科技部補助專題研究計畫成果報告
期末報告

基於物聯網概念的感測網路下針對群存取情形之有效率的認證與金鑰協議機制之研究

計 畫 類 別 ： 個別型計畫
計 畫 編 號 ： MOST 104-2221-E-041-007-
執 行 期 間 ： 104年08月01日至105年07月31日
執 行 單 位 ： 嘉藥學校財團法人嘉南藥理大學資訊多媒體應用系

計 畫 主 持 人： 劉川綱
共 同 主 持 人： 李忠憲
計畫參與人員： 碩士班研究生-兼任助理人員：蔡金瑞
大專生-兼任助理人員：周彥穎
大專生-兼任助理人員：莊長翰
大專生-兼任助理人員：李政佳

報 告 附 件 ： 出席國際學術會議心得報告

中 華 民 國 105 年 08 月 30 日

中 文 摘 要 ： 物聯網是一個新奇且流行的概念，他主要是由各種網路組成，無線感測網路就是其中一個，而且無線感測網路在這樣的網路概念下扮演吃重的角色，在這樣的網路下，每個使用者可以直接傳送控制命令到感測點或從感測器收集資料，因此這樣的網路，安全存取是很重要的，使用者認證就是無線感測網路下眾多安全議題中的其中一個，以前的認證機制總是專注在一個使用者與一個感測器之間的認證情形，但是對於未來的物聯網下的應用像是智慧家庭，無線感測網路在此環境皆會布置眾多的感測器，每個使用者通常都會想要再端時間或一次針對多個感測器進行控制，在這樣的網路存取情形下，我們叫他做是批次存取，因此本計畫建議一個認證與金鑰協議機制,它可以讓遠端使用者有效率地完成多個認證工作,而且我們的機制也考慮到利用雙因子安全缺失，因此我們也設計更安全的保護密碼機制，在我們的安全特性與效能評估中，我們機制也可以達到諸多安全目標，同時也保持一定的認證效率。

中 文 關 鍵 詞 ： 物聯網;無線感測網路;雙因子認證

英 文 摘 要 ： Internet of Things notion is an emerging and popular concept, which is composed of heterogeneous networks. Wireless sensor network plays a vital role in such notion, where the users can directly send control commands and gather sensed data to and from deployed sensors, respectively. Hence, in such network, access security is much more essential and the user authentication scheme is one of popular security topics in WSN. Previous authentication works usually focus on one user to one sensor accessing scenario. However, for future IoT applications, such as smart-home, there are a huge amount of sensor nodes in WSN architecture, where one user usually wants to control multiple sensor devices in a short time or at the same time. In such network phenomenon, we call it as a bunch of accesses scenario. Accordingly, this project proposes an authentication and key agreement scheme, which enables a remote user to efficiently complete multiple authentication processes at a time in a bunch of accesses scenario. This proposed authentication scheme is suitable for the resource-constrained WSN architecture. Further, our scheme also considers the security flaws of two-factor authentication and designs a stronger security protection. In our security feature and performance evaluation, our proposed scheme achieves several security goals and, meanwhile, ensures the efficiency.

英 文 關 鍵 詞 ： Internet of Things ;Wireless sensor network ; two-factor authentication

附件一

科技部補助專題研究計畫成果報告

（□期中進度報告/■期末報告）

（計畫名稱）

計畫類別：■個別型計畫　□整合型計畫

計畫編號：MOST 104-2221-E-041-007

執行期間： 104 年 8 月 1 日至 105 年 7 月 31 日

執行機構及系所：嘉南藥理大學資訊多媒體應用系

計畫主持人：劉川綱

共同主持人：李忠憲 教授

計畫參與人員：碩士班研究生-兼任助理人員：蔡金瑞

大學部學生-兼任助理人員:李政佳、莊長翰、周彥穎

本計畫除繳交成果報告外，另含下列出國報告，共 _2__ 份：

□執行國際合作與移地研究心得報告

■出席國際學術會議心得報告

□出國參訪及考察心得報告

中　華　民　國　　年　　月　　日

目錄

中文摘要

物聯網是一個新奇且流行的概念，他主要是由各種網路組成，無線感測網路就是其中一個，而且無線感測網路在這樣的網路概念下扮演吃重的角色，在這樣的網路下，每個使用者可以直接傳送控制命令到感測點或從感測器收集資料，因此這樣的網路，安全存取是很重要的，使用者認證就是無線感測網路下眾多安全議題中的其中一個，以前的認證機制總是專注在一個使用者與一個感測器之間的認證情形，但是對於未來的物聯網下的應用像是智慧家庭，無線感測網路在此環境皆會布置眾多的感測器，每個使用者通常都會想要再端時間或一次針對多個感測器進行控制，在這樣的網路存取情形下，我們叫他做是批次存取，因此本計畫建議一個認證與金鑰協議機制,它可以讓遠端使用者有效率地完成多個認證工作,而且我們的機制也考慮到利用雙因子安全缺失，因此我們也設計更安全的保護密碼機制，在我們的安全特性與效能評估中，我們機制也可以達到諸多安全目標，同時也保持一定的認證效率。

關鍵詞:物聯網;無線感測網路;雙因子認證。

英文摘要

Internet of Things notion is an emerging and popular concept, which is composed of heterogeneous networks. Wireless sensor network plays a vital role in such notion, where the users can directly send control commands and gather sensed data to and from deployed sensors, respectively. Hence, in such network, access security is much more essential and the user authentication scheme is one of popular security topics in WSN. Previous authentication works usually focus on one user to one sensor accessing scenario. However, for future IoT applications, such as smart-home, there are a huge amount of sensor nodes in WSN architecture, where one user usually wants to control multiple sensor devices in a short time or at the same time. In such network phenomenon, we call it as a bunch of accesses scenario. Accordingly, this project proposes an authentication and key agreement scheme, which enables a remote user to efficiently complete multiple authentication processes at a time in a bunch of accesses scenario. This proposed authentication scheme is suitable for the resource-constrained WSN architecture. Further, our scheme also considers the security flaws of two-factor authentication and designs a stronger security protection. In our security feature and performance evaluation, our proposed scheme achieves several security goals and, meanwhile, ensures the efficiency.

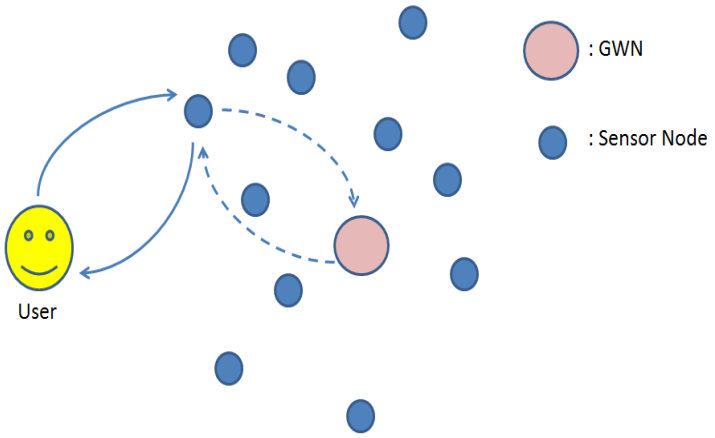
Keywords—Internet of Things ;Wireless sensor network ; two-factor authentication

一、前言

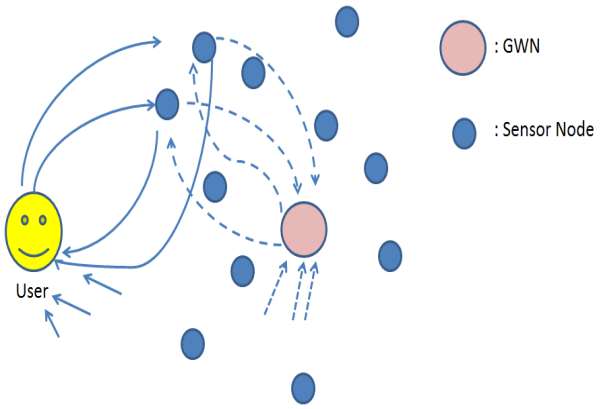
互聯網概念就是建構一個連結世界各式物品的全球網路，透過無處不在的物品連結在一起之後，未來，人們的生活將會越來越方便，這個網路概念也表示全球網路將由各式各樣的網路架構構成，在這樣龐大的網路架構下，無線感測網路預期會扮演很重要的網路技術，無線感測網路是由許許多多分佈在特定一個空間的感測器組成，第 25 篇的參考文獻有完整的無線感測網路的介紹，這篇文章裡面有描述感測網路的應用，技術與可能的挑戰之介紹。無線感測網路的應用程式[20]涵蓋生活各種應用，這些應用包含流量監控[15]，健康照護監測[17]，山崩監測[17]，資產追蹤[16] ，在參考文獻[14]中還有更多真實生活中運用感測網路的應用。根據互聯網概念，使用者可以直接從針對散佈於各地的感測器傳送控制訊號和收集訊號，因此在這樣網路，存取安全將非常重要，在沒有任何資訊安全保護情況下，存心不良的使用者將很容易可以將一些隱密的資料公開，因此，為了確保使用者的合法使用性，使用者認證在無線感測網路變得很重要也吸引很多研究人員關注這方面的研究，這方面的研究也一直有很多研究持續進行與改善舊有機制的缺失，然而，在無線感測網路下的感測器往往因為有限的資源限制下，複雜的認證演算法將不會是一個和適的認證方式，因此最近的研究還是比較偏向發展不會占太多設備資源的演算法為主，而對稱加密以及輕量級加密演算方式就是目前最主要的研究方向。

在參考文獻第 2 篇中的作者針對無線感測網路下的認證方式分類出五種認證模型，在這五類模型中的第五個模型就是比較適合於物聯網的環境，本計劃發現在第 13 篇參考文獻中,作者也引用這個認證通訊模型去模擬他的認證機制的通訊模型，這篇的作者也宣稱他的認證機制是第一位使用這個模型去做物聯網環境下的認證機制，他們的設計就是針對使用者在直接存取無線感測網路中一個感測器時，他的認證機制可以建立一個安全且健全的通訊通道，但是對於一些無線感測網路的應用上，使用者是有可能一次要存取更多的感測器資料或者要傳輸控制訊號給多個感測器，這個應用像是智慧家庭概念或者是一些機構需要進行多個控制器統一控制，在這樣的一個創新應用中，家裡的成員使用者或者機構的管理者通常會在短時間或同時間要一次存取控制一個以上的感測器，這樣的情況是十分可能發生的，像是針對所有窗戶進行關閉或者針對所有門窗進行監控等，這樣的動作需要一次針對多個感測器進行直接性的控制，然而在目前認證機制之下，需要針對一個一個感測器進行認證，其實這樣的認證方式是有其風險，因為這樣認證程序會造成多次認證流程，那麼惡意的攻擊者有機會在這樣的環境下或取到更多的資訊進行分析，甚至破解認證的機制，當然多次認證機制也會浪費網路資源與頻寬，像這樣一次需要針對多個感測器進行認證的情形我們稱為批次認證情形，根據以前的研究, 這種情況必須在短時間一再的啟動認證程序, 這樣容易產生沒必要的安全風險，而且這樣的方式也是很沒有效率的存取方式, 這樣的話, 惡意使用者會有足夠的時間去觀測認證過程中的認證資訊, 在圖一(a), 就是表示一個使用者對一個感測器認證通訊的基本認證模型, 而在圖一(b), 則是顯示在舊有的認證機制下

處理批次認證的情形，我們可以清楚看出來，舊有的機制對於批次認證確實可能產生沒必要的安全風險，而且也會浪費許多網路資源，在這個計畫裡，我們對無線感測網路下這樣的批次存取，提出一個新的資料存取模型，在我們的這個資料存取模型中，使用者只要連線到一批感測器中的其中一個感測器，之後就將認證訊號傳給這個感測器，然後這個被選中的感測器(在這個計畫中我們又稱此感測器為目標感測器)，就會把認證的任務傳給對應的網路閘道器，之後網路閘道器就會把認證的訊號跟金鑰資訊傳到其他的感測器，如此一來，所有的感測器都可以得到這次的安全通訊金鑰，並且，這些感測器也會回傳他們的金鑰資訊回網路閘道器，而網路閘道器也可以在把他收到的所有金鑰回傳給使用者。經由我們提出的認證演算法，批次存取認證只需要使用者做一次認證及金鑰協議演算法，如此一來， 我們提出的演算法在物聯網下的無線感測網路中，可以更節省網路資源又可以達到有效率的認證以及金鑰協議的程序，根據以上的概念，本計畫提出一個新的認證以及金鑰協議模型，這個模型可以確保整個認證通訊過程有很高的安全性。



圖一(a)：一對一基本認證通訊模型



圖一(b)：批次認證通訊模型

二、研究目的

本計畫提出一個可適用於無線感測網路下批次認證的認證以及金鑰協議機制，本計畫提出的機制，主要著眼在參考文獻[13]中提出的認證模型對於未來的物聯網環境是不適合的,雖然作者採用參考文獻[2]中種類中的第5種模型當成他的認證模型，這是第一次有研究者這樣引用此類模型，而他們認為這樣的模型才是適合於物聯網下的無線感測網路，因為它們認為在物聯網環境下所有的物品都應該是相互連接的，那麼在無線感測網路下的使用者在存取這些感測器也應該要直接連接並且存取資料，因此就算是認證機制也應該適用這樣的存取模式，也就是直接跟要認證的感測器進行連接不再經過網路閘道器，因此它們認為在這樣不同以往的資訊存取模式下，也應該要有不同以往的認證模型與演算法，然而這篇文章也是如同以往的認證方式，他們依舊是一對一認證方式，然而對於現在的無線感測網路，終端使用者將不再只是要存取一個感測器，而是多個，而且是短時間內要存取多個感測器的資料，所以若是根據第13篇的所建議的方式，那就要依序一次一次進行認證，依舊陷入之前的認證程序缺點，也就是無謂的風險與無謂的網路或資源的浪費。

所以本計畫的目的就是在考慮這個網路存取狀況下設計一個新的認證模型，我們也在這樣的新模型下設計一個新的認證跟金鑰機制。在參考文獻第５篇的作者發現智慧卡認證機制的安全缺點並且提出三個設計建議，就如這篇參考文獻所說，以往的安全問題其實都是起因於使用者的密碼及帳號太容易被破解，惡意使用者只要運用一些有系統地猜密碼工具就可以很快地破解密碼與帳號，這是因為人們在設計密碼與帳號時容易陷入常犯的設定習慣，諸如生日或自己的電話等，因此我們採納參考文獻第五篇的建議將我們的密碼與帳號重製機制進行防護，同時，我們在此計畫提出的演算法也達到基本的安全功能，像是安全金鑰協議，密碼防護，相互認證，以及低運算量的機制。

三、文獻探討

就如同上節描述，在無線感測網路下通常會有5種認證模型[2], 很多之前的研究都是偏重於網路閘道器轉傳的認證模型，網路閘道器轉傳模型主要是依賴網路閘道器為主，因為此閘道器是一台網路資源較豐富，設備較完全的無線感測設備，所以有很多的研究都提議網路閘道器在無線感測網路中應該要負責絕大多數的認證任務，雖然此設備可以負責絕大多數的認證機制與任務，但是，感測器依然需要負責一些認證過程中的計算任務，而就如同我們所說，這些感測器都是一些資源有限的設備，因此因此對這些設備而言，以往非對稱的加密演算都太複雜，之前，有一個非對稱的認證機制叫做tinyPK[3], 這個機制就是用RSA和Diffie-Hellman的協定所發展出的非對稱演算法，然而， 在參考文獻第6篇中的作者發現這個演算法在對抗安全攻擊時還是有他的弱點，其他非對稱演算法也因為需要很多的記憶體空間而無法在這些有限資源的感測器上實現[18-19]，這是因為他們都需要將很多的公共金鑰存放於所有的感測器上，在參考文獻第24篇中建議在無線感測網路下的智慧卡認證演算法，這個方法宣稱不會

有以往認證演算法的弱點，這個弱點就是可能洩露使用者密碼，也就是這類型的認證演算法將比以往的演算法更加安全，因此最近在無線感測網路下，以智慧卡密碼認證演算法的機制成為最吸引各個研究者的注意，許多的研究也都以此演算法的理念而發展各式各樣的認證演算法。最近幾年來，已經有許多的認證演算法就是以智慧卡為基礎發展而成[7-12](智慧卡認證演算法又稱為2項參數認證演算法), 而且，在此領域下，絕大多數的研究都是根據以往的認證演算法再發展而成的，例如，在參考文獻第8篇中的作者, 就是根據Das這個作者的演算法而發展出來的，他主要是針對上篇的演算法的弱點進行分析之後才提出他的演算法，另外, Khan和Alghathbar也是針對他之前的使用者認證機制進行改善，這些改善像是將密碼再進行編譯，還有修改密碼，相互認證諸如此類的安全事項...等，接下來，很多的研究也持續根據以往的研究加以發展更完善的認證演算法，我們接下來就開始來討論最近比較有名的智慧卡認證演算法以及金鑰協議機制，參考文獻第4篇中的作者Das就提出以密碼為基礎的動態使用認證演算法，這個演算法可以達到更好的安全性以及更佳的效率，他們宣稱他們的演算法有很多安全特性，就像有名的相互認證，密碼修正以及動態結點加入，他更宣稱這個演算法可以對抗很安全攻擊，而且在此篇的文獻中所用的演算法只用到XOR以及雜湊（HASH）的認證計算方式, 這種演算方式被公認為是比較適合於資源有限的無線感測網路內，但是在參考文獻第五篇中的作者則反駁他依舊無法達到許多安全目標，他也發現上篇文章中的演算法在對抗智慧卡安全破解攻擊以及內部組織權限攻擊時會有其弱點，甚至他更指出一個嚴重的弱點，這個弱點就是密碼揭露，一旦密碼揭露後,整體無線感測網路的運作將毫無安全可言，在參考文獻第二篇的作者也提出了一個暫時憑據為主的(temporal-credential-based) 相互認證機制及金鑰協議機制，他宣稱他的機制可以對抗許多安全攻擊，然而，在參考文獻第28篇中的作者就發現參考文獻第2篇的認證機制有其安全弱點，這些弱點就像是沒有辦法對抗智慧卡安全破解攻擊以及內部組織權限攻擊，還有密碼揭露的問題，在參考文獻第26，27篇的作者提出基於參考文獻第2篇的改善加強版的認證機制。最近在物聯網上許多創新且新穎的應用一直被提出，像是智慧屋的設計以及在各種領域下的設備控制，這些各式各樣的應用中，無線感測網路將於物聯網中扮演著非常重要的角色，很多在無線網路感測上的應用其實就是物聯網的一種應用，因為物聯網也是透過各式網路的合作方能成真，因此，在無線感測網路上的應用服務提供者必須提供使用者可以直接針對所有的感測器控制的權限，這是物聯網重要的中心概念，例如，智慧屋的服務供應商就要提供在物聯網環境下使用無線感測網路技術的所有住家感測器的控制服務，智慧屋的供應商也給終端使用者一個合法的使用者權限，以便針對在居家中的無線感測網路中之所有感測器有合法的存取權。

四、研究方法

本計畫主要是設計一個認證與金鑰協議演算法，這一節我們以以下四個小節介紹本計畫所設計之演算法與其設計概念，四小節概述如下：

1. 第一小節，我們先定義我們的認證演算法與金鑰協議模型
2. 第二小節我們計畫會詳細介紹我們演算法的設計理念與流程
3. 第三小節則為說明認證演算法的各個階段流程設計與認證的流程

接下來我們開始依據以下小節介紹本計畫之研究方法

4.1 新的認證與金鑰協議模型

首先一開始，我們先介紹在我們計畫中的認證與金鑰協議模型，在無線感測網路的架構下，會有很多的感測器散佈在目標區域，這些感測器會會根據其功能執行並收集感測資訊，感測網路下的網路閘道器會從這些散布的感測器上收集感測訊號並回傳到使用，但是在物聯網的環境下，使用者在收集感測訊號時會跳過網路閘道器直接與感測器通訊並收集訊號，因此，由於無線感測網路與物聯網的特性下，本計畫才規劃一個新的認證與金鑰模型，這個模型主要由四個關係模型組成，這四個關係模型分別描述在無線感測網路下，本計畫的認證與金鑰演算法運作時，各個設備間的運作關係，這些設備包括：感測器、網路閘道器、使用者以及從一群要認證的感測器中選出的目標感測器，這四個關係模型為(1)使用者與目標感測器關係模型 (2) 目標感測器與網路閘道器關係模型 (3)網路閘道器與一批要進行認證的感測器間的關係模型(4)網路閘道器與使用者間的關係模型，每個關係模型都是表示在本計畫的認證與金鑰演算法中兩個設備間的互動關係，這個模型就像是參考文獻第二篇所提出的五個模型中的兩個模型的混合模型，這兩個模型就是參考文獻第二篇所說的第二與第五個模型，以下我們說明這四個關係模型所描述的互動情形

- 使用者者與目標感測器關係模型: 這個模型是在說明使用者與目標感測器之間的互動情形，本計畫所設計的認證與金鑰演算法目的在於解決物聯網概念的下的無線感測網路如何處理批次認證要求，因此，使用者必須一次面對多個感測器的認證情形，在本計畫所提出的方式是先從這些感測器上隨機選取一個目標感測器，使用者會在認證之初先與這個目標感測器進行聯繫，這個感測器主要是負責將認證訊號傳送到網路閘道器，因此使用者首先會先登入這個目標感測器，之後目標感測器會在這個互動上對使用者進行認證確認，以確保是合法使用者正在進行登入的動作，並且開始接下來的認證程序

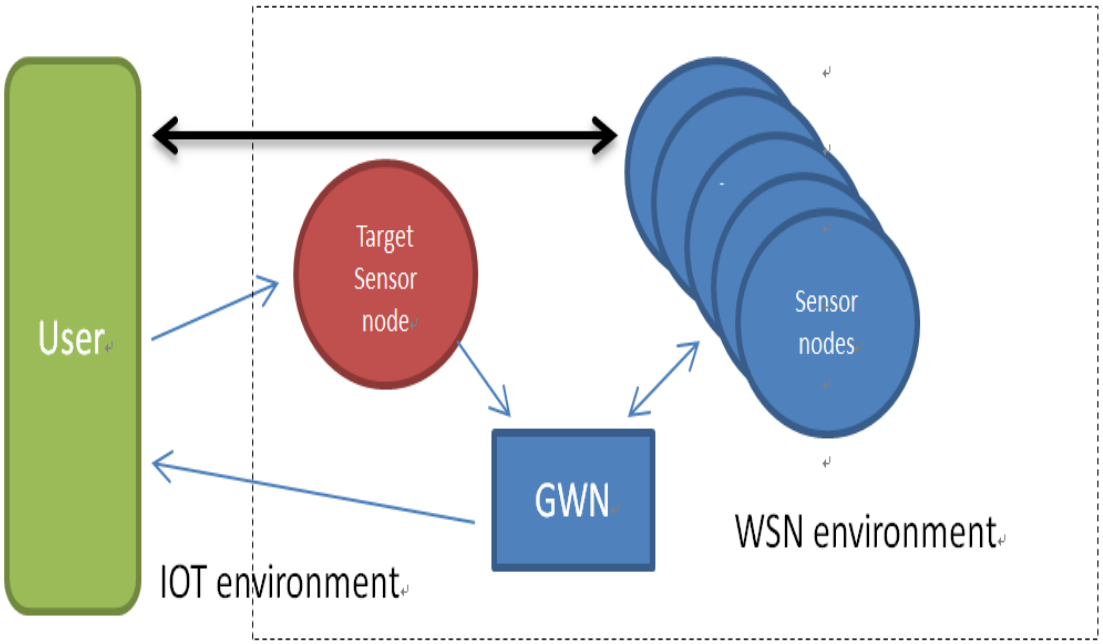
- 目標感測器與網路閘道器關係模型：這個模型主要是描述目標感測器傳送認證與金鑰協議資訊給網路閘道器，網路閘道器會把感測器送過來的資訊進行認證，確保傳來的資訊沒有問題，在確認這修資訊沒問題之下，才會將這些認證資訊進行轉送。

- 網路閘道器與其他感測器關係模型：這個模型就是在描述當網路閘道器轉送認證資訊給各個感測器，這些感測器會對收到的資訊進行認證，並且在確認之後收到使用者的金鑰後再回傳給網路閘

道器自身的金鑰，網路閘道器也會針對這些傳回來的資訊進行認證確認，以確定這些資訊確實由各感測器回傳回來的資訊，最後網路閘道器也會將這些收到的認證與金鑰協議資訊進行轉傳，這一來一往的認證過程就是這個模型所要描述的情形

- 網路閘道器與使用者關係模型：這個模型就是用來描述最後認證與金鑰協議階段，當網路閘道器將感測器送來的資訊回傳給使用者時，使用者將會對這些最後還傳回來的資訊進行確認，這些資訊包含最重要的感測器的金鑰，這金鑰將跟他本身的金鑰進行結合組成使用者與感測器間的認證金鑰，至此之後，使用者已經完成了認證與金鑰協議演算法並且可以開始利用認證金鑰對各個感測器進行直接存取的權限，這樣使用者將可以一次在短時間內與多個感測器進行通訊，這將節省許多網路資源，並且這個認證模型也是比較適用於物聯網的環境

在圖二中我們可以看到這個模型中各個設備角色在物聯網路認證的關聯，本計畫所提出的這個模型有別於參考文獻二中提出的五種模型，是一個全新的模型，這個模型結合物聯網與無線感測網路兩個網路的特性，但是，事實上，無線感測網路其實也是物聯網中的一支重要技術，他有許多感測網路應用，因此我們堅信，基於這兩種網路特性下的使用者認證與金鑰協議演算法確實有其重要性，而且他也會符合未來的網路技術趨勢。



圖二:新的認證模型

4.2 本計畫認證與金鑰協議演算法

就如同前幾節所說，本計畫中所提出的認證與金鑰演算法是針對批次認證情形而進行發展，在這樣的，本計畫規劃共有五個認證階段需要設計，這些階段包括有：第一階段為前置佈置感測器階段、第二階段為使用者與感測器註冊階段、第三階段為使用者登入階段、第四階段為認證階段以及第五階段為金鑰回復階段，這五個階段完成後就表示整個認證結束。接下來我們就一一說明在各階段我們計畫所設計的的認證細節，在說明之前我們以表一說明計畫內會使用參數

表一：計畫內會使用參數

參數	定義
S_j	感測點 j
U_i	使用者 i
SID_j	感測點 j 的認證 ID
UPW_i	由使用者 i 設定的密碼
MPK_i	重製的使用者 i 的密碼
RUP_i	使用者 i 的掩飾 ID
P_{GWN}	網路閘道器的私鑰
P_{GSj}	網路閘道器和感測點 j 的共享私鑰
ΔT	合法的傳送延遲時間
UID_i	使用者 i 的認證
q_i	智慧卡隨機產生的數值
T_{Ri}	從使用者傳出訊息的目前時間標記
T_{Sj}	目前從感測點傳出的時間標記
T_{CG}	在網路閘道器的目前時間標記
P_{GUi}	網路閘道器和使用者 i 的共享私鑰
I_{Sj}	在網路閘道器內有關感測點 j 的資訊
I_{Ui}	在網路閘道器內有關使用者 i 的資訊
RSN	目標感測器
SID_{Sa}	此符號表示所有使用者所控制的感測點之 ID 集合
Sa	使用者所控制的感測點集合
Ki	由使用者 i 產生的隨機臨時字串金鑰
Kj	由感測點產生的隨機臨時字串金鑰
SKij	由使用者 i 與感測點 j 產生的會議金鑰

第一階段：前置布置感測網路階段

根據物聯網概念，使用者可以直接對在無線感測網路下的特定感測器傳送控制訊號與收集資訊，每個無線感測網路在佈置之初皆有其應用領域，因此，當使用者想要對無線感測器進行存取時，提供這個無線感測網路的供應商需要提供一組使用者帳號與智慧卡給使用者，這個智慧卡上會針對單一使用者有儲存智慧卡的客製化帳號設定，所以在這階段每個感測器也都會被一組序號定義，這些感測器也會由供應商給一組私有金鑰，這組私有金鑰也會同時被網路閘道器儲存起來，當作未來在進行認證時會運用到的資訊，因此在佈置之初，網路閘道器會將每個感測器的帳號與金鑰進行儲存。

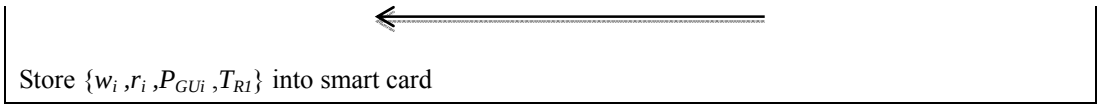
在我們的認證與金鑰演算法中，我們計畫使用者如果要存取一批感測器就需要針對目標感測器進行存取，使用者就必須要進行接下來的動作，這個動作也就是註冊，我們以圖三來描述這階段要做的事項

圖三：前置佈置感測網路階段

第二階段：註冊階段

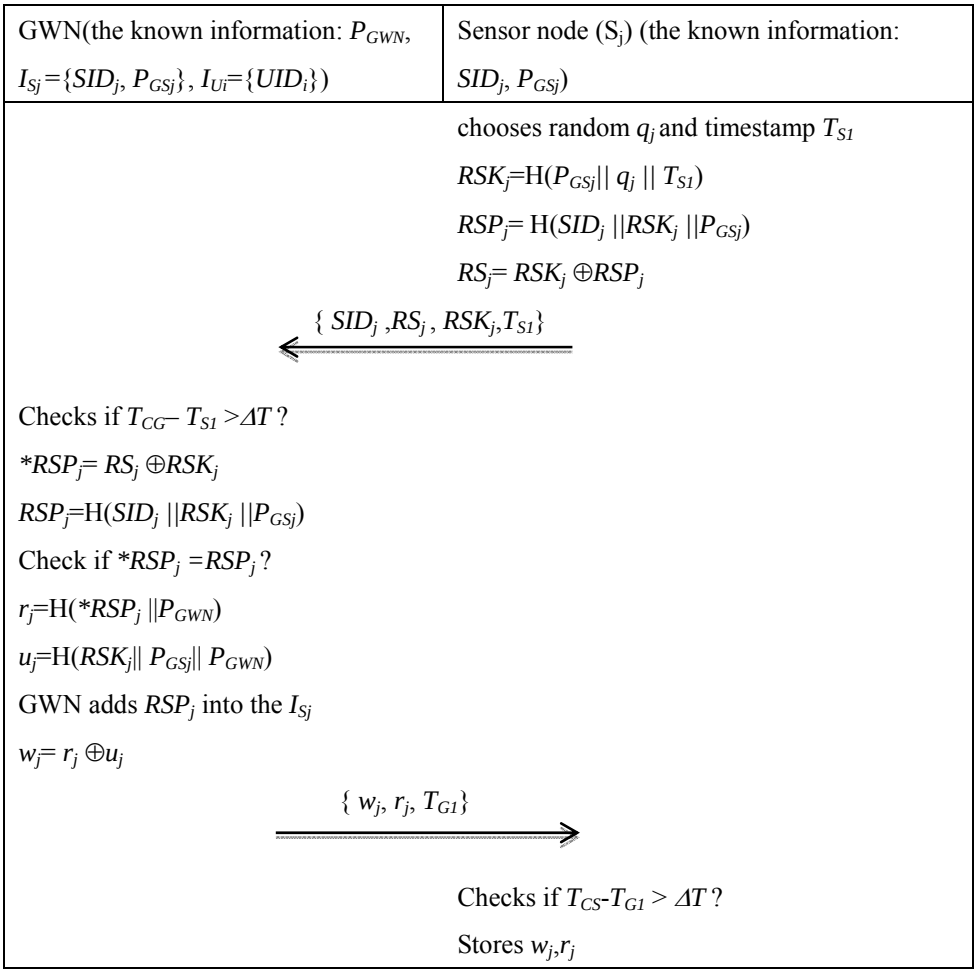
在使用者登入目標感測器之前，使用者和感測器必須向無線感測網路上的網路閘道器進行註冊並且獲取必要的資訊，這些資訊將作為之後認證所需的基本資料，因此我們必須先設計註冊程序的認證過程，這樣才可以確保註冊的正確性，由於註冊的動作有兩個設備必須完成，所以本計畫稱第一個註冊動作為使用者與網路閘道器註冊階段，這階段的註冊由使用者啟動，使用者利用智慧卡去啟動認證與金鑰協議程序，我們說明本計畫在此階段的註冊程序如下：

User(U_i) (the known information: UID_i, UPW_i)	GWN(the known information: P_{GWN}, $I_{Sj}=\{SID_j, P_{GSj}\}$, $I_{Ui}=\{UID_i\}$)
Generate a random q_i, and current timestamp T_{R1} $MPK_i=H(q_i \oplus UPW_i)$ $RUK_i=H(T_{R1} \| MPK_i)$ $RU_i= UID_i \oplus RUK_i$	
$\{RU_i, UID_i, T_{R1}\}$ →	
	Checks if $T_{CG} - T_{R1} > \Delta T$? $RUK_i= RU_i \oplus UID_i$ Generate random P_{GUi} associating with the user i $r_i=H(UID_i \| P_{GWN} \| P_{GUi})$ $u_i=H(RUK_i \| P_{GUi} \| r_i)$ $w_i= r_i \oplus u_i$ personalizes user's smart card USC $USC=\{w_i, r_i, P_{GUi}\}$
$\{w_i, r_i, P_{GUi}, T_{R1}\}$	



圖四： 使用者與網路閘道器註冊

結束了這個註冊動作後，另一個註冊動作也必須完成，本計畫稱第二個註冊動作叫做感測器與網路閘道器註冊階段，這個動作由感測器啟動，透過感測器對網路閘道器傳輸註冊資訊，以下就來介紹這個註冊動作下的兩個設備行為



圖五：感測器與網路閘道器註冊

完成註冊之後，則開始進行使用者登入動作

第三階段:登入階段

當使用者完成註冊動作後，即可以隨時進行認證動作，首先的動作就是登入整批感測器中的其中一個，也就是所謂的目標感測器，這個目標感測器是隨機選取，使用者在登入目標感測器之後，就會把認證資訊也一併傳給目標感測器，也會把使用者產生的金鑰一併傳遞過去，接下來我們一樣也是分成兩端說明登入認證過程，以下為本計畫所設計的登入程序

User(U_i) (the known information: UID_i, MPK_i)	RSN (S_j) (the known information: SID_j, P_{GSj} ,w_j,r_j)
SC login Input password MPK_i $*RUK_i$=H(T_{R1}|| MPK_i) $*u_i$=H($*RUK_i$|| P_{GUi}|| r_i) $*w_i$= $r_i \oplus *u_i$ Check if $*w_i = w_i$? RUP_i=H(T_{R2}|| UID_i) M_i=H(u_i|| P_{GUi} || T_{R2}|| r_i) Select random nonce K_i D_i= $K_i \oplus M_i$ Choose the RSN from S_a, and SID_{Sa} denotes the SID set of S_a. { RUP_i ,w_i, D_i , M_i ,T_{R2}, SID_{Sa} } ⟹ Checks if T_{CS}- T_{R2}> ΔT ?	

圖六：登入階段傳訊資訊

第四階段：認證階段

在這個階段，可以分成兩個認證階段，第一就是目標感測器與網路閘道器之間的認證過程，第二就是網路閘道器與感測器間的認證，首先先說明第一個認證過程，此過程是目標感測器會將所收到的資訊進行加密後並且將它的資訊傳送給網路閘道器，這些資訊包含有目標感測器的認證資訊與使用者傳送給目標感測器的資訊，我們也是利用兩端設備角度說明認證流程細節

1. 目標感測器與網路閘道器之間的認證

The RSN (S_j) (the known information: SID_j, P_{GSj} ,w_j,r_j)	GWN(the known information: P_{GWN}, I_{Sj}={SID_j, RSP_j, P_{GSj} }, I_{Ui}={ P_{GUi} , UID_i})
$u_j = w_j \oplus r_j$ L_j=H(P_{GSj}|| T_{R2}|| T_{S2}||SID_j) $\oplus$ u_j { RUP_i, w_i, D_i, M_i , T_{R2}, T_{S2}, w_j, L_j, SID_{Sa} } ⟹	Checks if T_{CG}– T_{S2} >ΔT ? r_j=H(RSP_j ||P_{GWN}) $*u_j = w_j \oplus r_j$ u_j= $L_j \oplus$H(P_{GSj}|| T_{R2}|| T_{S2}||SID_j)

checks if $*u_j = u_j$?

For each UID do

$*RUP_i = H(T_{R2} \| UID_i)$

Checks if any $*RUP_i = RUP_i$?

if yes, continue process ,or authentication fails.

$r_i = H(UID_i \| P_{GWN} \| P_{GUi})$

$*u_i = w_i \oplus r_i$

$*M_i = H(*u_i \| P_{GUi} \| T_{R2} \| r_i)$

check if $*M_i = M_i$?

$K_i = D_i \oplus *M_i$

圖七：目標感測器與網路閘道器之間的認證過程

2. 網路閘道器與感測器間的認證

經過目標感測器與網路閘道器之間的認證程序之後，網路閘道器會收到使用者傳來的金鑰，之後，網路閘道器會根據收到的訊號中擷取出需要溝通的感測器ID，網路閘道器就會將使用者金鑰與自己本身的認證資訊傳到各個感測器上，每個感測器將會收到這些資訊，以下即為我們設計之認證過程

GWN(the known information: P_{GWN}, I_{Sj}={ SID_j, RSP_j, P_{GSj} }, I_{Ui}={RUP_i , P_{GUi} , UID_i})	Sensor node (S_j) (the known information: SID_j, P_{GSj} ,w_j,r_j)
For each sensor node S_j in S_a $OSP_j = H(r_j \| SID_j \| T_{G3} \| T_{S2} \| T_{R2})$. $OSK_j = H(r_j \| P_{GSj} \| T_{G3} \| T_{S2} \| T_{R2})$ $OS_j = OSP_j \oplus OSK_j$ $GC_{ij} = H(OSP_j \| T_{G3} \| T_{S2} \| T_{R2}) \oplus K_i$ $\{OS_j, T_{G3}, T_{S2}, T_{R2}, OSK_j, GC_{ij}\}$ ⟹	
	Checks if $T_{CS} - T_{G3} > \Delta T$? $*OSP_j = OS_j \oplus OSK_j$ $OSP_j = H(r_j \| SID_j \| T_{G3} \| T_{S2} \| T_{R2})$ Check if $*OSP_j = OSP_j$? $K_i = GC_{ij} \oplus H(OSP_j \| T_{G3} \| T_{S2} \| T_{R2})$ Choose random nonce K_j $SK_{ij} = H(K_i \oplus K_j)$ $OC_{ij} = H(H(r_j) \| T_{G3} \| T_{S2} \| T_{R2} \| T_{S3}) \oplus K_j$ ⟸ $\{ OC_{ij}, T_{G3}, T_{S2}, T_{R2}, T_{S3}, OSP_j \}$
Check if $T_{CG} - T_{S3} > \Delta T$?	

Check if OSP_j=H(r_j||SID_j|| T_{G3}||T_{S2}|| T_{R2}) ?

$K_j = OC_{ij} \oplus$ H(H(r_j) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3})

OU_{ij} =H(H(r_i) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) $\oplus K_j$

圖八：網路閘道器與各感測器之間認證

認證階段透過這兩個子程序完成，當這個階段完成之後，每個感測器都會有獨一無二的金鑰對，因此接下來的工作就是要讓使用者知道感測器所產生的金鑰，如此方能配對成跟感測器端一樣的金鑰對，方能使整體通訊是安全的。

第五階段　金鑰回覆階段

目前為止，通訊金鑰已經由各感測器產生完畢，並且將這些資訊傳給網路閘道器，接下來由網路閘道器直接回傳回使用者，因此這階段的我們稱為金鑰回覆階段，以下即為我們設計之認證過程

User(U_i) (the known information: UID_i, RUK_i)	GWN(the known information: P_{GWN}, I_{Sj}={ SID_j, RSP_j, P_{GSj} }, I_{Ui}={ P_{GUi} , UID_i })
	V_{ij}=H(UID_i||r_i|| T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) OV_{ij}= $OU_{ij} \oplus V_{ij}$
	{ V_{ij} ,OV_{ij},T_{G3},T_{S2}, T_{R2}, T_{S3}, T_{G4}} ⟸
Checks if T_{CU}- T_{G4}>ΔT ? Checks if V_{ij} = H(UID_i||r_i|| T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) OU_{ij}= OV_{ij} $\oplus V_{ij}$ K_j= $OU_{ij} \oplus$ H(H(r_i) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) SK_{ij}=H($K_i \oplus K_j$)	

圖九：金鑰回覆階段

最後使用者跟要通訊感測器都獲取到會議金鑰，這些金鑰讓使用者可以一次跟多個感測器直接進行通訊，這樣的認證與金鑰協議方式符合物聯網的概念，也結合無線感測網路的架構特性，因此這樣的認證與金鑰協議機制對未來物聯網下的無線感測網路是一個可行且安全的方式

五、分析討論

在這一節我們利用我們認證與金鑰協議的機制評估計畫來評估本計畫的認證及金鑰協議機制的正確性與安全性，這個評估計畫包含兩個方向進行，安全性分析計畫，另一個是效能評估計畫，這兩種是目前在無線感測網路下最常規劃的兩種評估項目，以下我們來進行個別說明評估計畫：

在我們的這個安全分析計畫中，本計畫將驗證本計畫所提出的認證與金鑰協議演算法可以達到之前有名的認證研究中常述及的安全特性，這些安全特性主要有三點

- 安全的金鑰協議：安全金鑰協議是在認證協議的主要目的，本計畫所提出的認證與金鑰協議演算法共有五個階段，每個階段都規畫嚴謹的加密運算，讓金鑰資訊在傳遞過程中，沒有暴露在不安全保護下，而且利用 XOR 運算加密後，讓惡意的攻擊難以確認是否為金鑰資訊，並且也使用雜湊函數進行加密之後，惡意的攻擊者也更加難以回復原本訊息，因此金鑰在傳輸過程中是安全無虞的。

- 相互認證安全特性：本計畫提出的演算法也保有之前研究所說的相互認證機制，這是說每次傳輸到對方後，對方會做判斷是否這訊號是合法的，回覆回來的訊號，一樣也會進行認證動作，以便確認每次接收的訊號都是正確無誤的訊號，如此可以讓整體認證安全行性提高。

- 密碼防護安全特性：本計畫是利用目前主流的智慧卡認證方式，這種認證方式有效的降低使用者密碼被惡意攻擊者盜取的機率，因為密碼不再儲存於一台認證設備上，而是由使用這本身記憶起來為主，然而此方式也有其被詬病的缺點，就是不安全的密碼設計[5]，一般使用者在設計其密碼或許會因方便而以自己的身分證、電話或生日為設定密碼，惡意攻擊者在有機會拿到認證設備後，進行密碼破解就會很順利，因此本計畫設計的密碼以使用者的自設密碼加上系統隨機參數進行雜湊函數的運算，並且在得到新的密碼後將所有原有的密碼資訊清除，使用者只要記憶住此密碼就可以防止惡意攻擊者的密碼破解，也可以有安全的密碼防護效果。

本計畫也將進行驗證評估所提出的認證與金鑰協議演算法可以抵抗諸多有名的攻擊，我們的演算法將一一進行驗證

表二：各式安全攻擊特性

攻擊名稱	本計畫的機制應對方式
中間人攻擊(man-in-the-middle	這類攻擊一般是指攻擊者趁使用者在訊息傳

attacks)	送時，暗中讀取、插入及更改發送者和接收者之間的資訊。通常發生於傳送的訊號沒有加密或數位簽章等保護機制。在我們的機制中，雖然攻擊者可以擷取認證過程中所有的訊息，但我們機制都會對重要的認證資訊進行保護，這些保護包含利用雜湊函數，XOR 的計算，因此我們的機制可以抵抗這樣的攻擊
重播攻擊(replay attacks)	這類攻擊是指發送者和接收者之間的資訊遭到攔截並且被惡意地重新傳輸。在我們的機制，每次接收訊號時，我們都會檢視這些資料是否在合法時間內收到訊息，這樣即可以防止這樣的攻擊
假冒攻擊(impersonation attacks)	冒充合法使用者進行與接收端通訊，以達到欺騙的效果，在我們的機制，相互認證可以確保每次傳送的訊號都是合法的，重製過的密碼與ＩＤ也可以讓存心不良的使用者無法竊取真正的密碼與ＩＤ，這樣即可以防止這樣的攻擊
驗證表被竊取後攻擊(stolen-verifier attacks)	這類攻擊在於從伺服器端竊取驗證表格(Verification Table)，並且得到裡面使用者的秘密資訊。為避免這樣的攻擊，演算法避免使用驗證表格，則可避免此種攻擊方法。在我們的機制中沒有使用這樣的驗證表，因此可以防止這樣的攻擊
智慧卡破解攻擊(smart card breach attacks)	此類攻擊在於將智慧卡破解取得使用者施密資訊，以便冒充使用者，雖然在智慧卡的資料被攻擊者竊取是很危險的，但是要存取無線感測網路，沒有使用者密碼依舊無法成功，本計畫的機制重製了密碼，攻擊者難以突破此一密

	碼
內部特權者攻擊(privileged insider attacks)	此類攻擊主要是因為系統內擁有特權的人利用他所擁有的特權進而獲取使用者的私密資訊，並且對使用者權益造成損害，但是我們的機制中，密碼早已重製，因此很難由其他系統取得的密碼來存取無線網路
智慧卡被盜取攻擊(stolen smart card attacks)	此類攻擊是因為智慧卡被盜取後利用離線工具進行竊取智慧卡內部資料，以進行偽裝攻擊，但是要存取無線感測網路，沒有使用者密碼依舊無法成功，本計畫的機制重製了密碼，攻擊者難以突破此一密碼
使用一樣登入帳號與密碼進行多重登入攻擊(many logged-in users with the same login-id attacks)	利用合法的帳號進行多個登入動作，如果伺服器沒注意到這樣的非法登入情形，則這樣攻擊就完成了，但是我們的機制中，密碼早已重製，因此內部人很難由其他系統取得的密碼來存取無線網路
密碼修改攻擊(password change attacks)	此類攻擊在於獲取到使用者原有資訊後進行密碼修改，使合法使用者難以進行合法使用，反而為非法使用者使用，我們的機制中，密碼早已重製，且密碼由雜湊函數進行機密，因此很難取得密碼來存取無線網路
避網路閘道器攻擊(GWN bypassing attacks)	透過避開網路閘道器，使使用者誤認為對方才是閘道器，造成可能的資訊外露，在我們機制中，如果跳過網路閘道器，由於沒有使用者與感測器的資訊依舊無法進行偽裝

阻斷服務攻擊(denial-of-service attacks)	阻斷服務攻擊可分成不同層的攻擊，在本計畫主要以第三層攻擊為主，此類攻擊大都是利用多個攻擊者發出攻擊，讓伺服器難以應付過多的服務，本計畫利用防止重播攻擊方式避免此類攻擊，雖然這類攻擊難以防止，但是利用時間標記區間來防止，可以達到不錯效果

本計畫也與五年內在此領域著名的研究者進行比較，提出本計畫提出的演算法將更合適未來物聯網下的認證機制，以表三列出要比較成果。

表三 近年來有名的使用者金鑰與認證機制之安全參數比較

	項目	Das ML. [24] (2009)	Khan and Alghathbar[22] (2010)	Chen and Shih[21] (2010)	D. He [8] (2010)	H. Yeh[9] (2011)	Das et al. [4] (2012)	Xue et al. [2] (2013)	M. Turkanovic´ et al.[13] (2014)	Our proposed scheme
安全特徵	相互認證	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
	金鑰協議	No	No	No	No	Yes	Yes	Yes	Yes	Yes
	動態感測點加入	No	-	No	No	-	Yes	-	Yes	Yes
	變更密碼	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes
攻擊參數	密碼弱點安全攻擊(共有五項在附註中說明)	No	No	No	No	No	No	No	No	Yes
	Reply attack	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
	Stolen-verifier and privileged insider attacks	No	Yes	No	No	Yes	-	Yes	Yes	Yes
	Denial-of-service attacks	No	Yes	No	-	-	Yes	-	Yes	Yes
	GWN bypassing attacks	No	Yes	No	No	Yes	-	Yes	Yes	Yes

附註: 密碼弱點安全攻擊: 假冒攻擊,使用一樣登入帳號與密碼進行多重登入攻擊, 智慧卡被盜取攻擊,智慧卡破解攻擊, 密碼修改攻擊

效能評估計畫

本計畫也針對演算法可能會在各個設備上需要執行計算負載進行評估，這些計算負載評估主要是看執行雜湊函數的運算量做衡量，XOR 的運算量由於影響很小，所以大部分的研究者都忽略不計算，因此我們也以三個設備上的計算量為主要評估，這三個設備分別為感測器、網路閘道器、使用者終端設備為主，我們一樣也是以表 3 所標示的研究論文為比較對象，進行運算量的評估比較。

由表四可以看出本計畫中各個設備的計算負載量，雖然網路閘道器的計算量比較大，但是因為網路閘道器的運算能力比較強，其實是可以容忍的。

表四: 計算負載評估

	Das ML. [24] (2009)	Khan and Alghathbar [22] (2010)	Chen and Shih[21] (2010)	D. He [8] (2010)	H. Yeh [9] (2011)	Das et al. [4] (2012)	Xue et al. [2] (2013)	M.Turkanovic´ et al.[13] (2014)	Our proposed scheme
使用者	$3T_h$	$4\ T_h$	$4\ T_h$	$5\ T_h$	T_h+$2T_{ECC}$	$5\ T_h$ +$1T_{E/D}$	$7\ T_h$	$7T_h$	$8T_h$
感測點	T_h	$2\ T_h$	$1\ T_h$	$1\ T_h$	$3T_h$+$2T_{ECC}$	-	$6\ T_h$	$5\ T_h$	$5\ T_h$
網路閘道器	$4\ T_h$	$6\ T_h$	$5\ T_h$	$5\ T_h$	$4T_h$+$4T_{ECC}$	$2\ T_h$ +$1\ T_{E/D}$	$13\ T_h$	$7\ T_h$	$14\ T_h$
基地台	-	$2\ T_h$	-	-	-	$2\ T_h$ + $3\ T_{E/D}$	-	-	-

T_h: the time for the hash operation; T_{ECC}: the time for ECC decryption/encryption; $T_{E/D}$: the time for symmetric key decryption/encryption

六、結果與討論

在這個計畫中，我們提出在物聯網概念下在無線感測網路下一個新的認證與金鑰協定，此一協定跟之前不同的在於，本計畫的認證機制不再針對一個使用者對一個感測器的情形，而是針對未來物聯網應用下可能出現的無線感測網路存取方式，就是一個使用者對多個感測器控制的情形，在物聯網盛行的網路環境下，各種創新的應用勢必會一直被提出來，而無線感測網路的重要性也日益顯著，因此設計出一個合適的認證與金鑰協議是本計畫最大的目標，因此本計畫提出的認證機制完整地解決一對多的認證情形，並且將其成果進行發表，最初成果已經投稿到 NCWIA2015 並且獲得最佳論文，期刊的版本也於最近投出，因此本計畫的認證機制確實更適合在物聯網的感測網路下，我們也採用之前前人的建

議，將密碼問題進行修正，在我們的效能評估與攻擊應對中，我們的認證方法皆可以克服現今的認證問題與達到諸多安全特性，我相信此計畫對於國家在資訊安全上可以盡一份心力。

七、參考文獻

[1] L. Atzori, A. Iera, G. Morabito, (2010) "The Internet of things: a survey," Comput. Netw. 54, pp.2787–2805.

[2] Xue, K.; Ma, C.; Hong, P.; Ding, R. (2013) "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," J. Netw. Comput. Appl. 36, pp. 316–323.

[3] Watro R, KongD, CutiS, GardinerC, LynnC, KruusP, (2004) "TinyPK: securing sensor networks with public key technology," In Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks, SASN2004,Washington, DC, USA October, pp. 59–64.

[4] A.K. Das, P. Sharma, S. Chatterjee, J.K. Sing, (2012) "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," J. Network Comput. Appl. 35 (52), pp. 1646–1656.

[5] Ding Wang⇑, Ping Wang, (2014) "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," Ad Hoc Networks, 20, pp. 1–15

[6] Yuan J ,JiangC, JiangZ, (2010) "A biometric-based user authentication for wireless sensor networks," Wuhan University Journal of Natural Sciences ,15(3), pp. 272–276.

[7] G.M. Yang, D.S. Wong, H.X. Wang, X.T. Deng, (2008) "Two-factor mutual authentication based on smart cards and passwords," J. Comput. Syst. Sci. 74 (7), pp. 1160–1172.

[8] D. He, Y. Gao, S. Chan, C. Chen, J. Bu, (2010) "An enhanced two-factor user authentication scheme in wireless sensor networks," Ad Hoc Sensor Wireless Networks 10 (4), pp. 361–371.

[9] H. Yeh, T. Chen, P. Liu, T. Kim, H. Wei, (2011) "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, " Sensors 11 (5), pp. 4767–4779.

[10] C.-C. Lee, C.-T. Li, S. der Chen, (2011) “Two attacks on a two-factor use authentication in wireless sensor networks,” Parallel Process. Lett. 21 (1), pp. 21–26.

[11] P. Kumar, H. Lee, (2011) “Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks,” in: Wireless Advanced, IEEE, pp. 241–245.

[12] D. Sun, J. Li, Z. Feng, Z. Cao, G. Xu, (2013) “On the security and improvement of a two-factor user authentication scheme in wireless sensor networks,” Pers. Ubiquitous Comput. 17 (5), pp. 895–905.

[13] Muhamed Turkanovic´, Boštjan Brumen, Marko Hölbl, (2014) “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion”, Ad Hoc Networks 20, pp. 96–112

[14] K. Romer, F. Mattern, (2004) “The design space of wireless sensor networks,” Wireless Commun., IEEE 11, pp. 54–61.

[15] M. Bottero, B. Dalla Chiara, F.P. Deflorio, (2013) “Wireless sensor networks for traffic monitoring in a logistic centre,” Transp. Res. Part C: Emerg. Technol. 26, pp. 99–124.

[16] A. Pietrabissa, C. Poli, D.G. Ferriero, M. Grigioni, (2013) “Optimal planning of sensor networks for asset tracking in hospital environments,” Decis. Support Syst. 55, pp. 304–313.

[17] M.V. Ramesh, (2014) “Design, development, and deployment of a wireless sensor network for detection of landslides,” Ad Hoc Netw. 13, pp. 2–18.

[18] J. Xu, W.-T. Zhu, D.-G. Feng, (2009) “An improved smart card based password authentication scheme with provable security,” Comput. Stand. Interf. 31, pp. 723–728.

[19] R. Song, (2010) “Advanced smart card based password authentication protocol,” Comput. Stand. Interf. 32, pp. 321–325.

[20] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, (2002) “Wireless sensor networks: a survey,” Comput. Netw. 38, pp. 393–422.

[21] T.H. Chen, W.K. Shih, (2010) “A robust mutual authentication protocol for wireless sensor networks,” Etri J. 32, pp. 704–712.

[22] M.K. Khan, K. Alghathbar, (2010) “Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks,” Sensors 10, pp. 2450–2459.

[23] H.-F. Huang, Y.-F. Chang, C.-H. Liu, (2010) “Enhancement of two-factor user authentication in wireless sensor networks,” in: Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing: IEEE Computer Society, , pp. 27–30.

[24] Das ML. (2009) “Two-factor user authentication in wireless sensor networks,” IEEE Transactions on Wireless Communications, 8(3), pp. 1086–90.

[25] Akyildiz IF,Su W ,Sankarasubramaniam Y, CayirciE, (2002) “Wireless sensor networks: a survey,” Computer Networks, 38(4), pp. 393–422.

[26] C.-T. Li, C.-Y. Weng, C.-C. Lee, (2013) “ An advanced temporal credential based security scheme with mutual authentication and key agreement for wireless sensor networks,” Sensors 13, pp. 9589–9603.

[27] M. Turkanovic´ , M. Hölbl, (2013) “Notes on a temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks’’, Wireless Pers. Commun., pp. 1–16.

[28] D. Wang, C.-G. Ma, (2012) “On the (in)security of some Smart-card-based Password Authentication Schemes for WSN,” Cryptology ePrint Archive, Report 2012/581,. <http://eprint.iacr.org/2012/581.pdf>.

本人受本計畫補助的相關著作

[1] Chuan-Gang Liu*, Yu-Min Huo, I-Hsien Liu, Zhi-Yuan Su,Heng-Hua Liu, Jung-Shian Li (2016), “Novel RFID Blocking Scheme for Staying Tags in Error-Prone Wireless Channel”, NCWIA 2016, 高雄應用科大, 7/15-16

[2] 劉奕賢 盧建同 林長德 張家駿 林禹妡 劉川綱 李忠憲,"混合雲環境的整合式日誌蒐集", TANET 2015

[3] 劉川綱 謝愛家 徐宏修 劉奕賢 黃唯倫, "多閘道感測網路下使用者認證帳號洩漏改善", 2015年全國計算機會議

[4] 劉奕賢 、盧建同、林禹妡、林長德、張家駿、劉川綱、李忠憲, "混合雲日誌蒐集與分析系統", 2015全國電信研討會

[5] Chuan-Gang Liu, Yu-Min Huo, Wei-Li Huang, I-Hsien Liu, Jung-Shian Li(2016), “A new security design concept based on the Authentication protocol and anti-collision algorithm in RFID system” The 5th International Congress on Engineering and Information (ICEAI 2016), Osaka, May 10-12

[6] I-Hsien Liu, Chuan-Gang Liu, Kun-Hsuan Liu, Shun-Hsiung Yu, Zhi-Yuan Su and Jung-Shian Li (2016) “Distributed Node Scheduling Algorithms for Multiple Group Communications in Wireless Multi-hop Networks”, 12th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness”, JULY 7–8, 2016 | SEOUL, SOUTH KOREA

附件六

科技部補助專題研究計畫出席國際學術會議心得報告

日期：105　年 5 月 13　日

計畫編號	MOST　104-2221-E-041-007-		
計畫名稱	基於物聯網概念的感測網路下針對群存取情形之有效率的認證與金鑰協議機制之研究		
出國人員姓名	劉川綱	服務機構及職稱	嘉南藥理大學/副教授
會議時間	105 年 5 月 10 日 至 105 年 5 月 12 日	會議地點	日本大阪
會議名稱	(中文)第五屆工程與資訊國際研討會 (英文)The 5th International Congress on Engineering and Information (ICEAI 2016)		
發表題目	(中文)在 RFID 系統下一個基於認證協定與防碰撞機制的新安全設計概念 (英文)**A new security design concept based on the Authentication protocol and anti-collision algorithm in RFID system**		

一、參加會議經過

此會議已經於往年辦理過多次，是一個定期舉辦的國際研討會，此會議分成兩大主題：工程與資訊方面的議題，本人專門研究資訊網路安全問題,切合此會議資訊議題中的網路與資安議題，

因此本人投稿後，並且被接受，其接受函如圖一所示，此研討會於日本大阪市的大阪國際會議中心舉行，此次行程本人先於 5/8 到日

Acceptance Letter

Dear Chuan Gang Liu,

Thanks for submitting your paper.
On behalf of the Organizing Committee of the ***International Congress on Engineering and Information*** *(ICEAI 2016)*, we are pleased to inform you that the following submission was accepted as one of the Oral in this conference:

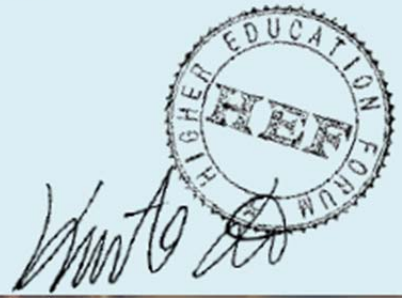
ID: ICEAI-1014
TITLE: A new security design concept based on the Authentication protocol and anti-collision algorithm in RFID system

The registration deadline for presenters is **March 5, 2016**.

Please note that the presenting author should complete the registration process and the payment before the above deadline. If none of the authors complete the registration by the above deadline, this submission will NOT be scheduled in the congress scientific program; furthermore, it will NOT be published in the conference proceedings.

Please note ICEAI is not authorized to assist with the VISA application beyond providing this invitation letter. Should your application be denied, ICEAI cannot change the decision of the Japan Ministry of Foreign Affairs, nor will ICEAI engage in discussion or correspondence with the MOFA or the Embassy of Japan on behalf of the applicant. Please no refund will be issued in any circumstances.

Please feel free to contact us if further information is needed.
We look forward to seeing you at ICEAI in Osaka, Japan.



Yours Sincerely,
The Program Committee of ICEAI 2016

Venue: Osaka International Convention Center
Conference Website: http://www.iceai.org/

圖一： 接受函

本準備，並於 5/13 離開日本，每日行程如下所描述

5 月 8-9 日:搭乘華航班機前往日本大阪，到達日本之後先行到飯

店 check in 並且熟悉日本的環境。

5 月 10 日:到大阪國際會議中心辦理報到並且領取資料,以及跟國際會議人員進行交流。其報到的照片如下所示，

圖二：報告會場

5 月 11 日:本人到國際會議中心聆聽演講並且於下午進行英文口頭報告本人的國際研討會論文內容

5 月 12 日:本人到國際會議中心聆聽演講並且與其他國際研討會人員進行交流

5 月 13 日:搭乘華航班機返回台灣

圖三：發表論文現場

這次參加的會議是亞洲地區為主的研討會，其名稱為第五屆工程與資訊國際研討會（ICEAI 2016），此次會議是匯集國際研究相關之工程與資訊等相關研究項目的文章，ICEAI 已經在亞洲各國辦理過，諸如澳門，上海，北京，日本京都等地，此次會議在日本大阪市國際會議中心舉辦，時間為 105 年 5 月 10 日至 105 年 5 月 12 日，為期三天，此期間來自世界各國的專業人士、各大學院校及研究機構與相關企業之菁英齊聚一堂，共同參與討論及 分享研究成果。此次會議中邀請到幾位知名的專業學者前來演講，此次的會議主題有

工程部分

Aeronautics and Astronautics　　Manufacturing engineering

Aerospace Engineering
Agricultural Engineering
Automotive Engineering
Biomedical Engineering
Ceramic Engineering
Chemical Engineering
Civil Engineering
Coastal engineering
Component Engineering
Computer Engineering
Construction engineering
Earthquake engineering
Electrical Engineering
Electronic Engineering
Environmental Engineering
Fire Protection Engineering
Genetic Engineering
Geotechnical engineering
Industrial Engineering
Instrumentation engineering
Materials engineering
Mechanical engineering
Mechatronics Engineering
Military Engineering
Mining Engineering
Municipal engineering
Naval Architecture
Nuclear Engineering
Ocean Engineering
Software Engineering
Structural engineering
Surveying and geographic information system (GIS)
Test Engineering
Textile engineering
Traffic engineering (transportation)
Transportation engineering
Vehicle Engineering
Water resources engineering (hydraulic engineering and hydrology)
Wind engineering

資訊部分

Advanced Computational Science and Applications
Advanced IT Medical Engineering
Advanced Management Information Systems and Services
Algorithms and Applications
Artificial Intelligence
Aspect Oriented Software Development
GIS Technology and Application
Hardware Computer Design
Human Computer Interface
Information Retrieval Knowledge Data Engineering
Information Security (Communication Security/Network Security/Data Security)

AOSD
Bioinspired Computing and Applications
Computer and network Security
Computer Architecture and VLSI
Computer Networks and Communications
Computer Security
Computer Simulation
Cyber Physical Systems
Data Communications
Data mining applications
Database and Data Mining
Digital Signal and Image Processing
Distance Learning and e- Education
e- Commerce
e- Education
Expert Systems
Information Systems
Internet and its Applications
Internet and Web Applications
Machine Learning
Media and Societal Innovation
Multimedia & Visual Programming
Natural Language Processing
Neural Networks
Parallel & Distributed Systems
Pattern Recognition
Robotics and Automation
Software Engineering
Virtual Reality Systems
Wireless Communication and Mobile Computing
Wireless Sensor Networks

其中本人投稿的主題為 Information Security (Communication Security/Network Security/Data Security)。 發表的題目為“A new security design concept based on the Authentication protocol and anti-collision algorithm in RFID system”大會安排於 5 月 11 日下午四點半到六點在會場內發表。

二、與會心得

本次參加國際研討會，讓本人得以到國外吸取國外先進學者的知識，並且獲知目前最新的網路資訊知識與安全防護的技術，而且在這次參加研討會的過程中，感覺到來自世界各地的研究人員相當努力於自己的研究領域，會場上大家都以英文為主要溝通

語言，並且也會針對論文發表的問題進行詢問，其研究與討論的情形讓本人印象深刻，在此會議也有諸多場次的論文發表，本人也挑了幾場進行聆聽，其中由 Tokyo University of Science 所報告之安全認證，題目為 Student Authentication Method by Update of Face Information in e-Learning System，與本人的研究較為相仿，本人也進行了解與聆聽，了解到目前利用數位學習系統的臉部資訊的認證方法，使本人學習到認證方面的諸多應用。

本次參與國際研討會，除了在會議中學習到的新知之外，針對此次國際會議過程中觀察到日本這個國家的環境與生活嚴謹度確實值得效法，會議結束後，參觀了當地著名的景點之外，本人還參訪當地的古蹟發現給人的感覺相當舒適整齊跟台灣的環境感覺格外不同，希望未來國家一樣可以如此，也對本人研究許下期許，希望可以其他各國菁英一同於網路安全方面貢獻心力

三、發表論文全文或摘要

本篇文章的摘要如下

Abstract

With the trend of IoT, Radio frequency identification (RFID) technique is getting more and more popular. The RFID system is constituted by the database, readers and tags, which the tag should pass the identification procedure of the reader via the identification data in database. During the identification process, the tag is easily exposed to an attacker due to their long sojourn time in RFID system. Usually, there are

two security topics in RFID systems, which are privacy protection authentication protection and anti-collision algorithm. Recently, the researches in RFID systems catch much attention and they usually focus on one topic of them. In this paper, we try to review the papers in both study topics and discuss the new and possible security design way to develop a robust and efficiency security solution in RFID systems. The new security solution in RFID systems is to keep the tag's private information from being revealed or tracked by any adversary when tags communicate with a reader through an unencrypted channel, usually including collision prevention and privacy protection. Our work finds the parameters and anti-collision scheme can be employed in authentication protocol in their respective scheme, which is new and novel security design and is very helpful for enhancing the security in RFID systems. Hence, in this paper, we try to discuss possible combinations of parameters in both authentication and collision prevention algorithm in a new security mechanism design. We believe this work can be an early study of new security solution design and useful in future RFID systems.

Keywords: RFID, IoT, Privacy Protection, Anti-collision, Authentication.

四、建議

此次參加會議，讓本人知道現今國際學術先進的研究最近近況，

並且此本人學習更多領域的知識，因此本人感謝科技部可以補助

經費讓本人可以到國外學習更多最新的網路知識。

五、攜回資料名稱及內容

本次參加會議帶回以下資料

1. 發表論文證明

2. 會議議程手冊

3. 會議註冊費收據

4. 會議論文電子檔（隨身碟）

5. 手提袋

六、其他

科技部補助計畫衍生研發成果推廣資料表

日期:2016/08/29

科技部補助計畫	計畫名稱: 基於物聯網概念的感測網路下針對群存取情形之有效率的認證與金鑰協議機制之研究
	計畫主持人: 劉川綱
	計畫編號: 104-2221-E-041-007- 學門領域: 資訊安全

無研發成果推廣資料

104年度專題研究計畫成果彙整表

計畫主持人：劉川綱	**計畫編號：**104-2221-E-041-007-
計畫名稱：基於物聯網概念的感測網路下針對群存取情形之有效率的認證與金鑰協議機制之研究	

成果項目					量化	單位	質化 （說明：各成果項目請附佐證資料或細項說明，如期刊名稱、年份、卷期、起訖頁數、證號...等）
國內	學術性論文	期刊論文			0	篇	
		研討會論文			4		1.Chuan-Gang Liu*, Yu-Min Huo, I-Hsien Liu, Zhi-Yuan Su, Heng-Hua Liu, Jung-Shian Li (2016), “Novel RFID Blocking Scheme for Staying Tags in Error-Prone Wireless Channel”, NCWIA 2016, 高雄應用科大, 7/15-16 2.劉奕賢 盧建同 林長德 張家駿 林禹妡 劉川綱 李忠憲,"""""""""混合雲環境的整合式日誌蒐集""""""""", TANET 2015 3.劉川綱 謝愛家 徐宏修 劉奕賢 黃唯倫,"""""""""多閘道感測網路下使用者認證帳號洩漏改善""""""""",2015年全國計算機會議 4.劉奕賢 、盧建同、林禹妡、林長德、張家駿、劉川綱、李忠憲, """"混合雲日誌蒐集與分析系統"""" 2015全國電信研討會
		專書			0	本	
		專書論文			0	章	
		技術報告			0	篇	
		其他			0	篇	
	智慧財產權及成果	專利權	發明專利	申請中	0	件	
				已獲得	0		
			新型/設計專利		0		
		商標權			0		
		營業秘密			0		
		積體電路電路布局權			0		
		著作權			0		
		品種權			0		
		其他			0		
	技術移轉	件數			0	件	
		收入			0	千元	
國外	學術性論文	期刊論文			0	篇	
		研討會論文			2		1.Chuan-Gang Liu, Yu-Min Huo, Wei-

						Li Huang, I-Hsien Liu, Jung-Shian Li(2016), “A new security design concept based on the Authentication protocol and anti-collision algorithm in RFID system” The 5th International Congress on Engineering and Information (ICEAI 2016), Osaka, May 10-12 2.I-Hsien Liu, Chuan-Gang Liu, Kun-Hsuan Liu, Shun-Hsiung Yu, Zhi-Yuan Su and Jung-Shian Li (2016) “Distributed Node Scheduling Algorithms for Multiple Group Communications in Wireless Multi-hop Networks”, 12th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness”, JULY 7 - 8, 2016	SEOUL, SOUTH KOREA
		專書			0	本	
		專書論文			0	章	
		技術報告			0	篇	
		其他			0	篇	
	智慧財產權及成果	專利權	發明專利	申請中	0	件	
				已獲得	0		
			新型/設計專利		0		
		商標權			0		
		營業秘密			0		
		積體電路電路布局權			0		
		著作權			0		
		品種權			0		
		其他			0		
	技術移轉	件數			0	件	
		收入			0	千元	
參與計畫人力	本國籍	大專生			3	人次	共計三位大專生參與計畫 嘉南藥理大學資訊多媒體應用系:李政佳,莊長翰,周彥穎
		碩士生			1		共有一位碩士生 成功大學 電通所:蔡金瑞
		博士生			0		
		博士後研究員			0		
		專任助理			0		
	非本國籍	大專生			0		

		碩士生	0		
		博士生	0		
		博士後研究員	0		
		專任助理	0		
其他成果 （無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。）					

科技部補助專題研究計畫成果自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現（簡要敘述成果是否具有政策應用參考價值及具影響公共利益之重大發現）或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估
   ■達成目標
   □未達成目標（請說明，以100字為限）
   　□實驗失敗
   　□因故實驗中斷
   　□其他原因
   說明：

2. 研究成果在學術期刊發表或申請專利等情形（請於其他欄註明專利及技轉之證號、合約、申請及洽談等詳細資訊）
   論文：□已發表　□未發表之文稿　■撰寫中　□無
   專利：□已獲得　□申請中　■無
   技轉：□已技轉　□洽談中　■無
   其他：（以200字為限）
   本計畫產出之論文已計畫投至國際期刊,本計畫部分初期內容亦發表於發表國內研討會NCWIA 2015

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性，以500字為限）
   本計畫提出一個可適用於無線感測網路下一對多的認證及金鑰協議機制，本計畫提出的機制，主要著眼在之前的文獻中提出的認證模型對於未來的物聯網環境是不適合的，我們認為在物聯網環境下所有的物品都應該是相互連接的，那麼在無線感測網路下的使用者在存取這些感測器也應該要直接連接並且存取資料，因此就算是認證機制也應該適用這樣的存取模式，也就是直接跟要認證的感測器進行連接，這樣的方式所代表的意義就是在認證機制下也應該適用物聯網的存取架構才是實際的方式，而且我們的機制主要針對以往一對一認證方式進行改良，因為對於現在的無線感測網路，終端使用者將不再只是要存取一個感測器，而是短時間內要存取多個感測器的資料，因此本計畫的內容對於未來物聯網的使用者認證是很有參考價值得，而且一對多的認證才可以避免無謂的風險與無謂的網路或資源的浪費，未來可以針對物聯網下多閘道感測器環境的感測點擷取攻擊的安全認證機制研發，讓未來物聯網的環境更加安全

4. 主要發現
   本研究具有政策應用參考價值：■否　□是，建議提供機關
   （勾選「是」者，請列舉建議可提供施政參考之業務主管機關）
   本研究具影響公共利益之重大發現：■否　□是

說明：（以150字為限）
本研究屬於理論居多的研究，因此若要成為政策尚有一段路要進行，因此建議再進行更多研究，再來進一步推廣較為適當。然而本研究所提出的認證方式確實有利於發現物聯網的資訊安全認證,尤其未來物聯網勢必成為大眾生活的一部分,
因此具有依舊具有很高的研究價值.