植基於 RFID 之移動裝置之位置驗證

洪國寶[#]　　陳世育[*]
中興大學資訊科學系
{gbhorng[#], s9456042[*]}@cs.nchu.edu.tw

摘要

由於科技進步，無線網路的發展，將形成一個 Ubicomp 的網路世界。而在此環境底下，將會出現許多經由使用者位置資訊來提供服務的服務，因此位置的驗證在 Ubicomp 的環境中也變的越來越重要。而在真實的環境中，驗證使用者的位置不是一件很困難的事，但是在 Ubicomp 的環境中，由於無線網路的關係造成了使用者具有移動性，所以驗證使用者的位置也變的越來越困難。因此我們提出了使用 RFID 的一種新應用架構 Mobile RFID 來達成位置驗證的工作。

關鍵字：Ubicomp，RFID，Mobile RFID，位置驗證

1. 簡介

隨著資訊科技的日新月異，從個人電腦發展到網際網路的盛行，進而到未來趨勢的主流也就是無線網路的架設。而由於無線網路普及的關係，將形成一個 Ubicomp[10](無所不在運算，Ubiquitous Computing)的網路世界。如此一來打造一個資訊化、數位化、人性化的資訊生活環境已成為未來必然的趨勢。

Ubicomp 這個名稱是由 Mark Weiser[12]所率先提出的。以人類學的角度來看，人們在世界上工作主要都是以分工合作的方式。電腦在其中只是扮演一種輔助的角色。但人們通常都將注意力放在電腦上，所以必須使電腦從人們的察覺中消失，並且要使它遍及人們工作的範圍甚至於達到無所不在的地步。

無所不在意味著想像世界上所有的裝置都使用無線網路相連在一起，而且數位通訊及運算動能的問題都已解決並且是到處都可買到的便宜商品。因此可以嵌入圍繞在我們四周的物品內，讓這些物品藉由彼此的溝通和合作變的更加的有效率，並且提高可用性而使得產能增加。

RFID[13, 14](無線射頻辨識系統，Radio Frequency Identification)是被視為可形成 Ubicomp 網路環境的核心技術之一，而這個技術已經被應用在許多方面，例如：身份識別，衣物管理…等。RFID 是由讀取器(Reader)與標籤(Tag)所組成的。一般來說人們攜帶標籤，而標籤內結合著身份證明或是帳號資訊，然後到有讀取器的地方獲得服務。而 Mobile RFID[6]是 RFID 的一種新的應用，它是將 RFID 的讀取器嵌入人們所使用的行動裝置，例如：手機，PDA…等。藉著使用行動通訊與無線網路使得 RFID 與無線感知網路結合在一起，而成為一種新的更有價值的服務方式。

在有線的網路架構下，要存取系統所提供的權限服務，一般都需要通過某些驗證。而驗證的方式又可以分為許多種甚至是多層驗證，通常來說根據某些我們所設定的，我們所攜帶的，或是我們本身所擁有的。例如：密碼、晶片卡、生物特徵…等。而在 Ubicomp 的網路環境底下，上述的驗證方式雖然仍是有效用的，但由於在此環境下，將會出現許多憑藉著使用

本研究接受國科會計畫編號 NSC95-2221-E-005-080 之部份經費補助

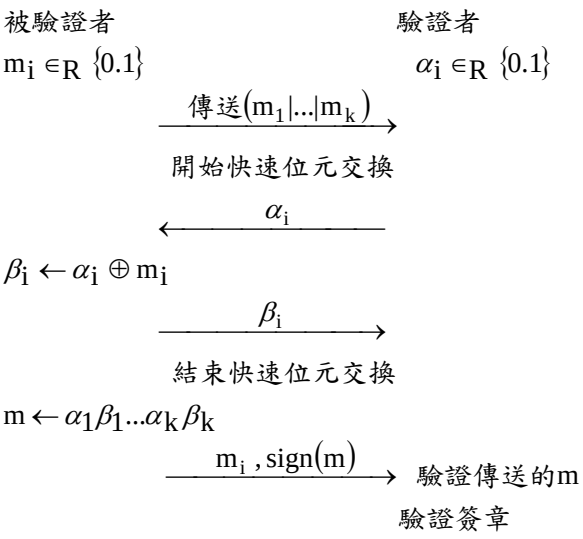
者的位置資訊來提供服務的服務，例如：在電影院附近可以接收到新片上映的通知訊息或是僅有在某個特定區域內才可存取的特殊權限…等。但提供服務的服務端要如何知道使用者目前的位置在那，然後再根據使用者的位置來判斷是否要提供服務給使用者。因此位置資訊在Ubicomp的網路環境下也就可以將它當作這許多種驗證方式中的一種。

在真實的環境中，想要確認一個使用者的位置應該是可以做到的事情，例如：要確定一個人是否在房間內，只需叫他去開燈，因為只有碰觸電燈開關才能開啟。但在 Ubicomp 的網路環境底下，因為無線網路的關係使得使用者位置變的具有移動性，而無法去確認使用者的位置所在，讓那些憑藉著使用者位置資訊來提供服務的服務，無法正確的判斷使用者的位置是否在服務的範圍內。因此位置的驗證在 Ubicomp 的網路環境中也就變的越來越重要，所以就有一些學者開始這方面的研究。

我們的做法是使用 Mobile RFID 的架構來達成位置驗證，運用了幾何空間[4, 7]的觀念及訊息傳播的速度不可能超過光速的原理，這兩個基本理論為我們方法中的理論基礎，其餘較詳細的部份將在下面的章節中提到。本篇文章剩餘的部份如下：第二章節介紹有關位置驗證的相關研究，第三章節說明我們的方法，第四章節將討論安全性及實用性，第五章節談未來研究方向，最後我們做一個簡短的結論。

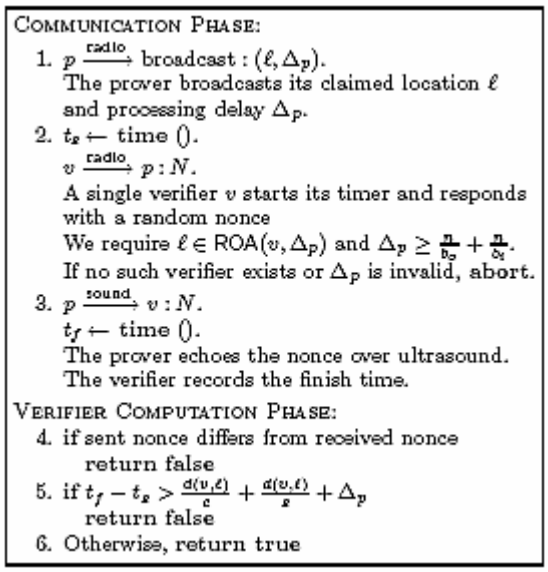
2. 相關研究介紹

在 1993 年時，S. Brands 和 D. Chaum 兩人提出了 Distance Bounding Protocols[1]這個方式，它是一種問答式(challenge-response)的方式，利用驗證者(verifier)與被驗證者(prover)間連續的快速交換一個位元的訊息時，每一個位元在兩方來回時所產生的延遲時間，然後取最大延遲時間的值來決定驗證者與被驗證者距離的上限，這個方式可以跟一些已知的加密驗證協定結合在一起，其協定如圖一所示。



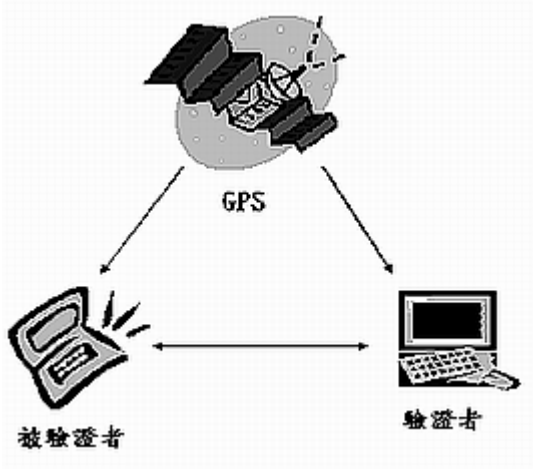
圖一：Distance Bounding Protocols

接著在 2003 年時，N. Sastry 等人定義了位置驗證的問題並提出了 Echo protocol[9]，在這邊他們利用了傳送媒介的傳送速度不同，並使用了多個驗證者去驗證使用者是否在它所聲稱的位置，並驗證這個位置是否在驗證者所包含的區域內。整個協定總共分為兩個方面，分別為通訊方面跟驗證方面，其詳細的協定流程請參考圖二所示。



圖二：Echo Protocol[9]

而 GPS(全球定位系統，Global Positioning System)[3]是另一種被研究來做為位置驗證的方法，利用繞行在地球軌道上的衛星，去測量使用者的經度、緯度、及高度後，以加密的方式送給驗證者去驗證是否在可提供服務的地方，其簡略的架構如圖三所示。其餘有關位置驗證的作法[2, 8, 11]多數依照上述所提及的三種方式之觀念在研究。



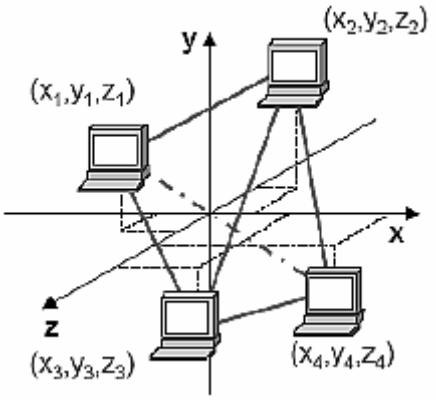
圖三：使用 GPS 之位置驗證

3. 我們的方法

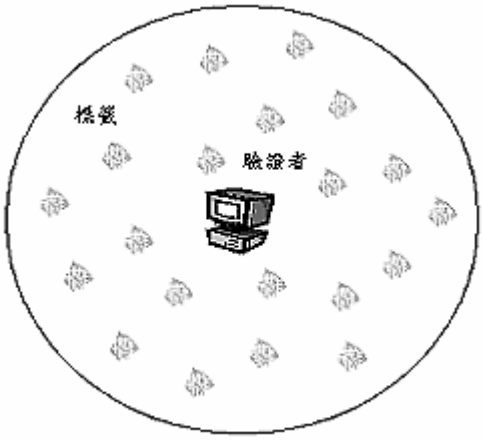
一般來說，要如何驗證是否在某個特定的區域內。最直觀的方式就是親眼所見。但是在無所不在的網路世界裡，想要做到所想的這樣是不可能的事情。所以我們必須利用一些在無所不在的網路世界中存在的架構來達成位置驗證的工作。而我們這邊所採用的方法是建構在 RFID 的一種新應用架構 Mobile RFID 上，使用了幾何空間座標的觀念來計算出被驗證者與驗證者之間的距離，並驗證此距離是否在驗證的範圍內。

3.1. 環境設定

將整個無所不在的網路世界想像成一個幾何的空間，而在這個幾何空間內的每個物體都可視為具有幾何座標的一個點，其網路所形成的幾何空間簡圖可見圖四所示。而環境的架構中，在驗證者的驗證範圍內，要部署很多的標籤，其架構圖如圖五所示。



圖四：網路幾何空間簡圖[7]



圖五：環境架構部署，在驗證者四周放置內含座標資訊的固定標籤

3.2. 基本理論

運用近代物理學所提到理論，那就是訊息傳播的速度永遠不會比光速還快。

3.3. 基本假設

被驗證者：具有內部高精準的 clock[5]且與驗證者同步。

驗證者：也具有內部高精準的 clock 且也與被驗證者同步，而且本身座標位置保密。

標籤：採用被動式標籤，僅能靠接收被驗證者的電磁波經內部線圈產生電力，傳送範圍小，價格便宜，內含座標位置資訊，在接收到被驗證者的要求時傳送本身的座標位置給被驗證者，而標籤本身是固定的。

3.4. 參數說明

D：幾何空間維度

i：佈置在驗證者四周的標籤個數，i 的個數至少必需為幾何空間維度+1 個。

M_i：標籤內的座標資訊；i=1.2.3…；$i \geq D+1$

M_t：被驗證者的座標

n：被驗證者接收到的標籤數目；$n \leq i$

x：從接收的 n 個標籤選 x 個出來；$x \geq D+1$

d：驗證者的距離範圍

r：被驗證者到驗證者的距離

t_a：被驗證者向標籤送出要求的時間

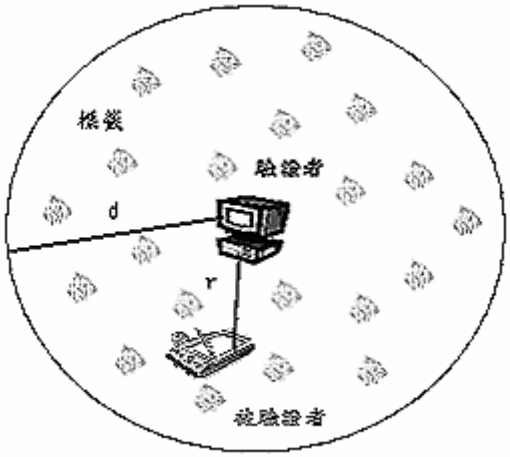
t_n：被驗證者接收 n 個標籤分別回應的時間

t_s：被驗證者向驗證者要求驗證的時間

t_e：驗證者接收被驗證者要求的時間

3.5. 完整架構

完整架構如下圖六所示



圖六：完整架構，若 $r \leq d$ 則表示被驗證者位於驗證者的服務範圍內。

3.6. 驗證流程

我們將驗證的流程分為兩個階段，第一階段：定位階段，被驗證者利用散佈在驗證者四周的固定標籤來計算出自己的座標位置，即被驗證者傳送要求訊息給標籤，標籤回應座標資訊給被驗證者，被驗證者利用接收的座標資訊及傳送接收的時間差來計算出自己的座標。第二階段：驗證階段，被驗證者傳送要求服務的訊息及自己的座標和傳送時間讓驗證者利用本身的保密座標與接收的座標去計算出與被驗證者的距離，然後再利用傳送接收的時間差去驗證計算出來的距離是否相符合，符合的話即位置驗證成功。詳細的流程如下：

定位階段

1. 被驗證者廣播要求訊息給散佈的標籤，並且記錄下廣播的時間 t_a。
2. 標籤接收訊息並傳送座標資訊 M_i 給被驗證者。
3. 被驗證者接收 n 個座標資訊，並記錄接收時間 t_n，若 $n < D+1$ 則放棄。
4. 被驗證者從 n 個座標取 x 個出來和 t_n-t_a 的時間差去計算自己的座標 M_t。
5. 計算出來的座標必須唯一，否則放棄。

驗證階段

1. 被驗證者傳送座標 M_t 及傳送時間 t_s 和要求服務訊息給驗證者。
2. 驗證者接收被驗證者座標 M_t 及記錄接收時間 t_e。
3. 驗證者利用本身的保密座標和被驗證者座標 M_t 去計算出兩人間的距離 r，若 $r > d$ 則放棄。
4. 然後驗證者再利用 t_e-t_s 的時間差乘以速率去驗證計算出來的 r 是否相符，不符的話則放棄。

4. 安全性及實用性

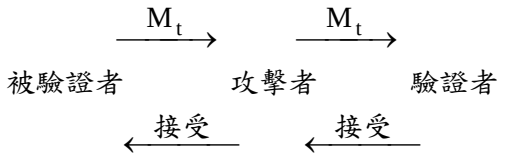
一般來講，在位置驗證方面會遇到的安全上的問題大多是位置欺騙問題，也就是說非法的使用者告訴提供服務的伺服器端，他位於它所提供服務的範圍內要伺服器提供服務，但實際上使用者並沒有在服務範圍內，因此位置驗證必須要滿足位置欺騙的問題，而位置欺騙問題大概又可分為四種。

一. 距離欺騙：

此種為最單純的欺騙問題，也就是使用者告訴伺服器他在它的服務範圍內，但實際上不是，而我們的方式是算出絕對距離，所以這個問題不會造成我們的危險。

二. man-in-the-middle 攻擊：

此種攻擊是指在被驗證者與驗證者間有一個攻擊者，他扮演假的被驗證者也扮演假的驗證者，分別向兩方進行欺騙，而導致他獲得伺服器服務，其示意圖如下圖七所示。而我們的方法因為有採用高精準的 clock 以及驗證者位置座標保密，所以攻擊者無法通過驗證。



圖七：man-in-the-middle 攻擊

三. 共謀攻擊：

此種攻擊是說被驗證者與攻擊者串通，被驗證者給予攻擊者驗證的資訊，而讓攻擊者通過驗證者的驗證，因為我們的方法驗證者位置座標保密，僅有被驗證者的位置座標及時間並沒有辦法通過驗證者的驗證。

四. 重送攻擊：

此種攻擊是使用已經通過驗證者驗證的資訊再重送一次，來取得驗證者的驗證進而得到服務。同樣的若有正確的被驗證者的座標位置，但由於驗證者的座標保密及精準的 clock，所以同樣還是沒辦法通過驗證。

實用性：

由於被動式標籤的價格便宜，體積小，在部署整個架構時，很容易就可以完成而且花費比使用感知器的位置驗證來的便宜，另外又由於標籤的傳輸距離有限，所以用來定位的話也會比使用基地台更為精準。

5. 未來的研究

由於我們的方法採用座標方式，所以被驗證者必須計算出自己的座標，因此未來的研究方向傾向於減少被驗證者的計算負擔，盡可能僅以標籤的資訊達到位置的驗證工作。

6. 結論

我們採用了幾何空間的觀念，將這觀念建構在 Mobile RFID 所形成的環境中，讓整個網路形成一個幾何空間，利用空間中的物體均有一幾何座標，將被驗證者的位置給計算出來並算出與驗證者的實際距離，我們的方法可以抵制上述的攻擊，而且建構起來又便宜。

參考文獻

[1] S. Brands and D. Chaum, “Distance-bounding protocols,” in Proc. Advances in Cryptology-EUROCRYPT’93, Lecture Notes in Computer Science, vol. 765, Springer-Verlag Berlin Heidel berg 1994, pp. 344-359.

[2] S. Capkun, L. Buttyan, and J. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks,” in Proceeding

of the lst ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'03), 2003, pp.21-32.

[3] D. Denning and P. MacDoran, "Location-Based Authentication: Grounding Cyberspace for better Security," in Computer Fraud and Security, Elsevier, 1996.

[4] M. Fujii, "Secure Positioning of Mobile Terminals with Simplex Radio Communication," http://arxiv.org/PS_cache/cs/pdf/0608/0608031.pdf.

[5] S. Knappe, V. Gerginov, P.D.D. Schwindt, V. Shah, H.G. Robinson, L. Hollberg, and J. Kitching, "Atomic vapor cells for chip-scale atomic clocks with improved long-term frequency stability," Optics Letters, vol. 30, no. 18, Sep. 2005, pp. 2351-2353.

[6] H. Lee and J. Kim, "Privacy threats and issues in Mobile RFID," Proceedings of the First International Conference on Availability, Reliability and Security(ARES'06), pp.510-514.

[7] T. S. E. Ng and H. Zhang, "Predicting Internet Network Distance with Coordinates-Based Approached," In Proc. of INFOCOM'02, pp.170-179.

[8] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in Proc. MASS05, Nov. 2005, pp. 834-840.

[9] N. Sastry, U. Shankar and D. Wagner, "Secure verification of location claims," in Proc. WiSe, Sep. 2003, pp.1-10.

[10] F. Stajano, "Security for Ubiquitous Computing," 2002.

[11] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," in Proc. OPODIS 2004, Lecture Notes in Computer Science, Vol. 3544, Springer-Verlag Berlin Heidelberg 2005, pp. 369.

[12] M. Weiser, "The Computer for the Twenty-First Century," Scientific American, Septemb-er 1991, pp.94-100.

[13] RFID Journal, "Merloni unveils RFID appliance," http://www.rfidjournal.com/article/articleview/369/1/1, April 2003.

[14] RFID Journal, "Nokia unveils RFID Phone Reader," http://www.rfidjournal.com/article/articleview/834/1/1/, March 2004.