 82, 395-411. doi:10.1016/j.future.2017.11.022

Khemissa H., and Tandjaoui D., 2015, "A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things," paper presented at *the 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, UK. doi:10.1109/NGMAST.2015.31

Li L., 2012, "Study on Security Architecture in the Internet of Things," paper presented at *the International Conference on Measurement, Information and Control*, Harbin, China. doi:10.1109/MIC.2012.6273274

Lin H., and Bergmann N. W., 2016, "IoT Privacy and Security Challenges for Smart Home Environments," *Information*, 7(3), 44. doi:10.3390/info7030044

Liu J., Xiao Y., and Chen C. L. P., 2012, "Authentication and Access Control in the Internet of Things," paper presented at *the 32nd International Conference on Distributed Computing Systems Workshops*, Macau, China. doi:10.1109/ICDCSW.2012.23

Salami S. A., Baek J., Salah K., and Damiani E., 2016, "Lightweight Encryption for Smart Home." paper presented at *the 11th International Conference on Availability, Reliability and Security*, Salzburg, Austria. doi:10.1109/ARES.2016.40

Uviase O., and Kotonya G., 2018, "IoT Architectural Framework: Connection and Integration Framework for IoT Systems," *Electronic Proceedings in Theoretical Computer Science*, 264, 1-17. doi:10.4204/EPTCS.264.1

Wu F., Xu L., Kumari S., Li X., Shen J., Choo K.-K. R., Wazid M., and Das A. K., 2017, "An Efficient Authentication and Key Agreement Scheme for Multi-Gateway Wireless Sensor Networks in IoT deployment," *Journal of Network and Computer Applications*, 89, 72-85. doi:10.1016/j.jnca.2016.12.008

Zhao K., and Ge L., 2013, "A Survey on the Internet of Things Security," paper presented at *Ninth International Conference on Computational Intelligence and Security*, Emeishan, China. doi:10.1109/CIS.2013.145