Gope 與 Hwang 採用 BSN 之健康照護系統認證機制的缺失
The Security Vulnerability of Gope and Hwang's Healthcare Authentication Scheme Using BSN

古方元 王美慈
Fang-Yuan Ku Mei-Tzu Wang
中國文化大學 中國文化大學
資訊管理所 資訊管理學系
研究生 副教授
moca77777@gmail.com meii@faculty.pccu.edu.tw

摘 要

物聯網（Internet of Things，簡稱 IoT）承載了網際網路、通訊業者的諸多資訊。在物聯網上，每個人都可以應用無線射頻識別(RFID)技術將真實的物體透過網際網路聯結，這些真實的物體不論是人類、動物、一般物品，都可以找到它們的具體位置。而運用物聯網（IoT）概念發展出的身體感測網路（Body Sensor Network，簡稱 BSN）則是其中最受矚目的技術，只要利用微小供電和輕巧的無線感測節點即可監控身體狀況。但使用此技術的同時，需考慮其安全性，患者的隱私相當重要。在 2016 年，Gope 與 Hwang 提出基於物聯網所發展出的 BSN 照護（BSN-care）來完成現代醫療體系中身體感測網路的主要安全需求；這些安全需求包含資料私密性、資料完整性、資料新鮮度、認證性、匿名性、安全定位。然後我們發現，Gope 與 Hwang 提出的協定仍無法避免中斷服務攻擊（IoS）。因此，我們在本研究中指出 Gope 與 Hwang 的安全協定之漏洞，透過中斷服務攻擊使協定中認證訊息不同步。
關鍵詞：物聯網、健康照護、匿名、認證機制、中斷服務攻擊。

Abstract

The Internet of Things sustain lots of information from the Internet and the communication industry. On IoT, each entity including human, animal, or even a material can be found using RFID technology. As an Internet of Things, Body Sensor Network have received larger attention in recent years. It uses small power supply and lightweight wireless sensor node to monitor a patient's situation. However, patients' privacy is important, we should consider about the security problems while using this technology. In 2016, Gope and Hwang proposed an authentication scheme in IoT-Based healthcare system, which uses Body Sensor Network, to accomplish the main secure requirements, including data privacy, data integrity, data freshness, authentication, anonymity, and secure localization. Hereafter, we figure out the authentication scheme that Gope and Hwang proposed, and find that it can't avoid from Interruption of Service (IoS). Then, we give an example to illustrate how the Gope and Hwang protocol is vulnerable when the LPU and the server lose their synchronization.
Keywords: IoT, healthcare, anonymity, authentication, IoS

1. 緒言

1999 年 Kevin Ashton 首先提出物聯網這個名詞，當時他開始為 P&G 引入 RFID 管理其供應鏈；2009 年，Ashton 在 RFID 期刊中回溯 1999 年所提出的狀況[1]。物聯網將現實世界數位化，應用範圍十分廣泛，並將分散的數位資訊統整。應用領域主要包括：運輸和物流領域、健康醫療領域、智慧環境（家庭、辦公、工廠）領域、個人和社會領域等，具有十分廣闊的市場和應用前景，其中最具代表的是應用在健康醫療領域[2]。

現代醫療環境中，物聯網（IoT）的使用技術替醫生與患者帶來便利，因為它們適用於各種醫療領域（如即時監控、患者資訊管理、和醫療管理）。運用物聯網（IoT）概念發展出的身體感測網路（BSN）則是其中最受矚目的技術，只要利用微小供電和輕巧的無線感測節點即可監控身體狀況。由於近年來世界各地的老人平均壽命穩定增長，有研究指出約有 89%的老人處於獨居狀態，且有 80%以上的老人患有一種以上的慢性病[3]。因此，許多創新的健康照護方案與工具與日俱增，基於物聯網之現代健康照護系統即是其中一例。

2016 年 Gope 與 Hwang 提出之匿名認證協定，是使用單向雜湊函數、隨機數及互斥或運算，達成 BSN 系統中局部處理單位與 BSN 的交互認證、匿名性、安全定位、防止重送與假冒攻擊、以及資料安全性[4]。然而，我們發現 Gope 與 Hwang 的協定，攻擊者可使用切斷電源的方式，耗損協定中的備用方案，進行中斷服務攻擊。本研究將針對該認證協定中的安全漏洞，提出其缺失並探討。

本研究其餘章節如下：第 2 節檢視 Gope 與 Hwang 之匿名認證協定，第 3 節描述我們發現 Gope 與 Hwang 匿名認證協定之缺失，第 4 節為本文之結論。

2. 文獻探討

Gope 與 Hwang 在本研究中將安全需求分為兩部分：網路安全性需求與資料安全性需求。網路安全性需求是由認證性、匿名性、安全定位組成；資料安全性需求則涵括了資料私密性、資料的完整正確性以及資料的新鮮度。他們所提之協定中，主要由兩個階段的程序所組成，分別為註冊與輕量匿名認證階段，而輕量匿名認證階段可以滿足所有網路安全性需求。以下將介紹各階段如何運作。

表一　Gope 與 Hwang 所提協定使用之符號註解

符號	定義
LPU	局部處理單位
S	身體感測網路伺服器 (BSN Server)
ID_L	LPU 的辨識碼
N_s	Server 產生的隨機數
ID_S	Server 的辨識碼
r_j	Server 產生的隨機數
AID_L	LPU 的一次性辨識碼
SID	LPU 的影子辨識碼
K_{ls}	LPU 和 S 的共享金鑰
K_{em}	LPU 和 S 的共享緊急金鑰
Tr_{seq}	追蹤序列號
N_l	LPU 產生的隨機數
LAI_l	基地台的區域辨識碼
h(.)	單向雜湊函數
$\oplus$	互斥或運算子(exclusive-or)
$\|\|$	資料連結運算子

2.1 Gope 與 Hwang 協定之註冊階段

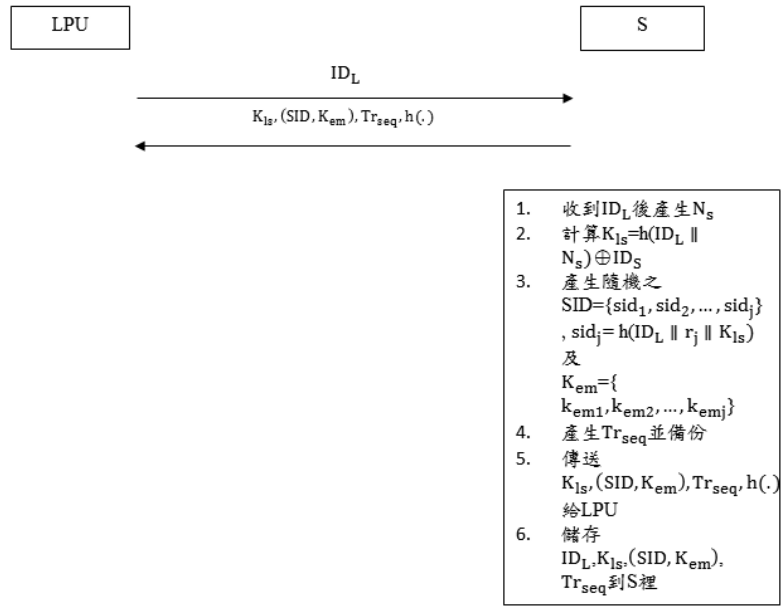
如圖一所示，在這個階段，使用者的 LPU 需先向 S 註冊。

LPU 透過安全通道傳送 ID_L 到伺服器 S。S 收到要求後，產生一隨機數 N_s 並計算 $K_{ls}=h(ID_L \| N_s) \oplus ID_S$。同時，S 產生一組不連續的影子辨識碼，$SID=\{sid_1, sid_2, \ldots\ldots, sid_j\}$，$sid_j=h(ID_L \| r_j \| K_{ls})$ 及一組隨機之共享緊急金鑰 $K_{em}=\{k_{em1}, k_{em2}, \ldots\ldots, k_{emj}\}$對應到 SID，然後 S 產生一隨機 32-bit 的 Tr_{seq} 並將其傳送給 LPU。最後，S 會透過安全通道傳送 $\{K_{ls}, (SID, K_{em}), Tr_{seq}, h(.)\}$給 LPU，並備份 ID_L, K_{ls}, (SID, K_{em}), Tr_{seq} 到資料庫中。

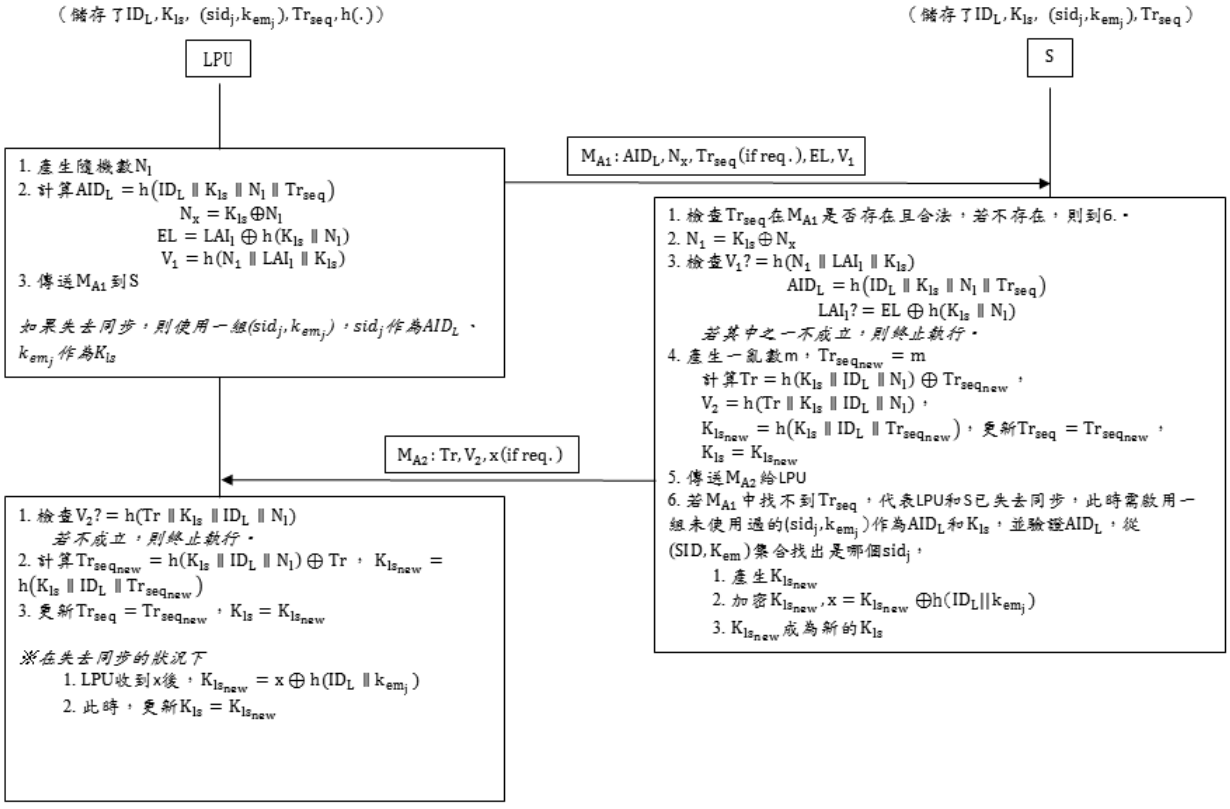
2.2 Gope 與 Hwang 協定之輕量匿名認證階段

如圖二所示，在認證階段，LPU 首先會產生一個隨機數 N_l ，並計算 $AID_L=h(ID_L \| K_{ls} \| N_l \| Tr_{seq})$，再用 LPU 與 S 的共享金鑰 K_{ls} 將 N_l 加密成 N_x，即 $N_x=K_{ls} \oplus N_l$；而後再將基地台的區域辨識碼 LAI_l 利用雜湊運算加密，$EL=LAI_l \oplus h(K_{ls} \| N_l)$，並產生訊息認證碼 $V_1=h(N_l \| LAI_l \| K_{ls})$供後續認證使用。完成以上步驟後，LPU 會傳送訊息 M_{A1} 到伺服器 S，M_{A1} 包含：AID_L、N_x、EL、 V_1。如果 S 有要求則傳送 Tr_{seq}。

接收訊息 M_{A1} 後，伺服器 S 會檢查 Tr_{seq} 是否存在於 M_{A1} 中且是合法的；若不存在，則到(6)。此時，解密 N_x 得到 $N_l=K_{ls} \oplus N_x$，並檢查 V_1 是否等於 $h(N_l \| LAI_l \| K_{ls})$，以及 AID_L 是否等於 $h(ID_L \| K_{ls} \| N_l \| Tr_{seq})$和 LAI_l 是否等於 $EL \oplus h(K_{ls} \| N_l)$。若其中之一不成立，則中止執行。檢查完成確認 LPU 為合法使用者之後，產生一亂數 m，使得 $Tr_{seqnew}=m$，並計算 $Tr=h(K_{ls} \| ID_L \| N_l) \oplus Tr_{seqnew}$，此舉乃是更新 S 裡的 Tr_{seq} 並加密成 Tr。然後產生訊息認證碼 $V_2=h(Tr \| K_{ls} \| ID_L \| N_l)$、並更新 K_{ls} 為



圖一　Gope 與 Hwang 協定之註冊階段



圖二　Gope 與 Hwang 協定之輕量匿名認證階段

$K_{lsnew}=h(K_{ls} \| ID_L \| Tr_{seqnew})$，則 $Tr_{seq}=Tr_{seqnew}$、$K_{ls}=K_{lsnew}$。更新完成後，S 會傳送一 M_{A1} 給 LPU，其中包含了 Tr、V_2、如有需求則傳送 x。

然而，在 S 接收了 M_{A1} 後，若發現 Tr_{seq} 不存在於 M_{A1} 之中、或者是不合法的，S 就將此狀況判定為不同步，因而回到此協定的第一步，從頭開始，並使用一組(sid_j, k_{emj})對應到 AID_L 與 K_{ls} 完成 M_{A1}。而 S 在接收 M_{A1} 後，原本需驗證 AID_L，但因為不同步、啟用了一組(sid_j, k_{emj})，便不需驗證 AID_L。此時，S 隨機產生 K_{lsnew}，加密 K_{lsnew}，使得 $x=K_{lsnew} \oplus h(ID_L \| k_{emj})$，而 K_{lsnew} 則成為新的 K_{ls}，並傳送 M_{A2} 至 LPU。

收到 M_{A2} 後，LPU 檢查 V_2 是否等於 $h(Tr \| K_{ls} \| ID_L \| N_l)$。若不成立，則終止執行；反之，則計

算 Tr_{seqnew} 及 K_{lsnew} ：$Tr_{seqnew}=h(K_{ls} \| ID_L \| N_l) \oplus Tr$ 、$K_{lsnew}=h(K_{ls} \| ID_L \| Tr_{seqnew})$，並將 LPU 內的 Tr_{seq} 更新成 Tr_{seqnew} 、K_{ls} 更新成 K_{lsnew}。但如果是在啟用替代方案的情況下，則 LPU 收到 x 後，解開密文 x，得出 $K_{lsnew}=x \oplus h(ID_L \| k_{emj})$ 並將 K_{ls} 更新成 K_{lsnew}。雙方訊息交換至此，即完成輕量匿名認證階段。

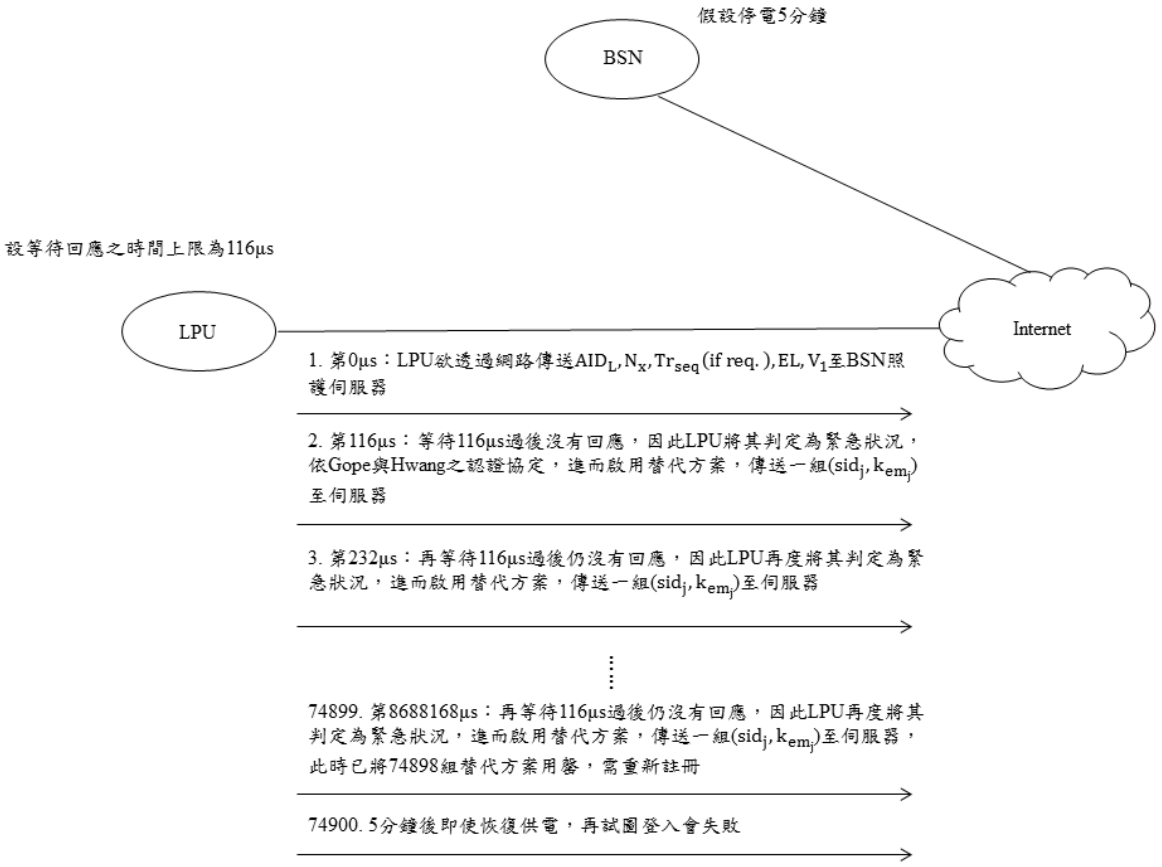
3. Gope 與 Hwang 協定之認證機制的缺失

在目前的環境中，年長者使用的智慧型手機內建記憶體 ROM 大多是 16GB。而根據 NCC「2016 年第 1 季 2G/3G/4G 行動通訊市場統計資訊」[5]，截至 2016 年 6 月止，第四代行動通訊（俗稱 4G LTE）的用戶數占比為 52.3%。因此我們假設健康照護系統使用者持有的是 ROM 16GB 的手機並搭配 4G LTE 網路服務。實測某電信商 4G LTE 服務的資料速率，上行速率為 4Mbps[6]。如表二，經計算後，假設距離不列入考量，在同步情況下，傳輸之資料長度為 264bits，則傳輸所需時間約為 66μs；若是在不同步的情況下，則傳輸之資料長度為 232bits，則傳輸所需時間約為 58μs。假設忽略處理時間、傳導時間、佇列時間，則 Gope 與 Hwang 的匿名認證協定中 LPU 與 S 之間通訊的等待回應時間：同步情況下為 132μs，不同步的情況為 116μs。

傳輸所需時間=總共傳輸的資料量/傳輸速率
(1Mbps 約等於 1000Kbps，1Kbps 約等於 1000bps)
同步情況下：
264 bits/4 Mbps=0.000066s=66μs
不同步的情況下：
232 bits/4 Mbps=0.000058s=58μs

表二　本研究假設之各符號長度

符號	長度(bit)
AID_L	92
N_x	20
Tr_{seq}	32
EL	40
V_1	80
K_{em}	20
SID	92



圖三　本研究假設之中斷服務攻擊示意圖

3.1 中斷服務攻擊

中斷服務攻擊是指任何導致伺服器不能正常提供特定使用者服務的攻擊。Gope 與 Hwang 認為他們的匿名認證協定能夠對抗阻絕服務攻擊，但本

研究發現若是以 IoS 攻擊仍有可能成功。他們的協定所主張的是：在緊急狀況發生、使得 LPU 與 S 雙方的 Tr_{seq} 不同步時，將以使用一組(SID, K_{em})的替代方案來應對。他們認為需使用此替代方案的緊急狀況發生的機會並不多，因此僅儲存合理數量的(SID, K_{em})。可以節省儲存之成本。然而，根據我們的觀察，這種緊急狀況僅適用於非惡意攻擊所造成之 LPU 與 S 的不同步。

根據我們對週遭使用者的觀察，以市面上標榜內建記憶體為 16GB ROM 的智慧型手機為例，扣除作業系統、手機內建程式……等等，使用者通常只剩 8GB 的空間可以自由運用。此時，對於使用者來說，一個輕量、節省儲存成本的應用程式大小不會超過 7MB。我們假設 Gope 與 Hwang 的健康照護系統在使用者手機端(LPU)使用了 7MB，又假設扣除應用程式本身佔去的空間後，此系統設計預留儲存替代方案的空間為 1MB，則在經過計算後，每一位使用者的智慧型手機可以儲存 74898 組(SID, K_{em})。

以下為我們的中斷服務攻擊。如圖三，我們假設目前有 500 位使用者同時登入伺服器。若攻擊者將電源切斷五分鐘，那麼在這五分鐘內，500 位正在連線的使用者的 LPU 就會因為 LPU 等不到 S 的回應，將其判定為緊急狀況，進而啟用一組(SID, K_{em})再登入 S。根據 Gope 與 Hwang 設計的演算過程，與前述原因相同，LPU 將因無法連線而自動判定為認證失敗。於是 LPU 會再重新啟用一組(SID, K_{em})，但由於電源被切斷、系統仍處於斷線，因此認證會再度失敗，如此周而復始。若 LPU 中儲存之合理數量的(SID, K_{em})為 74898 組，則在系統恢復連線前，74898 組(SID, K_{em})將被用盡，使得使用者須重新註冊才能登入。換句話說，即使系統已恢復連線，LPU 將再也無法登入伺服器。

若在攻擊者切斷電源的五分鐘內，此 500 位使用者之中，有發生真正的生理緊急狀況，例如：血壓過高、血糖飆高、中風……等等，其 LPU 試圖與 S 連線傳輸資料時，將因斷電而無法連線導致誤判雙方不同步而啟用替代方案。然而，我們假設(SID, K_{em})的合理數量為 74898 組，LPU 等待回應之時間上限為 116μs，則在 8.688168 秒後將會用盡所有緊急的(SID, K_{em})。那麼，在五分鐘後恢復供電、使用者於重新註冊前，LPU 仍無法傳送資料給 S 也無法呼叫救護車，使得使用者的生命安全堪慮。

3.2 訊息被竄改

依據 Gope 與 Hwang 協定之輕量匿名認證協定，S 與 LPU 會發生不同步的情形。在 S 與 LPU 不同步的情況下，假設攻擊者在 S 傳送訊息 M_{A2} 給 LPU 的過程中竄改了 M_{A2} 中未被保護的 x，則會使得 M_{A2} 送達 LPU 時，LPU 用已知的 ID_L 和 k_{emj} 進行雜湊運算並解密出 x 後，會得到假的 K_{lsnew}。但此時，LPU 對於 M_{A2} 中的 x 被竄改並不知情，因此 LPU 會把 K_{ls} 更新成被攻擊者竄改的 x 解密出的 K_{lsnew} 並儲存。這時，LPU 與 S 更新並儲存的 K_{ls} 就會不同。一旦 LPU 與 S 的 K_{ls} 不同，下次雙方要通訊時，就會因為資料不對稱而無法執行協定。

4. 結論

在這個日新月異的時代，網際網路已是生活中不可或缺的應用，然而同時亦容易出現各式各樣的安全疑慮。其中以物聯網為基礎概念發展出的身體感測網路健康照護系統，更需要將資訊安全做得滴水不漏。因此，本研究探討了 2016 年 Gope 與 Hwang 使用 BSN 之健康照護系統認證機制，美中不足的是，我們發現它滿足許多安全需求卻仍有缺失。在協定中的認證階段，LPU 與 S 每次通訊過程中都會更新資料，藉以防止重送或偽裝攻擊並維持資料新鮮度，甚至若雙方沒有同步更新資料，協定也有提供備用方案。然而，當 LPU 與 S 發生不同步時，攻擊者就有機會發動中斷服務攻擊。如何達到 Gope 與 Hwang 完成的安全需求，且不受中斷服務攻擊的威脅，仍是一項重大的挑戰與課題。

參考文獻

[1] Kevin Ashton, “That 'Internet of Things' Thing,” *RFID JOURNAL*, JUN 22, 2009, http://www.rfidjournal.com/articles/view?4986

[2] 物聯網，維基百科，https://zh.wikipedia.org/wiki/%E7%89%A9%E8%81%94%E7%BD%91

[3] R. Weinstein, “RFID: A technical overview and its application to the enterprise,” *IT Prof.*, vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[4] Prosanta Gope and Tzonelih Hwang, “BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network,” *IEEE SENSORS JOURNAL* , VOL. 16, NO. 5, MARCH 1, 2016

[5] 國家通訊傳播委員會_2G/3G/4G行動通訊市場統計資訊, 2016年第1季2G/3G/4G行動通訊市場統計資訊，http://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=3773&is_history=0&pages=0&sn_f=35983

[6] Hinet 連線速率測試(手機版), http://speed.hinet.net/portable.htm