具資料安全加密機制之無線傳輸血壓計

陳玉敏
中國醫藥大學護理系副教授
ym-chen@mail.cmu.edu.tw

王詠平
亞洲大學資通系碩士班研究生
Talk-bear0516@hotmail.com

林郁人
亞洲大學資通系碩士班研究生
He-shyo567320@yahoo.com.tw

柯賢儒*
亞洲大學電通系助理教授
hjko@asia.edu.tw

1、摘要：

本文提出基於 Ubiquitous healthcare(U-healthcare)觀念之生理訊號監測系統。我們將電子血壓計之信號藉由藍芽技術傳送至 PDA 後，再以適當方式回傳至後端伺服器。為了使受照護者的隱私及確保量測的生理資訊受到保護，本論文利用了 DES 及 RSA 之聯合加密演算法，分別針對受照護者資料以及 DES 演算法所設定之金鑰加密，使加解密速度及資訊安全達到適當的妥協。相對於過去護理人員以抄寫的方式記錄病人的生理量測的數據，回到護理站再以手動輸入至電腦做記錄。本論文所提出的方法將可有效改善其量測生理訊號之效率、正確性及安全性。

Abstract

In this paper, the authors propose a measuring system of physiological signals based on the concepts of Ubiquitous healthcare. By using the Bluetooth technology, the physiological signals can be transferred to a server appropriately via personal digital assistant (PDA). In order to protect the patients' privacy and preserve the security of the large number of measured signals, we use DES and RSA joint algorithms to encrypt all the data of the cared people and the key of DES algorithm, respectively. It provides the well-compromise between the speed of encryption/decryption and the information security. In contrast to the conventional nursing, that is, the nurses record the physiological data via hand write and input the data to a computer when they go back to the nursing station. Our proposed approach can effectively improve the efficiency, correctness, and security.

2、前言

由於現行的無線網路科技及無線感測的技術已相當成熟且價格低廉，例如目前大部分的筆記型電腦、Personal Digital Assist(PDA)、Smartphone 均已內建無線網路功能(Bluetooth、WiFi、Infrared Rays)已經相當普及。近兩年的研究中，已有使用筆記型電腦結合無線網路做為生理訊號收集器的研究[4]、[6]。然而，PDA 相較於筆記型電腦有更為輕巧可攜及價格更為低廉的優勢，因此，本論文提出一套以 PDA 為平台，以達成健康醫療資訊可以無線方式存取、低成本、高安全性及高效率的目的。此外，該系統也能使醫護人員

*Corresponding Author

即時瞭解病患的生理資料和健康狀態。在過去的文獻中，對於病患生理資料保護的討論較為薄弱，在本論文中將對此提出一種結合 RSA 及 DES 加密演算法的方式來增強病患隱私權的保護。

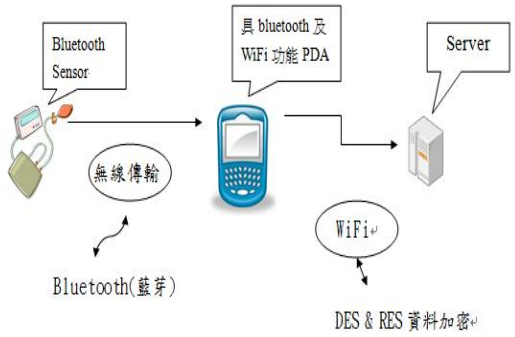

圖 1 感測網路基本架構

本論文所提出的基本架構如圖 1 所示，前端生理訊號感測器是使用具有 Bluetooth 功能的血壓計，其血壓計可量測受照護者之血壓及心跳，接著我們使用具有 Bluetooth 和 WiFi 功能的 PDA，將感測之資訊傳送至 PDA 並顯示於 PDA 的螢幕上，同時也能做儲存，之後檔案再藉由 WiFi 或其他適當的方式傳回後端的資料庫作歸檔，PDA 可讓醫護人員一次完成巡房測量後，將所有受照護者之生理感測資料儲存，並回傳至後端的伺服器，醫護人員可隨時從伺服器監控病患的生理狀態，將可增加護理人員的工作效率，並減少因以人工手抄資料發生登記錯誤的機率。

為提高對病患生理資訊隱私及安全性的保護，本論文所提出之照護系統將再加上安全加密技術進行生理資料加密，以確保傳送資料的安全性。在 Weerasinghe [2]的研究中，作者提出一種匿名就醫的運作模式。然而，在該論文中對於病患生理資料傳遞的加密模式並無具體的方法，因此本論文將於第四節中提出結合 RSA 及 DES 演算法的加密系統解決安全性的問題。

3、系統架構及系統說明：

傳統的生理血壓量測工具，體積較為龐大且價格也較為昂貴，現今雖有許多體積比較小且可攜帶方便的血壓計，但通常缺乏量測資料的數位輸出功能，因此其量測的資訊須經由人為方式記錄。

為了符合健康照護系統的需求，方便非電子專業醫療照護背景的人員建置符合需求的照護系統介面，本論文提出的系統已完成和中國醫藥大學護理系教授及醫護人員討論，並制定出所需要的系統功能及方便護士使用及介面，力求簡單易懂，以輔助護理站的護士人員進行病患血壓量測工作，有效收集個人資料的收集及存取。

3.1 藍芽傳輸：

近年來藍芽(Bluetooth)無線傳輸的技術發展相當成熟，若使用無線傳輸功能的血壓計，血壓計會利用藍芽模組(Bluetooth)傳送到使用端 PDA 裡發送程式再經由網路傳送伺服端接收程式，這樣的模式也把生理資料傳輸的問題獲得解決。

藍芽技術為低功率之無線網路傳輸技術，促使不同產品間達成短距離無線通訊，其無線電發射功率為 0dBm(class 3)傳輸範圍約 10 公尺，藍芽是由無線電、連結控制器、連結管理介面及主設備〔PC、PDA〕等組成，藍芽技術運作的原理主要是運用跳頻展頻技術方式，使藍芽晶片

的兩端，以某一特定形式的窄頻載波同步地在 2.4GHz 頻帶上傳送訊號。由於此系統是使用在醫院照護用，此藍芽傳輸的頻率並不會影響人體及造成危害。具 Bluetooth 功能血壓計的優點：

1. Bluetooth 具輕巧便攜帶的優勢。
2. 當 PDA 放置於固定點充電的同時 Bluetooth 能繼續保有行動感測的能力[5]。

3.2 PDA 接收收器

本論文採用 PDA 做為生理訊號之接收器，其優點可分列如下

1. PDA 相較於筆記型電腦更輕巧可攜。
2. PDA 可即時顯示目前生理狀態。
3. 經由 PDA 做轉傳也可以讓 PDA 可以在無網路連線的狀態下能繼續記錄(儲存)感測者的生理數值[5]。

3.3 病患 TAG 讀取

本論文所提出的系統使用了 socketscan 公司生產之 RFID / 紅外線雙用讀取器，用以讀取病患及護士的 TAG 資料，做為病患與護理人員之身分識別，該 RFID 讀取設備將直接內嵌於 PDA 上，除方便攜帶，病患及護理人員基本資料亦不易受到窺視[3]，如圖 2 。當讀取器讀取到病患的資料後即會產生一個含有護士及病患資訊的檔案，再使用血壓計量測病患的生理資訊後利用藍芽傳輸，醫護人員可於 PDA 的操作介面上點擊接收資料按鈕後，所有的生理資料將全自動傳到 PDA。

本論文中提及使用 RFID 的技術作為護理人員和受照護者之身分識別，經過實際與醫護人員討論中了解，RFID 並不一定是最佳的解決方案，使用上有困難的主要因素為辨識用的 Tag 過於昂貴，而且可能因為佩戴在受照護者身上，長時間壓迫或是折壓到 TAG 之天線之種種原因導致讀取失效或無法讀取。因此，有關於人員身分辨識我們採取 RFID/雷射條碼機雙模開發方式來測試出最佳的服務機制。

圖 2 RFID/雷射條碼 讀取 TAG

3.2 生理訊號通訊軟體設計：

生理訊號傳輸方式是藉由 VB.NET 裡的 SerialPort 元件來設計傳輸介面來連結具有 Bluetooth 功能的血壓計將所量測到的血壓及心跳數據接收然後顯示於 PDA 的介面，所設計界面如圖 3。

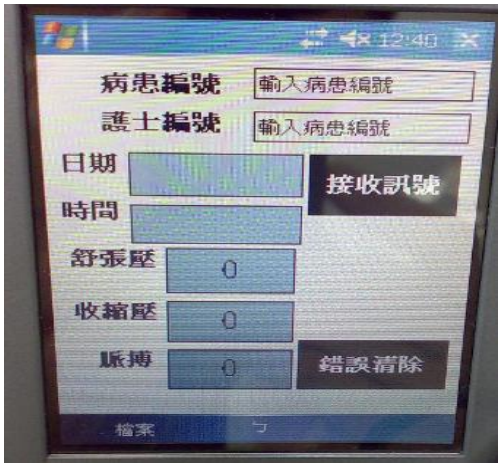

圖 3 PDA 設計之介面

為了將所寫之傳輸介面程式在 PDA 上面作執行，程式語言部分是使用 Microsoft Visual Studio 2005 裡 Windows CE 5.0 的開發環境作為基礎，且在執行程式時 PDA 上必需要安裝 Microsoft .Net Compact Framework 2.0，它是被設計用來執行於行動裝置的套件，如 PDA。

在此，我們使用 SerialPort 元件來做串列的傳輸，以達成 Bluetooth 血壓計和 PDA 之間傳輸的目的，其程式流程如圖 4。

```
serialPort.PortName = SetPortName(_serialPort.PortName)
        serialPort.BaudRate = SetPortBaudRate(_serialPort.BaudRate)
        serialPort.Parity = SetPortParity(_serialPort.Parity)
        serialPort.DataBits = SetPortDataBits(_serialPort.DataBits)
        serialPort.StopBits = SetPortStopBits(_serialPort.StopBits)
        serialPort.Handshake = SetPortHandshake(_serialPort.Handshake)
```

圖 4 SerialPort 元件

完成兩端連線後，醫護人員僅需點擊 PDA 程式介面上「接收資料」的按鍵即可將資訊傳到 PDA ，本論文所設計之通訊介面同時包含病患的編號、護士的編號、量測日期、時間、病患血壓及心跳等資訊，其使用者介面如圖 5 所示。

圖 5 傳送資料之確認

若傳輸過程中因血壓計誤動作而發生錯誤則按「清除資料」之按鍵，等清除之後再重新量測。若血壓計量測無誤，則按「儲存資料」按鍵，病患的資訊會被儲存成文字檔(依資料庫需求是儲存成 .txt 檔)，螢幕上的數據也會自動清除成初始值 0，此時即可繼續量測下一為病患，有關血壓量測的流程圖顯示如圖 6。

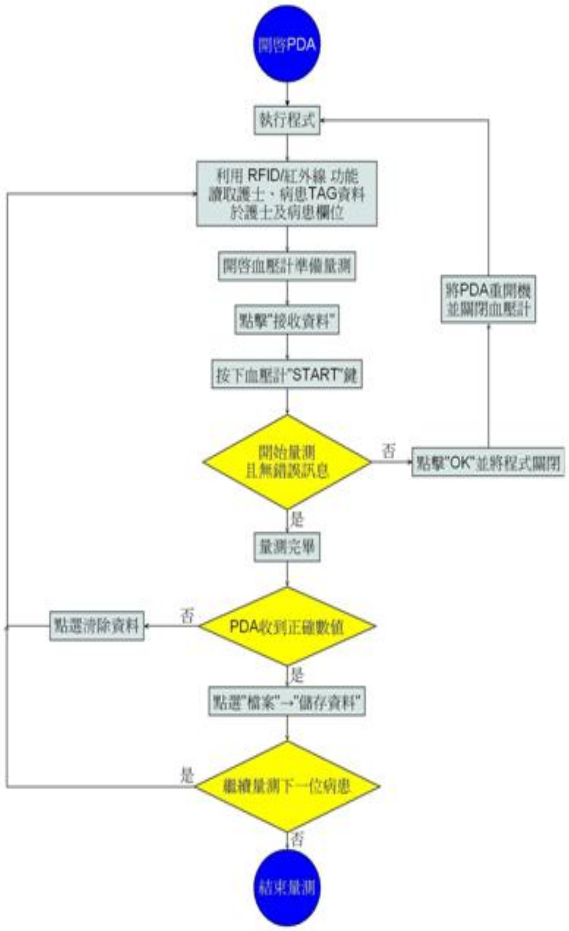

圖 6 血壓計量測流程圖

四、病患生理資訊加密系統：

對於病患個人的一些基本資料、健康狀況等醫療的資訊，如被有心人士刻意竊取外洩，會使病患隱私造成極重大的影響，以及個人權益受到威脅及傷害。現今幾乎所有醫院

裡，病患的診斷資料及其他醫療資訊大多都已完成數位化、電腦化，雖然數位化資訊為醫院帶來醫療效率的增加，但是醫療資訊的管理亦有諸多挑戰。因為，只要電腦一連上網路，就有機會遭受到駭客的入侵，讓駭客有機會接觸到病患的個人診療紀錄。在這方面，病患資料的保護，正是資訊安全上最需要被優先處理。

4.1 加密機制的架構：

本論文研究的架構是針對傳送病患生理資訊的安全性，配合現有的網路安全加密技術所研討出來的基本流程[1]。過程先是由血壓計利用 Bluetooth 傳送病患的生理資訊到醫療 PDA 上，並將所接收到的生理資訊在 PDA 上進行加密保護，由於 DES 屬於對稱式加密法，在加解密時雙方只需用同一把金鑰，但在開放式網路傳送金鑰的暴露性太高，所以會使用 RSA 加密技術對金鑰進行加密保護之後再傳送到後端資料庫，讓整體資料的安全性更進一步的得到保障，加密機制之架構如圖 7。

圖 7 PDA 傳輸加密之架構

從具有 Bluetooth 的血壓計接收到病患的生理資訊經由感測網路到 PDA 上進行儲存，儲存的資料裡包括病患的基本資料及生理資訊 patient_data，而利用 PDA 上已經建立的加密機制進行 patient_data 的加密保護。

為了將病患之生理資料加密，我們將其用 DES 演算法加密，如下式所示

$$ENP_{des} = E_{des}(Patient_{data}, K_{des}) \quad (1)$$

其中先利用 DES 加密函數 Edes 對 patient_data 作加密，而得加密之密文為 ENPdes，其中加解密金鑰 Kdes，因為在傳送到後端資料庫時是暴露的，因此是不安全的。

為了改善 DES 的加解密金鑰的安全性，我們針對加解密金鑰 Kdes 利用 RSA 演算法進行加密保護，即加密函數 Ersa 作加密保護得 RSA 密文 ENPrsa，其密文 ENPrsa 裡包括 Kdes 及 RSA 公開金鑰 Kpub 如下式所示：

$$ENP_{rsa} = E_{rsa}(K_{des}, K_{pub}) \quad (2)$$

DES 演算法進行對病患的生理資料作加密，另一個 RSA 加密演算法對 DES 的金鑰作加密，這兩種加密演算結束後再經由網路或其他適當方式傳送到後端資料庫進行解密。資料庫伺服器接收到後，先對 DES 的金鑰 ENPrsa 作解密，利用 RSA 的解密函數 Drsa 和 RSA 私鑰 Kprv 作 ENPrsa 解密而得生理資料的加密金鑰，如下式所示

$$K_{des} = D_{rsa}(K_{prv}, ENP_{rsa}) \quad (3)$$

另外，再由 Kdes 和 DES 解密函數 Ddes 對 ENPdes 作解密而得其最原始的生理資訊 patient_data(4)，

$$Patient\_data = D_{des}(K_{des}, ENP_{des}) \quad (4)$$

系統加(解)密保護之流程圖如下圖 8。

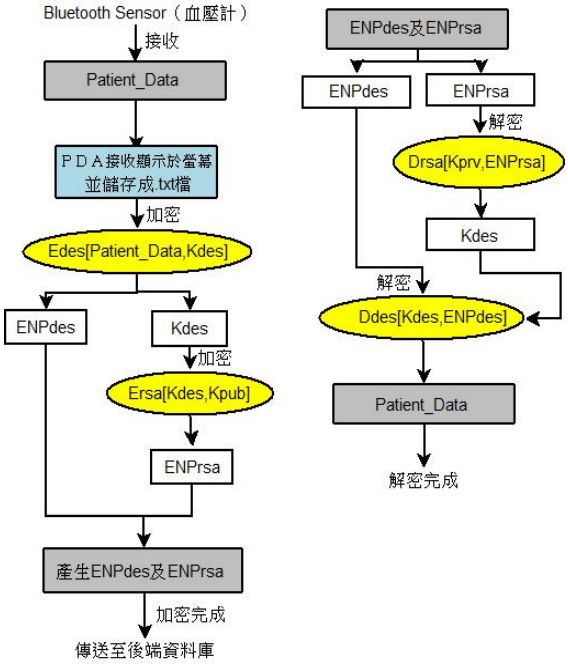

圖 8 加(解)密流程圖

4.2 資料加密的成果

本論文中，我們在 PDA 操作介面上設計一個加密的介面，內容包括了檔案名稱(輸入病患編號)以及輸入加解密金鑰的介面，並進行資料的加密保護產生加密檔，加密介面及密文檔如圖 9 及圖 10。

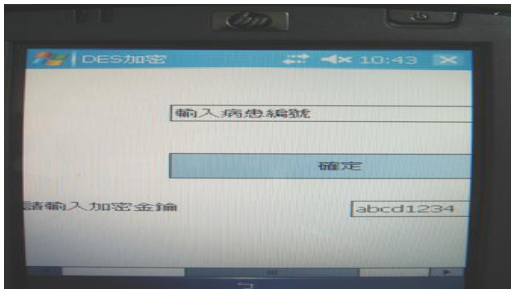

圖 9 加密介面

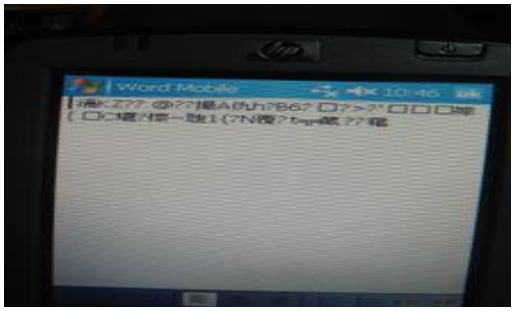

圖 10 密文檔

在生理資料檔案 DES 解密的過程，需輸入檔案名稱以及解密金鑰，解密金鑰與加密金鑰需同一把，若不同把則產生錯誤的指令，所顯示的是解密後的明文檔，和加密前的明文檔內容一樣，完成病患生理資料保護的功能。DES 解密介面及解密後之明文檔如圖 11。

圖 11 解密後之明文檔

5、結論

在本論文中，醫療專用 PDA 之研發重點為照護人員常使用到之PDA 應用程式，使照護人員對於病患之照護效率及可靠度能大幅提升，並藉由無線網路技術、無線感測網路、及射頻辨識 (RFID)之配合，我們完成下列項目：(1) U-healthcare 行動裝置巡房照護：配合讓病患使用具有 Bluetooth 功能血壓計，可將其生理訊號藉由無線傳輸之方式傳回 PDA，使醫護人員之工作效率提高，並由 RFID 技術之配合，使接收到之信號能對應正確之病患及醫護人員，提高巡房工作之可靠度。待醫護人員之 PDA 應用成熟之後，本計畫亦可進一步推廣至 U-healthcare 居家照護，使受照護者之生活品質得以提升。(2) 以 DES 加密保護對病患資料做加密以確保病患資料傳送的安全及隱私，再利

用 RSA 對 DES 的金鑰做加密以確保病患的資料不會外洩。未來亦可利用最新的網路協定 IPv6 與 PDA 在無線行動方面的優勢，創造出一個更完善的 U-healthcare 系統。

6、文獻參考

[1] Yi Hong, Timothy B. Patrick, Rick Gillis, "Protection of Patient's Privacy and Data Security in E-Health Services," *in the proceeding of the 2008 International Conference on BioMedical Engineering and Informatics*, 2008。

[2] Dasun Weerasinghe, Kalid Elmufti, Muttukrishnan Rajarajan and Veselin Rakocevic, "Patient's privacy protection with anonymous access to medical services," *in the proceeding of the Second International Conference on Pervasive Computing Technologies for Healthcare*, pp. 127-130, 2008.

[3] Won Jay Song, Sang H. Son, Munkee Choi, and Minho Kang " Privacy and Security Control Architecture for Ubiquitous RFID Healthcare System in Wireless Sensor Networks," in the *proceeding of International Conference on Consumer Electronics, 2006. ICCE '06.* pp. 239 – 240, 2006。

[4] 柯賢儒、黃子權，" U 化健康照護系統建置"，亞洲大學電腦與通訊學系碩士論文，2008. 7。

[5] 洪振展、黃秀園，" IPv6 U 化健康照護網路之研究以 PDA 為例"，亞洲大學電腦與通訊學系，2008.7。

[6] 黃博駿，"居家照護無線血壓計系統研究"，亞洲大學電腦與通訊學系碩士論文，2008.7。