余平、黃詩蓉（2020），『一個增強的 IoT 無線感測網路遠端認證機制』，*中華民國資訊管理學報*，第二十七卷，第一期，頁 111-142。

一個增強的 IoT 無線感測網路遠端認證機制

余平*
中國文化大學資訊管理學系

黃詩蓉
中國文化大學資訊管理學系

摘要

近年來 IoT 的發展應用越來越貼近我們的日常生活，根據研究顯示在醫療照護上將佔 IoT 整體應用的四成，顯示出 IoT 在醫療照護上的潛力。但無論在醫療照護、企業生產或生活應用上，常需由遠端存取各項需保密的資訊，若 IoT 感測器遭到攻擊或傳送的資訊被竊取，將會造成個人或企業的生命及財產權益受損，因此一個安全的 IoT 無線感測網路遠端認證機制有其必要性。本研究發現 Wu 等人於 2018 年提出認證機制中，匿名性保護及感測器取得攻擊的安全性不夠完善，本文除指出其機制存在的弱點及提出一個新的 IoT 無線感測網路遠端認證機制外，並以 Proverif 形式化及非形式化的安全性分析證明新機制的安全性，及利用與現有機制的效能及安全性比較證明新機制的實用性，以提供更佳的安全性及未來實用價值的 IoT 無線感測網路遠端認證機制。

關鍵詞：物聯網、無線感測網路、遠端認證、安全性分析

* 本文通訊作者。電子郵件信箱：yp@faculty.pccu.edu.tw
2019/08/16 投稿；2019/11/25 修訂；2019/12/16 接受

Yu, P. and Huang, S.J. (2020), 'An enhanced IoT wireless sensing network remote authentication scheme', *Journal of Information Management*, Vol. 27, No. 1, pp. 111-142.

An Enhanced IoT Wireless Sensing Network Remote Authentication Scheme

Ping Yu*
Department of Information Management, Chinese Culture University

Shih-Jung Huang
Department of Information Management, Chinese Culture University

Abstract

Purpose－The IoT (Internet of Thing) is a broad field with many different technologies and applications. In the last few years, they have collected the data into analytics to create value deriving from combining and analyzing from various sources. But these data have to be continuously available from a secure and flexible architecture. This study aims to design an enhanced IoT wireless sensing network(WSN) remote authentication scheme for accessing the IoT data through the gateway over a public channel. The result of security and performance analysis proves the scheme secure and efficient that can implement in real-life applications.

Design/methodology/approach－In this study, We review the researches that design for remote user authentication of IoT architecture. We use the security analysis to find the weakness of the proposed practiced scheme. Based on that scheme, we offer a new IoT WSN remote authentication scheme to avoid their leaks. The formal security analysis of Proverif tool and informal security analysis approaches id used to prove the security and the practicability of the new scheme.

Findings－The IoT has widely adopted in many applications. However, there exist various security and privacy issues. Notably, one of the most severe threats is to clone IoT devices for the goal of counterfeiting goods, which causes significant loss and

* Corresponding author. Email: yp@faculty.pccu.edu.tw
2019/08/16 received; 2019/11/25 revised; 2019/12/16 accepted

danger to users. Lots of authentication protocols are proposed based on physical functions. However, most of the existing schemes require secret parameters in IoT, which are vulnerable to physical attacks. In this study, we find the authentication scheme proposed by Wu et al. (2018) has practical value for multi-gateway based on WSNs. But we also find their scheme cannot resist several attacks. The findings also showed that design a remote user authentication scheme with secure and efficient is necessary.

Research limitations/implications－In this study, we follow three assumptions regarding the capabilities of an attacker. Firstly, an attacker has total control over the public channel connecting the users and the remote server that the adversary can intercept or modify any message. Secondly, an attacker may steal or get a smart device or IoT devices. Thirdly, the adversary attacker can retrieve the information from a smart device or IoT devices. From the previous three assumptions, we analyze the existing scheme and proposed scheme.

Practical implications－The WSNs of IoT provides practical security aspects are the challenging area in the research field, and many researchers still try to improve the efficiency of the system. Though, this paper presents relatively better efficiency compared with the related systems.

Originality/value－Since the IoT devices are constrained by battery power; The energy consumption should be minimum to increase the life-time of the network. It is noticeable that the efficiency of our scheme is relatively better in terms of computation cost than other related schemes.Therefore,it can be applied in practical implementation in the WSNS environment. We will try to improve the scheme more efficient without compromising several security aspects in the future.

Keywords: Internet of Things, wireless sensing network, remote authentication, security analysis

壹、前言

近年來隨著科技的發展，行動及無線網路的傳輸速度越來越快，並融入各項商業及生活的應用，讓我們增添不少便利。如隨時隨地搜尋各項訊息，或透過 GPS 定位及網路地圖獲取所在位置的相關資訊或前往的方法。近年來並成為社交及電子支付的重要工具，但也造成行動裝置中含有大量的個人隱私資訊，在便利性及安全性上產生雙刃劍的效果。此外，物聯網（Internet of Thing; IoT）的應用及需求層面日漸擴大，如環境中的溫溼度、智慧建築的各項裝置參數或病患的各項身體指數，皆可藉由低成本及大量配置的感測器來取得。可預期在不久的將來，物聯網將深入各個層面，成為生產或生活中不可或缺的工具，而行動裝置亦因持有率及便利性將成為物聯網身份認證（authentication）及存取資訊的重要工具，故行動裝置遠端認證及安全的存取物聯網中感測器資訊的安全機制成為重要的研究課題。

因個別的 IoT 感測器限於成本及電力無法提供長時間及長距離連結網路的驗證，通常由多個感測器組成無線感測器網路（wireless sensor network; WSN），並於每個 WSN 中配置具有較高運算能力的閘道器（Gateway）進行遠端使用者認證，讓使用者可於遠端利用通過感測器所在 WSN 的閘道器驗證，存取所需的感測器資訊。在多位學者提出的研究成果中，我們發現 2018 年 Wu 等（2018）提出的機制具有相當的實用價值，該機制適用於多閘道器（multi-gateway）所組成的無線感測網路（wireless sensor network; WSN），並可避免感測器取得攻擊（sensor capture attack）、使用者偽裝攻擊（user forgery attack）、閘道器偽裝攻擊（gateway forgery attack）、感測器偽裝攻擊（sensor forgery attack）及離線猜密碼攻擊（off-line guessing attack），並提供每次存取時所需的相互認證（mutual authentication）及會期金鑰（session key）的需求。但經由安全性分析，我們發現該機制具仍有部份的安全性缺失，如無法避免感測器取得攻擊、使用者偽裝攻擊及離線猜密碼攻擊，且無法確保相互認證及使用者的匿名性（anonymous）所需的安全性，因此本研究除說明 Wu 等人機制的弱點外，亦提出具有匿名性及避免感測器取得攻擊的改善機制，以符合安全需求，並利用程式化安全檢查工具 Proverif 2.00（Blanchet et al. 2018）形式化安全性分析（formal security analysis）及敘述性的非形式化（non-formal）安全性分析證明新機制的安全性，並與近期提出的相關機制進行安全性及效能分析比較，證明所提機制具有的安全性且適用於真實環境中。本文其餘各章節架構如下，第貳節說明本研究的研究背景，第參節簡介 Wu 等人的機制，第肆節提出 Wu 等人機制的安全漏洞，第伍節為本研究提出的新機制，第陸節為新機制的安全性分析，最後一節為本研究之結論及未來研究方向。

貳、文獻深討

一、遠端使用者認證（remote user authentication）

在遠端使用者認證研究方面，Lamport（1981）於 1981 年提出第一個使用者遠端認證機制，但需於伺服器儲存密碼列表，且在未加密通道中無法抵擋使用者仿冒攻擊的弱點。後續許多研究者如 Chang 與 Wu（1991）、Wu（1995）、Wang 與 Chang（1996）、Wu 與 Sung（1996）、Tan 與 Zhu（1999）及 Yang 與 Shieh（1999）皆提出各自的使用者遠端認證機制，以提昇效能及安全性。

二、智慧卡遠端使用者認證（remote user authentication of smart card）

如在使用智慧卡認證研究上，於 2002 年，Chien 等（2002）提出一個不需於伺服器儲存驗證表，提供使用者更新密碼，並具有低通訊及計算成本的智慧卡雙向使用者遠端認證機制。但 Hsu（2004）指出 Chien 等人的機制無法抵擋同步會談攻擊（parallel session attack）。2004 年，Juang（2004）提出一個增強 Chien 等人的新機制，保留舊機制的優勢，並利用無時間戳記方式避免舊機制的問題，並提供使用者與伺服器會期金鑰交換機制、無伺服器儲存驗證表及更改密碼功能；在 2006 年 Shieh 與 Wang（2006）指出 Juang 的機制因無時間戳記無法檢核傳輸訊息的完整性，將導致重送攻擊（replay attacks），並提出具更好效能及安全性的改良機制。在 2007 年，Vijayalakshmi 與 Raja（2012）指出 Shieh 與 Wang 的機制無法提供完美前向私密性（perfect forward secrecy）且會遭受內部攻擊，同樣在 2007 年，Wang 等（2007）指出 Yoon 等人的機制具有離線猜密碼、使用者仿冒、阻絕服務及無法檢測錯誤密碼登入問題，並提出改良機制。

三、多伺服器遠端使用者認證

在多伺服器（multi-server）分散式的認證研究中，於 2008 年，Tsai（2008）提出基於智慧卡且無需於伺服器及認證中心儲存驗證資訊的多伺服器認證機制，在 2009 年，Liao 與 Wang（2009）提出一個動態使用者帳號的遠端認證機制，其僅利用雜湊函數（hash function）即可在多伺服器環境下達成使用者匿名性。但 Lee 等（2010）指出 Liao 及 Wang 無法抵擋假冒伺服器及使用者的攻擊並提出增強的機制

四、基於生物特徵的遠端使用者認證

於 2010 年，Li 與 Hwang（2010）提出一個基於生物特徵（bio-informatics）且不用時間戳記並可抵擋重送攻擊的驗證機制，但 Li 等（2011）指出 Li 及 Hwang 的機制在攻擊者控制公開通道時，在不用知悉任何使用者及伺服器秘密下，可進行仿冒兩者的中間攻擊（man-in-the-middle attacks）。

五、基於動態帳號的遠端使用者認證

在動態變換使用者帳號以維持使用者匿名性的研究上，於 2011 年，Sood 等（2011）提出一個多伺服器架構下的動態使用者帳號的遠端驗證機制，Li 等（2012）顯示 Sood 等人的機制無法成功驗證使用者，會造成假冒攻擊及智慧卡遺失攻擊，同樣出改善機制。同於 2011 年 Cheng 等（2011）指出 Wang 等（2007）的機制具使用者仿冒及同步會期的攻擊，並提出新的機制，但後續的研究中發現 Chen 等人機制無法抵抗離線猜密碼等攻擊，如 Kumari 等（2013）及 Wang 與 Ma（2012）等人的研究均提出 Chen 等人機制的問題。於 2012 年，Tsaur 等（2012）指出之前許多機制均使用隨機值來抵抗重送攻擊但反而受到中間人攻擊，且經常使用時間戳記造成時間同步的成本，所以提出一個自我驗證的時間戳記技術，避免在多伺服器環境下可能產生的時間同步問題。在 2013 年，Tsai 等（2013）提出一個不需在資料庫記錄的使用者匿名驗證機制。在 2014 年，Leu 與 Hsieh（2014）指出 Lee 等（2011）的機制無法抵抗猜密碼、使用者及伺服器仿冒等攻擊，認為合法的使用可成為超級攻擊者，因其擁有一般攻擊者所沒有的系統資訊，並提出增強的機制。

六、三因子（three-factor）及動態帳號遠端使用者認證

在結合使用者密碼、生物特徵及智慧卡的三因子驗證上，於 2014 年，Mishra 等（2014）指出 Chuang 與 Chen（2014）的三因子驗證架構仍無法避免智慧卡遺失造成的使用者、伺服器仿冒及阻絕服務（denial-of-service）攻擊，並提出新機制。同年 Karuppiah 與 Saravanan（2014）同樣提出一個基於智慧卡的金鑰協商遠端認證機制並具有前向私密性，但 Shieh 與 Yu（2016）發現其機制仍有許多弱點。Kumari 等（2014）提出一個基於智慧卡的會議金鑰協商的遠端認證機制，聲稱可以抵抗智慧卡失竊攻擊、偽裝攻擊，且具有前向私密性、匿名性等。同年 Shi 等（2015）認為 Kumari 等人的機制仍然會受到智慧卡失竊攻擊、偽冒攻擊，並提出一套改善機制，且證明該機制能抵抗如離線猜密碼攻擊及偽裝攻擊等。同樣 Chaudhry 等（2015）指出 Kumari 等人的機制存在弱點，並提出新的機制。在

2015 年，Farash 等（2017）表示 Wen 等（2013）及 Shin 等（2015）漫遊服務認證機制具有相同的問題，Shin 等人的機制中使用者登入訊息會被追蹤及使用者與伺服器偽裝攻擊，Wen 等人機制因密碼驗證表洩露，導致使用者通訊秘密可被算出，Farash 等人亦提出改善機制，以防止前者發生的安全漏洞及攻擊，並證明該機制可以讓使用者在使用漫遊服務時能夠以匿名方式與伺服器作驗證。在 2016 年，Islam 等（2016）指出 Lin（2014）的機制無法驗證使用者密碼的正確性，輸入使用者帳號及錯誤密碼後，即可偽裝使用者登入伺服器，並提出改善的機制。

七、無線感測器網路（WSN）遠端使用者認證

在 IoT 安全性及遠端使用者認證上，過去已經有學者提出許多機制希望能達到安全認證，如 Dhillon 與 Kalra（2017）提出基於密碼、智慧卡和生物特徵的三因子遠端使用者認證機制，利用雜湊函式和互斥或（XOR）運算降低運算成本。另外，Amin 等（2016）也提出了基於 WSN 的三因子認證協議，改善了 Farash 等（2016）的機制，但是，Jiang 等（2017）發現 Amin 等人的機制中有幾項弱點。為了解決這些缺失，Jiang 等人提出了一種基於 Rabin 密碼系統的遠端使用者認證機制。Yang 等人（2017）提出 IoT 裝置因成本考量，較易受到外界取得其中的資訊，且當使用者需透過無線感測網路存取 IoT 裝置時，仍需考量使用者、IoT 感測器及 WSN 網路閘道器間的認證問題，因此如何設計一個具有安全性及實用價值的無線感測網路遠端認證機制，具有研究的價值。

參、Wu 等人使用者遠端 IoT 無線感測網路認證機制

Wu 等（2018）提出一個適用於多閘道器的使用者遠端 IoT 無線感測網路的認證機制，可適用於僅具輕量（較低運算能力）的個人健康 IoT 系統。該機制由註冊、登入認證及更改使用者密碼三個階段組成，其中在註冊階段皆在現有具安全性的私密通道進行，以確保安全性，而其餘階段則於以下分別簡單介紹個階段流程，本研究所使用的符號如表 1。

表 1：本研究所使用符號表

代號	說明	代號	說明
U_i	使用者 i	N_l	無線感測網路區域 l
SN_k	感測器 k	DB	伺服器資料庫
U_A	攻擊者 A	$M_{1\sim4}$	公開通道傳送的訊息
ID_i	使用者 i 識別碼	$\oplus$	互斥或運算子

PW_i	使用者 i 密碼	||	串聯運算子
GW_j	閘道器 j	$h()$	單向雜湊函數（one-way hashing function）
$WMSN$	無線醫療感測器網域	ΔT	最大的傳輸延遲時間
G_j	伺服器的私密金鑰（secret key）	SK_u	使用者會期金鑰（session key）
SG_k	感測器的私密金鑰	SK_g	伺服器會期金鑰
r_0,r_u,r_s,r_{hg}	隨機亂數	SK_s	感測器會期金鑰
CID_i	使用者 i 的匿名識別碼	——▶	公開通道（public channel）
SID_k,GID_j	感測器、伺服器識別碼	----▶	私密通道（private channel）

一、註冊階段

此階段分為兩個部分，第一部份為感測器註冊，為整個機制的前置流程，將欲使用的感測器向閘道器（GW）註冊，再擺放到欲設置的位置；第二部份為使用者註冊，使用者向 GW 進行註冊，在私密通道交換帳號及密碼，GW 收到後將自己的私密金鑰與使用者的傳遞的秘密資訊加密過後，再回傳給使用者，並儲存使用者 ID 在自己的資料庫當中，此階段之訊息都在已建立具有安全性的私密通道中進行交換。

- 感測器註冊：

每個感測器節點 SN_k 都有一個識別碼 SID_k，且屬於一個無線感測網路區域如 N_l，並由特定閘道器如 GW_j 負責連接及管理。首先 GW_j 為 SN_k 產生共用密鑰 $SG_k=h(SID_k||G_j||N_l)$ 及將$<SID_k, SG_k, GID_j>$存入感測器 SN_k 中，再將 SN_k 放置到適合的位置，GW_j 儲存$<SID_k, N_l>$至資料庫 DB 中，以便識別 SN_k 是否在管理的 N_l 中。

- 使用者註冊：

使用者利用自己的行動裝置來註冊及儲存資訊，步驟如下。

Step 1： U_i 輸入 ID_i 及 PW_i，產生隨機亂數 r_0，計算 $HPW_i=h(PW_i||r_0)$，透過私密管道傳送$< ID_i, HPW_i >$給 GW_j。

Step 2： GW_j 檢查 ID_i 是否存在資料庫，若存在則拒絕服務，因機制僅允許使用不同 ID 進行註冊，若通過 GW_j 儲存 ID_i 至 DB 及產生匿名識別碼 CID_i，計算 $A_1=h(CID_i||GID_j||G_j)\oplus HPW_i$，$A_2=h(ID_i||G_j)\ \oplus h(ID_i||HPW_i)$，透過私密通道傳送$<A_1, A_2, CID_i, GID_j>$給 U_i。

Step 3： U_i 計算 $A_3=h(ID_i||PW_i)\oplus r_0$ 再儲存$<A_1, A_2, A_3, CID_i, GID_j>$在自己裝置中。

二、認證階段

此階段閘道器會先檢查使用者與感測器的身分，並相互交換各自產生的隨機亂數，建立單次通訊的會期金鑰 SK。

Step 1：首先 U_i 輸入 ID_i 及 PW_i，行動裝置計算 $r_0=A_3\oplus h(ID_i||PW_i)$，$HPW_i=h(PW_i||r_0)$，選擇隨機亂數 r_u 及想存取的感測器編號 SID_k，計算 $B_1=A_1\oplus HPW_i=\ h(CID_i||GID_j||G_j)$，$B_2=B_1\oplus r_u$，$B_3=ID_i\oplus h(r_u||B_1)$，$B_4=h(CID_i||GID_j||SID_k||B_1||ID_i||r_u)$，最後透過公開通道傳送 $M_1=\{CID_i, GID_j, SID_k, B_2, B_3, B_4\}$給 GW_j。

Step 2：GW_j 收到 M_1 後，首先檢查 GID_j 是否正確，如為自己的識別碼，就於 DB 中搜尋<SID_k, N_l>即 SID_k, 是否曾於 N_l 註冊，若兩項都通過顯示收到的訊息確實為傳給此 WSN 進行認證，則 GW_j 計算 $B_1=h(CID_i||GID_j||G_j)$，$r_u=B_1\oplus B_2$，$ID_i=B_3\oplus h(r_u||B_1)$，檢查 ID_i 是否存在 DB，再檢查所收到的 B_4 是否與計算所得的值相同，即 B_4 是否等於 $h(CID_i||GID_j||SID_k||B_1||ID_i||r_u)$，如果兩個驗證中的任何一個沒通過，中斷此次登入，如在短時間內相同使用者帳戶 ID_i 嘗試三次沒有通過，則使用者將被封鎖，因使用者帳戶除閘道器 DB 外，並不儲存於任何裝置，且於傳輸過程中亦以隨機亂數 r_u 保護，攻擊者無法獲得來進行拒絕服務（Deny of Service, DoS)的攻擊。若通過檢查，GW_j 選擇隨機亂數 r_g，計算 $SG_k=h(SID_k||G_j||N_l)$，$B_5=h(SG_k||GID_j)\oplus r_u$，$B_6=h(r_u)\oplus r_g$，$B_7=h(SG_k||r_u||r_g)$，透過公開通道傳送 $M_2=\{SID_k, B_5, B_6, B_7\}$給 SN_k。

Step 3：SN_k 收到 M_2 後，首先檢查 SID_k 是否正確，若正確則計算 $r_u=B_5\oplus h(SG_k||GID_j)$，$r_g=B_6\oplus h(r_u)$，驗證 B_7 及 $h(SG_k||r_u||r_g)$兩者是否相同，若失敗中止登入，若通過則產生 r_s，計算 $SK_s=h(r_u||r_g||r_s)$，$B_8=h(SG_k||r_g)\oplus r_s$，$B_9=h(SK_s||SID_k||GID_j||r_s)$，並透過公開通道傳送 $M_3=\{B_8, B_9\}$給 GW_j。

Step 4：GW_j 收到 M_3 後，計算 $r_s=B_8\oplus h(SG_k||r_g)$，$SK_g=h(r_u||r_g||r_s)$，檢查 B_9 及 $h(SK_g||SID_k||GID_j||r_s)$兩者是否相同，如失敗則中止，如通過則產生新的匿名識別碼 CID_i^{new}，計算 $B_{10}=h(CID_i^{new}||GID_j||G_j)\oplus h(r_u||CID_i)$，$B_{11}=h(r_u||ID_i)\oplus r_g$，$B_{12}=h(r_u||r_g)\oplus r_s$，$B_{13}=h(h(ID_i||G_j)||r_s)\oplus CID_i^{new}$，$B_{14}=h(SK_g||ID_i||B_{10}||CID_i^{new})$，透過公開通道傳送 $M_4=\{B_{10}, B_{11}, B_{12}, B_{13}, B_{14}\}$給 U_i。

Step 5：當行動裝置收到 M_4，計算 $r_g=B_{11}\oplus h(r_u||ID_i)$，$r_s=B_{12}\oplus h(r_u||r_g)$，$SK_u=h(r_u||r_g||r_s)$，$CID_i^{new}=B_{13}\oplus h(A_2\oplus h(ID_i||HPW_i)||r_s)$，檢查 B_{14} 及 $h(SK_u||ID_i||B_{10}||CID_i^{new})$是否相同，若失敗停止，若通過則手機裝置計算

$A_1^{new}=B_{10}\oplus h(r_u||CID_i)\oplus HPW_i$，並更換$(A_1, CID_i)$為$(A_1^{new}, CID_i^{new})$。

當認證階段結束，U_i、SN_k及GW_j分別取得$SK_u= SK_k= SK_g=h(r_u||r_g||r_s)$建立單次通訊的會期金鑰$SK$

三、更改使用者密碼階段

如果使用者U_i想要更改密碼，必須先聯繫相對應GW_j的並完成認證。

Step 1：U_i選擇所需要的N_j，接著輸入ID_i及PW_i，行動裝置計算$r_0=A_3\oplus h(ID_i||PW_i)$，$HPW_i=h(PW_i||r_0)$，產生隨機亂數$r_u$，計算$B_1=A_1\oplus HPW_i=h(CID_i||GID_j||G_j)$，$B_2=B_1\oplus r_u$，$B_3=ID_i\oplus h(r_u||B_1)$，$B_{15}=h(CID_i||GID_j||B_1||ID_i||r_u)$，最後傳送$M_5=\{CID_i, GID_j, B_2, B_3, B_{15}\}$給$GW_j$作為要求更換密碼的請求。

Step 2：GW_j收到M_5後計算$B_1=h(CID_i||GID_j||G_j)$及$ID_i=B_3\oplus h(r_u||B_1)$並搜尋$ID_i$是否存在資料庫，如果存在$GW_j$計算$r_u=B_2\oplus B_1$，檢查$B_{15}$及$h(CID_i||GID_j||B_1||\ ID_i\ ||r_u)$是否相同，通過驗證後$GW_j$替$U_i$選擇一個新的匿名身分碼$CID_i^{new}$，計算$B_{16}= h(CID_i^{new}||GID_j||G_j)\oplus h(r_u||CID_i)$，$B_{17}=h(h(ID_i\ ||G_j)||r_u)\oplus\ CID_i^{new}$，$B_{18}=h(ID_i\ ||CID_i||\ CID_i^{new}||B_1||B_{16})$，最後傳送$M_6=\{B_{16}, B_{17}, B_{18}\}$給$U_i$作為更改密碼許可。

Step 3：U_i收到M_6後，計算$CID_i^{new}=B_{17}\oplus h((A_2\oplus h(ID_i||HPW_i))||r_u)$，檢查$B_{18}?= h(ID_i||CID_i||CID_i^{new}||B_1||B_{16})$，如果通過驗證後$U_i$輸入新的$PW_i^{new}$，接著行動裝置產生新的隨機亂數$r_0^{new}$，計算$HPW_i^{new}=h(PW_i^{new}||r_0^{new})$，$A_1^{new2} =B_{16}\oplus\ h(r_u||CID_i)\oplus HPW_i^{new}$，$A_2^{new}=A_2\oplus h(ID_i||HPW_i)\oplus h(ID_i||HPW_i^{new})$，$A_3^{new}= h(ID_i||\ PW_i^{new})\oplus r_0^{new}$，最後行動裝置更換$(A_1, A_2, A_3, CID_i)$為$(A_1^{new2}, A_2^{new}, A_3^{new}, CID_i^{new})$。

肆、Wu 等人使用者遠端 IoT 無線感測網路認證機制的安全漏洞

本研究在下列三項假設下進行 Wu 等人機制的安全漏洞分析，首先為允許攻擊者取得手機、智慧卡或感測器等裝置中的資訊（Yang et al. 2017），即攻擊者可利用各項電磁記錄或軟硬體破解方式，取得裝置上的資訊。第二項為資訊傳送通道的限制，資訊傳送通道可分為公開通道及秘密通道，由公開通道傳送的資訊是允許被攻擊者截取、竄改及控制的，相反的由秘密通道傳送的資訊是安全的（Messerges et al. 2002）。第三項為猜帳號及密碼的限制，本研究假設離線猜帳號及密碼並沒有時間上的限制，但假設帳號及密碼強度必須為弱帳號或弱密碼方能進行猜測，使用者設定的弱帳號或弱密碼通常為常見的單詞，數字排列或是用戶

相關的個人資訊，較容易被猜出，已有許多研究指出，雖可在多項式時間複雜度下同時猜出帳號及密碼，但需為弱帳號及弱密碼，且私密金鑰、赫序函數值及隨機亂數仍無法在多項式時間複雜度下猜出（Kumari et al. 2015）。在上述三項假設下，本研究探討 Wu 等人機制所具有資訊安全上的弱點如下列各節所述。

一、感測器取得攻擊

Wu 等人的機制允許感測器的資訊可以被 U_A 取得的攻擊，但假定 U_A 無法確認 U_i 所通訊的感測器。但本研究發現，假設 U_A 取得 SN_k 中的$<SID_k, SG_k, GID_j>$，並截取 M_2 的$<SID_k, B_5, B_6, B_7>$，計算 $r_u=B_5\oplus h(SG_k||GID_j)$，$r_g=B_6\oplus h(r_u)$，再取得 M_3 的$<B_8, B_9>$，算出 $r_s=B_8\oplus h(SG_k||r_g)$，$SK_s=h(r_u||r_g||r_s)$，可以取得此次的會期金鑰，$U_A$ 可以透過這些訊息接著計算出 $B_1=B_2\oplus r_u$，$ID_i=B_3\oplus h(r_u||B_1)$，$B_1^{new}=B_{10}\oplus h(r_u||CID_i)$來進行其他的攻擊，其中 B_1^{new} 可使用在下一次使用者登入時進行追蹤等攻擊，因為 B_1 每次登入後都會更換。此攻擊主要造成會期金鑰的洩漏，以及$<B_1, ID_i, B_1^{new}>$重要的資訊被計算出來，並導致其他攻擊。

二、使用者偽裝攻擊

根據上述感測器取得攻擊後，U_A 擁有$<B_1^{new}, B_1^{old}, ID_i, CID_i^{old}, SID_k, SG_k, GID_j>$的資訊，其中 B_1^{new} 與使用者擁有的 B_1 相同，而 B_1^{old} 及 CID_i^{old} 為上一回登入時使用，本研究發現傳送給 GW_j 認證的登入訊息不會去驗證 CID_i 是否為更改，僅驗證收到的 B_1 中 CID_i 是否與訊息中的 CID_i 相符，以及驗證 ID_i 這兩個項目，因此即使 U_A 使用舊的資訊去登入，只要$<B_1, CID_i, ID_i>$正確，就能偽裝使用者成功登入，步驟如下。

Step 1： U_A 計算 $B_{2A}=B_1\oplus r_{uA}$，$B_{3A}=ID_i\oplus h(r_{uA}\oplus||B_1)$，$B_{4A}=h(CID_i||GID_j||SID_k||B_1||ID_i||r_{uA})$，將 $M_{1A}=\{CID_i, GID_j, SID_k, B_{2A}, B_{3A}, B_{4A}\}$ 傳送給 GW_j。其中 r_{uA} 為攻擊者所產生隨機亂數

Step 2： GW_j 從 SN_k 傳來的 $M_3=\{B_8, B_9\}$算出 r_s 及驗證 B_9 完並與產生會期金鑰後，並傳回 M_4 給 U_A。

Step 3： U_A 計算 $r_g=B_{11}\oplus h(r_{uA}||ID_i)$，$r_s=B_{12}\oplus h(r_{uA}||r_g)$，$SK_u=h(r_{uA}||r_g||r_s)$，成功完成使用者偽裝攻擊，並獲得此次的會期金鑰。

三、離線猜密碼攻擊

此攻擊在兩種不同假設條件下進行，第一為取得使用者行動裝置中的資訊後，並繼續使用此裝置的攻擊。第二為在感測器取得攻擊後，取得使用者$<ID_i,$

B_1^{new}>資訊再取得使用者行動裝置中的資訊後執行攻擊，兩種攻擊的差別在於前者需要同時猜帳號及密碼，故需同時為弱帳號及弱密碼才能成功，後者則在已知帳號且不需監聽使用者下次登入的訊息，只需離線猜測密碼。以下分別為兩種猜密碼攻擊的詳細流程。

第一項條件下，假設攻擊者 A 取得使用者行動裝置中的資訊<A_1, A_2, A_3, CID_i, GID_j>並監聽此裝置下次的登入訊息 M_1 ={CID_i, GID_j, SID_k, B_2, B_3, B_4}，根據手機裝置中的<CID_i, GID_j >進行比對，若符合猜一組<ID_i^*, PW_i^*>，計算 $r_0^*=A_3\oplus h(ID_i^*||PW_i^*)$ ， $HPW_i^*=h(PW_i^*||r_0^*)$ ， $B_1^*=A_1\oplus HPW_i^*$ ， $r_u^*=B_1^*\oplus B_2$ ，最後驗證 $B_3?=ID_i^*\oplus h(r_u^*||B_1^*)$是否為相符，若相符表示成功猜出使用者密碼，否則重複以上動作直到相符為止。

第二種假設在完成感測器取得攻擊後，已取得<B_1, ID_i, B_1^{new}>，再取得使用者行動裝置中<A_1, A_2, A_3, CID_i, GID_j >，猜一個密碼 PW_i^*，計算 $HPW_i=B_1^{new}\oplus A_1$，$r_0^*=A_3\oplus h(ID_i||PW_i^*)$，最後驗證 $HPW_i?=h(PW_i^*||r_0^*)$是否為相符，若相符表示成功猜出使用者密碼，否則重複以上動作直到相符為止。

四、不具相互認證功能

Wu 等人認為 GW_j 藉由檢查 ID_i 及 B_4 驗證 U_i，然後檢查 B_9 驗證 SN_k，接著 SN_k 檢查 SID_k 及 B_7 直接驗證 GW_j，間接驗證 U_i，但本研究發現根據上述使用者偽裝攻擊，U_A 可利用一組正確的<B_1, CID_i, ID_i>便能成功登入，故 GW_j 無法有效驗證 U_i 是否為正確使用者的登入，故 Wu 等人的機制無法達到相互認證的要求。

五、不具使用者匿名性

假設攻擊者取得使用者裝置的<A_1, A_2, A_3, CID_i, GID_j>，將公開通道中的 M_1~M_4 的訊息記錄下來，根據 M_1 中的 CID_i 確認為 U_i 的登入訊息，再利用 M_1 中的 SID_k 取得特定感測器 SN_k 資訊<SID_k, SG_k, GID_j>，依據 M_2 中 B_5 及 B_6 計算 $r_u=B_5\oplus h(SG_k||GID_j)$，$r_{hg}=B_6\oplus h(r_u)$，依據 M_3 中 B_8 計算 $r_s=B_8\oplus h(SG_k||r_g)$，依據 M_1 中 B_2 計算 $B_1=B_2\oplus r_u$，$ID_i=B_3\oplus h(r_u||B_1)$，$B_1^{new}=B_{10}\oplus h(r_u||CID_i)$，接著計算 $HPW_i=A_1\oplus B_1$，最後得到 $CID_i^{new}= B_{13}\oplus h(A_2\oplus h(ID_i||HPW_i)||r_s)$，表示攻擊者可以計算出使用者 U_i 每次更換的匿名辨識碼 CID_i^{new}，故 Wu 等人的機制不具使用者匿名性。

伍、新的無線感測網路遠端認證機制

本研究基於 Wu 等人機制提出一個新的無線感測網路遠端認證機制，提供防止使用者偽裝攻擊及完整相互認證的功能。因 Wu 等人機制的弱點主因為 B_1,

CID_i 的可洩漏導致，假設我們不能防範 SN_k 的資料<SID_k, SG_k, GID_j>被取得，將使 U_A 可透過上述章節的攻擊獲得三個用來組合成會期金鑰的隨機亂數<r_u, r_g, r_s>，再計算出<B_1, ID_i, B_1^{new}>，因 B_1 及 ID_i 為 U_i 與 GW_j 的共同秘密，必須避免 B_1 及 ID_i 的洩漏，可利用修改 Wu 等人機制中會期金鑰的組成方法，將使用者與 GW 的隨機亂數予以加密，再傳送給 S_j，除節省感測器計算成本，並避免感測器取得攻擊因為 r_u 的洩漏導致<B_1, ID_i, B_1^{new}>被計算出來。本研究所提新機制同樣具有註冊階段、認證階段及密碼變更等三個階段，其詳細流程介紹如下，新機制所使用的符號與 Wu 等人的機制相同，如表 1。

一、註冊階段

此階段同樣分為兩個部分，第一部份為感測器註冊，與 Wu 等人機制步驟相同，為整個機制的前置流程，將欲使用的感測器擺放到欲設置的位置，再進行與 GW 交換秘密金鑰並寫入感測器，流程如圖 1；第二部份為使用者註冊，使用者向 GW 進行註冊，在私密通道交換帳號及密碼，GW 收到後將自己的秘密金鑰與使用者的秘密加密過後，再回傳給使用者，並儲存使用者 ID_i 再自己的資料庫當中，此階段之訊息都在私密通道中進行交換，其中新機制為在行動裝置驗證使用者身份，增加一個計算步驟，將可避免使用者輸入錯誤時，造成公開通道的通訊成本及 GW 的檢查成本，並可防止攻擊者利用使用者端的漏洞進行阻絕服務攻擊，流程如圖 2。詳細步驟說明如下。

- 感測器註冊：

每個感測器節點 SN_k 都有一個識別碼 SID_k，且屬於一個無線感測網路區域如 N_l，並由特定閘道器如 GW_j 負責連接及管理。首先 GW_j 為 SN_k 產生共用密鑰 $SG_k=h(SID_k||G_j||N_l)$及將<SID_k, SG_k, GID_j>存入感測器 SN_k 中，再將 SN_k 放置到適合的位置，GW_j 儲存<SID_k, N_l>至資料庫 DB 中，以便識別 SN_k 是否在管理的 N_l 中。

圖 1：新機制的感測器註冊階段

- 使用者註冊：

使用者利用自己的行動裝置來註冊及儲存資訊，步驟如下。

Step 1： U_i 輸入 ID_i 及 PW_i，產生隨機亂數 r_0，計算 $HPW_i=h(PW_i||r_0)$，透過私密管道傳送$<ID_i, HPW_i>$給 GW_j。

Step 2： GW_j 檢查 ID_i 是否存在資料庫，若存在則拒絕服務，若通過 GW_j 儲存 ID_i 至 DB 及產生匿名識別碼 CID_i，計算 $A_1=h(CID_i||GID_j||G_j)\oplus HPW_i$，$A_2=h(ID_i||G_j)\ \oplus h(ID_i||HPW_i)$，透過私密通道傳送$<A_1, A_2, CID_i, GID_j>$給 U_i。

Step 3： U_i 計算 $A_3=h(ID_i||PW_i)\oplus r_0$ 及 $A_4=h(ID_i||PW_i||r_0)$再儲存$<A_1, A_2, A_3, A_4, CID_i, GID_j>$在自己裝置中。

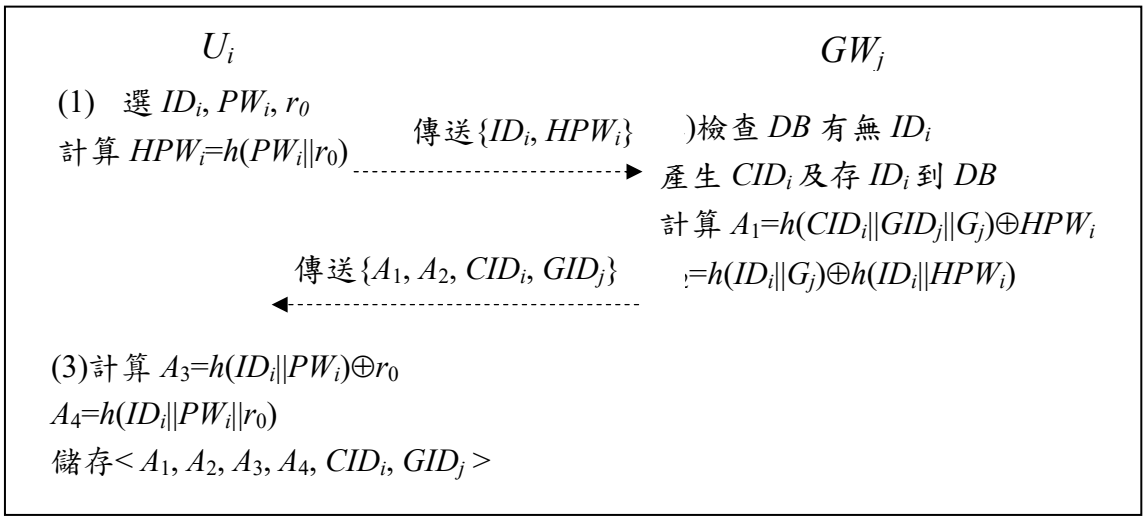

圖 2：新機制的使用者註冊階段

二、認證階段

此階段在接收到使用者的認證要求時，GW 會分別檢查使用者與感測器的身分，並相互交換所產生的隨機亂數，以建立此次通訊所使用的會期金鑰 SK 並更新使用者的匿名識別碼，其詳細步驟說明如下，流程圖如圖 3 至圖 5。

Step 1： 首先 U_i 選擇想存取的感測器 SN_k，輸入 ID_i 及 PW_i 至行動裝置後計算 $r_0=A_3\ \oplus h(ID_i||PW_i)$，檢查 A_4 及 $h(ID_i||PW_i||r_0)$是否相等，如不相等裝置停止登入，如通過驗證，裝置計算 $HPW_i=h(PW_i||r_0)$，選擇隨機亂數 r_u 及 SN_k 的感測器編號 SID_k，計算 $B_1=A_1\oplus HPW_i=h(CID_i||GID_j||G_j)$，$B_2=B_1\oplus r_u$，$B_3=\ ID_i\oplus h(r_u||B_1)$，$B_4=h(CID_i||GID_j||SID_k||B_1||ID_i||r_u)$，最後透過公開通道傳送 $M_1=\{CID_i, GID_j, SID_k, B_2, B_3, B_4\}$給 GW_j。

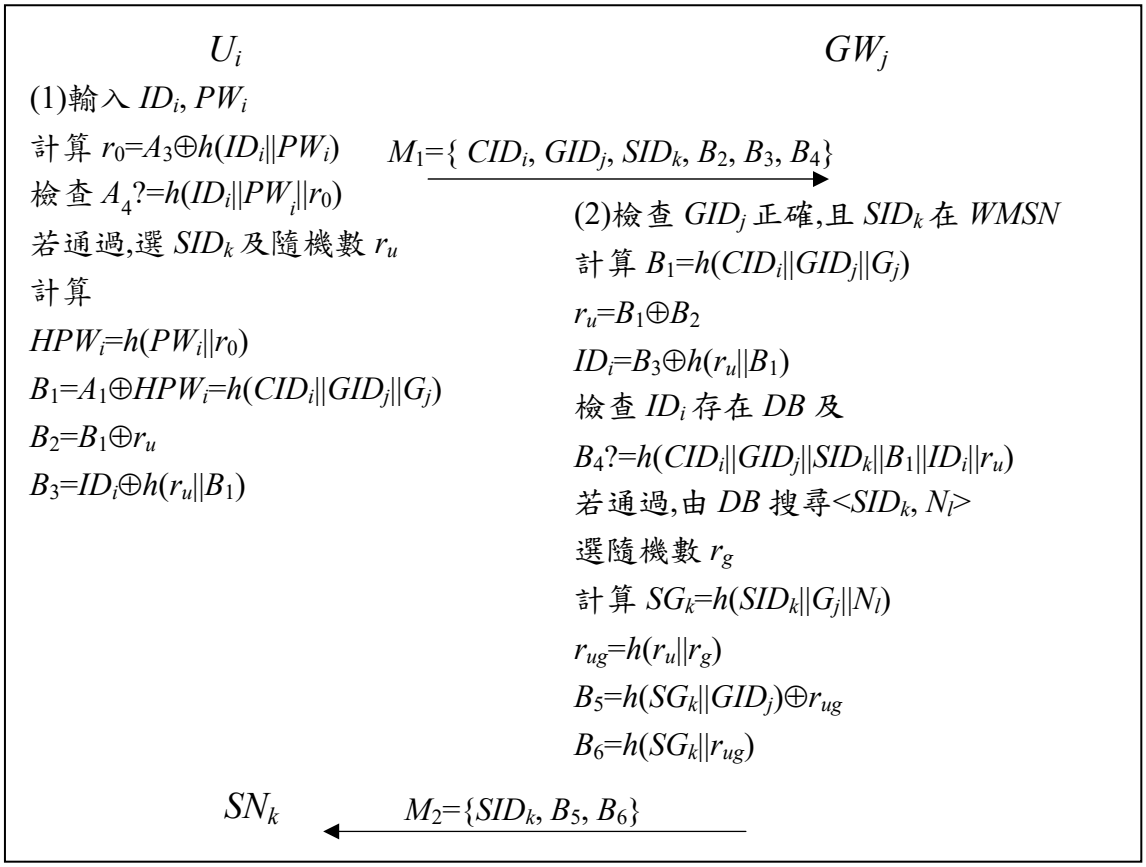

圖 3：新機制之認證階段-使用者登入階段

Step 2： GW_j 收到 M_1 後，首先檢查 GID_j 是否正確及 SID_k 是否存在所屬的 N_l，若屬實，GW_j 計算 $B_1=h(CID_i||GID_j||G_j)$，$r_u=B_1\oplus B_2$，$ID_i=B_3\oplus h(r_u||B_1)$，再檢查 ID_i 是否存在 DB，並檢查接收的 B_4 是否與計算的 $h(CID_i||GID_j||SID_k||B_1||ID_i||r_u)$相相等，如驗證中的任何一個未通過則停止登入，另如在短時間內嘗試三次沒有通過，使用者帳戶 ID_i 將被封鎖。若通過則 GW_j 選擇隨機亂數 r_g，計算 $SG_k=h(SID_k||G_j||N_l)$，$r_{ug}=h(r_u||r_g)$，$B_5=h(SG_k||GID_j)\oplus r_{ug}$，$B_6=h(SG_k||r_{ug})$，透過公開通道傳送 $M_2=\{SID_k, B_5, B_6\}$給 SN_k。

Step 3： SN_k 收到 M_2 後，首先 SN_k 檢查 SID_k 是否正確，若正確則計算 $r_{ug}=B_5\oplus h(SG_k||GID_j)$，檢查收到的 B_6 是否與計算 $h(SG_k||r_{ug})$的值相等，如不相等，SN_k 中止認證，若通過產生 r_s，計算 $SK_s=h(r_{ug}||r_s)$，$B_7=h(SG_k||r_{ug})\oplus r_s$，$B_8=h(SK_s||SID_k||GID_j||r_s)$，透過公開通道傳送 $M_3=\{B_7, B_8\}$給 GW_j。

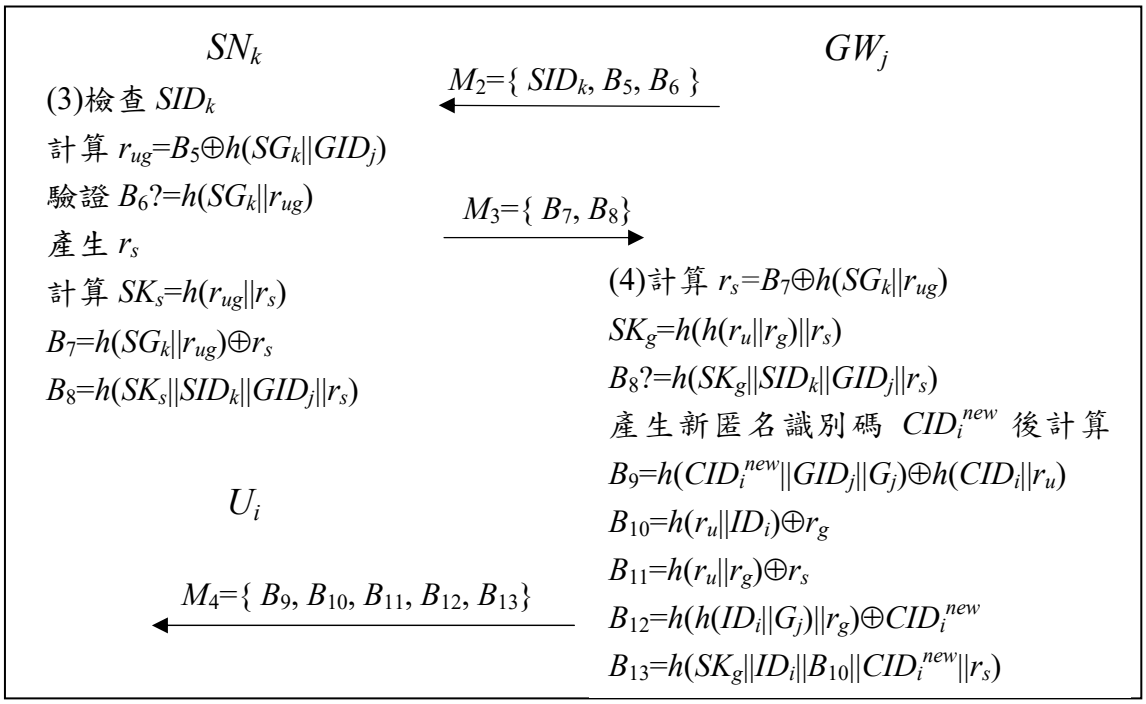

圖 4：新機制之認證階段-感測器及閘道器驗證階段

Step 4： GW_j 收到 M_3 後，計算 $r_s=B_7\oplus h(SG_k||r_{ug})$，再計算會期金鑰 $SK_g=h(h(r_u||r_g)||r_s)$，驗證 B_8 與 $h(SK_g||SID_k||GID_j||r_s)$是否相等，如不相等則終止認證，如通過則 GW_j 產生新的匿名識別碼 CID_i^{new}，計算 $B_9=h(CID_i^{new}||GID_j||G_j)\oplus h(CID_i||r_u)$，$B_{10}=h(r_u||ID_i)\oplus r_g$，$B_{11}=h(r_u||r_g)\oplus r_s$，$B_{12}=h(h(ID_i||G_j)||r_g)\oplus CID_i^{new}$，$B_{13}=h(SK_g||ID_i||\ B_{10}||CID_i^{new}||r_s)$，透過公開通道傳送 $M_4=\{B_9, B_{10}, B_{11}, B_{12}, B_{13}\}$給 U_i。

Step 5： 當 U_i 行動裝置收到 M_4 後，計算 $r_g=B_{10}\oplus h(r_u||ID_i)$，$r_s=B_{11}\oplus h(r_u||r_g)$，$SK_u=h(h(r_u||r_g)||r_s)$，$CID_i^{new}=B_{12}\oplus h(A_2\oplus h(ID_i||HPW_i)||r_s)$，檢查接收的 B_{13} 是否與計算的 $h(SK_g||ID_i||\ B_{10}||CID_i^{new}||r_s)$相等，如不相等終止驗證，若通過則手機裝置計算 $A_1^{\text{new}}=B_9\oplus h(CID_i||r_u)\oplus HPW_i$，並更換$(A_1, CID_i)$為$(A_1^{new}, CID_i^{new})$，並於下次登入時使用。

當認證階段結束，U_i、SN_k 及 GW_j 分別取得 $SK_u= SK_k= SK_g=h(r_u||r_g||r_s)$ 建立單次通訊的會期金鑰 SK

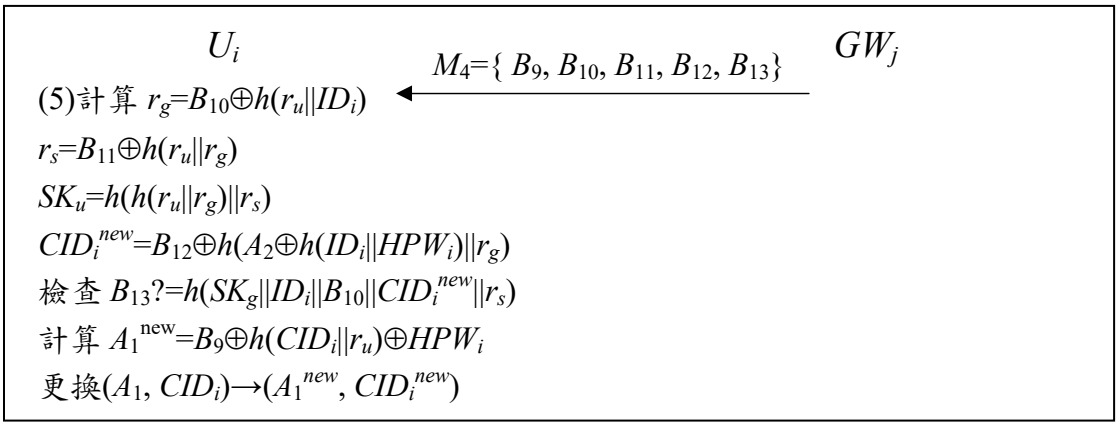

圖 5：新機制之認證階段-使用者驗證階段

三、使用者密碼變更階段

如果 U_i 想要更改密碼，此階段 Wu 等人機制設計為須先聯繫相對應 GW_j 完成認證，並更換匿名識別碼，使用者方能變更個人密碼，雖增加安全性，但表示使用者需能連繫到 GW_j 方能更改密碼。本研究的密碼變更階段，因具有在使用者裝置端的認證機制，僅需由使用者行動裝置完成，即使在離線或連繫不到 GW_j 區域時仍可完成，將可同時具有方便使用者時常變更密碼、節省通訊成本及安全性的優勢。詳細步驟如下說明，流程如圖 6。

Step 1： U_i 輸入 ID_i 及 PW_i，行動裝置計算 $r_0=A_3\oplus h(ID_i||PW_i)$，檢查 $A_4?=h(ID_i||PW_i||r_0)$，，如不相等裝置拒絕變更，如通過驗證，裝置計算 $HPW_i= h(PW_i||r_0)$，並提示 U_i 輸入新密碼。

Step 2： U_i 輸入新的 PW_i^{new}，行動裝置產生新的隨機亂數 r_0^{new}，計算 $HPW_i^{new}=h(PW_i^{new}||r_0^{new})$，$A_1^{new2} = A_1\oplus HPW_i\oplus HPW_i^{new}$，$A_2^{new}=A_2\oplus h(ID_i||HPW_i) \oplus h(ID_i||HPW_i^{new})$，$A_3^{new}= h(ID_i|| PW_i^{new})\oplus r_0^{new}$，$A_4^{new} =h(ID_i||PW_i^{new} ||r_0^{new})$最後行動裝置更換$(A_1, A_2, A_3, A_4)$為$(A_1^{new2}, A_2^{new}, A_3^{new}, A_4^{new})$。

U_i

輸入$<ID_i, PW_i>$

計算 $r_0=A_3 \oplus h(ID_i||PW_i)$

檢查 $A_4?=h(ID_i||PW_i||r_0)$

若通過，計算 $HPW_i=h(PW_i||r_0)$

輸入新的 PW_i^{new}

生成新隨機亂數 r_0^{new}

計算 $HPW_i^{new}=h(PW_i^{new}||r_0^{new})$

$A_1^{new2}= A_1 \oplus HPW_i \oplus HPW_i^{new}$

$A_2^{new}=A_2 \oplus h(ID_i \,||\, HPW_i) \oplus h(ID_i||HPW_i^{new})$

$A_3^{new} =h(ID_i||PW_i^{new}) \oplus r_0^{new}$

$A_4^{new} =h(ID_i||PW_i^{new}||r_0^{new})$

更換$(A_1, A_2, A_3, A_4) \rightarrow (A_1^{new2}, A_2^{new}, A_3^{new}, A_4^{new})$

圖 6：新機制的使用者密碼變更階段

陸、安全性分析

本研究為證明新機制所具有的安全性及效能，在本章第一節使用 ProVerif 工具進行形式化驗證（formal verification）安全性分析，驗證新機制在正常的執行中具有保密性及身分驗證的安全性，在第二節使用非形式化的傳統敘述式安全性分析，說明在遭受相關攻擊時，新機制如何抵抗及所具備的遠端認證安全性，最後第三節及第四節會以三個現有機制來做安全性以及效能的比較，以說明新機制所具有的實用價值。

一、形式化安全性分析

本研究使用 Proverif 2.00 軟體驗證新機制的安全性，Proverif 是一個知名的密碼學協定驗證工具，由 Bruno Blanchet 等人所開發（Blanchet et al. 2018），可由機制流程驗證機制是否具有保密性及身份驗證的安全性，保密性為驗證機制是否具有保守各項私有秘密的功能，如私有金鑰或會期金鑰等，身份驗證為檢查機制是否具有驗證真實身份的能力，即是否具有抵擋使用者仿冒的能力。Proverif 假設攻擊者可取得及控制所有公開通道中的訊息，但對加密的訊息需取得正確的密鑰方能解密。本研究編碼新機制的 Proverif 程式以測試所具的安全性，其中所使用的參數及函數代碼如圖 7，包含機制中所使用的通道、會期金鑰、私密金鑰、常

數、函數、方程式、攻擊查詢及事件等，其中[private]代表私有不可取得的資訊；通道 ch 代表傳輸所有驗證訊息的公開通道，sch0 與 sch1 為分別用在感測器註冊與使用者註冊時的私密通道；d 代表的是資料庫，h()代表的是雜湊函數，xor()代表的是互斥或運算，con()代表的是串接運算；前三個查詢（query）分別查詢攻擊者是否可取得組成會期金鑰的三個隨機數，即檢驗會期金鑰的安全性，最後一個查詢的 inj-event(UserAuth(id))==>inj-event(UserStart(id))是用來驗證兩個事件的執行順序是否正確，如果是正常執行則相同的使用者識別碼的使用者登入事件 UserStart(id)將會在驗證事件 UserAuth(id)前執行，即可防止仿冒及重送攻擊；最後 d 代表資料庫中的資料表。

參數宣告	函數宣告
(*-channels-*) free ch: channel. free sch0: channel [private]. free sch1: channel [private]. (*-session keys-*) free sku: bitstring [private]. free sks: bitstring [private]. free skg: bitstring [private]. (*-GW's secret key-*) free Gj: bitstring [private]. free SGk: bitstring[private]. (*-constants-*) free IDi: bitstring [private]. free PWi: bitstring [private]. const SIDk: bitstring. const GIDj: bitstring. const Nl: bitstring. table d(bitstring).	(*-functions-*) fun h(bitstring): bitstring. fun xor(bitstring, bitstring): bitstring. fun con(bitstring, bitstring): bitstring. (*-equations-*) equation forall m: bitstring, n:bitstring; xor(xor(m,n),n)=m. (*-queries-*) query attacker(sku). query attacker(sks). query attacker(skg). query id: bitstring; inj-event(UserAuth(id)) ==>inj-event(UserStart(id)). (*-event-*) event UserStart(bitstring). event UserAuth(bitstring).

圖 7：本機制 ProVerif 程式參數代碼屬性、函數及事件

使用者註冊部份代碼如圖 8，驗證部份代碼如圖 9，變數符號使用與新機制相同，其中以 u 為開頭的變數代表由使用者接收或計算所產生，除了 A1new 及 CIDinew，因其用於每次登入時皆會變換的動態識別碼。感測器註冊及驗證過程如圖 10，其中所有接收和計算的變數皆以 s 開頭。閘道器程式碼如圖 11 及圖 12，其中 GWReg1、GWReg2 及 GWAuth 分別表示閘道器在使用者註冊、感測器註冊及驗證的流程，所有接收和計算的變數皆以 g 開頭，最後一行指令 let GW = GWReg1|GWReg2|GWAuth 代表閘道器的定義由上述三部分組成，即表示 GW 所包含執行的過程。新機制 Proverif 程式執行結果如圖 13，各項結果皆為真，其中第一個結果顯示兩個事件 UserStart(id)和 UserAuth(id)可以按正常順序執行，其餘三個結果表明會期金鑰可以抵禦 Proverif 模擬的各種攻擊。

```
let User=
new r0:bitstring;
let HPWi=h(con(PWi,r0))in
out(sch0,(IDi, HPWi));
in(sch0,(A1:bitstring,A2:bitstring,CIDi:bitstring));
let A3=xor(h(con(IDi,PWi)),r0)in
let A4=h(con(IDi,PWi,r0))in
```

圖 8：本機制使用者註冊的 ProVerif 程式碼

```
!(
event UserStart(IDi);
new uru: bitstring;
let ur0=xor(A3,h(con(IDi,PWi))) in
if A4 = h(con(IDi,PWi,ur0)) then
let uHPWi = h(con(PWi,ur0)) in
let uB1= xor(A1,uHPWi) in
let uB2 =xor(uB1,uru) in
let uB3 = xor(IDi,h(con(uru,uB1))) in
let uB4 = h(con(con(con(con(con(CIDi,GIDj),SIDk),uB1),IDi),uru)) in
let M1=(CIDi,uB2,uB3,uB4) in
out(ch,M1);
in(ch,(uB9:bitstring,uB10:bitstring,uB11:bitstring,uB12:bitstring,uB13:bitstring));
let urg = xor(uB10,h(con(uru,IDi))) in
let urs = xor(uB11,h(con(uru,urg))) in
let sku = h(con(h(con(uru,urg)),urs)) in
let CIDinew = xor(uB12,h(con(xor(A2,h(con(IDi,uHPWi))),urg))) in
if uB13 = h(con(con(con(con(sku,IDi),uB10),CIDinew),urs)) then
let A1new = xor(xor(uB9,h(con(uru,CIDi))),uHPWi) in
let A1 = A1new in
let CIDi = CIDinew in
0
).
```

圖 9：本機制使用者認證的 ProVerif 程式碼

```
感測器註冊
let Sensor =in(sch1,SGk:bitstring);
```

```
感測器認證
!(
in(ch,(sB5:bitstring,sB6:bitstring));
new srs:bitstring;
let srug = xor(sB5,h(con(SGk,GIDj))) in
if sB6 = h(con(con(SGk,srug),srug)) then
let sks = h(con(srug,srs))in
let B7 = xor(h(con(SGk,srug)),srs) in
let B8 = h(con(con(con(sks,SIDk),GIDj),srs)) in
let M3 = (B7,B8) in
out(ch,M3);
0
).
```

圖 10：本機制感測器註冊/認證的 ProVerif 程式碼

```
閘道器處理使用者註冊
let GWReg1 =
in(sch0,(gIDi:bitstring,gHPWi:bitstring));
new gCIDi:bitstring;
let gA1 = xor(h(con(con(gCIDi,GIDj),Gj)),gHPWi) in
let gA2 = xor(h(con(gIDi,Gj)),h(con(gIDi,gHPWi))) in
insert d(gIDi);
out(sch0,(gA1,gA2,gCIDi)).
```

```
閘道器處理感測器註冊
let GWReg2 =
let gSGk = h(con(con(SIDk,Gj),Nl)) in
out(sch1,gSGk).
```

圖 11：本機制閘道器處理使用者/感測器註冊的 ProVerif 程式碼

```
let GWAuth =in (ch,(gCIDi2:bitstring,gB2:bitstring,gB3:bitstring,gB4:bitstring));
new grg:bitstring;
let gB1 = h(con(con(gCIDi2,GIDj),Gj)) in
let gru = xor(gB1,gB2) in
let gIDi2 = xor(gB3,h(con(gru,gB1))) in
get d(=gIDi2) in
if gB4 = h(con(con(con(con(gCIDi2,GIDj),SIDk),gB1),gIDi2),gru)) then
event UserAuth(gIDi2);
let gSGk = h(con(con(SIDk,Gj),Nl)) in
let gB5 = xor(h(con(gSGk,GIDj)),h(con(gru,grg))) in
let gB6 = h(con(gSGk,h(con(gru,grg)))) in
let M2 = (gB5,gB6) in
out(ch,M2);
in (ch,(gB7:bitstring,gB8:bitstring));
new gCIDinew:bitstring;
let grs = xor(gB7,h(con(gSGk,h(con(gru,grg))))) in
let skg = h(con(h(con(gru,grg)),grs)) in
if gB8 = h((con(con(skg,SIDk),GIDj),grs)) then
let gB9 = xor(h(con(con(gCIDinew,GIDj),Gj)),h(con(gru,gCIDi2))) in
let gB10 =xor(h(con(gru,gIDi2)),grg) in
let gB11 = xor (h(con(gru,grg)),grs) in
let gB12 = xor(h(con(h(con(gIDi2,Gj)),grg)),gCIDinew) in
let gB13 = h(con(con(con(con(skg,gIDi2),gB10),gCIDinew),grs)) in
let M4 = (gB9,gB10,gB11,gB12,gB13) in
out(ch,M4).

let GW =GWReg1|GWReg2|GWAuth.
```

圖 12：本機制閘道器認證的 ProVerif 程式碼

```
RESULT not attacker(sku[]) is true.
RESULT not attacker(sks[]) is true.
RESULT not attacker(skg[]) is true.
RESULT inj-event(UserAuth(id)) ==> inj-event(UserStart(id)) is true.
```

圖 13：本機制 ProVerif 程式碼執行結果 s

二、非形式化安全性分析

本節說明新機制非形式化的安全性分析，說明在遭受相關攻擊時，新機制如何抵抗及所具備的遠端認證安全性。

（一）抵抗感測器取得攻擊

在 Wu 等人的機制中，攻擊者取得某一感測器 S_j 的所有資訊後，可以算出另一感測器 S_k 的秘密金鑰。但新機制在遭受感測器取得攻擊的情況下，即使被取得感測器 S_k 的所有資訊且包含感測器的秘密金鑰$<SID_k, SG_k, GID_j>$，仍可以防止其他感測器之秘密金鑰被算出，因為 GW_j 傳送給 S_j 的訊息無法計算出$<r_u, r_g>$，防止$<B_1, ID_i, CID_i^{new}>$的洩漏，攻擊者便無法利用追蹤同一使用者以取得更多有助於攻擊的資訊，故本研究所提新機制可以抵抗感測器取得攻擊。

（二）抵抗使用者偽裝攻擊

在 Wu 等人的機制中，在感測器取得攻擊下，會洩漏 U_i 的 ID_i 及一組$<B_1, CID_i>$使得攻擊者能以這組資訊偽裝使用者進行登入。新機制將 GW_j 傳送給 S_j 的訊息縮減為 $M_2=\{SID_k, B_5, B_6\}$，其中在 GW_j 的計算方面將原本的 $B_6=h(r_u)\oplus r_g$ 改為 $r_{ug}=h(r_u||r_g)$，透過 $B_5=h(SG_k||GID_j)\oplus r_{ug}$，傳送包含使用者與 GW_j 的隨機亂數 r_{ug} 給 S_j，$B_6=h(SG_k||r_{ug})$為驗證 r_{ug} 的完整性，最後組成的會期金鑰 $SK_s=h(r_{ug}||r_s)$，其用意在於保護 r_u 的洩漏，使$<B_1, ID_i>$不被計算出來，如此一來攻擊者便無法使用一組舊的$<B_1, CID_i, ID_i>$進行使用者偽裝登入，故新機制可以抵抗使用者偽裝攻擊。

（三）具相互認證

要達到相互認證必須要確實將證實雙方身分的訊息安全的傳送給對方，並能驗證訊息是否被篡改或是冒用，以達到驗證身分的效果。新機制在使用者登入時使用 ID_i 搜索資料庫比對來進行直接驗證，B_1 包含與 GW_j 的秘密金鑰以及使用者的每次更換的匿名代碼 CID_i，確保使用者的 ID_i 以及新產生的匿名代碼 CID_i^{new} 不輕易被計算出來或是取得，使用使用者、閘道器及感測器仿冒無法達成，因此新能達成相互認證。

（四）具使用者匿名性

新機制在每一次使用者 U_i 認證階段結束，都會更換匿名識別碼 CID_i，可有效避免攻擊者追蹤特定使用者，即使攻擊者能透過公開通道取得之間流通的資訊，因 ID_i 不存在於任何公開訊息，也無法被攻擊者計算出來，辨別出是誰的訊息。此外，新機制將$<r_u, r_g>$予以加密，間接保護了 ID_i 及包含 G_j 秘密金鑰的 B_1，即使攻擊者取得手機裝置中的$<A_1, A_2, A_3, CID_i, GID_j>$也無法計算出 CID_i^{new}，其中 $CID_i^{new}=B_{12}\oplus h(A_2\oplus h(ID_i||HPW_i)||\ r_g)$，因此攻擊者無法取得每次更換的匿名代碼，故無法追蹤使用者，故新機制具使用者匿名性。

（五）抵抗離線猜密碼攻擊

本研究在第四章第三節的離線猜密碼攻擊提到有兩種攻擊方法，第一種需要手機裝置中的資訊<A_1, A_2, A_3, CID_i, GID_j >並監聽此裝置下次登入訊息 M_1 ={CID_i, GID_j, SID_k, B_2, B_3, B_4}，以同時猜測帳號及密碼的方式進行，雖然此方法沒有時間及猜測次數的限制，但同時猜測帳號及密碼若非弱帳號及弱密碼，所需的計算及時間成本較高，新機制仍無法防止此方式的攻擊。第二種方法是假設在感測器取得攻擊後的情況下取得<B_1, ID_i, B_1^{new}>，並取得使用者手機裝置中的資訊<A_1, A_2, A_3, CID_i, GID_j >下達成的，但新機制<B_1, ID_i, B_1^{new}>不會洩漏，因此新機制可以抵抗離線猜密碼攻擊。

三、安全性比較

綜述本章節第二節提到的內容，本節利用將 Amin 等（2016）、Wu 等（2017）機制及 Wu 等（2018）的三個物聯網使用者遠端認證機制與新機制進行七個項目的安全性比較，比較結果如表 2，結果顯示新機制更具安全性，其中 Yes 表示可抵抗該項攻擊或具備該項能力，No 則表示無法抵抗該項攻擊或不具備該項能力，詳細比較結果說明如下。

表 2：機制安全性比較表

安全性	Amin et al. (2016)	Wu et al. (2017)	Wu et al. (2018)	新機制
抵抗感測器取得攻擊	No	No	No	Yes
抵抗離線猜密碼攻擊	No	No	No	Yes
具有使用者匿名性	No	No	No	Yes
抵抗感測器偽裝攻擊	No	No	Yes	Yes
抵抗閘道器偽裝攻擊	No	No	Yes	Yes
抵抗使用者偽裝攻擊	No	No	No	Yes
相互認證性	No	No	No	Yes

備註：Yes：可抵抗或具備；No：無法抵抗或不具備

（一）抵抗感測器取得攻擊

Wu 等（2018）指出 Amin 等（2016）機制會因感測器資訊被攻擊者獲得，造成會期金鑰或其他感測器的秘密金鑰的洩漏，因此提出改善的機制，雖然 Wu 等（2017）及 Wu 等（2018）機制宣稱能在單一個感測器遭到攻擊而暴露自己的秘密金鑰後，仍不會造成其他感測器秘密金鑰的洩漏，但本研究發現在感測器遭到攻擊將會曝露使用者的相關資訊，仍會造成其它後續的攻擊，如使用者仿冒及其

它感測器秘密金鑰被洩漏等攻擊。但新機制透過加密使用者與閘道器所產生來計算會期金鑰的隨機亂數，避免被攻擊者取得，可有效避免感測器取得攻擊，並可以減少感測器運算一次雜湊函數的成本。

（二）抵抗離線猜密碼攻擊

在離線猜密碼攻擊中，如使用者的帳密同為弱帳號及弱密碼時，可假設攻擊者可同時猜測帳號及密碼，但所需的計算成本仍較僅需猜測密碼為高，故如能先利用已有的訊息，計算出使用者的帳號，再進行離線密碼將較具可行性，Amin 等（2016）、Wu 等（2017）及 Wu 等（2018）機制在感測器取得攻擊後，攻擊者皆可取得使用者的帳號，且具有檢測密碼正確性的方式，因此無法有效防禦離線猜密碼攻擊，新機制具良好匿名性，可避免使用者帳號洩漏，因此攻擊者只能使用同時猜測帳號及密碼的方法，方能驗證正確性，故新機制可避免攻擊者進行離線猜密碼攻擊。

（三）具有使用者匿名性

Amin 等（2016）的機制會將使用者匿名身分辨識碼存在智慧卡當中且不會去更換，若智慧卡資訊被取得則可以透過卡中資訊來追蹤使用者，因此不具有使用者匿名性。Wu 等（2017）及 Wu 等（2018）機制在每次認證階段的最後 GW_j 會產生一個新的匿名身分識別碼回傳給使用者更換裝置中的匿名身分識別碼，雖然每次都更換匿名識別碼，但在感測器取得攻擊下可得到使用者帳號及相關資訊，使攻擊者能利用公開通道中的資訊算出新的匿名身分識別碼，將無法達到使用者匿名性，而新機制無法算出使用者帳號，並可以防止新產生的匿名識別碼被攻擊者算出，故新機制具有匿名性。

（四）抵抗感測器偽裝攻擊、閘道器偽裝攻擊

Amin 等人（2016）與 Wu 等（2017）機制在遭受感測器取得攻擊後，攻擊者可取得更多資訊，如其他感測器的金鑰等，因此無法抵擋偽裝攻擊。Wu 等（2018）機制在遭受感測器取得攻擊之下，攻擊者必須再取得使用者裝置中的資訊才能計算出偽裝攻擊所需的訊息，因此攻擊者不容易達成偽裝攻擊，因為必須針對相符合的使用者去取得裝置資訊，才有機會達成攻擊，而本研究的機制即使在兩者的情況之下，攻擊者也無法計算出偽裝所需的資訊。

（五）抵抗使用者偽裝攻擊

Amin 等（2016）機制如上所述幾乎所有訊息皆能被攻擊者偽裝，而 Wu 等（2017）與 Wu 等（2018）機制相較不同的在於攻擊者只要取得一組舊的訊息$<B_1, CID_i, ID_i>$，攻擊者便能輕易偽裝成使用者進行認證，主要原因為 B_1 包含了使用

者的身分認證，我們的機制防止了 B_1 的洩漏，因此可以有效進行身分認證。

（六）可達到相互認證

相互認證必須確認雙方的身分正確，即抵抗使用者偽裝攻擊，Amin 等（2016)、Wu 等（2017）及 Wu 等（2018）等人機制無法落實身分的確認，但新機制能夠避免偽裝攻擊，具有相互認證的能力。

四、效能分析

我們在本節比較 Amin 等（2016）、Wu 等（2017）、Wu 等（2018）及我們的機制之效能運算成本，依照不同機制的各個階段進行歸類並比較，因註冊階段及更改密碼階段較少使用，登入階段及認證階段為機制最常用使用階段，故將後兩項加總為常用階段以與所有階段的總和進行比較，Wu 等（2017）機制中，具有透過遠端閘道器進行閘道器管理感測器登入的 case2，因其它機制皆無此階段故不列入比較，各項比較結果如表 3，其中 T_h 代表雜湊函數運算，雖然四個比較機制使用計有單向雜湊函數、互斥或運算及串接運算三種運算，其中互斥或及串接運算成本太小因此不列入計算，因不同硬體設備執行時間不同，較無比較依據，故僅以 T_h 運算次數進行比較。

表 3：機制效能比較表

階段	Amin 等（2016）	Wu 等（2017）	Wu 等（2018）	新機制
註冊階段	5 T_h	6 T_h	6 T_h	6 T_h
登入階段	5 T_h	5 T_h	4 T_h	4 T_h
認證階段	15 T_h	20 T_h	29 T_h	28 T_h
更改密碼階段	7 T_h	18 T_h	20 T_h	20 T_h
常用階段加總	20 T_h	25 T_h	33 T_h	32 T_h
所有階段加總	47 T_h	49 T_h	59 T_h	58 T_h

由表 3 的常用階段總和，可以發現 Amin 等（2016）的機制時間成本為最小，緊接著是 Wu 等（2017）的機制，但根據上一節的安全性分析，Amin 等（2016）與 Wu 等（2017）的安全性不夠完善，再來考慮到我們機制的時間成本以及提供的安全性，滿足了前者的安全性，且在時間成本上為接受範圍，因雜湊函數運算耗時短。

我們的機制是根據 Wu 等（2018）機制來增強，由效能比較表可看出我們的機制比 Wu 等（2018）機制在認證階段少一次雜湊函數的運算，且減少的那一次

運算正好是在感測器的部分，因 WSN 是屬於能量限制的環境，尤其是各感測器所具的電池能量更遠低於閘道器，且為考量 IoT 需低成本的大量製造，同因價格及電力的限制，其其計算能力自然相當低落，故要能在生活周遭或生產產品中大量的配置 IoT 感測器安全的使用，輕量的 IoT 使用者遠端認證機制就相當重要，將 $r_{ug}=h(r_u||r_g)$讓閘道器負責運算，使本機制除增加安全性之外，也考慮到感測器希望以低耗能為主，因而減輕感測器計算的負擔，將可更適用於大量配置 IoT 感測器的實際運用中。

柒、結論

隨著 IoT 的應用越來越普遍，我們希望有一個存取內部資訊的安全機制能夠運用於各種環境。因大量配置在生活週遭或生產環境下的 IoT 裝置，通常具有電池電力及通訊距離上的限制，亦希望在認證或存取資料，能提供更輕量的 IoT 運算，以符合其低成本及長時間運作的限制。此外，為符合 IoT 裝置低耗能的需求，通常由具較高運算效能的閘道器，組成無線感測網路來進行遠端使用者的認證，在通過認證後方能存取所需 IoT 裝置內的資料。但 IoT 裝置有時為偵測外部的資訊，會安置在不安全的實際環境中，因此機制必須承受得住暴露於外在攻擊者的侵襲。在文獻探討中我們發現，現存研究中 Wu 等（2018）所提出的機制符合上述各項需求，具有實用的價值。

但我們探討 Wu 等（2018）的認證機制的安全性分析，發現此機制具有兩個的弱點，第一點在於匿名性的部分檢查的不夠完善，即在登入時，閘道器並不會去直接認證匿名身分識別碼，因為匿名身分識別碼不存在於資料庫，而是藉由使用者透過加密傳送來的訊息來間接認證，而導致被使用過的登入訊息能夠再度被使用，第二點為感測器取得攻擊造成的後續更多的攻擊，如使用者偽裝及離線猜密碼攻擊，且機制若受到感測器取得攻擊會造成其他的感測器金鑰洩漏。在本研究中我們亦發現感測器資訊的洩漏會成為認證機制的弱點，但在感測器的運算效能的限制下，只能使用成本較低的加密方式。在此假設下，我們提出一個新的 IoT 感測網路遠端認證機制。主要貢獻在於，我們減少感測器需要計算的訊息及次數，交由具較高運算能力的閘道器計算完成後，再加密傳給感測器，避免感測器獲得過多使用者及閘道器所需保密的資訊，在感測器被攻擊者取得或複製後，用來建立其它攻擊，以保障使用者與閘道器需保密的秘密資訊。另外，本研究除減少感測器計算成本外，更具有加強其他安全性的貢獻，如匿名性、防偽造、猜密碼等，並利用形式化及非形式化的安全性及效能，說明本研究所提新的 IoT 感測網路遠端認證機制，將更具安全性及在實務生活上應用的可能性。在未來研究方向上，如何在 WSN 環境下提供更有效率的安全性仍為許多學者研究的議題，

雖然本研究提出具有較佳效率的認證機制，但如何能在更少研究假設下提出更較效能的機制，仍是我們未來值得努力的研究方向。

參考文獻

Amin, R., Islam, S.K.H., Biswas, G.P., Khan, M.K., Leng, L. and Kumar, N. (2016), 'Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks', *Computer Networks*, Vol.101, pp. 42-62.

Blanchet, B., Smyth, B., Cheval, V. and Sylvestre, M. (2018), 'ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial', available at https://ics.upjs.sk/~jirasek/krp/manual.pdf.

Chang, C.C. and Wu, T.C. (1991), 'Remote password authentication with smart cards', *IEE Proceedings E-Computers and Digital Techniques*, Vol. 138, No. 3, pp. 165-168.

Chaudhry, S.A., Farash, M.S., Naqvi, H., Kumari, S. and Khan, M.K. (2015), 'An enhanced privacy preserving remote user authentication scheme with provable security', *Security and Communication Networks*, Vol. 8, No. 18, pp. 3782-3795.

Chen, T.H., Hsiang, H.C. and Shih, W.K. (2011), 'Security enhancement on an improvement on two remote user authentication schemes using smart cards', *Future Generation Computer Systems*, Vol. 27, No. 4, pp. 377-380.

Chien, H.Y., Jan, J.K. and Tseng, Y.M. (2002), 'An efficient and practical solution to remote authentication: Smart card', *Computers & Security*, Vol. 21, No.4, pp. 372-375.

Chuang, M.C. and Chen, M.C. (2014), 'An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics', *Expert Systems with Applications*, Vol. 41, No. 4, Part 1, pp. 1411-1418.

Dhillon, P.K. and Kalra, S. (2017), 'A lightweight biometrics based remote user authentication scheme for IoT services', *Journal of Information Security and Applications*, Vol. 34, Part 2, pp. 255-270.

Farash, M.S., Chaudhry, S.A., Heydari, M., Sadough, S.M., Kumari, S. and Khan, M.K. (2017), 'A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security', *International Journal of Communication Systems*, Vol. 30, No. 4, pp. e3019.

Farash, M.S., Turkanovi, M., Kumari, S. and Hölbl, M. (2016), 'An efficient user authentication and key agreement scheme for heterogeneous wireless sensor

network tailored for the Internet of Things environment', *Ad Hoc Networks*, Vol. 36, Part 1, pp. 152-176.

Hsu, C.L. (2004), 'Security of Chien et al.'s remote user authentication scheme using smart cards', *Computer Standards & Interfaces*, Vol. 26, No. 3, pp. 167-169.

Islam, SK Hafizul, Obaidat, M.S., and Amin, R. (2016). 'An anonymous and provably secure authentication scheme for mobile user', *International Journal of Communication Systems*, Vol. 29, No. 9, pp. 1529-1544.

Jiang, Q., Zeadally, S., Ma, J. and He, D. (2017), 'Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks', *IEEE Access*, Vol. 5, pp. 3376-3392.

Juang, W.S. (2004), 'Efficient password authenticated key agreement using smart cards', *Computers & Security*, Vol. 23, No. 2, pp. 167-173.

Karuppiah, M. and Saravanan, R. (2014), 'A secure remote user mutual authentication scheme using smart cards', *Journal of Information Security and Applications*, Vol. 19, No. 4-5, pp. 282-294.

Kumari, S., Khan, M.K., Muhaya, F.B. and Kumar, R. (2013), 'Cryptanalysis of 'a robust smart-card-based remote user password authentication scheme'', *Proceedings of the 2013 International Symposium on Biometrics and Security Technologies (ISBAST 2013)*, Chengdu, China, July 2-5, pp. 247-250.

Kumari, S., Khan, M.K. and Atiquzzaman, M. (2015), 'User authentication schemes for wireless sensor networks: A review', *Ad Hoc Networks*, Vol. 27, pp. 159-194.

Kumari, S., Khan, M.K. and Li, X. (2014). 'An improved remote user authentication scheme with key agreement', *Computers & Electrical Engineering*, Vol. 40, No. 6, pp. 1997-2012.

Lamport, L. (1981), 'Password authentication with insecure communication', *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772.

Lee, C.C., Li, C.T., Chen, C.L. and Chang, R.X. (2010), 'On security of a more efficient and secure dynamic ID-based remote user authentication scheme', *Proceedings of the 10th International Conference on Intelligent Systems Design and Applications (ISDA 2010)*, Cairo, Egypt, November 29-December 1, pp. 1371-1375.

Lee, C.C., Lin, T.H. and Chang, R.X. (2011), 'A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards', *Expert Systems with Applications*, Vol. 38, No. 11, pp. 13863-13870.

Leu, J.S. and Hsieh, W.B. (2014), 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards', *IET Information*

Security, Vol. 8, No .2, pp. 104-113.

Li, C.T. and Hwang, M.S. (2010), 'An efficient biometrics-based remote user authentication scheme using smart cards', *Journal of Network and Computer Applications*, Vol. 33, No. 1, pp. 1-5.

Li, X., Niu, J.W., Ma, J., Wang, W.D. and Liu, C.L. (2011), 'Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards', *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp. 73-79.

Li, X., Xiong, Y., Ma, J. and Wang, W. (2012), 'An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards', *Journal of Network and Computer Applications*, Vol. 35, No. 2, pp. 763-769.

Liao, Y.P. and Wang, S.S. (2009), 'A secure dynamic ID based remote user authentication scheme for multi-server environment', *Computer Standards & Interfaces*, Vol. 31, No. 1, pp. 24-29.

Lin, H.Y. (2014), 'Chaotic map based mobile dynamic ID authenticated key agreement scheme', *Wireless Personal Communications*, Vol. 78, No. 2, pp. 1487-1494.

Messerges, T. S., Dabbish, E. A.and Sloan, R. H. (2002), 'Examining smart-card security under the threat of power analysis attacks', *IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 541-552.

Mishra, D., Das, A.K. and Mukhopadhyay, S. (2014), 'A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards', *Expert Systems with Applications*, Vol. 41, No. 18, pp. 8129-8143.

Shi, Y., Shen, H., Zhang, Y. and Chen, J. (2015), 'An improved anonymous remote user authentication scheme with key agreement based on dynamic identity', *International Journal of Software Engineering and Its Applications*, Vol. 9, No. 5, pp. 255-268.

Shieh, W.G. and Wang J.M. (2006), 'Efficient remote mutual authentication and key agreement', *Computers & Security*, Vol. 25, No. 1, pp. 72-77.

Shieh, W.G. and Yu, P. (2016), 'The weaknesses of karuppiah et al. S remote user mutual authentication scheme using smart card', *ICIC Express Letters*, Vol. 10, No. 12, pp. 2817-2822.

Shin, S., Yeh, H. and Kim, K. (2015), 'An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks', *Peer-to-Peer Networking and Applications*, Vol. 8, No. 4, pp. 674-683.

Sood, S.L., Sarje, A. K. And Singh, K. (2011), 'A secure dynamic identity based authentication protocol for multi-server architecture', *Journal of Network and*

Computer Applications, Vol. 34, No. 2, pp. 609-618.

Tan, K. and Zhu, H. (1999), 'Remote password authentication scheme based on cross-product', *Computer Communications*, Vol. 22, No. 4, pp. 390-393.

Tsai, J.L. (2008), 'Efficient multi-server authentication scheme based on one-way hash function without verification table', *Computers & Security*, Vol. 27, No. 3-4, pp. 115-121.

Tsai, J.L., Lo, N.W. and Wu, T.C. (2013), 'Novel anonymous authentication scheme using smart cards', *IEEE Transactions on Industrial Informatics*, Vol. 9, No. 4, pp. 2004-2013.

Tsaur, W. J., Li, J.H. and Lee, W.B. (2012), 'An efficient and secure multi-server authentication scheme with key agreement', *Journal of Systems and Software*, Vol. 85, No. 4, pp. 876-882.

Vijayalakshmi, P.R. and Raja, K.B. (2012), 'Performance analysis of RSA and ECC in identity-based authenticated new multiparty key agreement protocol', *Proceedings of the 2012 International Conference on Computing, Communication and Applications (ICCCA 2012)*, Dindigul, India, Febuary 22-24, pp. 1-5.

Wang, D. and Ma, C.G. (2012), 'Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards', *The Journal of China Universities of Posts and Telecommunications*, Vol. 19, No. 5, pp. 104-114.

Wang, S.J. and Chang, J.F. (1996), 'Smart card based secure password authentication scheme', *Computers & Security*, Vol. 15, No. 3, pp. 231-237.

Wang, X.M., Zhang, W.F., Zhang, J.S. and Khan, M.K. (2007), 'Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards', *Computer Standards & Interfaces,* Vol. 29, No. 5, pp. 507-512.

Wen, F., Susilo, W. and Yang, G. (2013), 'A secure and effective anonymous user authentication scheme for roaming service in global mobility networks', *Wireless Personal Communications*, Vol. 73, No. 3, pp. 993-1004.

Wu, F., Li, X., Sangaiah, A.K., Xu, L., Kumari, S., Wu, L. and Shen, J. (2018), 'A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks', *Future Generation Computer Systems*, Vol. 82, pp. 727-737.

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*, Vol. 89, pp. 72-85.

Wu, T.C. (1995), 'Remote login authentication scheme based on a geometric approach', *Computer Communications*, Vol. 18, No. 12, pp. 959-963.

Wu, T.C. and Sung, H.S. (1996), 'Authenticating passwords over an insecure channel', *Computers & Security*, Vol. 15, No. 5, pp. 431-439.

Yang, W.H. and Shieh, S.P. (1999), 'Password authentication schemes with smart cards', *Computers & Security*, Vol. 18, No. 8, pp. 727-733.

Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017), 'A survey on security and privacy issues in Internet-of-Things', *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp. 1250-1258.