保護使用者身分資訊的認證方案

楊伏夷　　陳冠宇
朝陽科技大學　　朝陽科技大學
資訊工程系　　資訊工程系
副教授　　研究生
yangfy@cyut.edu.tw　s10127636@gm.cyut.edu.tw

摘要

目前的網路環境中，利用密碼來做身分認證已經非常普及，但利用密碼還是沒辦法抵禦很多攻擊。在 2012 年，Xie 提出利用一次性雙因子認證方案，雖然這個方案改進以前許多認證方案的缺失，可以抵禦很多攻擊，但我們發現該方案仍然是不安全，因為他的方案無法抵禦假冒攻擊和重複註冊的漏洞。檢視漏洞的原因，資訊在公眾網路中明文傳遞是主要原因，本篇文章提出改善方案，減少使用者或是伺服器的秘密資訊在傳輸過程中出現，並增強使用者登入時的隱私保密性，利用對稱式加密技術將秘密資訊加密，減少被竊聽的攻擊。

關鍵詞：雙因子、假冒攻擊、對稱式加密技術、竊聽攻擊。

Abstract

In the current network environment, it is common to certify the identities by codes; however, many attacks are inevitable. In 2012, Xie proposed the one-time two-factor certification scheme. Although the scheme supplements the past plans and can resist many attacks, this plan is still insecure as it cannot resist impersonation attack and repeated registrations. The main reason of the leak is that information is transmitted via public network. In this paper, we proposed an improvement scheme and avoided the appearance of secret information of users or servers in transmission, thus enhancing the confidentiality of users' log-in and encrypting the secret information by Symmetric Encryption to avoid eavesdropping attack.

Keywords: two-factor, impersonation attack, Symmetric Encryption, eavesdropping attack.

1. 前言

最近幾年網際網路的環境越來越發達，不論是在網路上進行交易或是利用行動裝置，例如:智慧型手機、平板電腦…等等，都是越來越普及。使用者和伺服器要在不安全的網路環境下進行相互認證成為很重要的議題。植基於密碼的相互認證技術使用非常普遍，因為使用者只需要記住密碼。在 2002 年，Yeh 等人[1]提出一個利用智慧卡及一次性密碼的身分驗證方案，但是在 2004 年，Tsuji 和 Shimizu[2]指出 Yeh 等人的方案會遭受到竊取驗證資料的攻擊，並提出一個針對竊取攻擊的一次性密碼驗證方案；在 2005 年，Lee 等人[3]也針對 Yeh 等人方案的弱點提出了改善方案，改善智慧卡及使用一次性密碼的安全驗證方案。在 2007 年，Wang 等人[4]指出 Yoon 等人[5]的方案會遭受到密碼猜測攻擊、偽裝攻擊、阻斷伺服器服務攻擊，並提出一個改善方案，但是在 2009 年，Chung 等人[6]指出 Wang 等人的方案會遭受到假冒攻擊、智慧卡遺失攻擊，在 2011 年，Chen 等人[7]指出 Wang 等人的方案會遭受到假冒攻擊、平行會議攻擊，並提出一個改善的方案。在 2010 年，Holbl 等人[8]指出 Shieh 等人[9]提出的方案會遭受到智慧卡遺失攻擊和此方案沒有達到完美的向前保密性，在 2012 年，Xie[10]指出 Holbl 等人的方案會遭受到平行會議攻擊、假冒攻擊、智慧卡遺失攻擊、離線密碼猜測攻擊，並提出一個改善的方案。在本篇文章中，我們將回顧 Xie 提出的方案，且透過安全性分析指出此方案仍會遭受假冒攻擊和重複註冊的問題。

2. 回顧 Xie 的方案

Xie 提出的方案主要分為三個階段，註冊階段、登錄階段、金鑰協議階段。首先介紹該方案所使用的參數定義，如表一所示。

2.1 註冊階段

當使用者想要使用伺服器的服務時，使用者必須先向伺服器申請註冊，如圖一所示，註冊步驟如下:

步驟一:

首先使用者選擇密碼 PW 和身分 ID，經由安全通道將$\{ID\}$傳給伺服器。

步驟二:

當伺服器接收到訊息$\{ID\}$，接著計算 $d = h(ID \oplus X)$，然後將$\{d, ID, h(\ )\}$儲存到智慧卡裡面，最後將智慧卡經由安全通道傳給使用者。

表一. 參數定義

(p, q)	兩個大質數並滿足 $q \mid p-1$
g	g 是乘法群 G 的產生器，其序為 q，G 是模 p 乘法群 Z_p^* 的子群，$G \subset Z_p^*$。
U	使用者
ID	使用者 U 的身分
PW	使用者 U 的密碼
S	伺服器
$h(\ )$	一個安全的單向雜湊函數
(X, Y)	伺服器的公私鑰對, $Y= g^X \bmod p$
T_U	使用者產生的時戳
T_S	伺服器產生的時戳
$\oplus$	互斥或運算符號
$\|\|$	串接運算符號

步驟三:

當使用者收到智慧卡，接著計算 $R = d \oplus h(PW)$，並將 d 更換為 R。

2.2 登入及金鑰協議階段

當使用者想要登入伺服器時，必須傳送登入訊息給伺服器做驗證，如圖二所示，步驟如下:

步驟一:

首先使用者將自己的智慧卡插入讀取裝置，並且輸入自己的身分 ID 及密碼 PW。接著智慧卡產生隨機亂數 $c < p-1$，然後計算

$$d = R \oplus h(PW)$$
$$C_0 = Y^c \bmod p$$
$$C_1 = g^c \bmod p$$
$$C_2 = h(d \| C_0 \| T_U)$$

最後將登入訊息$\{ID, C_1, C_2, T_U\}$傳給伺服器。

步驟二:

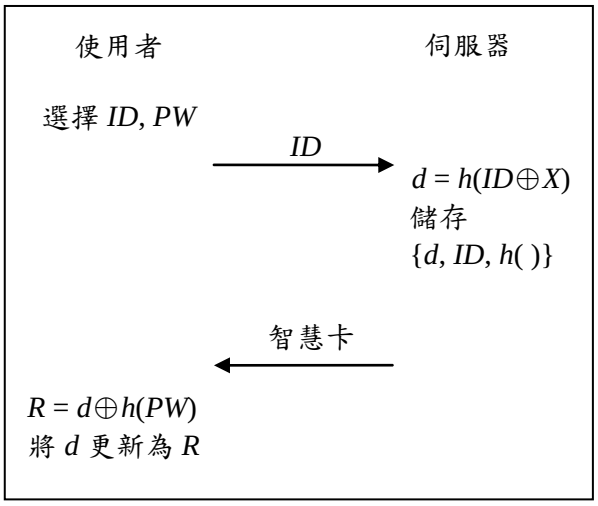
伺服器收到登入訊息後，首先驗證時戳是否符合$(T_S - T_U) \leqq \triangle T$，$T_S$為伺服器收到訊息的時間，$\triangle T$ 為預先定義的時間門檻。接著計算 $C_2' = h(h(ID \oplus X) \| (C_1)^X \bmod p \| T_U)$，並驗證 C_2'是否等於 C_2，如果都驗證成功，伺服器會認為使用者是合法的。

步驟三:

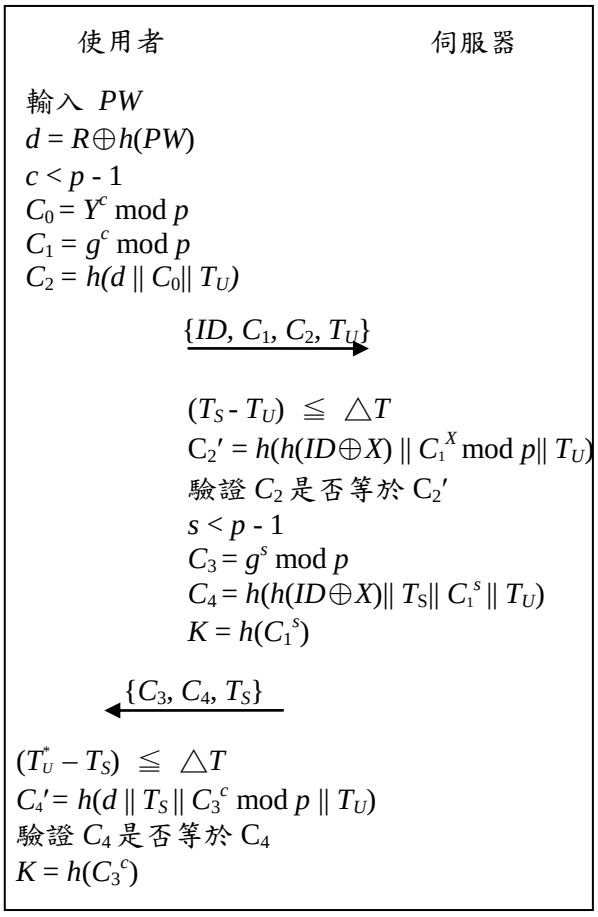
伺服器會選擇一個隨機亂數 $s < p-1$，接著計算

$$C_3 = g^s \bmod p$$
$$C_4 = h(h(ID \oplus X) \| T_S \| (C_1)^s \bmod p \| T_U)$$
$$K = h((C_1)^s \bmod p)$$

並將$\{C_3, C_4, T_S\}$傳給使用者。



圖一. 註冊階段



圖二. 登入及驗證階

步驟四:

當使用者收到訊息後，智慧卡會先驗證時戳是否符合$(T_U^* - T_S) \leqq \triangle T$，$T_U^*$為使用者收到訊息的時間。接著計算 $C_4' = h(d \| T_S \| (C_3)^c \bmod p \| T_U)$，並驗證 C_4'是否等於 C_4，如果都驗證成功，使用者會認為伺服器為合法的。

步驟五:

使用者也會計算 $K = h(C_3)^c \bmod p$，使用者和伺服器端會把 K 當作會議金鑰來進行溝通。

3. 安全性分析

在本章節我們指出 Xie 的方案仍然有安全漏洞存在。

(1) 假冒攻擊

在 Xie 提出的方案中，我們發現這個方案無法抵擋偽裝攻擊，當攻擊者想假冒使用者，將會執行下列步驟。

步驟一:

由於使用者註冊完後，伺服器並沒有儲存使用者的身份 *ID* 以及沒有確認 *ID* 是否有重複的情形。

假如攻擊者攔截到使用者的登入訊息{*ID*, C_1, C_2, T_U}，由於使用者所傳的訊息內 *ID* 並沒有經過保護，所以攻擊者可以拿到使用者的身份 *ID*。

步驟二:

攻擊者可以拿使用者的 *ID*，向伺服器註冊，攻擊者的智慧卡裡的資訊{*R*, *ID*, *h*( )}除了密碼和使用者的密碼不一樣以外，其他都和使用者相同。所以攻擊者只要利用自己的智慧卡和密碼登入，智慧卡算出的 $d = R \oplus h(PW)$會和使用者的 *d* 一樣，這樣就成功假冒成其他使用者。

(2) 保護使用者身分

由上述章節所敘述，Xie 提出的方案中，使用者身份的隱私保密性是非常脆弱的，使用者的身份 *ID* 沒有經過任何加密或是匿名保護，所以任何惡意攻擊者擷取登入訊息就可以輕易的得到使用者的身份。

4. 改進的方案

在此章節我們改善了 Xie 的方案來抵擋假冒攻擊和重複註冊的問題。在改進的方案裡，我們分為註冊階段、登錄階段、金鑰協議階段，各階段流程在下面依序介紹。

4.1 註冊階段

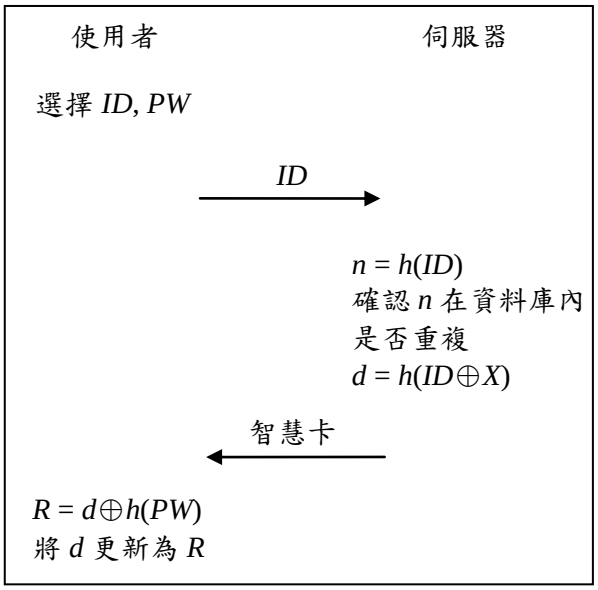
當使用者想要使用伺服器的服務時，使用者必須先向伺服器申請註冊，如圖三所示，註冊步驟如下:

步驟一:

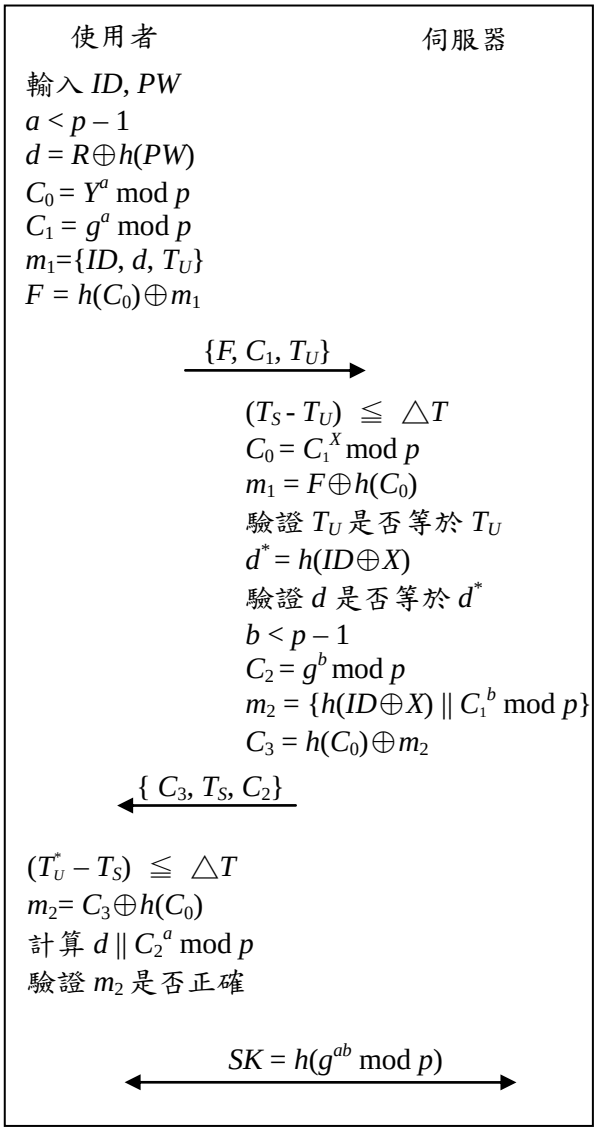
首先使用者選擇密碼 *PW* 和身分 *ID* ，經由安全通道將{*ID*}傳給伺服器。

步驟二:

當伺服器接收到訊息{*ID*}，接著計算 $n = h(ID)$，並確認 *n* 是否在資料庫內有重複，如果沒有重複的 *n*，繼續計算 $d = h(ID \oplus X)$，然後將{*d*, *h*( )}儲存到智慧卡裡面，最後將智慧卡經由安全通道傳給使用者。



圖三. 註冊階段



圖四. 登入及驗證階段

步驟三:

當使用者收到智慧卡，接著計算 $R = d \oplus$

$h(PW)$，並將 d 更新為 R。

4.2 登入及金鑰協議階段

當使用者想要登入伺服器時，必須傳送登入訊息給伺服器做驗證，如圖四所示，步驟如下:

步驟一:

首先使用者將自己的智慧卡插入讀取裝置，並且輸入自己的身分 ID 及密碼 PW。接著智慧卡產生隨機亂數 $a < p - 1$，然後計算

$$d = R \oplus h(PW)$$
$$C_0 = Y^a \bmod p$$
$$C_1 = g^a \bmod p$$
$$m_1 = \{ID, d, T_U\}$$
$$F = h(C_0) \oplus m_1$$

最後將登入訊息$\{F, C_1, T_U\}$傳給伺服器。

步驟二:

伺服器收到登入訊息後，驗證使用者是否合法。首先驗證時戳是否符合$(T_S - T_U) \leqq \triangle T$，$T_S$ 為伺服器收到訊息的時間，$\triangle T$ 為預先定義的時間門檻。接著計算 $C_0 = C_1^X \bmod p$，並利用 $h(C_0)$和 F 做互斥或運算得到 $m_1 = \{ID, d, T_U\}$，並驗證 T_U和使用者傳送過來的 T_U是否相同，如果相同會繼續計算 $d^* = h(ID \oplus X)$，並驗證 d^* 是否等於 d，如果都驗證成功，伺服器會認為使用者是合法的。

步驟三:

伺服器會選擇一個隨機亂數 $b < p - 1$，接著計算

$$m_2 = \{h(ID \oplus X) \,\|\, C_1^b \bmod p\}$$
$$C_3 = h(C_0) \oplus m_2$$

並將$\{C_3, T_S, C_2\}$傳給使用者。

步驟三:

當使用者收到訊息後，智慧卡會先驗證時戳是否符合$(T_U^* - T_S) \leqq \triangle T$，$T_U^*$為使用者收到訊息的時間。並利用 $h(C_0)$和 C_3 做互斥或運算得到 $m_2 = \{h(ID \oplus X) \,\|\, C_1^b \bmod p\}$，使用者也會計算 $d \,\|\, C_2^a \bmod p$，並與運算得到的資料 m_2 做驗證，如果都驗證成功，使用者會認為伺服器為合法的。

步驟四:

使用者和伺服器會同時計算出 $SK = h(C_2^a \bmod p)$ 和 $SK = h(C_1^b \bmod p)$，這把會議金鑰這是此次溝通用的金鑰。

5. 安全性分析

在本章節將對我們所提出的方案進行安全分析。

(1) 抵禦假冒攻擊

假如攻擊者 A 不是一個合法的使用者，他想要偽裝成一個合法使用者 B，他將執行下列步驟。

步驟一:

首先攻擊者 A 攔截使用者 B 的登入訊息$\{F, C_1, T_U\}$。

步驟二:

使用者 B 的身份 ID 包含在 F 內，雖然攻擊者 A 取得 $C_1 = g^a \bmod p$，還是沒辦法取得 F 內的訊息 m_1，因為 $h(C_0) = Y^a \bmod p = g^{aX} \bmod p$，攻擊者 A 會遇到離散對數問題，所以攻擊者 A 無法取得使用者 B 的身份 ID，藉由上述分析可以得知，偽裝攻擊在我們提出的方案裡是無法成功的。

(2) 抵禦離線密碼猜測攻擊

假設攻擊者 A 攔截使用者 B 的登入訊息$\{F, C_1, T_U\}$，以及得到戶用 B 的智慧卡並提取裡面的參數來進行離線密碼猜測，將執行下列步驟。

步驟一:

攻擊者 A 可以計算出 $d^* = R \oplus h(PW^*)$，並選擇隨機亂數 a^*，接著計算出 $C_0' = Y^{a^*} \bmod p$，計算出 $F^* = h(C_0') \oplus m_1'$。

步驟二:

攻擊者利用自己計算出的 F^*並跟攔截到的 F 比較是否相等。

由於攻擊者 A 無法取得使用者 B 的身份 ID，所以 F 的內容裡就包含兩個未知數 $\{ID, d\}$，另外 $C_0 = Y^a \bmod p = g^{aX} \bmod p$，攻擊者無法計算出 C_0，因為他會遇到離散對數的問題，因此我們提出的方案可以抵禦離線密碼猜測攻擊。

(3) 抵禦平行會議攻擊

在本方案中的兩個驗證資料 $F = h(C_0) \oplus m_1$和 $C_3 = h(C_0) \oplus m_2$，假設攻擊者將 C_3傳送給伺服器，伺服器首先驗證時戳會通過，但是伺服器將 C_3和 $h(C_0)$做互次或運算後，m_2裡面並沒有包含時戳，所以在第二次驗證時戳不會驗證成功，因此平行會議攻擊時無法成功通過驗證。

(4) 抵禦重送攻擊

假設攻擊者重送使用者的登入訊息$\{F, C_1, T_U\}$給伺服器，此訊息會被拒絕，因為訊息內的時戳已經超過正常延遲時間。假如攻擊者將時戳 T_U 替換成合法的時戳 T_A，這樣還是無法通過驗證，因為 F 內包含的時戳 T_U和 T_A並不相同，因此可以抵禦重送攻擊。

(5) 抵禦內部攻擊和使用者的匿名性

在本方案中，使用者的身份是受保護的，雖然伺服器端有儲存表格，但是使用者的 ID

都經過雜湊函數計算，即使遭受內部攻擊，攻擊者拿到表格也無法推算出使用者的 *ID*。

6. 結論

在本篇文章中，我們回顧 Xie 的方案，並藉由安全性分析來證明 Xie 所提出的方案還是有安全漏洞，Xie 的方案會遭受到偽裝攻擊和重複註冊的問題。因此我們針對這些弱點來改善此方案，也由安全性分析來證明我們的方案可以抵禦偽裝攻擊和重複註冊的問題，也證明了我們的方案較先前的方案更安全。

7. 致謝

審稿委員們寶貴的評論與建議以及國科會專案研究計畫補助部分經費，謹此致謝，計畫編號：NSC 101-2221-E-324-047。

參考文獻

[1] Yeh, T.C., Shen, H.Y. and Hwang, J.J. ‘‘A secure one-time password authentication scheme using smart cards’’, ***IEICE Transaction on Communication***, Vol.E85-B, No.11, pp. 2515–2518, 2002.

[2] Tsuji, T. and Shimizu, A. ‘‘One-time password authentication protocol against theft attacks’’, ***IEICE Transactions on Communications***, Vol.E87-B, No.3, pp. 523–529, 2004.

[3] Lee, N.Y. and Chen, J.C. ‘‘Improvement of one-time password authentication scheme using smart card’’, ***IEIC E Transaction on Communications***, Vol.E88-B, No.9, pp. 3765–3769, 2005.

[4] Wang, X.M., Zhang, W.F., Zhang, J.S. and Khan, M.K. ‘‘Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards’’, ***Computer Standards & Interfaces***, Vol.29, No.5, pp. 507–512, 2007.

[5] Yoon, E.J., Ryu, E.K. and Yoo, K.Y. ‘‘Further improvement of an efficient password based remote user authentication scheme using smart cards’’,***IEEE Transactions on Consumer Electronics***, Vol.50, No.2, pp. 612–614, 2004.

[6] Chung, H.R., Ku, W.C. and Tsaur, M.J. ‘‘Weaknesses and improvement of Wang et al.’s remote user password authentication scheme for resource-limited environments’’, ***Computer Standards & Interfaces***, Vol.31, No.4, pp. 863–868, 2009.

[7] Chen, T.H., Hsiang, H.C. and Shih, W.K. ‘‘Security enhancement on an improvement on two remote user authentication schemes using smart cards’’, ***Future Generation Computer Systems***, Vol.27, No.4, pp. 377–380, 2011.

[8] Holbl, M., Welzer, T. and Brumen, B. ‘‘Attacks and improvement of an efficient remote mutual authentication and key agreement scheme’’, ***Cryptologia***, Vol.34, No.1, pp. 52–59, 2010.

[9] Shieh, W.G. and Wang, F.M. ‘‘Efficient remote mutual authentication and key agreement’’, ***Computers & Security***, Vol.25, No.1, pp. 72–77, 2006.

[10] Xie, Q.“Improvement of a security enhanced one-time two-factor authentication and key agreement scheme”, **(Scientia Iranica)** ***Transactions D: Computer Science & Engineering and Electrical Engineering***, Vol.19, No.6, pp.1856-1860, 2012.

[11] Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold, “Efficient, DoS-resistant, secure key exchange for internet protocols,” ***Security Protocols: 9th international workshop***, Cambridge, UK, April 25-27, LNCS 2467, pp. 27-39, 2002.

[12] Blaze, M., “Efficient, DoS-resistant, secure key exchange for internet protocols (Transcript of Discussion),” ***Security Protocols: 9th international workshop***, Cambridge, UK, April 25-27, LNCS 2467, pp. 40-48, 2002.

[13] Camenisch, J. and Thomas, G., “Efficient attributes for anonymous credentials,” ***In Proceedings of the 15th ACM conference on Computer and communications security***, pp. 345-356, 2008.

[14] Dey and Weis, S. , “PseudoID: Enhancing Privacy in Federated Login,” ***Hot Topics in Privacy Enhancing Technologies***, pp. 95-107, 2010.

[15] Han, J., Zhu, Y., Liu, Y., Cai, J., and Hu, L., “Provide Privacy for Mobile P2P Systems,” ***First International Workshop on Mobility in Peer-to-Peer Systems*** (MPPS) (ICDCSW'05), ICDCSW, Vol. 8, pp. 829-834, 2005.