透過中介層機制
達到資料在物聯網下的可用性與安全性

王淑卿	陳慶維	王順生*	嚴國慶*
朝陽科技大學	朝陽科技大學	朝陽科技大學	朝陽科技大學
資訊管理系	資訊管理系博士班	工業工程與管理系	企業管理系
教授	研究生	副教授	教授
scwang@cyut.edu.tw	s10114901@ cyut.edu.tw	sswang@cyut.edu.tw	kqyan@cyut.edu.tw

*: 聯絡人

摘要

隨著資訊技術不斷演進，以及 IPv6 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、網路以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。由於過去有關物聯網中介層之研究，無法解決物聯網環境可能出現不準確的資料、龐大複雜化的資料以及資料不安全性的問題。因此，本研究提出一個中介層框架來進行感知層資料的過濾與整合，以獲得有意義的資訊，且在應用層與感知層之間，以數位簽章的概念提出輕量安全機制，經由中介層讓兩層的身分具有可驗證性與不可否認性，進而實現物聯網環境的可用性與可靠性。

關鍵詞：物聯網、中介層、數位簽章。

Abstract

Nowadays, information technology are developing rapidly, and resulting in the vigorous development of the IPv6. The new concept of the future network applied to the smart objects which have sense, network and compute ability, and transfer of data between the objects, the novel network environment is called Internet of Things (IoT). There are not only existed past components of the network environment, but also have the smart objects in the IoT. Therefore, there are hundreds of millions of the amount of data in the IoT. The past researches of middleware layer in the IoT have not discussed the inaccurate information, large and complex information and data insecurity issues. Thus, a framework of middleware layer is proposed to solve the problem, through data filtering and integration to draw meaningful information. In addition, the digital signature is used to establish a lightweight security mechanism between the application and the perception layer. Through the framework of middleware layer, the identity of the application and the perception layer will have a verifiable and non-repudiation, and the availability and reliability of the IoT can be obtained.

Keywords: Internet of Things, Middleware Layer, Digital Signature.

1. 前言

網路最早開始於電腦間的網際網路(Internet of Computers)，經由點對點(Peer to Peer；P2P)的網路拓樸串連成全球網路(Global Network)的型態，像是全球資訊網(World Wide Web；WWW)的網路平台上提供服務。在過去數年的發展過程中，人們已逐漸被融入到網際網路的環境，更創造出社群網路(Social Network)的模式。當人們開始願意在虛擬的平台上共享自己的資源，便創造出許多商業模式的平台，正宣告網路轉變為以人為導向的網路型態(Internet of People)[10]。

由於現今終端設備的處理能力與儲存容量不斷提升，以及設備有越來越小化的趨勢，加上資訊技術與網路型態不斷的改良與創新，人類的生活正逐漸進入一個始終連接(Always Connect)網路的世代。以往個人電腦是用戶端(Client)主要是連接網路的設備，隨著越來越多網路技術被開發，並且日趨成熟，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。

近幾年，有線網路與無線網路相關的議題已經被學者廣泛定義與研究，並且於網路層推出新的網際網路通訊協定 IPv6(Internet Protocol version 6)，IPv6 於 1998 年 12 月由網際網路工程任務小組(Internet Engineering Task Force, IETF)透過RFC2460標準規範所定義，主要為了解決 IPv4 位元址空間不敷使用的問題，因為 IPv4 只用 32 位元大小，IPv6 則是 128 位元大小[37]。所以 IPv6 的推出，將會使更多物件(Objects)擁有可連上網路的能力。因此，一個未來網路(Future Internet)的新概念將被廣泛的研究與應用，稱之為物聯網(Internet of Things；IoT)[6,10,23]。

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，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[15,36]。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、物件與物件以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)[35]。

項目識別主要是物件具有可以識別身分的標籤(Tags)(例如 RFID 或者 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，或是探勘有用的資訊。嵌入式系統則應用於感測設備或物件中，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。

物聯網涵蓋的範疇相當廣泛，有關物聯網所面對的挑戰大都是過去網路環境中常發生的問題，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、無線感測網路以及無線射頻技術等，都能成為物聯網環境下的組件(Component)。因此，在大規模的物聯網環境下，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[15]。其主要差別在於過去是以人為導向的網路環境，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。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)[10]，因為物聯網不僅包含網路運算環境，智能物件更是扮演重要角色，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。

由於過去 Thiago 等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)的研究[19]，無法解決物聯網環境可能出現不準確的資料、龐大複雜化的資料以及資料不安全性的問題。因此，本研究將基於不準確的資料、龐大複雜化的資料以及資料安全性等議題進行深入探討。

1. 不準確的資料：

服務供應商根據不同需求而設置不同感測與驅動設備的參數，當參數蒐集完成後服務供應商要獲取資訊時，可能發生資料不符合服務供應商設置的需求，或者因參數設置錯誤而導致蒐集到錯的資料。因此，將造成錯失掉的資料無法復原，以及無法有效監控與更新現存的資料並過濾不正確的資料。

2. 龐大複雜化的資料：

在物聯網的環境中，單一區域可能存在數種類型的智能物件與服務，所以可能出現一個或多個服務供應商為了提供一種或數種的服務，佈署數種不同類型感測設備來蒐集相同或不同的資料。當感測設備蒐集到資料後，便會直接回傳給服務供應商。所以可能出現資料量龐大且複雜，無法由這些不正確的資料找出有意義的資訊。因此，如何經由中介層事先萃取出服務供應商所需的資料，以降低龐大複雜化資料的問題，使服務供應商能經由中介層來獲取有意義的資料，是此研究的重點之一。

3. 資料的不安全性：

物聯網環境中的感測標籤所隱藏的是微量資料，主要可讓感測設備能快速讀取及識別標籤內的數據。然而有些感測設備能涵蓋的範圍較廣，如果資料在感測過程中被截取頻段，進而取得數據，或者進行數據竄改，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，例如資料竊取，可能會影響後端系統的安全或改變自動化處理流程等[20]。除此外，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以及身分，才能夠準備接收到真正所需要的資料。

根據上述，由於物聯網環境可能存在不同類型的智能物件，讓所有具有感測、運算以及網路的物件彼此能進行資料傳遞，如圖 1 所示。由於不同類型的智能物件應用的標準不一致，因此物聯網需要一個可用性的中介層框架來整合不同型態與不同性質的資料。亦即，將不同類型的感測設備進行整合，並且制定標準化(Standardization)的機制，經由一個中介層(Middleware Layer)讓彼此之間能達到互通性(Interoperability)。此外，物聯網未來將面臨感測器與驅動設備之間以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[10]。因此，必須加入對資料安全與保密機制以及來源端的身分識別。

本研究提出一個中介層框架負責執行應用層與感知層多種複雜的處理程序，可達到異質性資料的過濾與整合，將複雜化的資料萃取出有意義的資料回傳到應用層服務供應商。此外，為了增強中介層與感知層以及應用層之間的身分識別，本研究加入數位簽章(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知道感知層實體物件的身分，以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，進而提升物聯網環境下的可靠性與可用性。

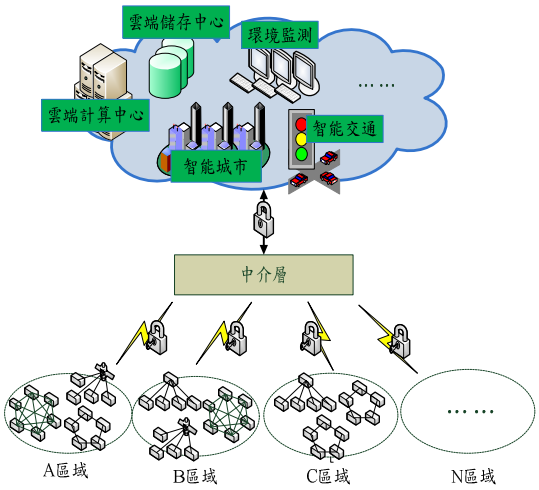

圖 1 物聯網的示意圖

本文在第 2 節將說明各國物聯網的發展現況、物聯網的相關應用、數位簽章、及過去物聯網中介層的相關研究，第 3 節說明本研究所提出在物聯網所建構的以服務為導向之架構，第 4 節為此服務導向架構的作業流程說明，第 5 節為實例說明，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網路運算技術，包含雲端運算、無線感測網路以及無線射頻技術。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，以龐大的運算與儲存資源，來處理大量的使用者需求。而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。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。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，如便利商店、超級市場及港口業務等領域，主要目的在於減少成本開銷、節約能源及提升流程效率。

在本節中將探討各國物聯網的發展現況及當前企業建立的物聯網雛形，並且深入探討目前有關物聯網中介層的相關研究。除此之外，也將列出過去學者尚未考量的問題，其中安全性的問題在現存的中介層中皆未進行研究，因此在本研究中將使用數位簽章來進行應用層與感知層的識別認證。

2.1 各國物聯網的發展現況

● **美國**

2009 年，IBM 公司於歐巴馬就任總統的首次工商業領袖圓桌會議上，提出智慧地球的概念，建議政府積極投資智慧型基礎設施，鎖定的範圍包含：醫療保健、政府管理、交通運輸、能源等數項與人民有關的各項領域。亦即將感測器嵌入和裝載在電網、鐵路、建築、油氣管道等物件中，讓物與物之間能互相傳遞訊息，再透過超級電腦與雲端運算進行訊息整合，將物件融合到大眾社會。因此，IBM 的智慧地球理念[34]，成功獲得美國總統歐巴馬積極的肯定，並且將物聯網提升為國家戰略目標，接續簽署總額 7870 億美元的 American Recovery and Reinvestment Act(ARRA)法案，在智慧電網、生物醫學以及資訊技術等領域上推動物聯網的發展。

美國強調雲端運算資料中心，將是物聯網架構下不可或缺的角色。因此，2010 至 2011 年，美國聯邦政府頒布雲端運算的相關文件以及聯邦雲端運算策略白皮書，前者提出由政府來進行風險授權的計畫，對雲端運算服務進行安全評估與授權認證，經由一次認證多次使用(Authorize Once, Use Many)的方式提升雲端運算環境的評估，進而降低風險評估的費用。後者則是每年從資訊技術 800 億美元的經費中投入 200 億美元興建雲端運算資訊系統架構、研發雲端運算的技術以及應用[25]。

● **歐盟**

2005 年 4 月，歐盟正式頒布未來 5 年歐盟資訊通訊政策框架，稱為 i2010。整合不同通訊網路以及終端設備。在 2009 年 6 月提出 Internet of Things-An Action Plan for Europe，內容包含物聯網架構的管理、安全性、標準化與未來發展等 9 個面向、14 項發展內容以及 10 條對歐盟國家政策建議。在 2009 年 9 月歐盟於 Seventh Framework Programme(FP7)中發佈 Internet of Things Strategic Research Road Map，明確規劃 2010 年、2015 年及 2020 年三個階段物聯網的研究計畫，其中包含識別技術、通訊技術、網路技術等 12 項關鍵技術以及汽車、醫療、能源等 18 項重點開發領域[33]。

● **日本**

從 2000 年起，對 IT 產業提出三階段發展歷程，從 e-Japan、e-JapanII 到 u-Japan，最後發展至目前發展重點 i-Japan。e-Japan 的核心價值是發展網路頻寬基礎建設，以實現超高速網路環境為目標，進而帶動電子商務的興起，以及培育經濟動脈的人才。e-JapanII 重點發展在醫療、教育、政府、金融等七大領域的 IT 技術。為物聯網提早建立資訊網路、政策法規以及人才培育[26]。

2004 年 5 月日本 Ministry of Internal Affairs and Communications(MIC)正式提出以發展無所不在(Ubiquitous)為目標的 u-Japan 國家戰略，建設一個隨時隨地，任何物件以及任何人均能相互傳遞訊息的網路環境以及 IT 技術。u-Japan 架構的理念是以人為導向實現人與人、物與物以及人與物之間的通訊，即稱為 4U(Ubiquitous、Universal、User-oriented 與 Unique)，已經將物聯網的概念納入 u-Japan 國家戰略中[26]。

2009 年 7 月，日本以人為導向的理念且總結過去發展所產生的問題為基礎，發佈以 2015 年為限的中長期資訊技術發展戰略，稱為 i-Japan。在公共事業著重於開發政府電子化系統、醫療健康資訊系統以及有關人民的食衣住行的資訊技術。因此，發展出電子病歷、遠端醫療、遠端教育以及智能運輸系統等應用，進而將物聯網的概念實現在交通、醫療、教育與環境監測等領域上。目前日本政府將以雲端運算的效能，來解決物聯網產生的海量資訊[26]。

● **南韓**

南韓與日本在 IT 技術的建置上，十分類似，其目的皆是以無所不在為目標，開始發展一系列的國家戰略計畫，目前已經發展到 u-Korea。u-Korea 是以過去的 IT 技術為基礎，從 1997 年提出 Cyber-Korea 21 計畫，開始推動網際網路普及化，並且計畫在 2011 年對 RFID 及雲端運算等技術開始進行基礎設施的建置。南韓所發表的 u-IT839 計畫，將無所不在的網路概念納入在此計畫中，主要發展 RFID 技術、物聯網應用於 u-Home(居家網路)、Telematics / Location based 等重點[28]。

u-Korea 主要是經由建置智慧網路及開發新型的資訊技術應用，建立起無所不在的資訊化社會(Ubiquitous Society)，藉由 IT 技術帶給人民食衣住行育樂等各方面更便利的生活品質。因此，u-IT 核心為 u-City 計畫以及 Telematics 發展計畫。u-City 是應用新興資訊通訊技術，來整合各城市的資訊技術基礎設施與服務。Telematics 則是著手發展車用資訊通訊服務，有助於汽車產業的發展。在 2011 年

提出雲端運算國家戰略，計畫在 2014 年建立起雲端運算產業，並且興建大型雲端資料中心，主要是將雲端運算的優勢應用於計算與分析物聯網海量的資訊[28]。

- **中國**

2009 年中國致力於發展物聯網相關的技術與應用，政府規劃將突破感測網路以及物聯網的關鍵技術，開始佈署未來 IPv6 時代相關的技術研發。因此，在十二五發展規劃以及七大戰略性新興產業，把物聯網視為關鍵發展重點，並將大量投資於智慧電網、智慧交通以及智慧物流等領域。但目前面臨兩項問題而阻礙 IT 技術的發展，一是標準尚未制定，二是關鍵技術仍然有待突破。原因在於物聯網的標準，國際尚未有明確的訂定，使得國與國、企業與企業間難以互相通訊，導致目前無法將各個領域的應用整合成國家物聯網，雖然已經在各領域建置基礎設施，甚至已經有相關應用服務，但仍無法跨領域結合。目前正與德國、美國與韓國共同組成國際標準制定聯盟，未來在物聯網發展與整合上，將會有一大進展[31]。

- **台灣**

台灣行政院在愛台灣十二建設藍圖明確指出智慧台灣、智慧生活產業與環境是未來國家發展的政策之一。因此，從 m-Taiwan、i-Taiwan 至 u-Taiwan，積極發展物聯網相關技術以及產學合作。在學校，分別有台灣大學的智慧生活科技創新與整合中心及成功大學的人本智慧生活科技整合中心等，分別進行與物聯網相關技術的發展，包括射頻辨識、無線感測、MEMS、IC 設計、網通設備、3G 與 WiMAX。近年台灣政府積極擴展六大新興產業，包括醫療照護、綠色能源、精緻農業、文化創意、觀光旅遊及生物科技。以及四大智慧產業，包括雲端運算、智慧電動車、智慧綠建築與發明專利產業，為物聯網產業的核心應用。台灣已經具有成熟的通訊基礎以及產業鏈結、設備製造與應變能力，但礙於國際標準尚未訂定，仍無法將國內資源進行整合。現階段傾向與中國進行合作，並成立兩岸物聯網產業推動聯盟，結合兩國專業技術產業，成立系統整合團隊，期盼能為資通訊產業帶來成長的契機以及帶動整體經濟的成長[27,30]。

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。由於物聯網目前處於正在發展的階段，不同通訊、感測設備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[13]。由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產生的海量資料。因此，物聯網與雲端運算結合後所產生的問題，是必須被重視的課題之一。

2.2 物聯網的相關應用

- **台灣基隆港-台北港務分局[29]**

台北港務局使用 ZigBee 結合 RFID 技術，形成自動化作業流程有效的降低貨輪靠港的時間。貨櫃車進出港時，以攝影機進行車牌辨識，並且使用光學字元辨識系統進行比對。接續應用 RFID 技術，讓每輛貨櫃車辦理 RFID 通行證，只要通過車道上 RFID 讀取器，便能進行快速感應，然後結合辨識資料與後端系統進行比對，核對貨櫃車輛以及駕駛人身分。當貨櫃車到港後，再經由 ZigBee 技術取到報到卡，在 ZigBee 的掃描器上進行掃描，就能得知貨櫃放置的區域。此外，可提供貨櫃車卸貨後，便能直接裝載其他貨櫃進行配送。

經由自動化進出港管理流程，從原本人工作業所耗費的 55 秒，縮短為 20 秒通行，降低貨櫃駕駛等待時間的成本。再者，經由資訊系統蒐集的資料進行分析，便能找出航商貨櫃的最佳調度方式，避免出現車道擁塞、縮短貨櫃車裝卸貨等待時間以及貨輪靠港的時間。

- **台灣全家便利商店[25]**

為了能有效監控全家便利商店各分店的能源消耗，從 2005 年開始，全家便利商店與工研院能源與環境研究所，共同研發網路型分散式能源管理系統的技術。在設備上安裝溫濕度感測設備，包括應用在開放式冰箱、走入式冰箱、空調以及是內外環境，再經由 RS485 雙絞線將感測資料回傳到能源管理系統控制器，然後進入空調設備的介面，來自動化調整設備的溫度。此外，透過感測器的應用改善以往維修流程。過去設備毀損需經由店員描述，再由維修人員進行維護，但是店員對設備的專業知識不足，無法準確說明設備毀損程度，增加維修人員誤判的可能性，進而影響整體維修流程。如今透過感測設備能得知設備毀損發生的問題，簡化傳統維修的流程。

未來全家便利商店希望能增加感測器的

運算能力，讓部分資料由感測器進行微量的運算，減少後端系統處理海量資料所耗費的時間，以及探勘出隱性運算規則，例如經由蒐集到的用電量以及設備使用資訊來分析出用電運算規則，進而提供台灣電力公司對電收費的標準。

- **美國量販超市-Wal-Mart[16,38]**

2005 年，美國知名連鎖量販超市 Wal-Mart 應用 RFID 技術，提出不中斷供貨服務，由總部即時掌握各分店庫存量，並且與下游供應商進行整合，將銷售資訊直接提供給供應商，讓供應商直接出貨。

RFID 標籤可放置在每項商品中，一來可準確掌握每件商品的銷售數量，二來 Wal-Mart 各分店店員能經由 RFID 讀取器即時知道商品數量，並且綜合商品資訊，直接經由總部後端系統告知供應商，讓供應商即時補貨，以及淘汰不熱門的商品，保持顧客滿意程度，進而降低庫存與物流成本，以及提升品牌競爭力。

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工要相對應的私鑰製作，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[17,18]。

數位簽章的方法可被歸類為兩大類。(1)直接式數位簽章，(2)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[17,18]。

2.4 過去物聯網中介層的相關研究

過去已有學者探討在物聯網環境下的未知的拓樸架構與深異質性的議題。

1. 未知的拓樸架構[19]：

物聯網環境下存在不同服務性質的感測與驅動設備，因此一個區域位置可能同時共存不同設備的拓樸架構。然而，物聯網的拓樸架構有一個主要的特性，便是可以動態加入未知的拓樸架構。服務供應商為了加入一個新服務，便會新增一組設備並建造此設備的拓樸架構，因此可能需要一次回傳不同性質的資料之需求。根據此種類型的服務組合，要如何以最佳的方式進行資料蒐集，將是中介層必須存在的原因以及面臨的議題。

目前已存在許多為了解決物聯網中介層的策略，這些策略皆以服務導向設計來解決未知以及動態的網路拓樸。部分的策略是專注在網路上使用抽象化的設備作為服務，如 HYDRA[5,21,22]、SENSEI[14]、SOCRADES[7]與 COBIS[32]等。另一部分的策略則是專注於資料/資訊的抽象概念，並集成為服務，如 SOFIA[8] 、 SATware[11] 與 Global Sensor Networks(GSN)[2]。這些策略的共通點，皆是在現存的網路、無所不在以及無線感測網路與驅動設備網路環境中以傳統的服務/資源發現方法(Discovery Methods)來處理未知拓樸架構的問題[3,12,24]。如 SOCRADES 提供設備層與服務層之間的發現方法，應用 WS-discovery 來發現 WS Web Service 或 RESTful 機制來發現 RESTful 的服務。

2. 深異質性[19]：

隨著硬體設備不斷的提升，但是礙於成本的考量，在物聯網環境下，新的感測(Sensing)或驅動(Actuating)設備將不會經常取代已佈署的設備，因此物聯網的基礎設施將存在不同的異質性設備。此外，不同的網路服務供應商將根據不同的網路服務來使用多種不同性質的感測與驅動設備，如觀測誤差分佈(Error Distributions)、取樣速率(Sampling Rate)或空間分辨率(Spatial Resolution)等，不論是功能(Functional)與非功能(Non-Functional)的特性將導致形成一個深異質性(Deep Heterogeneity)物聯網環境。

目前廣泛使用語義學(Semantics)以及元數據(Metadata)來克服物聯網下深異質性的問題。部分策略是使用本體論的方法去模仿感測器的領域知識及資料描述[4,5,9]。另一部分的策略，則更進一步的實現情境資訊[6]或服務描述[7]。許多策略皆以虛擬(Virtual)/語義感測器的概念來支持服務組件的類型，如HYDRA、GSN及SATware。

由於上述過去學者在物聯網中介層的研究，皆未考慮資料的可用性及安全性的問題。因此，本研究在三層式物聯網架構上提出一個中介層來解決過去學者尚未考慮的問題。

3. 三層式物聯網架構

在本研究中提出三層式的物聯網架構，由上而下分別為應用層(Application Layer)、中介層(Middleware Layer)及感知層(Perception Layer)，如圖2所示。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。每個網路服務將對應一至多個感知層設備的拓樸架構，兩層之間以中介層來進行資訊傳遞與資料處理。

中介層的處理程序分別有設備與服務監控(Devices and Services Monitoring)、事件識別(Event Identification)、通訊管理(Communication Management)、策略管理(Policy Management)、輸出入處理(Input/Output Handling)、遠端管理(Remote Management)以及資訊日誌(Information Logging)。

當應用層經由中介層向感知層發出數據需求，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數據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。當感知層的數據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，將處理完的數據回傳到應用層，以進行後續的相關應用服務。

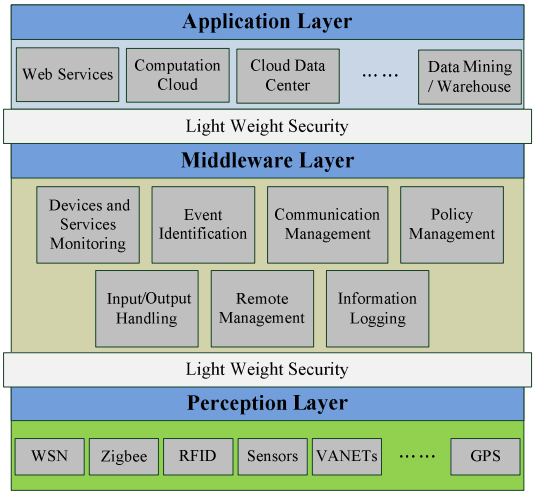

圖 2 三層式物聯網架構圖

4. 三層式物聯網架構工作流程

在本節中將說明在中介層的處理程序，包括：設備與服務監控、事件識別、通訊管理、策略管理、輸出入處理、遠端管理以及資訊日誌的工作流程。

- **設備與服務監控：**此程序負責監控雲端平台上服務供應商的需求以及監控每一個服務需求所需的感測設備。當服務供應商的每一個需求經過中介層時，設備與服務監控程序將監控每一筆需求是否正常執行以及確認服務來源端身分，並且將執行過程記錄到資訊日誌。

  設備與服務監控程序會監控感知層的感測裝置，(1)以 Heartbeat 進行故障的診斷，藉以監控每個感測設備是否正常運作以及是否有發生故障的情況等。(2)當感測設備經中介層收到應用層的服務需求時，則會將蒐集數據的封包傳到中介層，此時設備與服務監控會進行封包的監控，分別識別封包的來源端是否為應用層服務所需的感測設備，再來偵測封包數據是否遭到竄改以及判斷是否為惡意攻擊的封包。最後，如果是一個安全的封包則會進行解密，然後

由事件識別程序處理，以上處理程序將會紀錄到封包日誌庫。設備與服務監控的工作流程如圖 3 所示。

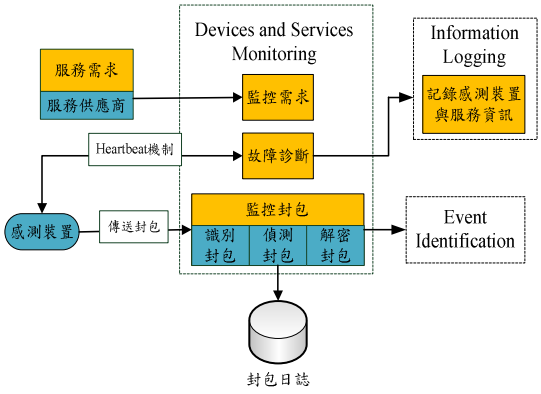

圖 3 設備與服務監控的工作流程

- **事件識別**：當封包經由設備與服務監控程序處理後，在事件識別程序將會對封包傳遞的數據進行判斷是否為一個事件封包。事件封包的定義為急迫性封包，代表感測設備蒐集到的數據是必須立刻通知應用層的服務。因此，將以一個獨立事件來進行資料傳送，在傳送到應用層的服務時，則會再判斷資料是否控制該區域的實體物件。如果是，則會進行輸出入處理程序。所以在此判斷式中，會根據應用層的不同服務設定該服務的門檻值條件，以門檻值條件來觸發處理程序。如果不是，則會經由資訊日誌中儲存應用層的服務資訊來傳送到屬於該事件的服務。如果封包不是一個事件，則會以通訊管理程序來處理。事件辨別的工作流程，如圖 4 所示。

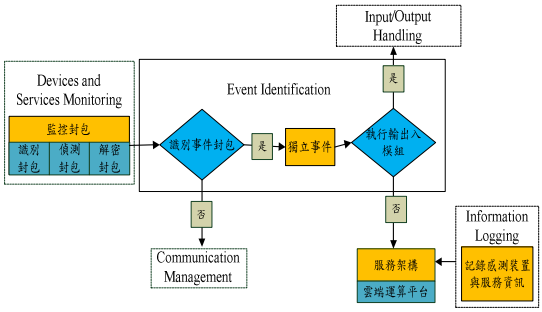

圖 4 事件辨別的工作流程

- **通訊管理**：若封包的類型不是急迫性的封包，此類型的封包進入到通訊管理程序時，則先以應用層服務類型進行分類。非急迫性類型的封包定義為：(1)可能是區域必須週期性蒐集的封包，(2)可能是經由應用層服務提出某種數據需求的封包。當封包分類完後，根據每個分類將不完整的封包、不符合應用層服務需求的封包以及不合理的封包進行過濾，過濾後再執行壓縮的程序。換言之，當非急迫性類型的封包進入到通訊管理程序時，先以應用層服務類型進行分類，當封包分類完後，再根據每個分類將不完整的封包、不符合應用層服務需求的封包以及不合理的封包進行過濾，過濾後再執行壓縮的程序。

  壓縮的定義為：(1)將重複紀錄的資料以[服務類型，數值，次數]進行傳遞，(2)將同一個服務所需的不同資料進行整合，(3)以每個服務傳輸距離為群，將傳輸距離相近的服務整合為一群。最後，經由資訊日誌中儲存應用層的服務資訊，再傳送到屬於該壓縮後資料的服務或服務群。通訊管理的工作流程如圖 5 所示。

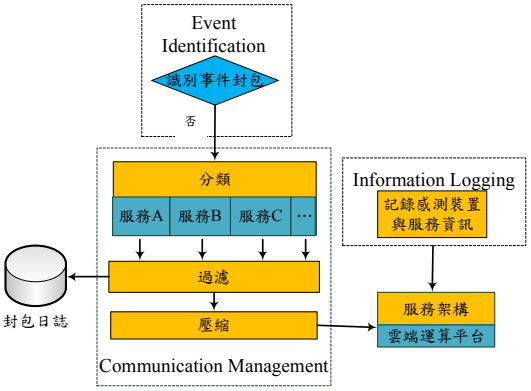

圖 5 通訊管理的工作流程

- **輸出入處理**：此程序是根據事件識別程序中，以應用層的不同服務來設定該服務的門檻值條件，進而驅動此程序。當特定類型的事件發生時，除了立刻通知應用層的服務外，還必須立即控制來源端附近的實體物件。如發生車禍的事件時，可能導致交通阻塞的情況，因此必須辨識此環境的交通狀況來調整附近路口的紅綠燈秒數，以減緩此區域交通阻塞的情況。所以當執行輸出入處理程序時，還必須將該事件傳送到屬於該事件的服務。圖 6 所示為輸出入處理的工作流程。

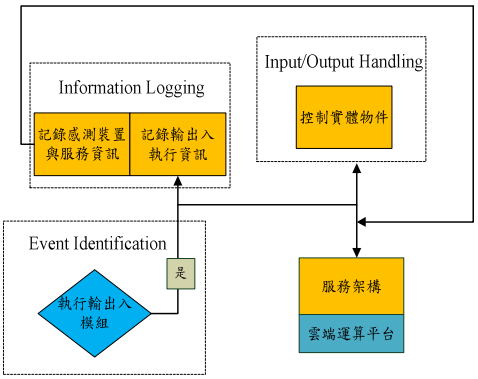

圖 6 輸出入處理的工作流程

- **遠端管理**：此程序的目的是讓應用層服務供應商得以遠端來評估與設定感測設備。在感測設備對外通訊未遭損壞為前提，遠端的管理者(1)可以進行初步的系統恢復或數據備援，即時性的進行感測設備的控管。(2)可以對感測設備進行數值校準，來調整蒐集數據的相關屬性。(3)可以對常閒置的感測設備進行短暫的關閉，以達到節約能源為目的。因此，不論是應用層供應商執行的步驟或感測設備運作時的狀態，皆儲存到資訊日誌中。圖 7 所示為遠端管理的工作流程。

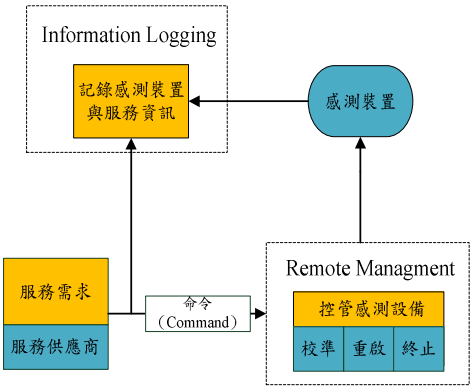

圖 7 遠端管理的工作流程

- **策略管理**：應用層的服務供應商可以為區域性的感測設備與實體物件制訂一個區域性或跨區域的協同式執行策略，供應商可以透過儲存在資訊日誌的歷史資料進行探勘，找出不同感測設備之間或不同實體物件之間或兩者之間的共通性與關係，來制訂策略。如可以設定區域性的感測設備，當其為微量計算時，可以經由鄰近有計算能力的實體物件進行簡易分析，再將分析後的資料經中介層傳遞。因此，策略管理可以儲存由服務供應商制訂的策略，每當一種策略執行實體物件或感測設備時，則會將執行過的歷程儲存到資訊日誌中。圖 8 所示為策略管理的工作流程。

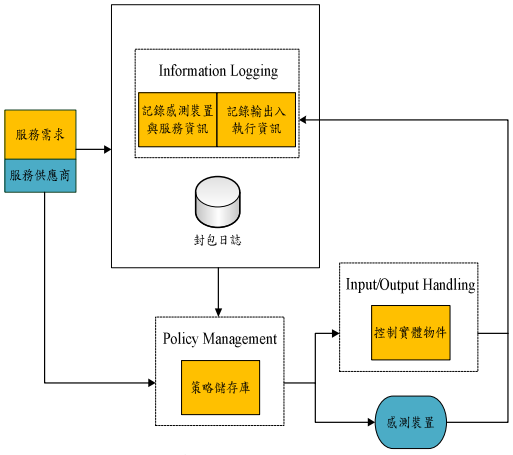

圖 8 策略管理的工作流程

- **輕量安全機制**：本研究在應用層與中介層以及感知層與中介層之間，應用數位簽章的概念讓來源端與目的端可以獲得雙方的身分資訊，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。

  首先，來源端蒐集到的資料會經由雜湊演算法將資料轉為固定長度的訊息摘要，以來源端的私密金鑰對其加密形成一簽體，傳送到中介層來進行認證與程序的處理。中介層擁有來源端的公開金鑰與私密金鑰，先經由來源端的公開金鑰進行解密其確認來源端身分，再經由雜湊演算法檢查來源端傳送的內容，接續執行中介層相關的處理程序，當程序完成後，再以雜湊演算法與來源端私鑰與中介層私鑰加密形成第二階段簽體，傳送到目的端。當目的端收到中介層的簽體時，將會經由來源端與中介層的公鑰進行解密，並使用雜湊演算法，得到中介層處理後的資訊。圖 9 所示為輕量安全機制的流程。

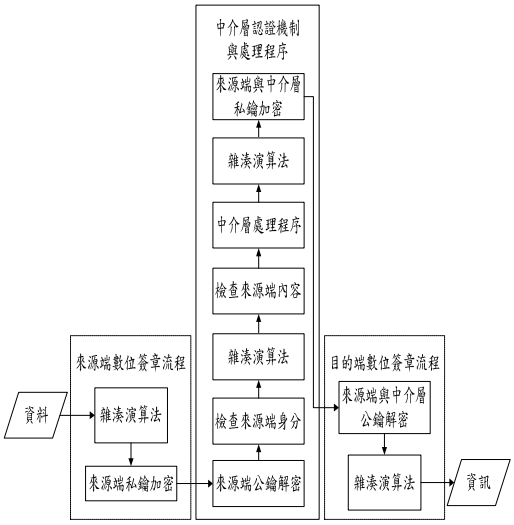

圖 9 輕量安全機制的流程

5.結論與未來研究

在物聯網的環境下,因為存在著大量異質性的智能物件負責蒐集應用層每個服務供應商所需的資訊,所以可能產生龐大且複雜化的資料。因此,本研究在物聯網下提出中介層框架,負責過濾與整合海量的資料,讓服務供應商最終能得到有意義的可用資訊。此外,本研究為了使應用層與感知層能獲得彼此身分識別,降低資料傳輸到錯誤的目的端以及資料被竊取的風險。因此,加入了數位簽章輕量安全機制,提供兩者之間能進行身分的可驗證性與不可否認性。透過本研究所提出的中介層框架與輕量安全機制,能提升物聯網環境下資料的可用性與可靠性。

由於本研究僅提出物聯網的中介層框架及數位簽章的概念。未來將針對本研究的中介層框架的流程進行更深入的研究,進一步針對事件識別以及資料分類、過濾與壓縮進行探討,並且提出適用於物聯網下中介層的方法。此外,再針對輕量安全機制提出適用於物聯網下的數位簽章演算法,並且加入資料機密性與完整性的特性,以提高物聯網傳輸的安全性。

再者,中介層將資料整合後的資訊傳輸到應用層,當資訊上傳至應用層可能發生資訊壅塞的情況。因為由中介層傳送來的資訊存在著急迫性的事件,像是土石流、火災、地震或車禍等資訊,必須立即通報相關單位進行處理。因此,未來將更深入探討應用層中的排隊理論,並且如何有效將資訊分配給適合的資源進行處理,以達到快速處理需求為目的。

致謝

這篇論文是國科會計畫(NSC101-2221-E-324-032 與 101-2221-E-324-034)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] Aberer, K., Hauswirth, M. and Salehi, A., "Infrastructure for Data Processing in Large-scale Interconnected Sensor Networks," ***Proceedings of International Conference on Mobile Data Management***, pp. 198-205, 2007.

[3] Al-Masri, E. and Mahmoud, Q.H., "Investigating Web Services on the World Wide Web," ***Proceeding of the 17th International Conference on World Wide Web***, pp. 795-804, 2008.

[4] Eid, M., Liscano, R. and El Saddik, A., "A Universal Ontology for Sensor Networks Data," ***Proceedings of the IEEE International Conference on Computational Intelligence for Measurement Systems and Applications***, pp. 59-62, 2007.

[5] Eisenhauer, M., Rosengren, P. and Antolin, P., "Hydra: A Development Platform for Integrating Wireless Devices and Sensors into Ambient Intelligence Systems." ***The Internet of Things***, pp. 367-373, 2010.

[6] 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.

[7] Guinard, D., Trifa, V., Karnouskos, S., Spiess, P. and Savio, D., "Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-demand Provisioning of Web Services," ***IEEE Transactions on Services Computing***, Vol. 3, No. 3, pp. 223-235, 2010.

[8] Honkola, J., Laine, H., Brown, R. and Tyrkko, O., "Smart-M3 Information Sharing Platform," ***Proceedings of IEEE Symposium on Computers and Communications (ISCC)***, pp. 1041-1046,

2010.

[9] Liu, J. and Zhao, F., "Towards Semantic Services for Sensor-rich Information Systems," ***Proceedings of the 2th International Conference on Broadband Networks***, pp. 967-974, 2005.

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

[11] 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.

[12] Meshkova, E., Riihijarvi, J., Petrova, M. and Mahonen, P., "A Survey on Resource Discovery Mechanisms, Peer-to-peer and Service Discovery Frameworks," ***Computer Networks***, Vol. 52, No. 11, pp. 2097-2128, 2008.

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

[14] Presser, M., Barnaghi, P., Eurich, M. and Villalonga, C., "The SENSEI Project: Integrating the Physical World with the Digital World of the Network of the Future," ***IEEE Communications Magazine*****,** Vol. 47, No. 4, pp. 1-4, 2009.

[15] 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.

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

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

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

[19] 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.

[20] 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.

[21] Zhang, W. and Hansen, K., "Semantic Web Based Self-management for a Pervasive Service Middleware," ***Proceedings of the 2th IEEE International Conference on Self-Adaptive and Self-Organizing Systems***, pp. 245-254, 2008.

[22] Zhang, W. and Hansen, K., "An Evaluation of the NSGA-II and MOCell Genetic Algorithms for Self-management Planning in a Pervasive Service Middleware." ***Proceedings of the 14th IEEE International Conference on Engineering of Complex Computer Systems***, pp. 192-201, 2009.

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

[24] Zhu, F., Mutka, M. and Ni, L., "Service Discovery in Pervasive Computing Environments," ***IEEE Pervasive Computing***, Vol. 4, No. 4, pp. 81-90, 2005.

[25] 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.

[26] 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.

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

[28] 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.

[29] 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.

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

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

[32] CoBIs project, Cobis final project report deliverable 104 v 2.0, Tech. Rep., 2007, http://www.cobis-online.de/files/Deliverable_D104V2.pdf.

[33] European Commission, “ICT in FP7” http://www.libnet.sh.cn:82/gate/big5/cordis.europa.eu/fp7/ict/.
[34] IBM, “Smarter Planet - United States”, Nov. 2010, http://www.ibm.com/smarterplanet/us/en/.
[35] International Telecommunications Union, ITU Internet Reports 2005: The Internet of Things. Executive Summary, Geneva: ITU, 2005.
[36] MIT, “MIT Auto-ID Laboratory,” 2010, http://autoid.mit.edu/cs/.
[37] RFC2460-“IPv6” 1998, http://tools.ietf.org/html/rfc2460.
[38] Wal-mart, 2008, http://corporate.walmart.com/.