一個以身分為基礎的高效率身分認證協定

Fuw-Yi Yang　　Hung-Yumr Chen

Department of Computer Science and Information Engineering,

Chaoyang University of Technology

yangfy@cyut.edu.tw　　s9627617@cyut.edu.tw

摘要

隨著無線網路普及化，許多使用者透過無線網路來做資訊傳輸，使用時首先使用者必須去基地台註冊自己的身分，經過驗證身份合法性後，才能夠跟基地台達成通訊。在身分驗證時，等待和回應的時間過於長久，便會消耗過多的行動裝置電力。在 2004 年，有學者提出加入時間戳章的方法，可以有效改善在無線網路傳輸環境中，行動裝置和基地台之間的等待和回應時間。但是攻擊者卻可以透過偽造時間戳章的方式，來達到攻擊的目的。因此我們提出新的方法改善之，利用共同協商金鑰和對稱式密碼系統，降低通訊和計算量，且在計算過程中加密時間戳章，達到安全性和效率的提昇，使得我們的協定能夠運用於行動裝置環境中。

關鍵字:身分驗證密碼系統、使用者鑑別、行動裝置。

Abstract

In mobile communication, most of the mobile devices are powered by batteries. In order to economize the power consumption of mobile devices, some ID-based one-move authentication protocols have been proposed. Adopting ID-based reduces the bit length of the authentication data. Using one-move protocol lessens the delay-time which is the period waiting for a response from the intended party during the authentication phase.

The paper demonstrates that some of the previous ID-based one-move authentication protocols suffer from the impersonation attack. New protocol is proposed to mend the weakness and to improve the efficiency of communication and computation. The improvement makes our scheme suitable in wireless environment.

Keyword: Identity-based cryptosystem, User identification, Mobile device.

1. 緒論

近年來行動通訊和網路技術的蓬勃發展和普及化，運用手機或電腦無線上網對於現代人來說，已經不再是難題，因此行動裝置如何達成跟基地台間通訊，和如何驗證使用者身份等問題，於技術發展階段都會慢慢被受重視。

在 1984 年，Shamir 提出一個基本的公鑰加密系統概念，此協定能夠把使用者的身分資訊當成加密的公開金鑰[1]。使用者有能力在驗證簽章的時候不必透過第三者驗證，也不必進行交換公開金鑰和秘密金鑰的動作，使用者使用唯一的身分資訊（如：姓名、地址或 e-mail…等）來當作公開金鑰。在 1991 年，Maurer-Yacobi 提出一個以身份為基礎的非交談式公鑰加密協定，並在 1996 年推出了最終的版本[2]，此協定使得使用者不用產生認證的交談公開金鑰就能驗證身份資訊。在 1998 年，Tseng-Jan 提出以身份為基礎的交談式公鑰分配系統 [3]，由於身份就是公開金鑰，使用者在跟任何人確認身分時，僅需透露使用者自己的身份，使用三回合的身份認證協定，就可達成身份認證的目標。但是將同樣的系統移植到無線網路環境時，三回合的認證協定，代表行動裝置和基地台之間的資料傳遞共有三筆，彼此之間需等待資料的到來，又因為行動裝置的電力是有限的，所以必須改善行動裝置和基地台傳輸的等待和回應時間。為解決此一不足之處，Hwang et al.在 2004 年提出單一回合的身份認證協定[4]，在產生驗證訊息的同時，加入時間戳章的觀念，用以改善行動裝置跟基地台認證時的等待和回應時間，使得整個架構更適合在無線網路環境下執行。但是此協定，並沒有提出保護時間戳章的機制，導致攻擊者能透過偽造時間戳章的方法達到攻擊。

隨後在 2006 年時，Chou et al.提出了改善 Hwang et al.技術協定的方法[5]，利用加密時間戳章，防止攻擊者的攻擊，但是仍然無法有效防止類似的攻擊。有鑑於上述的問題，我們提出了改善的方法，用以改善以上的密碼安全漏洞，並且讓我們提出的協定也適合在無線網路的環境中使用。

在本論文中，將在第二章節回顧 Hwang et al.'s 技術協定，第三章節討論 Chou et al.攻擊問題，並且提出我們對 Hwang et al.技術協定的攻擊方法，第四章說明我們所提出的協定，並在第五章和第六章做安全和效能分析講解。

2. 回顧 Hwang et al.'s scheme

基本上 Hwang et al.'s 協定承襲了 Tseng-Jan's 協定的有利優點，使用者身分就是他的公鑰。一個可信任的權限管理機構(TA)產生系統的參數：$N = p_1 p_2 p_3 p_4$ 是四個質數的乘積，每個質數(p_j , j = 1…4)的數值範圍為 10^{60} 到 10^{70} 之間，且滿足 $(p_j - 1)/2$ 為質數，N 就是往後計算的共同模數。參數 p_j 如上設定，則 TA 可以利用後門資訊來計算離散對數，不知後門資訊者無法對 N 分解因數。TA 從 $Z_{\phi(N)}$ 中選取一個整數 e 和私鑰 d 滿足 $ed = 1 \bmod \phi(N)$；從 $Z_{\phi(N)}$ 選取一個亂數 t，$\phi(N)$表示為一個 Euler's totient function；g 是 Z_N^*的元素但也是每個有限群 GF(p_j)，j = 1…4 的原根；$h(\cdot)$ 表示為一個單向的雜湊函數。TA 公告系統的公開金鑰是:{N, g, e, $h(\cdot)$}, 私密金鑰{d, t, p_1, p_2, p_3, p_4}則秘藏之。

底下將 Hwang et al.'s 協定分為註冊階段與加入階段敘述之。

註冊階段:

假設使用者 Alice 其身份以 ID_a 表示之，欲加入系統，Alice 應先顯示身份證件，TA 審查合格之後，使用後門資訊來計算離散對數 $\log_g(ID_a^2) \bmod N$ 及 $s_a = et\log_g(ID_a^2) \bmod N$，將 s_a 發給 Alice 以為日後身份認證之用。

加入階段:

行動裝置 M(其身份以 ID_m)表示之，將透過下列三個步驟跟基地台 B(其身份以 ID_b 表示之)達成使用者身分認證。圖一表示整個身分認證的流程。

步驟 1:

行動裝置(M)從 Z_N^* 選取一個隨機亂數 k，並產生一個時間戳章 T，隨後算出 Y 和 Z：

$Y = (ID_m^2)^k \bmod N$，

$Z = (ID_b^2)^{ks_m T} \bmod N$。

傳送訊息 $L = \{(ID_m \| Y \| Z), T\}$給基地台(B)。

步驟 2:

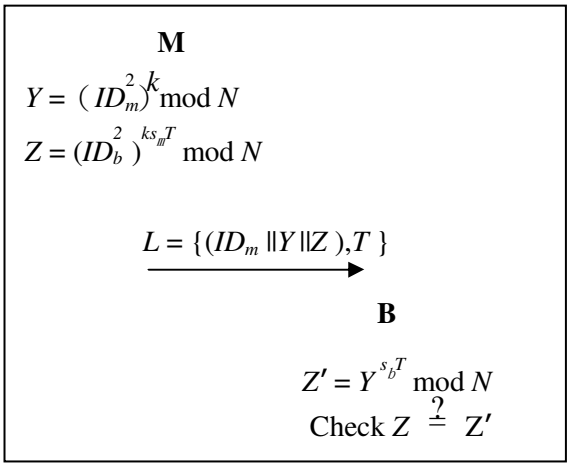
從行動裝置(M)收到訊息 L，基地台(B)計算：

$Z' = Y^{s_b T} \bmod N$。

步驟 3:

基地台(B)確認等式 $Z' = Z$ 是否成立，假如成立則基地台(B)確認行動裝置(M)的身份為有效的。

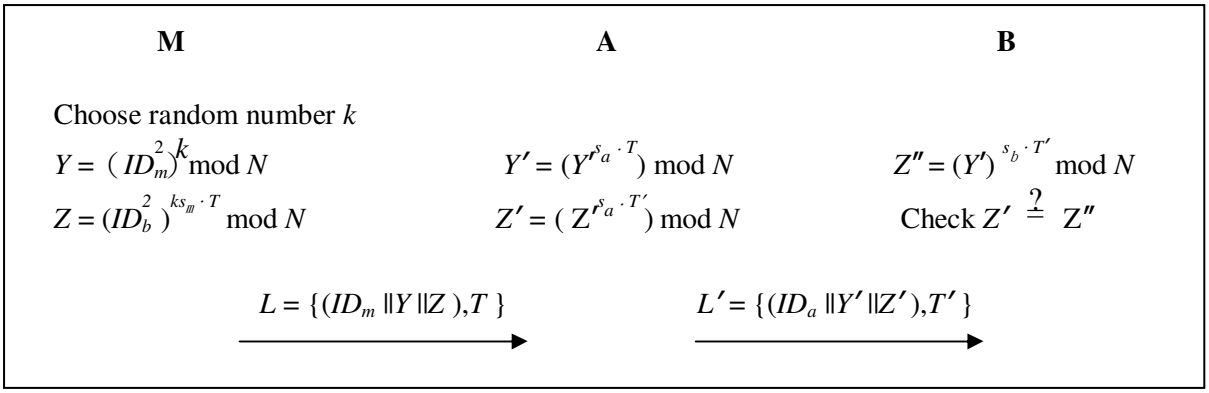
我們可以發現所有的傳輸訊息在上述的步驟中跟在 Tseng-Jan's 協定都是一樣的，除了在過程中多附加了時間戳章 T。即，Hwang et al.'s 協定利用時間戳章 T 來建造單通道使用者身份驗證系統，解決行動裝置在無線網路傳輸環境內的回應和等待時間。



圖一 Hwang et al.'s scheme 傳輸過程

3. 討論

Hwang et al.提出的架構較大的缺點，就是在傳輸過程中時間戳章沒有受到任何保護。在 2006 年時，Chou et al.提出了一個偽造攻擊方法，攻擊 Hwang et al.。圖二為 Chou et al.等學者提出的攻擊過程。



圖二 Chou et al.'s attack

針對 Hwang et al.'s scheme 的漏洞，我們提出了另一個偽造攻擊方法。圖三為我們提出的對 Hwang et al.'s scheme 的偽造攻擊方法。

步驟 1:

行動裝置(M)從$\{0,1\}^l$中隨機選取一個亂數 k，並產生一個時間戳章 T，隨後算出 Y 和 Z：

$Y = (ID_m^2)^k \bmod N = g^{ks_m/(et)} \bmod N$，

$Z = (ID_b^2)^{ks_m T} \bmod N = g^{kTs_b s_m/(et)} \bmod N$。

步驟 2:

當時間戳章 T'的時候，惡意的攻擊者(A)途中攔截行動裝置(M)所傳輸的訊息，並對接收到的訊息(ID_m, Y, Z, T)加以偽造。首先計算 T 與 T' 的最小公倍數，再平衡 Y 與 Z 的指數部分即可完成為冒名攻擊：

$w = \text{lcm}(T, T')$，

$Y' = (Y)^{w/T'} \bmod N = g^{wks_m/(T'et)} \bmod N$，和

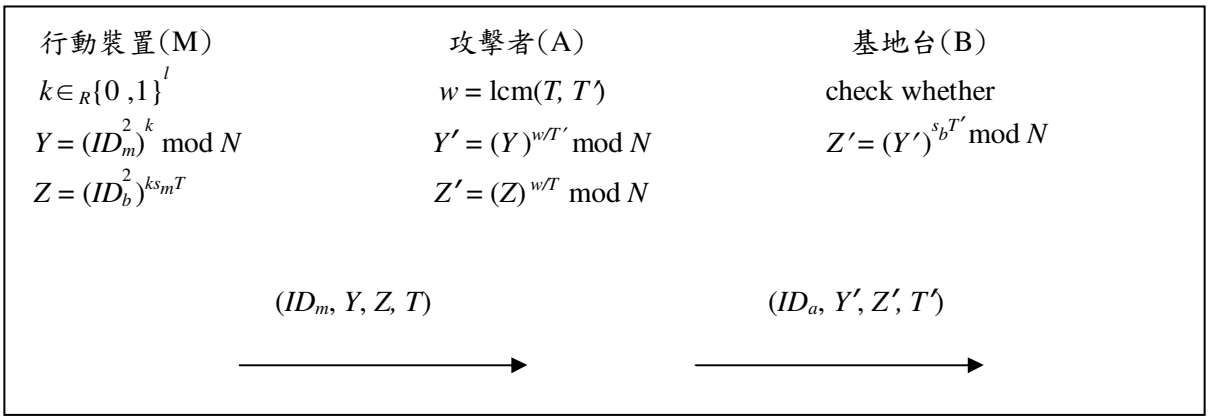
$Z' = (Z)^{w/T} \bmod N = g^{wks_b s_m/(et)} \bmod N$。

步驟 3:

假設攻擊者意欲假冒 ID_a，當做完 Y'與 Z'之運算之後，攻擊者就會把加工的訊息(ID_a, Y', Z', T')，傳送給基地台(B)做驗證，基地台收到後，會驗證下列訊息：

$Z = (Y')^{s_b T'} = g^{wks_b s_m/(et)} \bmod N$。

由運算完後的結果，可以發現攻擊者只要在通訊媒體截取一個有效的認證資料，並不需要任何使用者 ID_a 的私鑰 S_a，即可以在任何時刻假冒 ID_a，成功的通過基地台(B)的驗證。如果基地台與使用者之間未採取進一步的通訊金鑰協商，則攻擊者可以直接跟基地台做傳輸，或者攔截行動裝置(M)所傳輸到基地台(B)的訊息，竄改或偽造行動裝置所傳送的正確訊息，達到攻擊的目的。



圖三對 Hwang et al.'s scheme 的偽造攻擊方法

4. 我們的協定

經過討論可以發現 Hwang et al.提出的架構較大的缺點，就是時間戳章在傳輸過程，沒有受到任何保護，使惡意攻擊者能輕易發動偽造攻擊。

在我們協定中，行動裝置和基地台通訊時，時間戳章是受到保護的，而使得惡意的攻擊者，無法去達到竄改或者偽造的目的，而行動裝置在加入階段中，與基地台使用交談金鑰來互相驗證彼此身份，達到安全性提昇的目的。

我們的架構繼承之前 Tseng-Jan 提出架構的優點，把使用者的身分資訊當作加密的公鑰。使用單一次的通訊即可完成使用者身分驗證的動作，使用參數$\{N, g, e, d, t, p_1, p_2, p_3, p_4\}$跟 Tseng-Jan 提出的架構都相同。底下將我們的協定分為註冊階段與加入階段敘述，闡釋行動裝置(M)如何產生對稱金鑰並且與基地台(B)達成協商交談金鑰以及互相驗證。

註冊階段:

假設使用者 Alice 其身份以 ID_a 表示之，欲加入系統，Alice 應先顯示身份證件，TA 審查合格之後，使用後門資訊來計算離散對數 $\log_g(ID_a^2) \bmod N$ 及 $s_a = et\log_g(ID_a^2) \bmod N$，將 s_a 發給 Alice 以為日後身份認證之用；故行動裝置(M)及基地台(B)註冊完畢之後，分別擁有秘密金鑰和公開金鑰(s_m, ID_m)與(s_b, ID_b)。

加入階段：

完成加入階段之後，行動裝置(M)及基地台(B)共享的交談金鑰為 K_{bm}，加入階段如下兩個步驟，圖四為整個加入階段的加密和驗證過程。

步驟 1:

行動裝置(M)從 $\{0, 1\}^l$ 中選取任意亂數 t，l 是安全等級參數。設 T_m 為時間戳章，則共同享有的長期交談金鑰 K_{bm}、密文訊息 C 和訊息摘要 T_G 計算如下：

$K_{bm} = ((ID_b)^2)^{s_m} \bmod N$

$= K_e \| K_m$ (把 K_{bm} 分成兩組金鑰)，

$C = E_{k_e}(t, T_m)$，

$T_G = T_{K_m}(C, ID_b, ID_m)$

傳送訊息(C, ID_m, T_G)給基地台(B)。

以上使用對稱式加密函數$(E_{k_e}(\cdot))$產生密文訊息 C，使用不可逆的雜湊函數$(T_{k_m}(\cdot))$產生訊息摘要 T_G，其中 k_e 與 k_m 分別是加密函數及雜湊函數的金鑰。

步驟 2:

當基地台(B)收到訊息(C, ID_m, T_G)後，先計算共同享有的長期交談金鑰 K_{bm}，驗證訊息摘要 T_G 和解密 C，執行程序如下：

$K_{bm} = ((ID_m)^2)^{s_b} \bmod N$

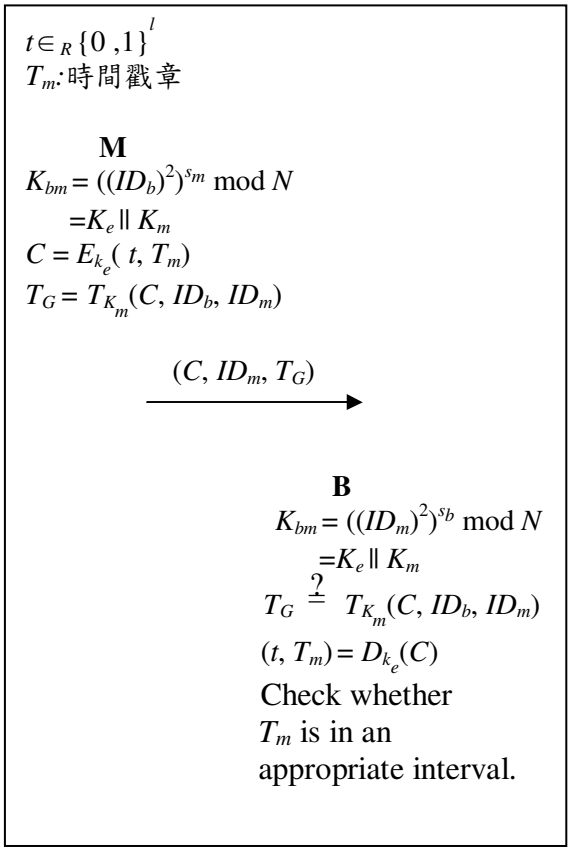
$= K_e \| K_m$ (把 K_{bm} 分成兩組金鑰)，

確認 $T_G = T_{K_m}(C, ID_b, ID_m)$，

$(t, T_m) = D_{k_e}(C)$，

確認 T_m 是正確的時間戳章。

以上 $D_{k_e}(\cdot)$是相對於 $E_{k_e}(\cdot)$的對稱式解密函數，用來得到亂數 t 與時間戳章 T_m，其中亂數 t 可以當作短期共同享有的交談金鑰。



圖四加密和驗證流程

5.效能分析

在這章節，我們提出跟 Hwang et al.的協定做完整的計算效能分析。在他們的協定內，是以加入時間戳章的方法，減少通訊過程中的等待時間，提高通訊傳送效率。我們提出的協定，傳送加密時間戳章訊息、使用者身份訊息和簽章給基地台，即可完成驗證，花費通訊量

比 Hwang et al.的協定還要更有效率。

設若公開金鑰密碼系統中，n 為 1024 位元的合成數($|n| = 1024$)，安全等級參數 $l = 160$，$|ID|$位元長度為 160 位元。對稱式密碼系統若使用 AES，則輸出位元大小為 128 位元。由於指數運算的計算量極大於對稱式密碼系統的計算量，因此在計算量的分析中，我們將忽略這個項目。

表一 效能分析

	Hwang et al. 之協定	我們的協定
通訊花費	2368	480
指數運算花費	3	2

在我們的協定中，短期共享交談金鑰由行動裝置(M)產生，不需透過協商過程即可獲得，並且所有的驗證參數皆使用對稱式金鑰密碼系統做演算，當協定執行時，只需較低的通訊量以及計算量，因此，我們的協定能夠實際地運用在行動裝置上。

6. 安全分析

Hwang et al.等學者提出的協定，是在傳送階段加入時間戳章和運算困難的離散對數問題上面。我們所提出的協定，運用對稱式密碼系統，對時間戳章加以加密，改善 Hwang et al.時間戳章被偽造攻擊的問題，達到更安全的效果。

攻擊 1. 若攻擊者想藉由可得知的資訊計算出交談金鑰，我們的協定是可以抵抗的。

攻擊者可在行動裝置(M)與基地台(B)通訊時，中間攔截訊息取得(C, ID_m, T_G)，但計算交談金鑰 K_{bm}，會遇到解因式分解問題，因為必須得知行動裝置(M)的密鑰 s_m，而 s_m 只有行動裝置使用者知道，因此，攻擊者無法取得 s_m 來計算共同交談金鑰。

攻擊 2. 若攻擊者想進行偽造攻擊，我們的協定是可以抵抗的。

在我們的協定中，已經嵌入了使用者驗證機制，攻擊者若想偽造合法訊息(C', ID_m, T_G')，使得基地台驗證成功，那攻擊者必須知道正確的共同協商金鑰 K_{bm} 的值，使得 C'與 T_G'為合法訊息，然而在協定中，共同協商金鑰 K_{bm} 並未包含在通訊資訊內，因此，我們的協定是可以抵抗偽造攻擊的。

攻擊 3. 若攻擊者想進行重複攻擊，我們的協定是可以抵抗的。

由於我們的協定把時間戳章經過加密加入在驗證資料內，而行動裝置每次所傳送訊息的時間戳章皆為不同的數值，因此，攻擊者無法使用先前儲存的時間戳章，使得 B 驗證成功。

7. 結論

在本篇論文中，我們可以看出 Hwang et al.提出的架構，很容易遭受惡意使用者的偽造攻擊。而我們所提出的解決方法，能夠把時間戳章在多一層保護下加入我們的協定，且只要經過一次通訊就能夠完成驗證使用者身份的動作，還保留了減低使用者和基地台的傳輸和等待驗證時間的優點，使得我們提出的協定，也能夠適合在無線傳輸網路環境內運用。

8. 參考文獻

[1] Shamir, Identity based cryptosystems & signature scheme, *Advances in Cryptology, CRYPTO'84, Lecture Notes-Computer Science*, 1984, pp. 47-53

[2] U.M. Maurer, Y. Yacobi, A non-interactive public-key distribution system, *Des Codes and Cryptography (1996)*, pp.305-316

[3] Y.M. Tseng, J.K. Jan, ID-based cryptographic schemes using a non-interactive public-key distribution system, *Computer Security Applications Conference, 1998, Proceedings., 14th Annual 7-11*, Dec. 1998 , pp.237 - 243

[4] M.S. Hwang, J.W. Lo, and S.C. Lin, An efficient user identification scheme based on ID-based cryptosystem, *Computer Standards & Interfaces*, Vol. 26, October 2004, pp. 565-569.

[5] Jue-Sam Chou, Yalin Chen, and Chu-Hsing Lin, An improvement of an efficient user identification scheme based on ID-based cryptosystem, *Sensor Networks, Ubiquitous, and Trustworthy Computing 2006. IEEE International Conference*, Vol. 1, June 2006, pp. 558 – 561.