透過安全水準協議與輕量安全機制提昇物聯網的安全性

王順生
朝陽科技大學
工業工程與管理系
副教授
sswang@cyut.edu.tw

王淑卿*
朝陽科技大學
資訊管理系
教授
scwang@cyut.edu.tw

陳慶維
朝陽科技大學
資訊管理系博士班
研究生
s10114901@cyut.edu.tw

*: 聯絡人

摘要

隨著資訊技術不斷演進，以及網路通訊技術的日漸成熟，一個以未來網路的新概念應用於具有感測、網路及運算功能進而發展成智能物件(Smart Object)，使物件與物件能進行資料傳遞，形成新興的網路環境，稱之為物聯網(Internet of Things；IoT)。在物聯網環境下，不僅存在過去網路環境的組件，更加入智能物件，因此將形成數以億計的資料量。然而，龐大的資料量將造成感知層高計算的成本。因此，本研究在感知層使用安全水準協議(Security Level Agreement)的概念來降低計算的成本，並在中介層與感知層之間以數位簽章的概念提出輕量安全機制，經由中介層讓感知層內感測節點的身分具有可驗證性與不可否認性，進而提升物聯網的安全性。

關鍵詞：物聯網、安全水準協議、中介層、數位簽章。

Abstract

Currently, information technology is developing rapidly, and resulting in the vigorous development of the network technology. The new concept of the future network is applied to the smart objects which have sensing, networking and computing abilities, and the ability to transfer data between the objects; the novel network environment is called the Internet of Things (IoT). In addition to the past components of the network environment, there are also smart objects in the IoT. Therefore, there are hundreds of millions of bits in the data of the IoT. However, the huge amount of data that will result high computational cost in the perception layer. Therefore, in this study, the security level agreements are used to reduce the cost of computing in the perception layer. In addition, a framework of middleware layer is proposed to solve the problem, through data filtering and integration to draw meaningful information. However, the digital signature is used to establish a lightweight security mechanism between the application and the perception layer. Through the framework of the middleware layer, the identity of the application and the perception layer will have a verification and non-repudiation, and the security of the IoT can be obtained

Keywords: Internet of Things, Security Level Agreements, Middleware Layer, Digital Signature.

1. 前言

網際網路(Internet)最早應用於電腦間的網際網路(Internet of Computers)，透過點對點(Peer to Peer；P2P)的拓樸架構，形成全球網路(Global Network)的型態，如在全球資訊網(World Wide Web；WWW)的網路平台上提供服務。經數年，人們逐漸成為網際網路環境中的物件，進而生成社群網路(Social Network)的模式，創造出更多商業模式的平台，因此網路型態走向以人為導向的網際網路(Internet of People)[13]。

隨著終端設備的處理能力與儲存容量不斷提升，現今設備逐漸演進成可攜式的行動設備。以及資訊技術與網路環境不斷的改良與創新，促使網路型態越來越多樣化，如無線網路(Wireless Network)、無線感測網路(Wireless Sensor Network)等，進而形成無所不在的網路環境，因此人們的生活正邁向始終連接(Always Connect)的網路世代。

1998 年 12 月網際網路工程任務小組(Internet Engineering Task Force；IETF)從 RFC2460 標準規範定義新的網際網路通訊協

定 IPv6(Internet Protocol version 6)，目的在解決 IPv4 中 32 位元址空間不敷使用的問題，進而定義出 IPv6 擁有 128 位元址大小[43]。IPv6 的實現將使更多物件(Objects)擁有連接網路的能力。因此，一個未來網路(Future Internet)的新概念被廣泛的研究與應用，稱之為物聯網(Internet of Things；IoT) [7][13][30]。

物聯網存在的問題與挑戰大都是過去網路環境中常發生的議題，因為物聯網環境涵蓋的組件(Component)包含現今廣泛被研究的雲端運算及過去所探討的分散式運算、無線網路、無線感測網路及無線射頻技術等網路環境。因此，在物聯網環境下，處理真實世界(Physical World)的資訊將會更加錯綜複雜，甚至將過去於網路環境中探討的議題轉換到物聯網環境時，將會出現顯著的差異性[18]。

其中最主要的差別在於過去的網路環境是以人為導向，然而在物聯網環境下不僅是以人為導向，甚至加入更多多元化的智能物件。除此之外，因物聯網不僅包含網路運算環境外，智能物件更扮演重要角色，當所有智能物件都擁有微量的資料時，便會形成數以億計的資料量，所以物聯網比現存的網際網路將更複雜並具有海量資料(Data Deluge)[13]。

過去已有學者在物聯網中介層(Middleware Layer)的深異質性(Deep Heterogeneity)與未知拓樸架構(Unknown Topology)進行相關的研究[24]，但其研究結果無法解決物聯網環境可能出現不準確的資料、龐大複雜化的資料及資料不安全性的問題。Wang 等學者，已針對上述未被探討的問題提出中介層框架與工作流程，並且制定出感知層與中介層之間的輕量安全機制[25]。

本研究接續 Wang 等學者所提出的中介層框架與安全機制[25]，深入探討在物聯網感知層環境下的安全性。物聯網環境中的感測標籤所隱藏的是微量資料，主要可讓感測節點能快速讀取及識別標籤內的數據。然而有些感測節點能涵蓋的範圍較廣，如果資料在感測過程中被截取頻段，進而取得數據，者進行數據竄改，將導致物聯網內的資訊系統、自動化流程及資料分析機制受到相當程度的影響，如資料被竊取，可能會影響後端系統的安全或改變自動化處理流程等[25]。

由於物聯網環境下存在數以萬計的智能物件，服務供應商可能在一個區域佈署一到多種不同型態的智能物件或一個區域存在多個服務供應商所佈署的智能物件，因此服務供應商必須知道每一個智能物件佈署的位置及身分，才能準確接收真正所需要的資料。物聯網未來將面臨感測節點與驅動設備之間及智能物件與後端系統之間的隱私性(Privacy)、身分管理(Identity Management)、安全性(Security)與存取控制(Access Control)的議題[13]。

除此之外，本研究深入探討感知層內感測節點間資料傳遞過程的安全性問題及訂定適用於 Sink Node 所涵蓋範圍的安全水準協議(Security Level Agreement；SLA)。因為 Sink Node 的涵蓋範圍可能存在數以萬計的感測節點，當所有感測節點都必須進行高安全性加密技術時，可能造成計算量非常龐大；然而，如果使用低安全性加密技術時，距離 Sink Node 較遠的感測節點可能產生資料被竊取的風險。

本研究為了提昇感知層及中介層之間的身分識別，加入數位簽章(Digital Signature)的機制，提供身分的可驗證性(Authentication)與不可否認性(Non-repudiation)，讓應用層的服務透過中介層可以獲知感知層實體物件的身分，及感知層實體物件經由中介層將資料準確傳輸到發出需求的服務。在本研究中，提出一個以 Sink Node 為中心，延伸出一個正六邊形(Hexagon)的涵蓋率(Coverage)，藉以接收感測節點的資料傳遞，並在正六邊形的涵蓋範圍內劃分出安全水準協議，以降低資料被竊取的風險與資料進行加密技術的計算成本。

本研究在第 2 節將說明物聯網的發展與概念、安全水準協議、數位簽章、及無線感測網路的密鑰管理機制，第 3 節說明本研究所提出在物聯網建構的三層式物聯網架構，第 4 節說明物聯網感知層安全水準協議，第 5 節為輕量安全機制的工作流程，最後一節則是結論及未來的工作。

2. 文獻探討

物聯網環境納含眾多的網路運算技術，包含雲端運算、無線感測網路及無線射頻技術。近年來雲端運算的概念逐漸被實現在當前的網路運算環境中，其以龐大的運算與儲存資源，來處理大量的使用者需求。由於無線感測網路與無線射頻技術日漸成熟，使物與物之間能經由網路與感測技術更快速的傳遞資料。

在本節中將說明物聯網的發展與概念，及當前的發展趨勢。再者，因本研究將探討適用於物聯網感知層的安全水準協議，所以將說明從服務水準協議延伸而來的安全水準協議。由

於物聯網感知層最主要的應用技術是無線感測網路，因此將探討無線感測網路的密鑰管理機制。本研究將在感知層與中介層間建立輕量安全機制，因此將說明數位簽章的概念與特性，並應用在本研究中進行資料的識別認證。

2.1 物聯網的發展與概念

物聯網的概念最早由麻省理工學院(Massachusetts Institute of Technology；MIT)在 1999 年提出雛形，其利用無線射頻識別技術(Radio-Frequency Identification；RFID)來結合網際網路架構，從 P2P 擴展成機器對機器(Machine to Machine；M2M)之間的溝通[18][42]。且在 2005 年由國際電信聯盟(International Telecommunications Union；ITU)所提出來，陳述的概念是未來世界的任何物件(Any Thing)將能在任何時間(Any Time)與任何地點(Any Place)相互連接與資訊傳遞，以及物件將具備感知(Sensory)與智能(Intelligent)的功能，涵蓋的範疇包括人與人、物件與物件及人與物件之間的互通。ITU 對物聯網定義出四個維度，分別是項目識別(Item Identification)、感測器與無線感測網路(Sensors and Wireless Sensor Networks)、嵌入式系統(Embedded Systems)及奈米技術(Nano Technology)[41]。

項目識別主要是物件具有可識別身分的標籤(Tags)(如 RFID 或 Quick Response codes(QR-codes)等)，來讓裝載有感測能力的設備進行感測或掃描，以及讓物件之間能相互溝通與傳遞訊息。感測器與無線感測網路則是佈署感測器於區域環境而形成的無線感測網路，負責監測與蒐集區域內的訊息，或探勘有用的資訊。嵌入式系統則應用於感測節點或物件中，主要賦予運算、儲存、感測與傳輸的能力，進而形成智能環境。奈米技術是未來物聯網核心技術之一，透過奈米技術將可提升物聯網環境中設備的效能，無論是感測器或智能物件，將有助於物聯網的發展。

近幾年各國政府將物聯網的建置與應用視為國家未來的戰略計畫之一，更以階段的方式來規劃未來數年網路基礎設施的建置，以實現物聯網的環境與服務，包括美國[32][40]、歐盟[39]、南韓[35]、日本[33]、中國[38]與台灣[34][37]等國家。各國政府開始著重於物聯網相關技術的發展與基礎設施的建置，並且以無所不在為目標持續進行研究。

除了各國政府努力推動物聯網的相關計畫外，業界也紛紛開始建立物聯網的雛形架構，如美國 Wal-Mart 超級市場[20][44]、台灣全家便利商店[32]及基隆港-台北港務分局港口業務[36]等領域，主要目的在於減少成本開銷、節約能源及提升流程效率。

由於物聯網目前處於正在發展的階段，不同通訊、感測節點與協定仍存在標準不一致的現象，使得物聯網處於難以擴展的階段，將是未來研究與挑戰的議題。再者，雲端運算從 2009 年至今，相關技術已日漸成熟，各個國家已將雲端運算與物聯網結合成新型態的應用[15]。雲端運算的環境佈署成物聯網後端計算與分析的資源池，藉由雲端運算的效能來更快速處理物聯網中所產生的海量資料。

2.2 安全水準協議

由於資訊科技技術的進步，企業逐漸利用資訊科技來輔助企業內外部的營運，將過往紙本或本機上的各種業務，經由區域網路或廣域網路的方式，形成 e 化的作業環境。此外，企業除了自建 e 化環境的基礎設施，更能倚賴提供租賃(Leased)或外包(Outsourced)的軟硬體供應商，來完成企業 e 化的建置，以降低 e 化的建置成本[8]。

因此，企業與軟硬體供應商皆會共同簽署服務水準協議(Service Level Agreements；SLAs)，來得知軟硬體供應商是否有確實提供企業的需求，但是企業往往只知道軟硬體供應商可以提供的功能與規格，卻無法從服務水準協議得知軟硬體供應商給予的安全程度。因此，許多研究開始探討服務水準協議與安全程度進行結合，讓企業可以得知資料或系統放置在軟硬體供應商是具有安全性[8]。

近年來，雲端運算概念與科技技術逐漸實踐在現今的網際網路服務及企業本身，藉此提供與擁有更多元化的網路服務，包括基礎設施即服務(Infrastructure as a Service；IaaS)、平台即服務(Platform as a Service；PaaS)及軟體即服務(Software as a Service；SaaS)。

過去服務水準協議已在服務導向架構(Service Oriented Architectures；SOA)及網路服務(Web Services)被考量[2][10]，在雲端運算的環境下，更是雲端運算興起的組成之一。因為雲端運算的趨勢，是經由網際網路的方式，讓需求者與供應商進行需求與功能的建置，因此必須訂定出兩方角色不可否認的契約內容，但供應商在服務水準協議上並沒強調需求者所

能得到的安全程度[12]。

歐洲網路與資訊安全局(European Network and Information Security Agency；ENISA)認定雲端運算環境服務水準協議必須具備不同層級安全程度，制定適用於雲端運算環境的服務水準協議(Cloud Security Level Agreements；SecLA)，因此服務水準協議的合同為解決歐洲雲端運算策略的重要方針[6]。

物聯網環境下的感知層存在許多不同性質的感測節點，感測節點包括感測器、使用者使用的行動感測裝置及許多微控制器等設備。因此在一區域內可能涵蓋數以萬計的感測裝置，所以本研究將根據安全水準協議訂定適用於物聯網感知層的安全水準協議，以確保資料傳輸過程是具有安全性，及有效改善資料量龐大而造成計算成本增加的問題。

2.3 數位簽章

數位簽章為電子簽章(Electronic Signature)中的其中一種技術，電子簽章的定義指以電子形式存在，依附在電子文件並與其邏輯相關，可用以辨識電子文件簽署者身分及表示簽署者同意電子文件內容。數位簽章是使用雜湊函數(Hash Function)，將電子文件轉為固定長度的數位資料(稱之為訊息摘要(Message Digest)，以簽署者的私密金鑰對其加密形成一簽體，使任何人可使用未轉化前的原始資料訊息、簽體及與私鑰相關連之公鑰，驗證該簽體是否使用與簽章公鑰相對應的私鑰製作，以及簽體制作後，原始資料訊息是否遭受竄改[1]。

數位簽章必須具備三項特性與六項條件，三項特性：(1)驗證簽章的作者、日期與時間；(2)在簽章的同時，必須能夠確認訊息的內容；(3)發生爭議時，簽章可經由第三方驗證來解決。六項條件：(1)數位簽章取決於簽署過的訊息；(2)數位簽章必須使用傳送者獨有的資訊，可以預防偽造與否認的發生；(3)數位簽章必須容易產生；(4)數位簽章必須容易簽章與驗章；(5)數位簽章無法經由計算的方式來偽造；(6)數位簽章的副本必須能保留於記憶體。因此，數位簽章具有身分鑑定性與不可否認性[21][22]。

數位簽章的方法可被歸類為兩大類，分別為直接式數位簽章與仲裁式數位簽章。

直接式數位簽章只有來源端與目的端參與，並且目的端擁有來源端的公開金鑰，執行流程由來源端以私密金鑰簽署欲傳送的訊息或以雜湊值進行加密。若要達到資料機密性，則可先簽署數位簽章，再利用目的端的公開金鑰進行加密。但直接式數位簽章的缺點是只建立來源端私密金鑰的安全性，如果來源端遺失私密金鑰，將可能否認訊息的傳送。

仲裁式數位簽章在來源端與目的端之間建立仲裁者，當來源端傳送訊息給目的端，仲裁者便驗證來源端已簽署的訊息，並附上時間戳記傳送給目的端，仲裁者可經由信任系統(Trusted System)來實作，或者使用對稱式或公開金鑰加密法來實作。因此，仲裁式數位簽章可以解決直接式數位簽章的缺點[21][22]。

2.4 無線感測網路的密鑰管理機制

無線感測網路的環境是由一個大量空間分布(Spatially Distributed)的小型設備所組成，主要負責協同監測環境條件及將蒐集的資料發送給命令中心(Command Center)。小型的設備通稱為感測節點、感測器、無線通訊設備或小型微控制器等設備[29]。無線感測網路是物聯網感知層的重要組件，主要負責區域性資料的蒐集。無線感測網路過去經常被應用在軍事與民生領域，包括戰場監測(Battlefield Surveillance)、動植物棲息地監測(Habitat Monitoring)、醫療保健(Healthcare)及交通控制(Traffic Control)等應用範疇。由於無線感測網路是基於在無線網路的環境下進行資料間的傳遞，因此在資料傳輸的過程或感測節點本身可能會遭受到不同類型的惡意攻擊或接收到誤導性的資料，如資料被偽造、感測節點身分被仿冒或資料被截取等攻擊。

近年來，無線感測網路的安全議題已廣泛被探討，學者將密鑰的管理分成不同的類別[10][4][3][17][23][26]，部分研究是探討加解密技術(Encryption Techniques)及密鑰建立機制(Key Establishment Mechanism)[29]。

加解密技術一般可被分為對稱式(Symmetric)加解密技術、非對稱式(Asymmetric)加解密技術及混合式(Hybrid)加解密技術。對稱式加解密技術因在加解密過程所需要的計算能力與時間複雜度較低，適合應用在低成本的感測節點上，因此廣泛被應用在無線感測網路環境。換句話說，對稱式加解密技術能提供強壯的安全強度，需要更多的計算能力，因此感測節點需要更大的計算與儲存能力，但是需要花費更多設備建置的成本。

因此本研究採用對稱式加密技術中的仲裁式密鑰，藉以解決物聯網感知層中感測節點進行資料傳輸的安全性問題。仲裁式密鑰的建立是基於一個信任的實體，因此有三個策略可執行密鑰的建立，其中主密鑰的生成基於預先配置策略[5]、基站參與策略[16]、及第三方可信任節點策略[5]。

在密鑰的生成基於預先配置策略中，分為主密鑰與溝通密鑰。主密鑰必須預先被分配和儲存在無線網路環境的感測節點，如果感測節點之間需要互相溝通時，則經由主密鑰與一組亂數值進行交換，獲得感測節點之間的溝通密鑰。生成基於預先配置策略的好處是具有無限可擴展性及感測節點不需太大的儲存體。然而缺點是如果主密鑰被竊取時，溝通密鑰則會被獲得[9]。如果要改善此策略，則必須在產生溝通密鑰時，替換原本的主密鑰，但這種策略則會造成無線感測網路的複雜性提高[31]。

在基站參與策略中，每一個感測節點與基站共享一個密鑰。當兩個節點需要溝通時，基站必須送出加密後的共享密鑰。換言之，基站參與策略具有完善的應變能力，但缺乏好的可擴展性[16]。

在第三方可信任節點策略中，兩個感測節點之間的密鑰建立，則是基於第三方具有公信力的節點來生成[5]，因此在密鑰的管理與建立上，皆經由第三方運行，感測節點本身無須太大的計算量以及能力。

3. 三層式物聯網架構

本研究所定義的物聯網拓樸架構，主要由各區域所部屬的Sink Node負責蒐集雲端服務供應商的需求，每一個區域存在不同服務的感測節點，每個網路服務將對應一至多個感知層設備的拓樸架構。中介層在本研究的定義為負責雲端端口的資料認證與處理，並且透過中介層來管理每個感測節點的金鑰與簽章的存放，如圖1所示。

本研究所提出的三層式物聯網架構，由上而下分別為應用層(Application Layer)、中介層(Middleware Layer)及感知層(Perception Layer)。應用層為多元化網路服務，包含當前存在的網路服務及由物聯網的智能物件延伸而來的網路服務。兩層之間以中介層來進行資訊傳遞與資料認證與處理，經由設備與服務監控代理人(Devices and Services Monitoring Agent)及認證中心(Authentication Center)來進行資料的認證，認證的歷程與簽章將會被記錄在資訊日誌(Information Logging)中。當認證成功的資料將會由事件識別(Event Identification)、通訊管理(Communication Management)、策略管理(Policy Management)及遠端管理(Remote Management)進行資料的處理程序，資料經中介層處理後，便經由中介層與應用層之間的輕量安全機制，把資料傳送到應用層上的服務供應商，如圖2所示。

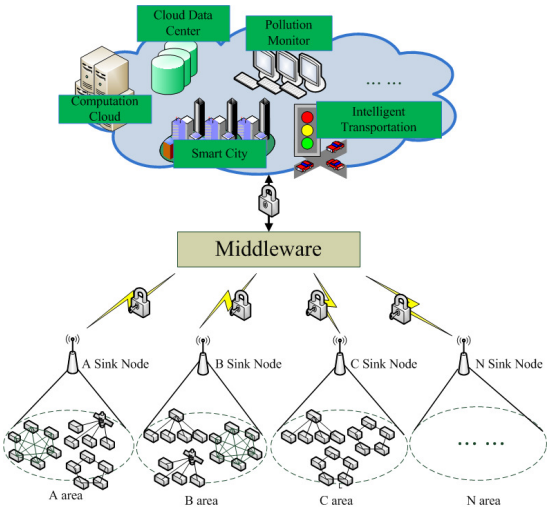

圖 1 物聯網的拓樸架構

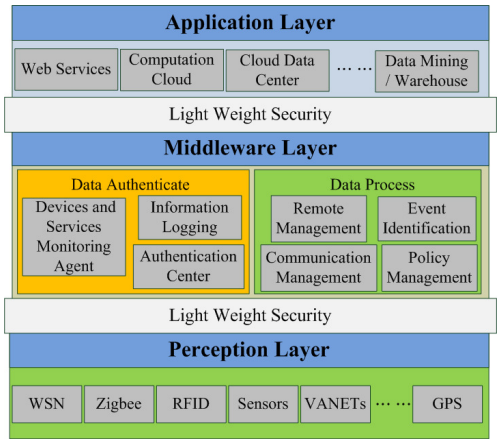

圖 2 三層式物聯網架構圖

當應用層經由中介層向感知層發出資料需求，應用層會發送服務識別身分給中介層，然後感知層蒐集到的資料會透過輕量的安全機制(Light Weight Security)，讓中介層能識別數據封包的來源端，並且以適合感知層的加密格式來提高封包傳遞的安全性。當感知層的資料經由中介層處理完後，中介層則會依應用層每一個服務的識別，經由屬於兩者之間的輕量

的安全機制，將處理完的資料回傳到應用層，以進行後續的相關應用服務。

4.物聯網感知層安全水準協議

本研究利用正六邊形涵蓋範圍的概念，規劃適合於感知層安全水準協議的機制。六邊形涵蓋率經常被應用在無線網路的環境[19][28]，如第三代行動通訊技術(3rd Generation；3G)、LTE(Long Term Evolution)與WiMax(Worldwide Interoperability for Microwave Access)。六邊形是由圓形延伸而來的概念，因此六邊形每個對角與中心的距離相等。換言之，六邊形是由六個等腰三角形組成。無線網路環境使用六邊形的原因是六邊形與六邊形之間是相鄰且趨近於無縫涵蓋範圍，因此能讓行動節點或資料進行無縫傳輸。

本研究在正六邊形的涵蓋率下，建置適合於物聯網感知層的安全水平協議。為了減少中心點Sink Node負載量過大及加密計算時間過長，因此劃分出三階段安全水平協議。在初始定義上，從中心點到最外層相連接的1/3邊長連結而成的六個等腰三角形大小為Level 1的涵蓋範圍，Level 2則是2/3的邊長連結而成的六個三角形大小，Level 3則是整個正六邊形的大小，如圖3所示。

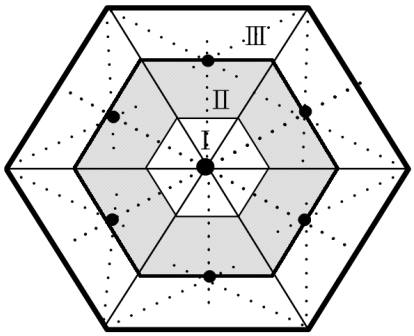

圖 3 三階段安全水平協議

Level 1的安全水準協議是最接近中心點，正常情況下所涵蓋的感測節點數量最少，且Sink Node位在Level 1的範圍內，因此Level 1範圍內的感測節點最接近Sink Node，所需的加解密技術無需太複雜。因此，本研究針對在Level 1範圍內的感測節點使用雜湊函數 $h(.)$，將需要進行傳輸的資料 *OM* 進行加密。

Level 2涵蓋的感測節點數量比Level 1來得多，而且離Sink Node的距離比Leve1來得遠，因此制定Level 2的安全水準協議，則須經由Sink Node生成出介於Level 1與Level 2之間的感測節點的密鑰。在Level 2中的每個感測節點在傳遞資料到Sink Node時，除了將資料進行 $h(OM)$外，必須使用由Sink Node生成的密鑰進行傳輸，所以最終傳輸的加密結果為$[K_{l2,Si} \| h(OM)]$。

Level 3涵蓋的範圍最廣，亦即Level 3與Level 2之間的感測節點數量最多，因為資料數量龐大，因此進行加密時將耗費相當大的計算成本，所以在進行資料加密時不宜使用繁雜的加密技術。但如果使用過於簡易的加密技術，則資料在傳遞到Sink Node的過程中，可能會造成被竊取或竄改資料的風險。

因此，本研究從Sink Node的總涵蓋率去計算每一個等腰三角形的重心，來做為多重行動代理節點(multi-Mobile Agent Node；multi-MAN)。multi-MAN負責接收每一個等腰三角形下Level 3涵蓋範圍內感測節點的資料，每個multi-MAN則會擁有Sink Node產生的密鑰 $K_{l3,MANi}$，再將資料加密後的結果$[K_{l2,MANi} \| h(OM)]$傳遞到Sink Node。最後，Sink Node將把所接收的資料進行整合，傳送到中介層進行資料的認證與處理，表1為本研究輕量安全機制使用到的數學符號表參數。

5.輕量安全機制的工作流程

本研究在感知層與中介層間，應用數位簽章獲得感知層中感測節點的身分資訊，以確保資料的可靠性。因此，採用數位簽章內的第三方仲裁式方法，經由中介層為第三方認證來進行來源端與目的端雙方的資料傳輸。

$K_{SNi,MW}$, K_{SNi} 與 K_{AC} 的生成

在本研究的架構中，感知層必須經由中介層進行身分的驗證。*SN* 與 *MW* 之間會動態生成一把會議金鑰 $K_{SNi,MW}$。$K_{SNi,MW}$ 的生成方式是把 K_{SNi} 與 K_{mw} 進行XOR轉換，此會議金鑰主要建立 *SN* 與 *MW* 安全的溝通管道。*SN* 傳送的 *OM* 將會透過會議金鑰進行訊息加密，因為 *SN* 的 K_{SNi} 可能有被破解的風險，因此在傳輸過程加入會議金鑰，主要提升 *SN* 與 *MW* 傳輸過程中的安全性。

Table 1. 輕量安全機制之數學符號表

MW	中介層(Middle Ware)
DSMA	中介層內的服務與設備監控

	代理人
SN_i	Sink Node i 的身分識別碼
AC	中介層內的認證中心
$r_{DSMA}(.)$	亂數產生函式，使用 $DSMA$ 的私密金鑰
K_{SNi}	SN_i 與 $DSMA$ 所分享的一把私密金鑰
K_{AC}	AC 與 $DSMA$ 所分享的一把私密金鑰
K_{MW}	MW 與 $DSMA$ 所分享的一把私密金鑰
$K_{SNi,MW}$	SN_i 與 MW 產生一把會議金鑰 (Session Key)
$E(K,[OM])$	使用金鑰 K 加密訊息 OM
$h(.)$	雜湊函數
TS	時間戳記
OM	SN_i 傳送給 MW 的原始訊息 (Original Message)
SRy	服務供應商 y 發出蒐集資料的需求
$DSMA_{pro}$	$DSMA$ 發出探查 (probe) 訊息，要求 SN_i 傳送資料
ACK_{req}	AC 發出私密金鑰更新的需求
$SN_{i,areq}$	SN_i 發出主動傳送資料的需求

首先$DSMA$開始計算每一個區域SN_i的私密金鑰 $r_{DMA}(SN_i)$與 AC 的私密金鑰 $r_{DMA}(AC)$，並且分別載入到感測節點 SN_i 以及認證節點 AC，形成 K_{SNi} 與 K_{AC}。

認證階段

$SN_i \rightarrow DSMA$: $OM \| E(K_{SNi}, K_{SNi,MW}, [SN_i \| h(OM)])$

$DSMA \rightarrow AC$: $E(K_{AC}, [SN_i \| OM \| E(K_{SNi}, (K_{SNi,MW}), [SN_i \| h(OM)]) \| TS])$

Sink Node SN_i 蒐集到的資料會經由雜湊演算法 $h(.)$將 OM 轉為固定長度的訊息摘要 $h(OM)$，以 SN_i 的私密金鑰 K_{SNi} 以及 SN_i 與中介層 MW 共同擁有的 $K_{SNi,MW}$ 對其加密形成一簽體，傳送到中介層中的設備與服務監控代理人$DSMA$以及認證節點AC來進行認證與程序的處理。SN_i 擁有 K_{SNi} 是經由 $DSMA$ 產生而來，因此 $DSMA$ 先進行第一階段 K_{SNi} 以及 $K_{SNi,MW}$ 認證，確認 SN_i 的身分。接續 $DSMA$ 將驗證後的訊息傳送到 AC，AC 經由 $DSMA$ 產生而來的 K_{AC} 取得 SN_i 的明文，並且將簽章 $E(K_{SNi}, (K_{SNi,MW}), [SN_i \| h(OM)])$ 以及時間戳記 TS 儲存在資訊日誌，明文資料將由中介層各程序進行資料處理。

本研究所提出的認證流程有兩種情境，圖 4 所示為本研究所提出的資料認證流程：

(1) 服務供應商或$DSMA$發出探查(probe)訊息進行蒐集資料。

(1.1)

(a) 當服務供應商需要感知層設備的資料時，會經由 $DSMA$ 傳送通知訊息給 SN_i。在通知訊息中 $DSMA$ 寫入服務供應商的需求 SR_y，K_{SNi} 是 $DSMA$ 生成給 SN_i 新的私密金鑰，替換原有的 K_{SNi}，及中介層的私密金鑰 K_{MW}，主要與 SN_i 原有的 K_{SNi} 進行 XOR 來產生會議金鑰。

(b) $DSMA$ 會週期性的要求各區域 SN_i 傳送資料。因此，$DSMA$ 發出探查(probe)訊息的請求，在訊息中寫入中介層的私密金鑰 K_{MW}，主要與 SN_i 原有的 K_{SNi} 進行 XOR 來產生會議金鑰。

(1.2) SN_i 蒐集好原始資料後，以 $h(.)$將明文形成固定長度的訊息摘要，並且回傳 SN_i 認證後的 K_{SNi}，及 XOR 後的會議金鑰 $K_{SNi, MW}$，傳送到 $DSMA$。

(1.3) $DSNA$ 以 AC 的私密金鑰 K_{AC}，將 SN_i 加密後的資料再一次進行加密，並且傳送經 $DSNA$ 認證後的 K_{SNi} 與 $K_{SNi,MW}$，及時間戳記 TS 給 AC。

(1.4)

(a) AC 比對 K_{AC}、K_{SNi} 與 $K_{SNi,MW}$ 是否正確，如正確的話，則會將從 SN_i 經 $DSNA$ 到 AC 的簽章儲存在資訊日誌。

(b) 回傳 AC 私密金鑰更新的訊息。

(1.5) (1.5a)與(1.5b)同步更新 Sn_i 與 AC 的私密金鑰。

接續由 SN_i 主動發出資料傳送的需求，在物聯網環境下除了周期性蒐集感知層的資料外，感知層的感測設備具有智能化的功能，當發生不合理的數據時，則必須立刻傳輸到中介層進行資料分析與處理。

(2) SN_i 蒐集到急迫性的資料必須立即經由 $DSMA$ 認證並且傳輸服務供應商。

(2.1) SN_i 主動發出經加密後的資料傳

送需求 $SN_{i,areq}$ 給 *DSMA*。

(2.2) *DSMA* 確定 SN_i 身分後便回傳新的 K_{SNi} 以及中介層的私密金鑰 K_{MW}。

(2.3) SN_i 蒐集好原始資料後，以 *h(.)*將明文形成固定長度的訊息摘要，並且回傳 SN_i 認證後的 K_{SNi}，及 XOR 後的會議金鑰 $K_{SNi,\ MW}$，傳送到 *DSMA*。

(2.4) *DSNA* 以 *AC* 的私密金鑰 K_{AC}，將 SN_i 加密後的資料再一次進行加密，並且傳送經 *DSNA* 認證後的 K_{SNi} 與 $K_{SNi,MW}$，及時間戳記 *TS* 給 *AC*。

(2.5)

(a) *AC* 比對 K_{AC}、K_{SNi} 與 $K_{SNi,MW}$ 是否正確，如正確的話，則會將從 SN_i 經 *DSNA* 到 *AC* 的簽章儲存在資訊日誌。

(b) 回傳 *AC* 私密金鑰更新的訊息。

(2.6) (2.6a)與(2.6b)同步更新 Sn_i 與 *AC* 的私密金鑰。。

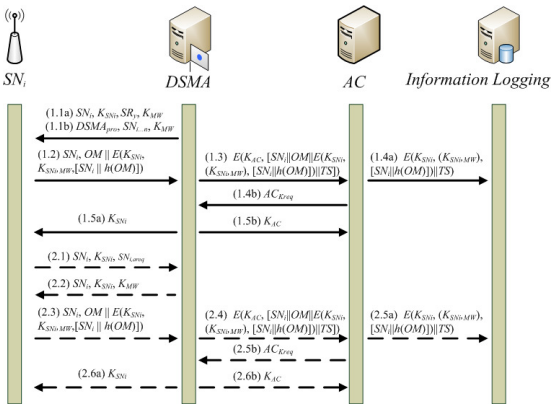

圖 4 資料認證流程

6.結論與未來研究

由於物聯網環境存在數以萬計的智能物件，所以可能會產生海量的資料量。為了讓服務供應商與需求者能確保在物聯網環境下能安全的進行資料傳遞，因此，會使用加密技術來保全資料的完整性，但是當每一筆資料都必須進行安全加密時，將會造成物聯網感知層計算成本的提高，以及造成 Sink Node 本身負載量太大。因此，本研究在物聯網感知層中，提出基於正六邊形的安全水準協議，經由三階段安全水準協議來分擔物聯網環境中所擁有的資料量，利用各階段屬性的不同，簡化加密技術，以降低感知層的計算成本，並且仍具有相對的安全保護。

除此之外，本研究在感知層與中介層之間使用仲裁式數位簽章架構及對稱式加密法來傳輸資料，經由 *DSMA* 生成 SN_i 與 *AC* 兩方的私密金鑰及 SN_i 與 *MW* 之間的會議金鑰。因此 SN_i 將蒐集的資料傳輸到中介層時，必須擁有 *DSMA* 所發佈的私密金鑰才能進行資料的傳輸。為了避免 K_{SNi} 被攻擊者竊取與解密，本研究在在傳輸過程額外加入 SN_i 與 *MW* 共同擁有的 $K_{SNi,MW}$ 來保證資料的完整性、身分的可驗證性及不可否認性的原則，並且將傳輸過程產生的簽章及時間戳記儲存在中介層的資訊日誌，來證明資料的可信任程度。

由於本研究提出在物聯網安全水準協議是初步的概念，目前僅考量到資料傳遞時可能發生的威脅，未來將持續探究 Sink Node 的備援節點機制及跨區域資料的傳遞，以建立更完整的物聯網安全水準協議。

致謝

這篇論文是國科會計畫 NSC102-2221-E-324 -008 研究成果的一部份，在此我們感謝國科會經費支持這個計畫的研究。

參考文獻

[1] 謝銘祥、陳群顯，***電子簽章法之研究***，碩士論文，東吳大學法律學系研究所，2000。

[2] Andrieux, A., Karl, C., Dan, A., Keahey, K., Ludwig, H., Nakata, T., Pruyne, J., Rofrano, J., Tuecke, S. and Xu, M., "Web Services Agreement Specification (WS-Agreement)," ***Global Grid Forum***, Vol. 2, 2004.

[3] Boyle, D., Kim, S. and *Newe*, T., "Securing Wireless Sensor Networks: Security Architectures," ***Journal of Networks***, Vol. 3, No. 1 pp. 7, Jan. 2008.

[4] Camtepte, SA. and Yener, B., "Key Distribution Mechanisms for Wireless Sensor Networks: A Survey," ***Technical report TR-05-07***, 2005.

[5] Chan, H. and Perrig, A., "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," ***The 24th annual joint***

conference of the IEEE computer and communications societies, Vol. 1, pp. 524-535, Mar. 2005.

[6] Dekker, M. and Hogben, G., "Survey and Analysis of Security Parameters in Cloud SLAs Across the European Public Sector," ***Survey and analysis of security parameters in cloud SLAs across the European public sector***, 2011.

[7] Gavras, A., Karila, A., Fdida, S., May, M. and Potts, M., "Future Internet Research and Experimentation," ***ACM SIGCOMM Computer Communication Review***, Vol. 37, No. 3, pp.89-92, 2007.

[8] Henning, R., "Security Service Level Agreements: Quantifiable Security for the Enterprise?," ***The ACM Workshop on New security paradigms***, pp. 54-60, 1999.

[9] Lai, B., Kim, S. and Verbauwhede, I., "Scalable session key construction protocol for wireless sensor networks," ***IEEE Workshop on Large Scale RealTime and Embedded Systems,*** pp. 7, 2002.

[10] Lee, H., Kim, YH., Lee, DH. and Lim, J., "Classification of key management schemes for wireless sensor networks," ***International Workshop on Application and Security service in Web and pervAsive eNvironments***, Vol. 4537, pp. 664-673, June 2007.

[11] Ludwig, H., Keller, A., Dan, A., King, R.P. and Frank, R., "Web service level agreement (WSLA) language specification," ***IBM Corporation***, pp. 54-60, 2003.

[12] Luna, J., Ghani, H., Vateva, T. and Suri, N., "Quantitative Assessment of Cloud Security Level Agreements: A Case Study," ***Security and Cryptography***, pp. 64-73, 2012.

[13] Louis, C. and Johan, E., "The Internet of Things – Promise for the Future? An Introduction," ***The IST-Africa Conference Proceedings***, pp.1-9, 2011.

[14] Massaguer, D., Hore, B., Diallo, M., Mehrotra, S. and Venkatasubramanian, N., "Middleware for Pervasive Spaces: Balancing Privacy and Utility," ***Lecture Notes in Computer Science (LNCS)***, Vol. 5896, pp. 247-267, 2009.

[15] Neil, G., Raffi, K. and Danny, C., "The Internet of Things," ***In the Scientific American***, 27 Sep. 2004.

[16] Perrig, A., Szewczyk, R., Wen, V., Cullar, D. and Tygar, JD., "SPINS: Security Protocols for Sensor Networks," ***Wireless Networks***, Vol. 8, No. 5, pp. 521-534, Sep. 2002.

[17] Ren, X. and Yu, H., "Security Mechanisms for Wireless Sensor Networks," ***International Journal of Computer Science and Network Security***, Vol. 6, No. 3, pp. 155-156, Mar. 2006.

[18] Sarma, S. E., Weis, S. A. and Engels, D. W., "RFID Systems and Security and Privacy Implications," ***The 4th International Workshop on Cryptographic Hardware and Embedded Systems***, pp.454-469, 2002.

[19] Schoenen, R. and Walke,, B.H., "On PHY and MAC Performance of 3G-LTE in a Multi-hop Cellular Environment," ***International Conference on Wireless Communications, Networking and Mobile Computing***, pp. 926-929, Oct. 2007.

[20] Songini, M., "Wal-Mart Shifts RFID Plans", ***Computerworld***, Vol. 41, No. 9, pp.14, 2007.

[21] Stallings, W., ***Network Security Essentials: Applications and Standards***, 4th ed, Prentice Hall, 2010.

[22] Stallings, W., ***Cryptography and Network Security Principles and Practice***, 5th ed, Prentice Hall, 2010.

[23] Sun, D. and He, B., "Review of Key Management Mechanisms in Wireless Sensor Networks," ***Acta Automatica Sinica***, Vol. 23, No. 12, pp. 900-906, Nov. 2006.

[24] Thiago, T., Sara, H., Val´erie, I., and Nikolaos, G., "Service Oriented Middleware for the Internet of Things: A Perspective," ***Towards a Service-Based Internet Lecture Notes in Computer Science***, Vol. 6994, pp 220-229, 2011.

[25] Wang, S.C., Chen, C.W., Wang, S.S. and Yan, K.Q., "To Achieve Data Availability and Reliability by a Middleware Framework Underlying the IoT Environment," ***The 2014 International Conference on Business and Information***, 2013.

[26] Xiao, Y., "Security in Distributed, Grid, Mobile and Pervasive Computing," ***CRC Press***, Auerbach Publications, 2006.

[27] Xue, Y., Zhihua, L., Zhenmin, G. and Haitao, Z., "A Multi-layer Security Model for Internet of Things," ***Internet of Things***

Communications in Computer and Information Science, Vol. 312, pp 388-393, 2012.

[28] Yen, S.P., Talwar, S., Lee, S.C. and Kim, H., "WiMAX Femtocells: a Perspective on Network Architecture, Capacity, and Coverage," ***IEEE Communications Magazine***, Vol. 46, No. 10, pp. 58-65, Oct. 2008.

[29] Zhang, J. and Varadharajan, V., "Wireless Sensor Network Key Management Survey and Taxonomy," ***Journal of Network and Computer Applications***, Vol. 33, No. 2, pp.63-75, Mar. 2010.

[30] Zhou, Q. and Zhang, J., "Research Prospect of Internet of Things Geography," ***The 19th International Conference on Geoinformatics***, pp.1-5, 2011.

[31] Zhu, S., Setia, S. and Jajodia, S., "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks," ***The tenth ACM conference on computer and communications security***, pp. 62-72, Oct. 2003.

[32] 工業技術研究院-全家便利商店, 2008, http://www.itri.org.tw/chi/publication/pdf/205/205_focus.pdf.

[33] 日本資訊通信產業總務省(MIC), 2012, http://www.libnet.sh.cn:82/gate/big5/www.soumu.go.jp/menu_seisaku/ict/u-japan_en/index.html.

[34] 行政院科技會報, 2012, http://www.bost.ey. gov.tw/News_Content.aspx?n=5331137415276DD6&s=3304410EBA0B3188.

[35] 南韓通信委員會(KCSC), 2012, http://www.libnet.sh.cn:82/gate/big5/www.kocsc.or.kr/eng/01_About/Message.php.

[36] 財團法人資訊工業策進會-台北港務分局, 2010, http://www.iii.org.tw/service/3_1_1_c.aspx?id=670.

[37] 經濟研究院(Taiwan Institute of Economic Research), 2012, http://www.tier.org.tw/comment/tiermon201008.asp.

[38] 電子&電腦資訊網, 2012, http://www.compotechasia.com/a/__/2012/0314/21082.html.

[39] European Commission, "ICT in FP7" http://www.libnet.sh.cn:82/gate/big5/cordis.europa.eu/fp7/ict/.

[40] IBM, "Smarter Planet - United States", Nov. 2010, http://www.ibm.com/smarterplanet/us/en/.

[41] International Telecommunications Union, ITU Internet Reports 2005: The Internet of Things. Executive Summary, Geneva: ITU, 2005.

[42] MIT, "MIT Auto-ID Laboratory," 2010, http://autoid.mit.edu/cs/.

[43] RFC2460-"IPv6" 1998, http://tools.ietf.org/html/rfc2460.

[44] Wal-mart, 2008, http://corporate.walmart.com/.