全球行動網路之外部代理授權的匿名認證機制

溫柏旻
開南大學多媒體與行動商務學系(研究生)
m10108007@mail.knu.edu.tw

楊仁和
開南大學多媒體與行動商務學系(助理教授)
jenhoyang@mail.knu.edu.tw

摘要

本篇論文研究在全球行動網路環境的身份認證機制，先前學者提出的相關認證機制普遍使用運算量較大的公開金鑰密碼系統，故本文將提出一個全新的全球行動網路之外部授權的匿名認證機制來改進。在我們的方法中，用戶僅於初次訪問外部基地台時需要向主基地台進行認證，之後由外部基地台對用戶進行代理授權，且主基地台不需驗證表格儲存用戶認證資料，使用計算的方式得知使用者是否合法，比起先前學者的方法可以降低維護驗證表格成本與儲存空間的需求。此外，考慮到行動裝置的運算能力普遍不高，本文使用互斥或運算及單向雜湊函數來達到低運算量且具有高安全性之設計，故本文所提出的方法將比先前學者的方法更安全及有效率。

關鍵字：外部代理授權、低運算量、全球行動網路、匿名性、交互認證。

Abstract

In this paper, we propose a new authentication mechanism with the anonymity for global mobility networks. In the proposed mechanism, the mobile user is just authenticated once by home agent for roaming services, and thus the authentication mechanism does not need to maintain a large mapping table. That is, the storage space and the searching time can be greatly reduced in the proposed mechanism. In addition, we use one-way hash function and exclusive or to design the proposed mechanism. Thus, the computation costs can be also reduced while performing the proposed authentication process for roaming services. According to the above reasons, the proposed mechanism is securer and more efficient than the related works.

Keywords: VLR authorization, global mobility networks, anonymity, mutual authentication

1. 前言

隨著全球行動網路技術的發展，以及行動用戶的快速增加，使得行動商務成為現今最熱門的市場與服務。全球行動網路可分為行動用戶、外部基地台與主基地台三個角色，透過認證的方式提供合法用戶行動漫遊服務，且行動網路的架構只需於外部基地台電波涵蓋範圍下即可存取服務，不像傳統有線網路需要在一個固定的連線點才能夠存取網路。然而行動網路的傳輸媒介是使用無線電波，以廣播的方式將資訊於空氣中傳輸，如此資訊將容易被攻擊者竊聽，因此於行動網路環境下提供安全的認證機制成為重要的議題。

自 2000 年以來有許多學者提出利用全球行動網路相關認證機制，Zhu and Ma [11]指出過去相關認證機制主要利用公開金鑰密碼系統(RSA)來設計，然而現今公開金鑰密碼系統多使用 RSA-1024(即金鑰長度 1024 bit)，在行動設備普遍運算效能較低的情況下，可能無法負荷如此高的運算量，進而影響效能。因此，他們提出低運算量並具有匿名性之認證機制，而後根據他們的方法，其後有許多的全球行動

網路認證機制相繼被提出[1,3,4,5,6,7,8,9,10,12]。

Kang et al. [3] 於 2011 年，指出 Wu et al. [9] 所提出的機制有未達成匿名性的安全性問題，故提出改善方法。在 2012 年，Hu et al. [2] 指出 Kang et al.的機制中具有安全性漏洞，攻擊者能夠產生在相同主基地台註冊用戶的身分識別碼，並提出修正方法。

上述相關研究的方法中普遍採用公開金鑰密碼系統來做簽章或加解密運算，但是公開金鑰密碼系統的運算量對於行動裝置仍是個負擔，故於本篇論文將提出一個利用低運算量的互斥或運算以及單向雜湊函數的行動網路認證機制，將先前學者在身分認證過程中經常用來儲存用戶驗證資訊的驗證表格取消，當行動用戶進行身分認證時，主基地台以運算的方式來驗證行動用戶身份，可以節省主基地台之儲存空間與維護大量用戶驗證資料表格的維護成本。

假設用戶身分為合法的，則可經由授權的方式使外部基地台自行為用戶產生出一組暫時性身分識別碼，供用戶於該外部基地台漫遊時使用，因此，若用戶於相同外部基地台存取服務的情況下，就不需要一直向主基地台進行認證，故我們的方法與相關方法比較將更有效率。接著，我們在下一章節介紹 Hu et al.之方法。

2. Hu et al.之機制

本節將介紹 Hu et al. [2]方法的初始以及交互認證階段。其方法有三個參與者：行動用戶、外部基地台以及主基地台，所使用的符號如表一所示。

表一、Hu et al.的方法之符號說明

符號	敘述
MU	行動用戶(Mobile User)
FA	外部基地台(Foreign Agent)
HA	主基地台(Home Agent)
PW_x	角色 x 的密碼
ID_x	角色 x 的身分識別碼
$h(.)$	單向雜湊函數
T_x	角色 x 所產生的時戳(Timestamp)
$(M)_x$	用對稱金鑰 x 加密
$E_{Px}(M)$	使用公開金鑰 Px 加密訊息
$S_{Sx}(M)$	使用私密金鑰 Sx 對訊息簽章
$\|\|$	字串連接運算
$\oplus$	互斥或運算
k	交談金鑰

註冊階段

步驟一、 行動用戶將身分識別碼 ID_{MU} 傳送給主基地台 HA。

步驟二、 主基地台收到後，產生私密亂數 m 並使用私密參數 N 計算用戶密碼 $PW_{MU}=h(N \| ID_{MU})$、$r_1 = h(N \| ID_{HA})$ 以及 $r_2 = h(N \| ID_{MU}) \oplus ID_{HA} \oplus (ID_{MU} \| m)_N$，並將相關資訊寫入智慧卡 $SmartCard=(ID_{HA}, r_1, r_2, h(.))$後，將完成註冊資訊$\{PW_{MU}, SmartCard\}$ 透過安全通道(secure channel)回傳給行動用戶儲存。

認證階段

步驟一、 行動用戶於行動裝置輸入密碼 PW_{MU} 後，設備會選取亂數 x_0, x 與時戳 T_{MU}，計算出 $n = h(T_{MU} \| r_1) \oplus r_2 \oplus PW_{MU}$ 和 $L = h(T_{MU} \oplus PW_{MU})$，並使用 L 加密得到 $(h(ID_{MU}) \| x_0 \| x)_L$，之將$\{n, (h(ID_{MU}) \| x_0 \| x)_L, ID_{HA}, T_{MU}\}$傳送給外部基地台。當外部基地台收到後確認 T_{MU} 後產生私密亂數 b 與時戳 T_{FA}，使用私密金鑰 S_{FA} 計算簽章 $SS_{FA}((h(ID_{MU}) \| x_0 \| x)_L, T_{MU}, Cert_{FA})$ 後，將$\{b, n, (h(ID_{MU}) \| x_0 \| x)_L, T_{MU},$

SS_{FA}, $Cert_{FA}$, T_{FA}}一起傳送給主基地台。

步驟二、 主基地台驗證簽章 $Cert_{FA}$ 與時戳 T_{FA}，若為合法則計算$(ID_{MU} \| m)_N = n \oplus h(T_{MU} \| h(N \| ID_{HA})) \oplus ID_{HA}$ 和 $L = n \oplus h(T_{MU} \| h(N \| ID_{MU}))$，接著用私密參數 N 解出 ID_{MU}、及 L 解出$(h(ID_{MU}) \| x_0 \| x)_L$ 後，比較 $h(ID_{MU})$是否相同。若為相同則繼續計算 $W = EP_{FA}(h(h(N \| ID_{MU})) \| x_0 \| x)$，並產生亂數 c 與 T_{HA}，與簽章 $Ss_{HA}(h(b, c, W, Cert_{HA}))$，將$\{b, c, W, Ss_{HA}, Cert_{HA}, T_{HA}\}$回傳給外部基地台。

步驟三、 外部基地台確認簽章與時戳 T_{HA}，並使用 P_{FA} 解出 W 取得 $h(h(N \| ID_{MU}))$、x_0、x，並計算交談金鑰 $k = h(h(h(N \| ID_{MU})) \| x \| x_0)$ 以及 $(TCert_{MU} \| h(x_0 \| x))_k$ 後將$\{(TCert_{MU} \| h(x_0 \| x))_k\}$傳送給行動用戶。

步驟四、 行動用戶計算交談金鑰 $k = h(h(h(N \| ID_{MU})) \| x \| x_0)$，使用 k 從 $(TCert_{MU} \| h(x_0 \| x))_k$ 解出 $h(x_0 \| x)$，並確認 $h(x_0 \| x)$是否相同，相同則為合法，行動用戶能夠認證外部基地台是合法的，本流程結束。

根據以上敘述，我們可以發現 Hu et al.的機制雖然補強了 Kang et al.之機制，不過在行動裝置運算能力普遍有限的情況下，使用公開金鑰密碼系統可能使行動裝置效能降低，此外時戳的使用也有對時的問題，為了解決上述缺點，我們將在下一章節提出我們的方法。

3. 本文所提出之認證機制

本文所提出的方法分為行動用戶註冊與交互驗證兩個階段。且包含了三個主要參與者：行動用戶、外部基地台及主基地台。本方法所使用的符號如表二所示。

表二、符號說明

符號	敘述
MU	行動用戶
FA	外部基地台
HA	主基地台
ID_a	角色 a 的身分識別碼
PW	行動用戶的密碼
$h(.)$	單向雜湊函數
C_a	加密後的資訊
r_a	角色 a 所產生之亂數
$TIDa\text{-}b$	用戶於角色 a 與 b 間的暫時 ID
$\oplus$	XOR 運算
$\|$	字串連結運算
X_a	角色 a 的私密金鑰
$A \stackrel{?}{=} B$	比較 A、B 是否相等

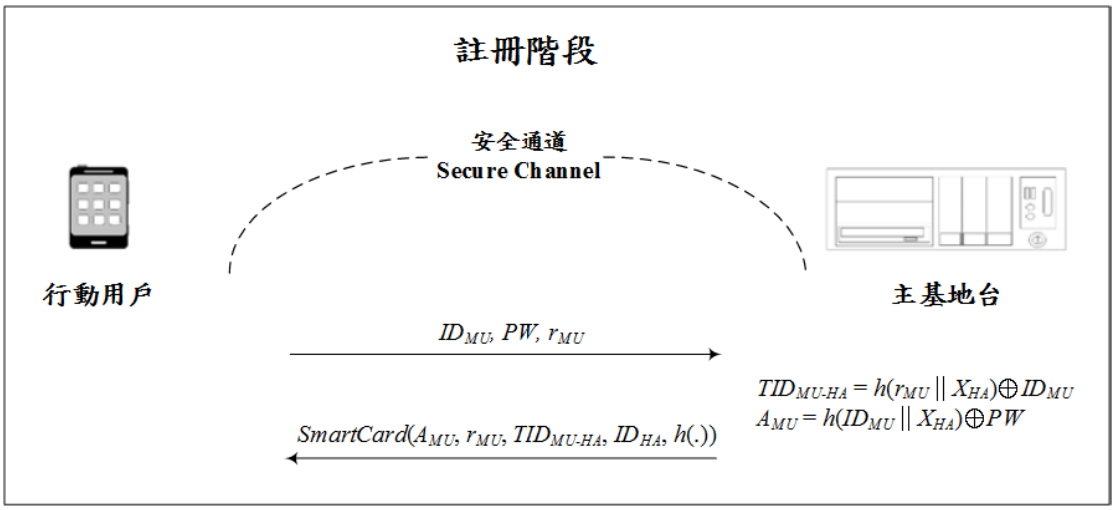
行動用戶註冊階段

在這個階段中，行動用戶 MU 透過安全通道向主基地台 HA 註冊，以取得身分認證相關資訊。

步驟一、 行動用戶將自身的身分識別碼 ID_{MU}、密碼 PW 及亂數 r_{MU} 傳送給主基地台。

步驟二、 主基地台計算出 $TID_{MU\text{-}HA} = h(r_{MU} \| X_{HA}) \oplus ID_{MU}$ 後，再計算 $A_{MU} = h(ID_{MU} \| X_{HA}) \oplus PW$，並寫入智慧卡中，再將$\{SmartCard(A_{MU}, r_{MU}, TID_{MU\text{-}HA}, ID_{HA}, h(.))\}$透過安全通道回傳給行動用戶。

本階段詳細流程如圖一所示。



圖一、本文所提出方法之註冊階段

交互認證階段

此階段中，行動用戶於外部基地台服務範圍內漫遊，並且進行相互認證，此階段步驟詳細說明如下。

步驟一、 行動用戶於行動裝置輸入密碼 PW 得到 $h(ID_{MU} \| X_{HA}) = A_{MU} \oplus PW$，裝置產生時戳 T_{MU} 並計算 $C_1 = h(h(ID_{MU} \| X_{HA}) \| T_{MU})$ 後，將 $\{r_{MU}, C_1, T_{MU}, TID_{MU\text{-}HA}, ID_{HA}\}$ 傳送給外部基地台。

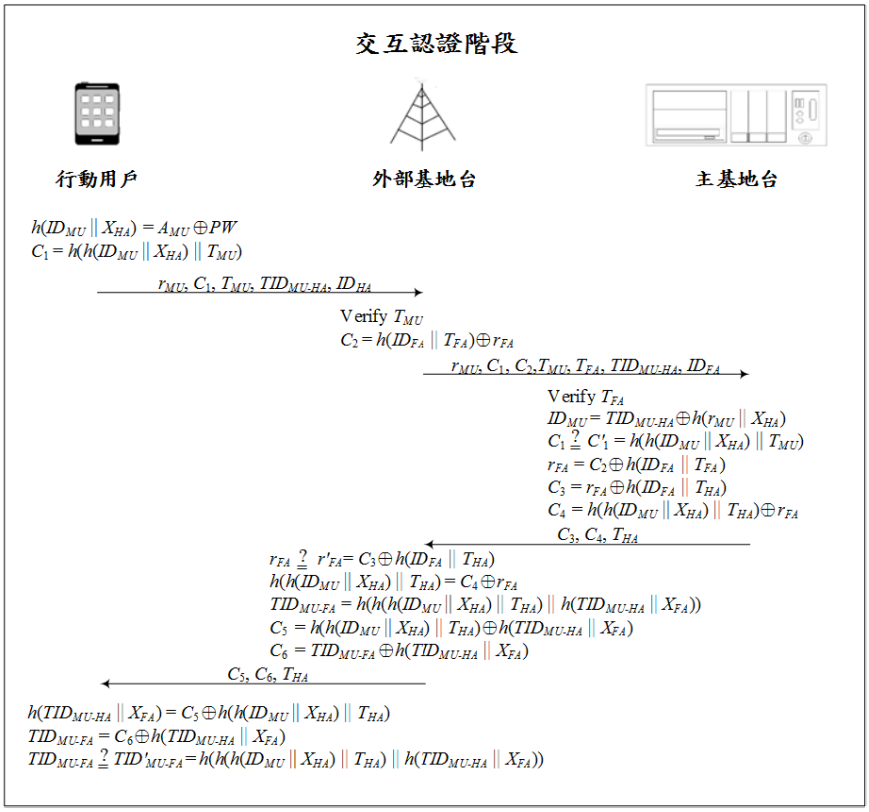
步驟二、 外部基地台於用戶初次訪問時，將直接向用戶的主基地台確認該行動用戶是否合法，故外部基地台確認時戳 T_{MU} 後，即產生時戳 T_{FA} 與 r_{FA} 並計算出 $C_2 = h(ID_{FA} \| T_{FA}) \oplus r_{FA}$ 後，將 $\{r_{MU}, C_1, C_2, T_{MU}, T_{FA}, TID_{MU\text{-}HA}, ID_{FA}\}$ 傳送給用戶之主基地進行身分認證。

步驟三、 主基地台首先確認外部基地台之時戳 T_{FA} 是否有效，之後計算出用戶 $ID_{MU} = TID_{MU\text{-}HA} \oplus h(r_{MU} \| X_{HA})$ 與 $C'_1 = h(h(ID_{MU} \| X_{HA}) \| T_{MU})$，比較 C'_1 是否與收到的 C_1 相同，若相同則該用戶為合法的。當用戶為合法時，主基地台接著產生時戳 T_{HA} 並計算 $r_{FA} = C_2 \oplus h(ID_{FA} \| T_{FA})$、$C_3 = r_{FA} \oplus h(ID_{FA} \| T_{HA})$ 與 $C_4 = h(h(ID_{MU} \| X_{HA}) \| T_{HA}) \oplus r_{FA}$，最後將 $\{C_3, C_4, T_{HA}\}$ 回傳給外部基地台表示用戶認證完成。

步驟六、 外部基地台收到後計算 $r'_{FA} = C_3 \oplus (ID_{FA} \| T_{HA})$，並與原先暫存的 r_{FA} 進行比較，若相同則用戶之主基地台為可信的。接著計算出 $h(h(ID_{MU} \| X_{HA}) \| T_{HA}) = C_4 \oplus r_{FA}$ 及後續用戶認證時使用之參數 $TID_{MU\text{-}FA} = h(h(h(ID_{MU} \| X_{HA}) \| T_{HA}) \| h(TID_{MU\text{-}HA} \| X_{FA}))$，最後計算出 $C_5 = h(h(ID_{MU} \| X_{HA}) \| T_{HA}) \oplus h(TID_{MU\text{-}HA} \| X_{FA})$ 與 $C_5 = h(h(ID_{MU} \| X_{HA}) \| T_{HA}) \oplus h(TID_{MU\text{-}HA} \| X_{FA})$，並將 $\{C_5, C_6, T_{HA}\}$ 回傳給行動用戶。

步驟七、 用戶收到後可利用保有的 $h(ID_{MU} \| X_{HA})$ 計算出 $h(TID_{MU\text{-}HA} \| X_{FA}) = C_5 \oplus h(h(ID_{MU} \| X_{HA}) \| T_{HA})$，接著解出 $TID_{MU\text{-}FA} = C_6 \oplus h(TID_{MU\text{-}HA} \| X_{FA})$ 後，同樣算出 $TID'_{MU\text{-}FA} = h(h(h(ID_{MU} \| X_{HA}) \| T_{HA}) \| h(TID_{MU\text{-}HA} \| X_{FA}))$ 並與解出的 $TID_{MU\text{-}FA}$ 比較，若相同則可認證外部基地台與主基地台，並且之後用戶於此外部基地台漫遊時可直接使用此 $TID_{MU\text{-}FA}$ 與外部基地台進

行認證。本階段之流程圖如圖二所示。



圖二：本文所提出方法之交互認證階段

根據上述步驟，我們可以得知行動用戶於認證時不會傳送其 ID_{MU}，而是透過使用暫時性的 ID 完成身分認證並達到匿名性，並以低運算量之運算達到資料之完整性與機密性之功能，將於下一章節進行安全性討論與分析。

4. 討論與分析

在此節中，我們對本文所提出的方法做安全性的分析，以下我們提出幾種攻擊方法來分析安全性以及與 Hu et al.的架構作計算成本之比較。安全性分析如下。

外部攻擊(Outsider attack)

假定有一外部攻擊者試圖破解主基地台之私密金鑰 X_{HA} 以騙取服務，然而此方法並不可行，因為具有該私密金鑰 X_{HA} 的參數如 A_{MU}、$TID_{MU\text{-}HA}$ 皆有單向雜湊函數保護，且私密金鑰 X_{HA} 並不會單獨存在或是公開傳送，故我們的方法能夠抵擋外部攻擊。

內部攻擊(Insider attack)

假定有一內部攻擊者試圖破解主基地台之私密金鑰 X_{HA} 以騙取服務，然而同樣不可行，內部攻擊者即使取得 $h(ID_{MU} \| X_{HA}) = A_{MU} \oplus PW$，但私密金鑰 X_{HA} 為主基地台所保有並有單向雜湊函數所保護，且私密金鑰 X_{HA} 並不會單獨存在或是公開傳送，故內部攻擊者無法破解取得 X_{HA}，也證實我們的方法能夠抵擋外部攻擊。

偽裝攻擊(Impersonation attack)

假定有攻擊者擷取合法用戶認證之參數 $\{r_{MU}, C_1, T_{MU}, TID_{MU\text{-}HA}, ID_{HA}\}$，試圖偽裝為合

法用戶以騙取服務，然而此法並不可行，因為當合法用戶進行認證時會產生出時戳，若攻擊者傳送過期的時戳，將會被外部基地台所發現，並且用戶認證參數 $C_1 = h(h(ID_{MU} \| X_{HA}) \| T_{MU})$與時戳一起經過單向雜湊函數運算，攻擊者無法隨意竄改，故我們的方法能夠抵擋偽裝攻擊。

重送攻擊(Replay attack)

假定有一攻擊者擷取合法用戶認證之參數{ r_{MU}, C_1, T_{MU}, $TID_{MU\text{-}HA}$, ID_{HA}}，試圖將合法用戶之參數重新發送給基地台以騙取服務，然而此方法並不可行，當攻擊者將合法用戶認證參數重新發送時會因為時戳過期而使認證失效且會被基地台所發現，而時戳與認證參數皆經過單向雜湊函數所保護，故攻擊者無法隨意更改時戳內容，也證實我們的方法能夠抵擋重送攻擊。

驗證表竊取攻擊(Stolen-Verifier attack)

假定有一攻擊者的攻擊目標為主基地台之驗證表格或是用戶行動裝置之 SIM 卡，以取得機密資料，然而此種攻擊並不可行，如 $ID_{MU} = TID_{MU\text{-}HA} \oplus h(r_{MU} \| X_{HA})$與比較 $C_1 = h(h(ID_{MU} \| X_{HA}) \| T_{MU})$是否相同，在我們的方法中主基地台以計算的方式取代查詢驗證表格，因此攻擊者沒有辦法攻擊存取認證資訊的驗證表格取得機密資料，且由於行動用戶 SIM 卡之認證資料由使用者自行設立之密碼所保護，故即使使用者不小心遺失其行動裝置被攻擊者所撿到，由於攻擊者並不知道認證時所需要之密碼，因此無法取得相關資料或服務，故根據上述理由我們的方法能夠抵擋驗證表竊取攻擊。

計算成本分析：

本節將呈現 Hu et al.與我們的方法之計算成本比較表，我們的方法沒有使用公開金鑰密碼系統的運算，採用最簡易的互斥或運算以及單向雜湊函數之運算，故能夠達到快速、有效率且高安全性之功用，兩種方法之比較表如表三所示。

表三、兩種方法之計算成本比較

方法 / 參與者	Hu et al.的方法	我們的方法
行動用戶	6H+3X+2S	6H+3X
外部基地台	4H+2P+1S	5H+5X
主基地台	6H+5X+1P	8H+8X
總計	16H+8X+3	19H+16X

H：單向雜湊函數

X：互斥或運算

S：秘密金鑰密碼系統加/解密運算

P：公開金鑰密碼系統加/解密運算

5. 結論

本文提出一個全新的全球行動網路之外部代理授權的匿名認證機制，為了符合行動裝置運算需求，採用高效率且低運算量之互斥或運算來對認證參數進行加密，並結合單向雜湊函數使認證參數更佳安全，具備機密性與完整性。使用者於認證過程中皆以暫時性之身分識別碼進行認證，達到匿名性之功用。且由於主基地台於認證時無須查找驗證表格，故可節省儲存空間與驗證表格維護成本。而合法用戶可透過代理授權的方式向外部基地台取得暫時性身分識別碼並使用服務，無須頻繁的向主基地台進行認證。根據上述理由，本文的方法不僅更加安全有效率，且更適於行動網路之環境。

致謝

本篇論文特別感謝由行政院國家科學委員會研究計劃，混合雲端服務上之金鑰管理與認證加密機制，計劃編號 NSC 102-2410-H-424-019 所提供之支援。

參考文獻

[1] C. C. Changa, C. Y. Lee, and Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks", *Computer Communications*, Vol. 32, No. 4, pp. 611-618, Mar. 2009.

[2] J. B. Hu, H. Xiong, and Z. Chen, "Further improvement of an authentication scheme with user anonymity for wireless communications", *International Journal of Network Security*, Vol. 14, No. 5, pp. 297-300, Sep. 2012.

[3] M. Kang, H. S. Rhee, and J. Y. Choi, "Improved User Authentication Scheme with User Anonymity for Wireless Communications", *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, Vol. 94, No. 2, pp. 860-864, 2011.

[4] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electron*, Vol. 53, no. 5, pp. 1683-1687, Oct. 2006.

[5] J. S. Lee, J. H. Chang, and D. H. Lee, "Security flaw of authentication scheme with anonymity for wireless communications", *IEEE Communications Letters*, Vol. 13, No. 5, pp. 292-293, May. 2009.

[6] K. Li, A. Xiu, F. He, and D. H. Lee, "Anonymous authentication with unlinkability for wireless environments", *IEICE Electronics Express*, Vol. 8, No. 8, pp. 536-541, Jan. 2011.

[7] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks", *Mathematical and Computer modeling*, Vol. 55, No. 1–2, pp. 214-222, Jan. 2012.

[8] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure anonymous authentication protocol with unlinkability for mobile wireless environment", *IEEE Conference on Anti-Counterfeiting, Security and Identification* (*ASID*), pp. 1-5, Taipei, Taiwan, 24-26 Aug. 2012.

[9] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications", *IEEE Communications Letters*, Vol. 12, No. 10, pp. 722-723, Oct. 2008.

[10] J. Xu, and D. Feng, "Security flaws in authentication protocols with anonymity for wireless environments", *ETRI Journal*, Vol. 31, No. 4, pp. 460-462, Aug. 2009.

[11] J. Zhu, and J. Ma, "A new authentication scheme with anonymity for wireless environments", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp. 231-235, Feb. 2004.

[12] P. Zeng, Z. F. Cao, K. K. Choo, and S. B. Wang, "On the anonymity of some authentication schemes for wireless communications", *IEEE Communications Letters*, Vol. 13, No. 3, pp. 170-171, Mar. 2009.