改善 Chen 等人利用行動裝置適用於衛星通訊系統的自我認證機制

陳金鈴
朝陽科技大學資訊工程系
副教授
clc@mail.cyut.edu.tw

鄭凱文
朝陽科技大學資訊工程系
研究生
s9927630@cyut.edu.tw

摘要

在 2009 年，Chen 等人提出了利用行動裝置藉由衛星通訊達到更廣泛的溝通目的，在協定當中，出現了安全性方面的漏洞，造成行動使用者的資訊可能會被偷取。當攻擊者截取行動使用者的資訊後，就能進行假冒使用者攻擊，因此我們提出了改善的方法，讓行動裝置藉由衛星通訊系統做溝通，達到更安全的保護。

關鍵詞：衛星通訊系統、假冒使用者攻擊、行動裝置。

Abstract

In 2009, Chen et al. proposed the use mobile devices via satellite communications to reach a wider range of communication goals. In the protocol, there has some security loopholes may cause the information be stolen. When the attacker intercepts the information, the attacker will attack the communication system. Hence, we propose an improvement scheme to enhance the system security and achieve the most complete protection.

Keywords: satellite communication system; impersonal attack; mobile device

1. 前言

最近幾年來，資訊的發展相當的快速，網路的使用也越來越普遍，網路的普及化，造就了網路無國界，類似於地球村的感覺，不管是無線網路或是有線網路通訊，都帶來許多的便利性。傳統的衛星通訊系統，採用靜止衛星 GEO(Geosynchronous Equatorial Orbit)，與地球的赤道同步運行，但是距離相當遙遠，造成傳輸訊號延遲的問題，所以最近低軌道衛星 LEO(Low-Earth-Orbit)逐漸受到重視，利用低軌道衛星建立衛星通訊系統，減少信號的縮減和傳輸的延遲。

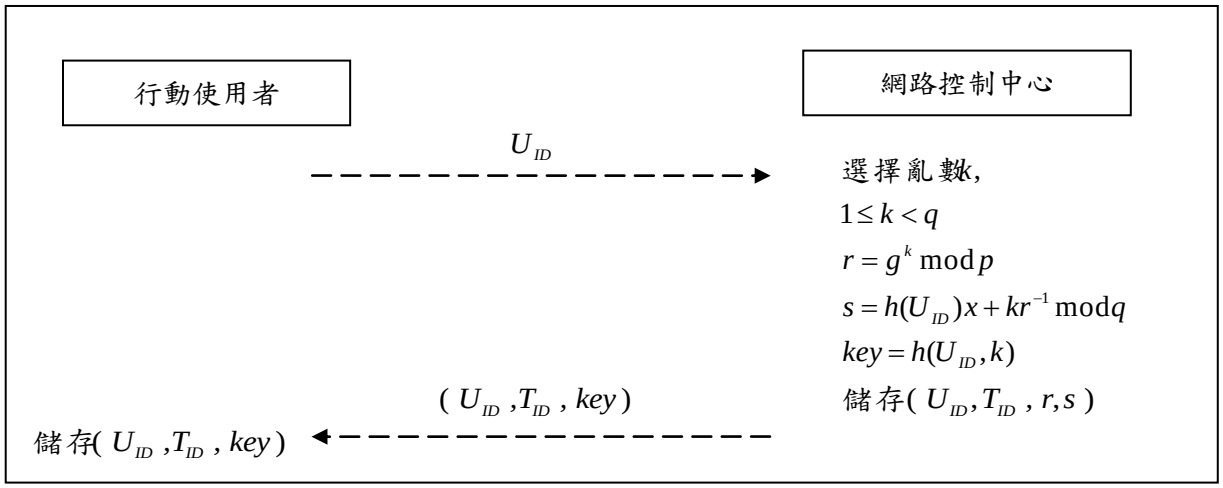
在 1996 年，Cruickshank 提出了以 PKC(public key cryptosystem)的衛星通訊系統[5]，但是卻因為計算量過高，造成行動裝置負擔過重。之後在 2003 年，Hwang 等人[7]提出以 SKC(secret key cryptosystem)的衛星通訊系統，減少了計算量的負擔。之後在 2009 年 Chen 等人提出的自我驗證機制用於衛星通訊系統[4]，這個機制可以減少通訊成本，對於行動裝置可以更輕量化的執行通訊協定，不會讓過大的計算量成為阻礙。在 Chen 等人的協定當中，主要基於會議金鑰協定作為通訊安全的依據，使得協定達到安全的通訊。但是在協定中，對於行動使用者方面的保護，並未做到確實，讓攻擊者可以根據這些弱點進行攻擊或是偷取資訊。因此我們針對 Chen 等人的協定進行改善，讓通訊協定更為安全，讓攻擊者不會有機可乘，在改善後的協定中，能增加使用者隱私性的保護以及抵擋攻擊者假冒使行動用者進行通訊，另外對於行動使用者接收到網路控制中心傳來的資訊，做到交互認證的檢測。

在回顧 Chen 等人的協定中，是基於低軌道衛星 LEO 作為主要通訊的橋樑，以建立衛星通訊系統，為了讓衛星通訊系統更有效率以及安全，我們列了以下的需求。

(1) 交互認證:在行動使用者和網路控制中心之間運用交互認證達到安全性的保證[3,4,5,7,13] 。

(2) 機密通訊:在無線網路世界中，資訊容易受到竊聽，所以運用會議金鑰協定確保行動使用者和網路控制中心通訊是安全的[4] 。

(3) 行動使用者私密性:對於在通訊系統上，運用匿名身分進行傳輸，讓行動使用者的資



圖一 Chen 等人註冊階段流程

訊受到保護 [4,12] 。

(4) 低計算量:對於運用在行動裝置上面擁有低計算量的特性，使通訊系統更適合運用在行動裝置上面 [4,7,13] 。

(5) 最小信任:行動使用者對於網路控制中心給予最少的信任，讓網路控制中心儲存最少的機密資訊 [4,12] 。

(6) 已知金鑰安全:若通訊的安全性是基於會議金鑰，因此會議金鑰就必須具有獨立性，以防止被攻擊者推斷出下次的會議金鑰 [3,4]。

2. 回顧 Chen 等人的協定

在 Chen 等人所提出的自我認證機制運用於行動裝置的衛星通訊的協定當中，此協定分為三個階段: 初始化階段、註冊階段、驗證階段。首先說明在協定當中使用到的參數以及符號的表示。

2.1 本文中所用到協定的參數說明：

U_{ID}	:行動裝置的使用者身分代碼
T_{ID}	:暫時性的身分代碼
LEO_{ID}	:衛星的身分代碼
pw	:行動使用者的密碼
x	:網路控制中心的私鑰
$MAC_k(\ )$	:單向雜湊函數包含了金鑰 k
$[m]_k$	:對明文 m 以 k 做對稱式加密
$h(\cdot)$	:單向雜湊涵數
$A \stackrel{?}{=} B$	:判斷 A 是否等於 B
$\oplus$	:做互斥或運算
⟶	:一般通道
⋯⋯▸	:安全通道

2.2 初始化階段:

網路控制中心會先產生長期使用的私鑰和相對應的公鑰說明如下。

網路控制中心會先選擇一個大質數 p 和從乘法群 Z_p^* 中產生 g，g 的序為 q(q 是一個大質數，為 p-1 的因子)。其安全性是基於解離散對數的困難問題。

網路控制中心會選擇一個長期使用的私鑰 x，x 的範圍為 $1 \le x < q$。網路控制中心的相對應公鑰為 $y = g^x \bmod p$ 。

2.3 註冊階段:

行動使用者向網路控制中心註冊成為合法的使用者，其流程如圖一所示。

步驟一: 行動使用者先提交 U_{ID} 給網路控制中心。

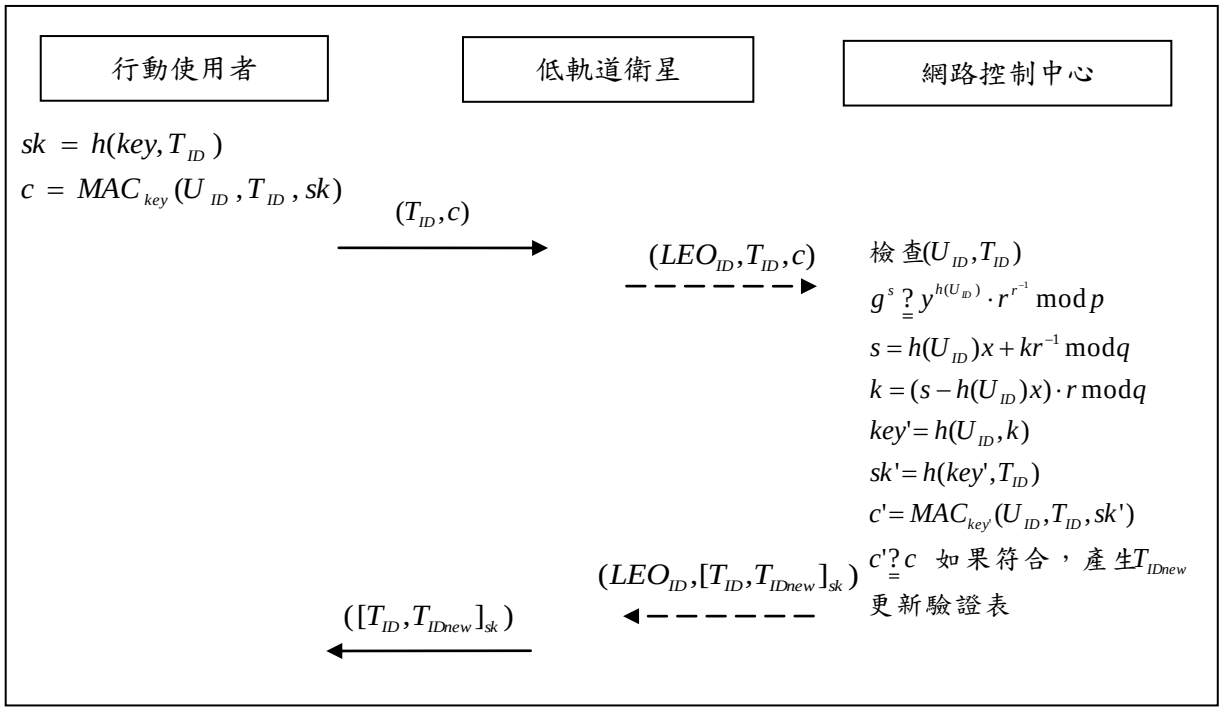
步驟二: 網路控制中心會先決定一個初始的暫時性身分代碼 T_{ID}，當每次成功認證之後會被更新。網路控制中心選擇一個亂數 k，$1 \le k < q$。

計算 $r = g^k \bmod p$ 和

$s = h(ID)x + kr^{-1} \bmod q$ 。

產生行動使用者的主要金鑰 $key = h(U_{ID}, k)$ 。

網路控制中心儲存 (U_{ID}, T_{ID}, r, s) 並



圖二 Chen 等人驗證階段流程

傳送訊息 (U_{ID}, T_{ID}, key) 給予行動使用者。

步驟三: 行動使用者接收到訊息之後，即儲存 (U_{ID}, T_{ID}, key) 在行動裝置中。

2.4 驗證階段:

當行動使用者要與其他行動使用者互相通訊時，須要先經過驗證動作，其流程如圖二所示。

步驟一: 行動使用者必須計算會議金鑰 $sk = h(key, T_{ID})$
$c = MAC_{key}(U_{ID}, T_{ID}, sk)$ 之後
傳送驗證訊息 (T_{ID}, c) 給低軌道衛星。

步驟二: 當低軌道衛星接收到行動使用者的驗證訊息後，把衛星身分代碼 LEO_{ID} 附加在驗證訊息上傳給網路控制中心。

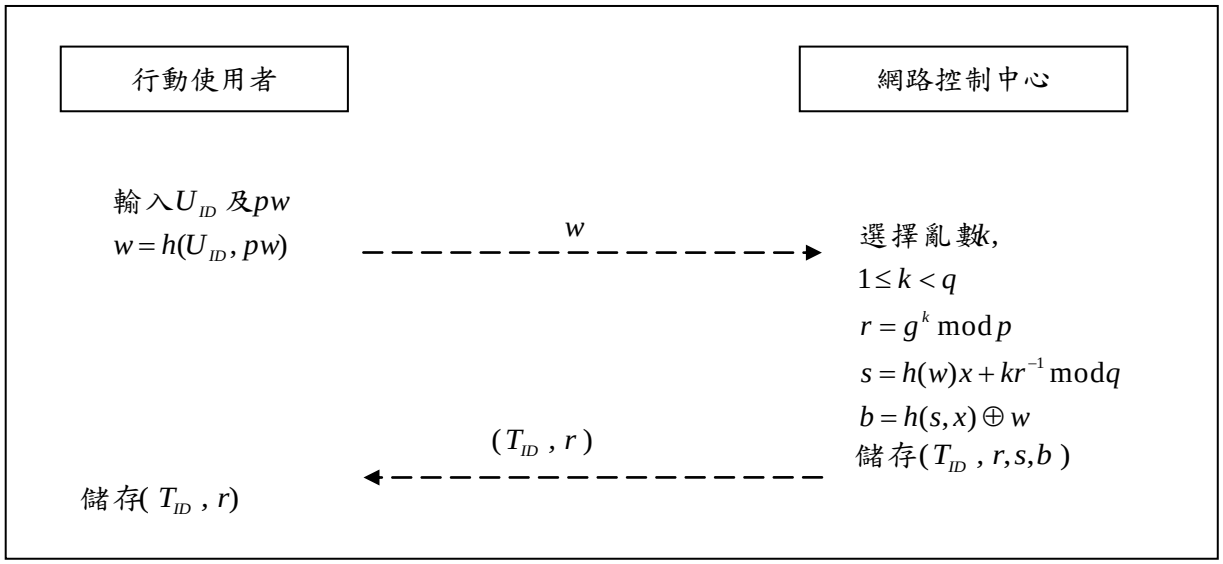
步驟三: 當網路控制中心收到訊息之後，會先檢查低軌道衛星是否合法。之後會去從驗證表當中找尋相對應的資訊 (U_{ID}, r, s) 。
驗證簽章 $g^s \stackrel{?}{=} y^{h(U_{ID})} \cdot r^{r^{-1}} \bmod p$ ，經由 $s = h(U_{ID})x + kr^{-1} \bmod q$ 式中得到 $k = (s - h(U_{ID})x) \cdot r \bmod q$ 解出 k 值。計算行動使用者金鑰 $key' = h(U_{ID}, k)$ 和會議金鑰 $sk' = h(key', T_{ID})$ 。計算 $c' = MAC_{key'}(U_{ID}, T_{ID}, sk')$ 並且檢查 $c' \stackrel{?}{=} c$ 。如果不符合，則表示交互驗證失敗；如果符合，認證訊息和會議金鑰將會被確認為合法。接著產生一個暫時性的身分代碼 T_{IDnew} 並且更新儲存的驗證表。把訊息 $(LEO_{ID}, [T_{ID}, T_{IDnew}]_{sk'})$ 回傳給低軌道衛星。

步驟四: 低軌道衛星收到訊息之後轉發訊息 $[T_{ID}, T_{IDnew}]_{sk}$ 給行動使用者。行動使用者收到訊息對訊息解密之後，更新暫時性身分代碼 T_{IDnew} 做為下次認證訊息時使用。

2.5 Chen 等人的缺失:

對於所回顧 Chen 等人的協定當中，協定看似是安全的，其實是潛藏著一些漏洞，有可能被攻擊者所攻擊，下面列出協定中有問題的地方:

1. 當行動裝置不小心掉了的時候，如果被惡意的攻擊者所偷取時，存在行動裝置的資訊將會遭受到竊取， (U_{ID}, T_{ID}, key) 這些資訊就可能被攻擊者所取得[10,11]。



圖三改善後的註冊階段流程

2. 假冒使用者攻擊：當攻擊者擁有 (U_{ID},T_{ID},key) 這些資訊後可以計算出 $sk=h(key,T_{ID})$ 和 $c=MAC_{key}(U_{ID},T_{ID},sk)$ 有了這些資訊攻擊者就可以使用行動裝置進行假冒使用者攻擊[6,9,10,11]。

3. 使用者在接收到網路控制中心端所傳回的訊息後，沒有與加密訊息的金鑰做比對，因為在協定當中，會議金鑰 sk 可能被推算出來，從網路控制中心截取 (U_{ID},T_{ID},r,s) ，再從行動使用者截取 (U_{ID},T_{ID},key) ，可以推導出來會議金鑰 $sk=h(key,T_{ID})$ ，裡面訊息將會被竄改，導致下次請求服務驗證時，計算出來的 $c=MAC_{key}(U_{ID},T_{ID},sk)$ 會有錯誤而形成驗證錯誤。

因此，我們對協定進行改善，藉以達到更加安全的通訊。在改善的協定中，在行動使用者方面，加上了交互認證，確保和網路控制中心之間的通訊是安全的；在改善的協定裡，把原來協定加以改善，讓行動裝置不儲存有任何有關於行動使用者的敏感資訊，如此可以保障行動使用者的隱私安全。

3. 改善後的協定

3.1 初始化階段:

網路控制中心會先產生長期使用的私鑰和相對應的公鑰說明如下。

網路控制中心會先選擇一個大質數 p 和從乘法群 Z_p^* 中產生 g，g 的序為 q(q 是一個大質數，為 p-1 的因子)。其安全性是基於解離散對數的困難問題。

網路控制中心會選擇一個長期使用的私鑰 x，x 的範圍為 $1\le x<q$。網路控制中心的相對應公鑰為 $y=g^x \bmod p$ 。

3.2 註冊階段:

行動使用者向網路控制中心註冊成為合法使用者，其流程如圖三所示。

步驟一: 行動使用者輸入身分代碼 U_{ID} 及密碼 pw 計算 $w=h(U_{ID},pw)$，之後行動使用者提交 w 給網路控制中心。

步驟二: 網路控制中心會先決定一個初始的暫時性身分 T_{ID}，當每次認證成功之後會被更新。

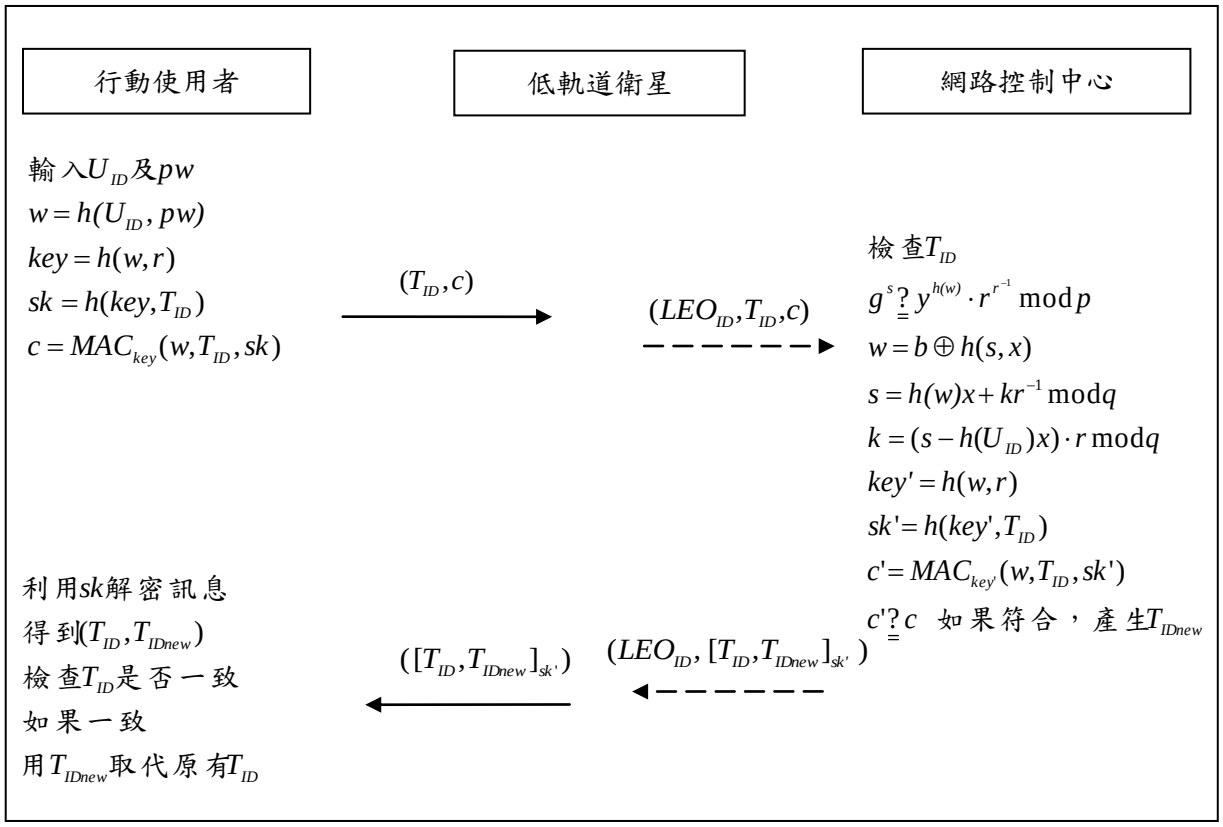
網路控制中心選擇一個亂數 k，k 值的範圍為 $1\le k<q$。

計算 $r=g^k \bmod p$ 和

$s=h(w)x+kr^{-1} \bmod q$

$b=h(s,x)\oplus w$ 。

之後利用私鑰 x 和簽章 s 把行動使用者的資訊加以保護。網路控制中心儲存 (T_{ID},r,s,b) 並把訊息 (T_{ID},r) 傳送給行動使用者。



圖四改善後的驗證階段流程

步驟三: 行動使用者接收到訊息之後，儲存 (T_{ID},r) 在行動裝置中。

3.3 驗證階段:

當行動使用者要與其他行動使用者互相通訊時，須要先經過驗證動作，其流程如圖四所示。

步驟一: 首先行動使用者必須先輸入身分代碼 U_{ID} 及密碼 pw 讓行動裝置計算 $w=h(U_{ID},pw)$ 及 $key=h(w,r)$。行動裝置計算會議金鑰 $sk=h(key,T_{ID})$ $c=MAC_{key}(w,T_{ID},sk)$ 之後傳送驗證訊息 (T_{ID},c) 給低軌道衛星。

當低軌道衛星接收到行動使用者的驗證訊息後，把衛星身分代碼 LEO_{ID} 附加在驗證訊息上傳給網路控制中心。

步驟二: 當網路控制中心收到訊息之後，會先檢查暫時身分代碼 T_{ID} 是否合法。之後會去從驗證表當中找尋相對應的資訊 (r,s,b)。驗證簽章 $g^s \stackrel{?}{=} y^{h(w)}\cdot r^{r^{-1}} \bmod p$ 是否曾被修改過。之後利用參數 b 以及網路控制中心本身私鑰 X 及簽章 s 解出行動使用者的資訊 $w=b\oplus h(s,x)$。再由 $s=h(w)x+kr^{-1} \bmod q$ 式中得到 $k=(s-h(U_{ID})x)\cdot r \bmod q$ 解出 k 值。計算出行動使用者金鑰 $key'=h(w,r)$ 和會議金鑰 $sk'=h(key',T_{ID})$。計算 $c'=MAC_{key'}(w,T_{ID},sk')$ 並且檢查 $c' \stackrel{?}{=} c$。如果不符合，則表示交互驗證失敗；如果符合，認證訊息和會議金鑰將會被確認為合法。接著產生一個暫時性的身分 T_{IDnew}，並且更新儲存的驗證表並且把訊息 $(LEO_{ID},[T_{ID},T_{IDnew}]_{sk'})$ 回傳給低軌道衛星。

步驟三: 低軌道衛星收到訊息之後轉發訊息 $[T_{ID},T_{IDnew}]_{sk'}$，給予行動使用者。

步驟四: 行動使用者收到訊息，利用本身的會議金鑰 sk 把訊息解密獲得 $(T_{ID},T_{IDn})_e$。

把原有的 T_{ID} 和接收到的訊息做比對，確保訊息的一致性，當確認無誤之後，把 T_{IDnew} 取代原有的 T_{ID}。因此下次行動使用者和網路控制中心的會議金鑰變成 $sk_{new}=h(key,T_{ID})$。

4.安全分析

對於所提出的改善協定，可以抵擋攻擊者不同種類的攻擊，改善之後的協定讓安全性更為提升，即使行動裝置掉了，也保證行動使用者的資訊是安全的，以下敘述為改善協定之後的安全分析。

交互認證

交互認證是 Chen 等人的協定當中所遺漏的，在改善的協定中，驗證階段網路控制中心所回傳的驗證訊息，當行動使用者，接收到訊息後，利用本身的會議金鑰 sk 和網路控制中心所回傳的會議金鑰 sk' 做比對，如果符合，就把訊息做解密，得到 T_{ID} 和 T_{IDnew} 兩個暫時身分代碼，在 Chen 等人的協定當中，會議金鑰 sk 是可能被推算出來的，所以我們的協定中，做第二次的驗證訊息程序，判斷加密的訊息，是否有被篡改過。如果網路控制中心所傳來的暫時身分代碼和行動使用者原有的暫時身分代碼相同，即交互認證成功。之後更新暫時身分代碼 T_{IDnew}，因此下次行動使用者和網路控制中心的會議金鑰變成 $sk_{new}=h(key,T_{ID})$。

已知金鑰安全

當攻擊者攔截了之前訊息的會議金鑰，也無法利用舊有的會議金鑰推導出下次的會議金鑰，因為會議金鑰的建立為 $sk=h(key,T_{ID})$ 當中的 T_{ID} 是每次進行認證都會是不相同的，所以有會議金鑰獨立的特性。

使用者私密性

對於每次驗證通訊，行動使用者都以暫時身分代碼 T_{ID} 及 c 進行通訊和驗證，然而在改善的協定當中也避免了儲存行動使用者的身分資訊，只儲存 (T_{ID},r)，所以對於行動使用者的私密性，進行了嚴格的把關，讓每次通訊都不會透露使用者的真實身分。

抵擋偷取驗證表攻擊

當攻擊者對於網路控制中心內部進行驗證表的偷取，也無法用來假冒合法使用者或是合法的網路控制中心，即使攻擊者掌握了 (T_{ID},r,s,b) 也無法透過 $s=h(w)x+kr^{-1}\bmod q$ 解出 k 值，這是因為攻擊者無法推算出網路控制中心長期使用的私鑰 x。我們改善了讓網路控制中心端沒有明文儲存使用者的資訊，並且讓註冊的行動使用者儲存最少的資訊在行動裝置上，網路控制中心端也給予最小的信任，儲存經由行動裝置計算過後的值作為行動使用者資訊，而不是使用明文來傳遞註冊的訊息，達到對行動使用者和網路控制中心最完善的保護。

抵擋假冒使用者攻擊

在改善後的協定當中，不儲存行動使用者的身分代碼 U_{ID}，即使行動裝置掉了，攻擊者也無法進行假冒使用者攻擊。在改善的協定中行動裝置裡面也沒有儲存任何關於行動使用者的資訊，行動裝置只有儲存 T_{ID} 及 r，沒有任何有關於行動使用者的敏感資訊，當進行驗證時，行動使用者必須輸入註冊的身分代碼 U_{ID} 及密碼 pw 進行驗證動作，在網路控制中心，利用簽章 $s=h(w)x+kr^{-1}\bmod q$ 來保護行動使用者的資訊，攻擊者無法從簽章值 s 當中拿取行動使用者的資訊來進行假冒使用者攻擊。

抵抗假冒伺服器攻擊

對於衛星通訊，以現實的觀點去切入，攻擊者要假冒網路控制中心，以成本說需要大量的花費才能去偽造一個衛星，所以偽造網路控制中心是困難的。另外當行動使用者在傳送認證訊息 $c=MAC_{key}(U_{ID},T_{ID},sk)$，假冒的伺服器是沒有當時網路控制中心的私鑰 x，$b=h(s,x)\oplus w$ 無法解出參數 w，建立會議金鑰須有參數 w 才能建立行動使用者金鑰 $key=h(w,r)$，也才能建立會議金鑰 $sk=h(key,T_{ID})$ 和行動使用者通訊。

抵擋重送攻擊

協定當中，即使攻擊者攔截到訊息 (T_{ID},c)，也無法進行重送攻擊，因為在協定當中，每次會議金鑰的建立，$sk=h(key,T_{ID})$ 都包含了 T_{ID} 變數，然而 T_{ID} 每次成功驗證後都會有 T_{IDnew} 取代舊有的 T_{ID}，所以攻擊者無法進行重送攻擊。

抵擋行動使用者偷取網路控制中心私鑰

在改善的協定中，行動使用者擁有資訊只有 (T_{ID}, r)，即使行動使用者，偷取網路控制中心所儲存資訊 (T_{ID}, r, s, b)，去推算出網路控制中心私鑰 x 是不可行的，因為只有簽章值 $s = h(w)x + kr^{-1} \bmod q$ 才有使用網路控制中心的私鑰 x，行動使用者即使偷取資訊，也無法推算出正確的網路控制中心的私鑰 x，防止了內部攻擊的可能性發生，也能防止其他行動使用者的資訊發生外洩。這是因為每個使用者的資訊，都以網路控制中心的私鑰 x 加上簽章 s，保護每個行動使用者的資訊。當行動裝置計算出 $w = h(U_{ID}, pw)$ 後，在簽章值 s 當中還有兩個未知參數 x 及 k，所以行動使用者無法得知私鑰 x 的值。

5. 結論

對於 Chen 等人的協定進行改善之後，對於行動使用者的敏感資訊保護，以及抵抗假冒使用者的攻擊。且當使用者不小心把行動裝置弄丟了，也不需要擔心敏感資訊曝光，因為並沒有任何敏感資訊是直接存於行動裝置當中的，對於行動使用者資訊有一定的程度的保護。

我們所提的改善方案有以下特色:

(1) 讓行動裝置不小心掉了，也無損對於安全性之確保。
(2) 利用網路控制中心本身的私鑰以及簽章，來保護行動使用者所註冊的資訊。
(3) 防止了合法的使用者去偷取網路控制中心的私鑰防止了內部攻擊的可能性發生。
(4) 讓網路控制中心及行動使用者儲存最少的資訊，達到對行動使用者和網路控制中心最完善的保護。
(5) 利用交互認證，讓行動使用者和網路控制中心之間通訊更為安全。

參考文獻

[1] Aziz, A., Diffie, W., Privacy and authentication for wireless local area networks, ***IEEE Personal Communications***, pp. 25-31, 1994.

[2] Chen, B.H., Improvements of authenticated encryption schemes with message linkages for message flows, ***Computers & Electrical Engineering***, Vol. 30, No. 7, pp.465-469, 2004.

[3] Chen, T.H., Hsiang, H.C., Shih, W.K., Security enhancement on an improvement on two remote user authentication schemes using smart cards, ***Proceedings of 11th International Conference on Parallel and Distributed System***, Vol. 2, pp. 73–77, 2005.

[4] Chen, T.H., Lee, W.B., Chen, H.B., A self-verification authentication mechanism for mobile satellite communication systems, ***Computers & Electrical Engineering***, Vol. 35 , No. 1, pp.41-48, 2009.

[5] Cruickshank, H.S., A security system for satellite networks, ***IEEE Satellite System Mobile Communications and Navigation***, pp. 187- 190,1996.

[6] Hsu, C.L., A user friendly remote authentication scheme with smart cards against impersonation attack, ***Applied Mathematics and computation***, Vol. 170, No. 1, pp.135-143, 2005.

[7] Hwang, MS., Yang, C.C., Shiu, C.Y., An authentication scheme for mobile satellite communication systems, ***Operating Systems Review of ACM***, pp. 145-148, 2003.

[8] Hwang, R.J., Su, F.F., A new efficient authentication protocol for mobile networks, ***Computer Standards & Interface***, Vol. 28, No. 2, pp.241-252, 2003.

[9] Kim, S.K., Chung, M.G., More secure remote authentication scheme, ***Computer Communications***, Vol. 32, No 6, pp.1018-1021,2009.

[10] Lin, H.Y., Security and authentication in PCS, ***Computer & Electrical Engineering***, pp.225-248,1999.

[11] Song, R.G., Advanced smart card based password authentication protocol, ***Computer Standards & Interface***, Vol. 32, No. 5-6, pp.321-325, 2010.

[12] Wang, Y.Y., Liu, J.Y., Xiao, F.X., Dan, J, A more efficient and secure dynamic ID-based remote user authentication scheme, ***Computer Communications***, Vol. 32, No. 5, pp. 583-585, 2009.

[13] Wen, G.S., Jian, M.W., Efficient remote mutual authentication and key agreement, ***Computers & Security***, Vol. 25, pp.72-77, 2006.