行動通訊使用者認證與匿名方法
User Authentication and Privacy in Mobile Communicatio

Jyh-Shin Hsieh*(謝志欣)
國立中興大學資訊科學研究所
台中市國光路 250 號
shin@cs.nchu.edu.tw

Gwoboa Horng(洪國寶)
國立中興大學資訊科學研究所
台中市國光路 250 號
gbhorng@cs.nchu.edu.tw

摘要

匿名(anonymity)可以保護個人身份在無線及行動通訊中不被截取，進一步保護個人私密資料不被竊取。我們將針對目前的系統(GSM, CDPD)及改進 GSM 系統的方法(我們稱爲 traveling alias) 就匿名上的安全性加以討論，並提出一個類似 micropayment[15]的新架構：利用前一次通訊所使用的匿名和通訊金鑰(session key)，以及使用者和 HLR 共享的秘密金匙，經過一個 Hash Function 來產生下一次的匿名，通式如下：$A_i = H(A_{i-1}, Ks_{i-1} \oplus K_{uh})$；也就是說此次通訊所使用的匿名在上一次的認證時就已經決定了。

我們的架構對外界和對 VLR 都可達到匿名的功能，在計算上並不會增加使用者行動主機的負擔，同時可以避免一些外在非法的攻擊，與 GSM 和改進 GSM 的方法[11]比較之下有較佳的成效。

關鍵詞：匿名(anonymity)，HLR，VLR，traveling alias，session key。

一、前言

由於通訊技術的進步及提昇，使得無線通訊成爲當今的一股新潮流；而無線通訊可在任何地方、任何環境達到通訊的目的，給予人類一種無遠弗界的便利，也因此人類對無線通訊越來越喜歡也越來越依賴。然而無線通訊的媒介又和傳統的有線通訊不同，因爲無線通訊是使用電波在開放空間中傳遞資料，所以任何人都可輕易接收這些資料，因此有了許多安全性方面的考量。在無線通訊中需考量的安全性[3,6,12]包含了以下幾項：資料保密(Data Encryption / Decryption)[3、識別協議(Authentication Protocol)[3,5,7,12]、匿名(anonymity)等；而匿名是個重要的議題，因爲有關 mobile user 的目前位置(location 及所使用的 Identity 都是屬於個人私密資料，也是有企圖的攻擊者(非法第三者)最感興趣的部份，因此必須對這些資料加以保密，解決這問題的方法就是使用匿名[1,2,4,7,11,12]。

Mobile user 必須先在一個區域(Home domain) 註冊，當使用者在別的區域(Visit domain) 要取得系統提供的服務時，Visit domain 必須透過 Home domain 對使用者的身份做驗證，以確定是否爲合法使用者；通常使用者必須提出一個能代表身份的 ID 給 home domain 來驗證，而此時就會遭到入侵者(intruder)竊聽，而曝露使用者的身份，入侵者可藉此得到更多此使用者的個人私密資料。另外在身份認證時，Visit domain 也應該無法得知使用者真正的 ID，如此才能保障使用者的安全，因爲如果 Visit domain 可以得知使用者的 ID，那麼入侵者就可藉由僞裝成 Visit domain 來得知使用者的身份，進而得知使用者的一些個人私密資料。因此我們需要使用匿名來保護使用者的 identit 。

使用者所使用的機器(之後稱爲行動主機)在計算能力上並比不上 Visit domain 和 Home domain ，而太過於複雜的計算會造成行動主機的負擔，相對於 Visit domain 和 Home domain 並不用特別考慮計算複雜度，因此在使用匿名時必須考慮在使用者方面儘量降低計算複雜度，將複雜的計算交由 Visit domain 或 Home domain 去執行。另一方面若匿名需由 Home domain 記錄與真實 ID 的對應關係，則 Home domain 必須建立一個對應資料庫來儲存這些資料。萬一此資料庫被入侵，則使用者和匿名的相對關係就會被得知，利用此對應關係可找出目前使用者位置、使用者通訊記錄，進而取得使用者的私密資料；又或者此資料庫毀損，對應關係被破壞，將會造

成使用者在通訊初始時無法通過認證，無法使用通訊系統，因此我們在應用匿名與真實 ID 對應資料庫的系統中，必須將資料庫安全也考慮進去。

隱藏使用者的 ID 並不只爲了滿足不可追蹤性，而是爲了要能隱藏使用者和管理認證中心的多變關係。因此針對使用者 ID 隱私的安全性，可將匿名的需求加以分類[11]：

1.C1：隱藏使用者 ID 不被竊聽者(Eavesdroppers)知道。許多現存的做法都有達到這項需求，而最好的匿名做法應該是：就算非法第三者去分析這些 aliases 也無法得知使用者的 ID。

2.C2：隱藏使用者 ID 不被外部的認證機構(Foreign Authorities)知道。外部的認證機構(即我們所提到 VLR)不需要去知道使用者的 ID；外部的認證機構只需要去證明使用者是否有權使用其提供的服務及擁有足夠資訊向主認證機構(Home Authority)要求帳單即可。

3.C3：隱藏使用者和認證機構的關係不會被外界得知。以較高層級的隱私權來看，保護使用者和 Home Authorit 的存在關係不被未認可的第三團體(Third Party 得知是很重要的。

4.C4：隱藏主認證機構(Home Authority)的 ID 不被外部認證機構(Foreign Au thority)知道。當使用者需要被 Visit domain 驗證身份時，Foreign Authorit 爲了取得身份認證會和 Home Authority 通訊；因此僅管使用者真正的 ID 已經隱藏起來，但是他和 home 的關係會被 Foreign Authorit 得知。

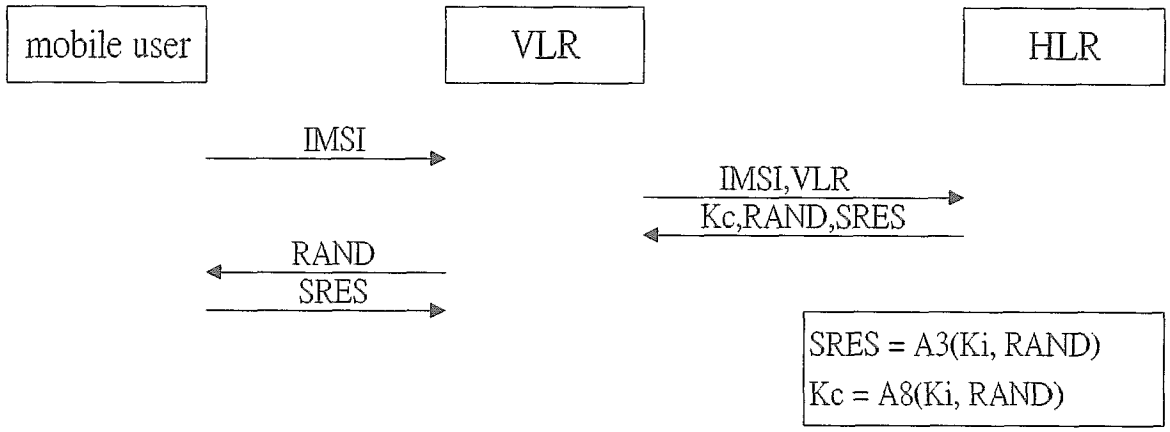
5.C5：隱藏使用者的行爲不被主認證機構(Home Authority)知道。在某些特殊的情形下，使用者不想讓 Home Authority 知道他的遷徙，也就是說除了使用者以外沒有人知道使用者的位置。

我們將針對目前的系統(GSM, CDPD)在匿名上的安全性加以討論，並提出一個新的架構來達到匿名的需求。我們的架構對外界和對 VLR 都可達到匿名的功能，而且在計算上並不會增加使用者行動主機的負擔，同時可以避免一些外在非法的攻擊，與 GSM 和改進 GSM 的方法[1](之後稱爲 Traveling alia 系統)比較之下有較佳的成效。本文的內容架構如下：第二節介紹一些已經使用的系統及相關背景知識，及使用中的系統有何缺點及一些已提出的改進方法，第三節針對前述的改進方法再加以探討，並提出我們的方法，第四節將探討其安全性及實用性，第五節對本文做一個總結。

二、背景知識及相關研究

就目前的加解密及認證系統而言，可大致分爲兩大類，一爲 shared key cryptosystem 、一爲 public key cryptosystem[2,4]。Shared ke 的系統是指通訊雙方共享一個私密鑰匙，可應用此私密鑰匙加解密資料，同時可達到認證的效果。Shared key 系統針對匿名的作法是提出 traveling alias(是一種 Temporary ID)的做法，也就是當使用者在別的 domain(Visit domain)時並不是使用真正的 ID，而是用 traveling alias 代替 ID 透過 Visit domain 向 Home domain 驗證使用者身份，進而取得 Visit domain 的信任，獲得 Visit domain 的服務及使用權。而 Public key 的系統是使用公開金匙來加密資料、私密金匙來解密資料。針對匿名的作法並沒有特別隱藏 ID，使用者用 Home domain 的公開金匙加密 ID 送給 Visit domain，再由 Visit domain 送給 Home domain 使用其私密金匙解密，Home domain 驗證身份正確再將 ID 及驗證結果送回給 Visit domain；若要在 Visit domain 也做到匿名，則使用者可於一開始加密時就使用 Temporary ID，而 Home domain 有 Temporary ID 和真正 ID 的對應表，用來驗證使用者的合法性，通訊中就使用 Temporary ID 來代替身份。

目前所使用的系統中以歐洲的 GSM(Global System of Mobile)是最早提供匿名的功能[7,10,14]；在 GSM 系統中，使用者先向母系統註冊中心(Home Location Register, HLR)登記註冊，取得一個唯一代表使用者身份的 IMSI(International Mobile Subscriber Identity)，而且使用者和 HLR 有一共享的私密金匙，Ki。在 GSM 的協議中使用到三種函數，A3、A5 及 A8。A8 是用來生成 session key, Kc 的單向函數；A3 是使用者面對 HLR 的挑戰(Challenge)而產生回答(Response)所依據的單向函數；而 A5 是使用 Kc 爲加密密匙的加解密函數。當使用者移動到 HLR 所控制的系統外，其通訊服務都是由 VLR 來完成。



圖一、 GSM 的認證協議(Authentication Protocol)

圖一顯示 GSM 認證協議的步驟[7,14]。以下是 GSM 認證協議的步驟介紹：

Step 1：使用者將其 IMSI 送給 VLR

Step 2：VLR 將 IMSI 傳送給該使用者的 HLR

Step 3：HLR 依據和使用者共享的私密金匙 Ki，再加上隨機亂數 RAND，利用 A3 演算法產生 SRES [SRES = A3(Ki, RAND)]；利用 A8 演算法產生 session key, Kc [Kc = A8 (Ki, RAND)]。將此三個數值傳送給 VLR 用以驗證使用者身份。

Step 4：VLR 傳送 RAND 給使用者當 Challenge

Step5：使用者傳送 SRES 給 VLR 當 Response，VLR 可藉由 HLR 和使用者的 SRES 來達到驗證使用者的身份。

系統中是採用一個 TMSI(Temporary Mobile Subscriber Identity)來達到匿名。使用者將 IMSI 送給 VLR 再向 HLR 驗證使用者的合法性，經過 HLR 的驗證爲合法使用者，則 VLR 會指定一個 TMSI 給使用者，之後通訊建立，使用者便以此 TMSI 來和 VLR 通訊並要求所需的服務，來達到身份保密的目地；也就是說使用者在此 VLR 要再次通訊時，Step1 到 Step3 可省略，使用者只須傳送 TMSI 給 VLR 即可做驗證身份的工作。在這裡有一點需要特別提出來的，當干擾太多造成同步產生問題時，使用者的 TMSI 無法被 VLR 所接受，或當使用者剛到一個新的 VLR 時，沒有辦法取得之前使用的 TMSI 時，此時只好使用 IMSI 傳送給 VLR 送往 HLR 做身份確認，此時就在 VLR 便沒有達成匿名了。

另一個系統是北美洲使用的 CDPD(Cellular Digital Packet Data)[4,7 。CDPD 所採用的方法是先使用 Diffie-Hellma 的金匙交換協議產生一個共享的私密金匙，包含使用者和 VLR、VLR 和 HLR 的兩把金匙，再利用此私密金匙將 ID 加密來傳送作爲身份確認，身份驗證無誤便可開始通訊。在 CDPD 中有兩個較大的缺點：(1)VLR 知道使用者的 ID，沒有達到完全的匿名；(2)Diffie-Hellma 協議本身就有的問題，非法第三者可以僞裝成 VLR 從中得知使用著的 ID。

就[1]提出的匿名需求對 GSM 系統而言，GSM 系統滿足了 C1(不被外界得知)，當 GSM 系統使用 TMSI 時就滿足了 C2(不被 VLR 得知)；而 CDPD 系統只滿足了 C1，因此不論是 GSM 或 CDPD 都無法保證完整的隱私。真正的匿名要能達到不只在合法的系統(authorized party 不會被得知真正的 ID，甚至於在不合法的系統(unauthorized party)也能達到匿名。

而之前所提到 GSM 的 Temporary ID(TMSI 主要是由 Visit domain 選擇並記錄對應關係，再送給使用者做下次通訊時所用的 ID，當此 Temporary ID 遺失或無法通過驗證時，使用者便需要在傳遞真正的 ID(IMSI)做驗證身份用，同時 Visit domai 再產生一個新的 Temporary ID 給使用者。因此在 GSM 的系統下並不能達到完全匿名，因爲當 Temporary ID 遺失，或在通訊過程出問題(例如：使用者的機器因關機或電力不足以致於無法接收)，使用者都必須以真正的 ID(即 IMSI)來做通訊時的 ID，此時便可能遭受非法第三者竊取，而曝露使用者的一些個人資料。

在[11]中提出一種新的作法來改進 GSM 的缺點，就是用 traveling alias(和 temporary ID 是相同的意思)來代替真正 ID，而此 alias 是由使用者自行產生，並非由 Home domain 來產生或由 Visit domain 來分配；主要作法是利用 Home domain 的公開金匙(Ph)將使用者產生的 nonce, Na 以及 Na 和使用者 ID 做 exclusive-or 的值一起加密：Ph(Na, Na⊕Uid)[7,8,11]；將這串資料透過 Visit domain 送給 Home domain ，外界與 Visit domain 無法解開此資料可達到匿名，而 Home domain 可藉由私密金匙解開此資料，再將 Na 和 Na⊕Uid 做 exclusive-or 運算便可得到 Uid，先對 Uid 驗證其合法性，確認是合法使用者時再對 Uid 做 certification 送給 Visit domain，此時 Visit domain 得到 certification 便可知使用者的合法性，進而開放權限給使用者，讓使用者可以使用該系統所提供的服務。而且如果使用 Ph(Na, Na⊕Uid)來做匿名，不會有被非法第三者冒用的危險；除非使用者的 ID 被得知，否則非法第三者無法偽裝成該使用者。圖二是此認證步驟的程序[11]。在此對圖二做一些補充說明：

U：終端使用者(end-user)

Uid：終端使用者 U 的 ID

AS_r：Remote domain 的 Authentication Server(即 VLR)

AS_h：Home domain 的 Authentication Server(即 HLR)

K_u：使用者在 home domain 的 strong key

N_x：X 產生的 Nonce

P_x,S_x：X 的 Public ke 和 Secret key

K_{xy}：X 和 Y 共享的 secret key

$TICK_{Kx}(K_s)$：利用 Kx 計算出來包含 Ks 的 ticket

以下是對 Traveling ali a 認證協議的步驟介紹：

Step1：使用者產生 Nonce, N_u，接著計算 alias $P_h(N_u, N_u \oplus Uid)$，並且用 Ku 來產生單向認證訊息(one-way authentication message)。將這些訊息一併送給 AS_r。

Step2：AS_r 也自行產生 Nonce, N_r，並將 $P_r(N_r)$儲存起來，同時產生 alias $P_h(N_r, N_r \oplus AS_r)$。接著 AS_r 使用 K_{rh} 計算包含 $AUTH_{uh}$ 的認證訊息。再將這些訊息一同送給 AS_h。

Step3：當 AS_h 收到訊息後，便進行以下的步驟：

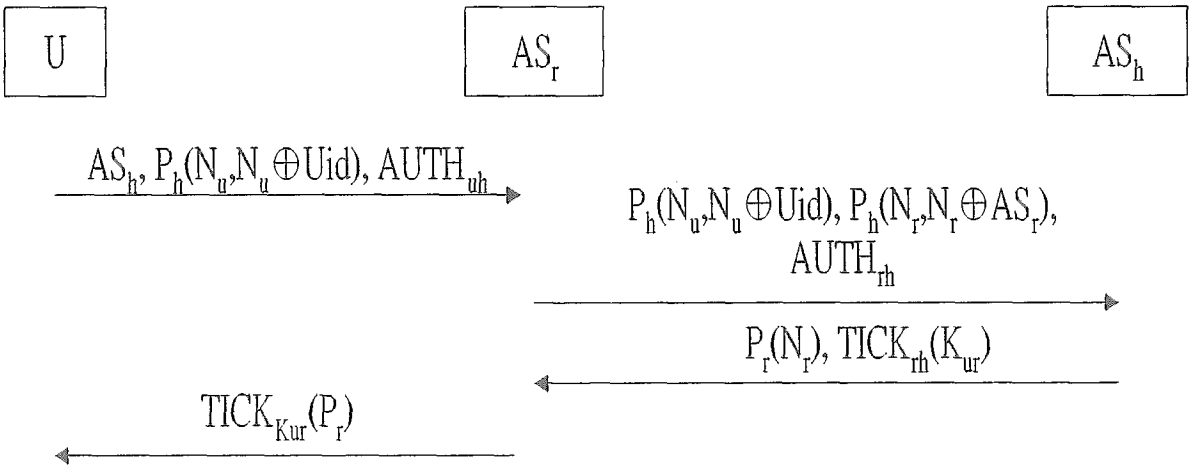
(1)AS_h 利用 S_h 解開使用者的 alias，得到 N_u，再做一次 XO 的動作便可以得到 Uid。

(2)AS_h 跟(1)一樣可以獲得 AS_r 的 ID 和 N_r。

(3)AS_h 查看 Uid 和 AS_r 來取得共享的 secret key，利用此 secret key 來驗證 $AUTH_{rh}$。

(4)最後 AS_h 將 $P_r(N_r)$和包含用來與使用者在 remote domain 通訊的 K_{ur} 之 ticke 一併送給 AS_r。

Step4：ASr 將其 Public key, Pr 送給使用者。如果使用者在 AS_r 已有新 ID,Uid_r 而要再次通訊時爲避免使用同一個 alias(即 $P_h(N_u, N_u \oplus Uid)$)，可以使用 $P_r(N_1, N_1 \oplus Uid_r)$當做新的 alias，此時 ASr 便可以求得 Uid_r。此方法允許使用者在每次認證時使用不同的 ID。



圖二、Traveling ali a 的 Authentication protocol

這種作法有幾個優點：(1)只用一次的 alias：每次通訊就產生一個新的 alias，因爲同一個 alias 使用時間太長容易被察覺 alias 和真正 identit 的對應關係。(2)每次產生的 alias 並沒有相關：每次產生的 alias 都是由不同的 nonce 來決定，因此 aliase 彼此間並沒有相關，也就是無法由上一次的 alias 來求得這次的 alias。(3)Visit domain 無法得知真正的 identit ：只有擁有私密金匙的 Home domain 才有辦法解開此訊息，得知真正的 identit 。

此種做法滿足之前所提到的 C1,C2 的要求，若要達到 C3 等級(使用者和 HLR 關係不被外界知道)則使用者需要將 Home domain 的 alias 也計算出來，Home domain 的 alias 需要用 Visit domain 的公開金匙 Pv，因此在認證程序之前，使用者要先取得 Visit domai 的公開金匙。

三、匿名及認證架構

之前提到的改進方法，如果我們仔細去評估，可以找到一個缺點：如果在 VLR(即 AS_r)內部的不法份子和外界攻擊者合作，按照之後的認證步驟，即可取得和使用者 A 通訊的 K_{ur}。攻擊者 B 便可以僞裝成使用者在此一 VLR 通訊，送出和使用者相同的訊息給 ASr，經過認證步驟核可，取得 Pr，便可以開始通訊，而且不用付費，因爲 B 使用的是 A 的身份來通訊。圖三便是描述該方法的缺失。

因此我們提出一個類似 micropayment[15]的新方法來避免這些攻擊，同時達到匿名的安全性。我們的方法是利用前一次通訊的匿名 A,和 session key, K s及與 HLR 共享的 secret key, K_{uh} 經過一個 Hash Function 產生新的匿名，式子如下：

$$A_i = H(A_{i-1}, Ks_{i-1} \oplus K_{uh})$$

一開始使用者 A 使用 HLR 所發給的匿名 A_1 來進行認證，取得第一次的 session key, K_1，此時使用者和 HLR 都可計算出下一次的匿名 $A_2 = H(A_1, K_1 \oplus K_{uh})$，依此類推，使用者和 HLR 可以產生之後的所有匿名。也就是說使用者 A 在通過此次身份認證後，取得此次 session ke 就計算出下一次的匿名並將其儲存於行動主機上，在下一次通訊時身份認證就使用此次儲存起來的匿名；HLR 也會在送出 session ke 之後計算下一次匿名，將下次匿名和真正 ID 的對應關係儲存起來，做爲下一次身份認證時的依據。我們的認證架構是以[1]的方法爲基礎，加入時戳(timestamp)做輔助，詳見(下頁))圖四。

以下是圖四的一些補充說明：

A'：A 此次通訊的匿名

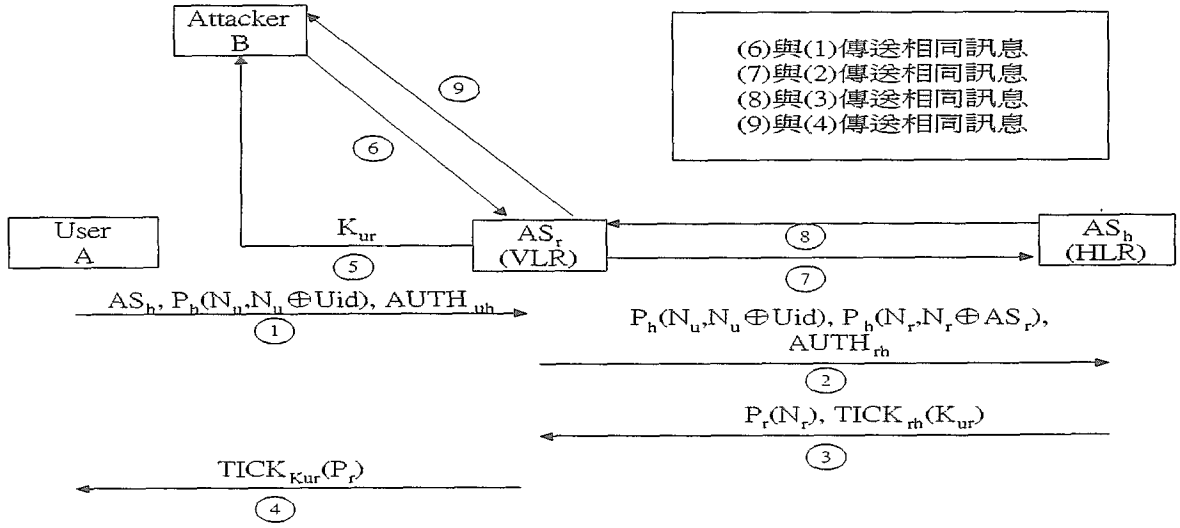
N_a：Nonce

Tx：X 所產生的 Timestamp

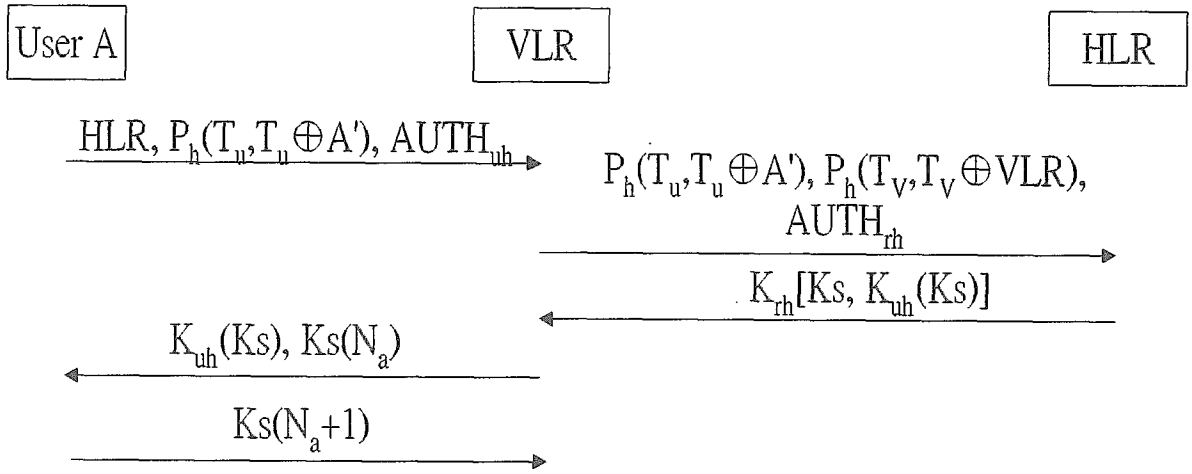
P_h, S_x：X 的 Public ke 和 Secret key

K_{xy}：X 和 Y 共享的 secret key

$AUTH_{xy}$：利用 K_{xy} 所計算出的 authentication message



圖三、可能的攻擊



圖四、利用 Hash functio 做匿名的認證架構

我們的認證架構的步驟如下：

Step1：使用者利用前一次的匿名和 session key 計算這一次的匿名 A'，再採用[1]的作法，將 nonce 改爲 timestamp，將 T_u 和 A'做運算，再計算認證訊息，將這些資料一併送給 VLR。

Step2：同 Step 1，利用 T_v 取代 N_r，做爲 VLR 的匿名；接著 VLR 使用 K_{rh} 計算包含 $AUTH_{uh}$ 的認證訊息，再將這些認證訊息一同送給 HLR。

Step3：當 HLR 收到訊息後，便進行以下的步驟：

(1)HLR 利用 S_h 解開使用者的 alias，得到 T_u，再做一次 XO 的動作便可以得到此次匿名 A'。HLR 可在資料庫查詢使用者 A 的真正身份。

(2)HLR 跟(1)一樣可以獲得 VLR 的 ID 和 T_r。

(3)HLR 查看和 VLR 來取得共享的 secret key,K_{rh}，利用此 secret key 來驗證 $AUTH_{rh}$。再查看和 A 共享的 secret key, K_{uh}，驗證 $AUTH_{uh}$。

(4)通過驗證後，產生使用者和 VLR 通訊的新 session key, Ks，將 Ks 及使用者的 timestamp, T_u 一同以 K_{uh} 加密，和 Ks 一併以 K_{rh} 加密送往 VLR；同時計算下一次使用者的匿名 A" = H(A', $K_s \oplus K_{uh}$) 儲存於資料庫中。

Step4：VLR 接收到訊息解密可得 Ks。產生一個 nonce 用 Ks 加密，將此訊息和 K_{uh}(Ks,Tu)一併送給使用者。

Step5：使用者以 K_{uh} 解密得知 Ks，再以 Ks 回應訊息給 VLR 以確認，同時計算下一次的匿名 A" = H(A', $K_s \oplus K_{uh}$)將其儲存於本身的行動主機上。

在下一節我們將針對我們的系統做安全性的考量分析，以及和其它系統的比較，來證明我們的架構較原有的系統更加安全。

四、安全性考量

在我們的架構中，使用者不會被外界非法使用者及 VLR 得知真實身份，因此有達到之前所提 C1(不被外界得知),C2(不被 VLR 得知)的要求；我們可以將原來以明文傳送的 HLR 以 VLR 的公開金匙加密，如此便可以達到 C3(使用者和 HLR 關係不被外界得知)的要求。再者使用者方面只有使用 XO 和 Hash function 的計算，就計算上而言不會太複雜。以先前討論到的性質來看，我們的架構採用 alias，外界非法攻擊者無法得知使用者真正的 ID；以 VLR 的角度來看，無法解開 alias 的訊息，連使用者的匿名都無法取得，更不可能得知使用者真正的 ID 了。

以第三節所提到的攻擊方法來看我們的架構，這種攻擊法在我們架構下是不可能成功的。如果 VLR 串通外界攻擊者，依認證步驟在取得 session key, Ks 後，攻擊者要假冒使用者在此 VLR 通訊是不可能的，因爲在身份認證時就無法通過；因爲 HLR 的匿名和真實 ID 對應表在每次認證步驟完成前就已更新(step3 到 step4

之間)，因此當攻擊者假冒使用者重送認證資料時，HLR無法得知使用者的真實身份，就無法對此次使用者認證，此次使用者(非法攻擊者)也就無法使用通訊資源。

綜觀我們所設計出來的架構，其優點如下：

1. 計算簡單：使用者端只需計算 XO 和 Hash function 的值，不會太過複雜，也不會增加使用者端的負擔。
2. 匿名不會重覆：每次的匿名取決於上次匿名和 session key 及 shared ke ，就算攻擊者取得上次的匿名也無法得知此次通訊所用的匿名。
3. 匿名安全性：除非能取得使用者和 HLR 共享的 secret key，再加上有辦法得知上次匿名和 session ke ，還必須知道使用何種 Hash function，才有可能算出這次的匿名。也就是說攻擊者必須取得四項資料才能得知使用者的匿名爲何，而此四項資料並不容易取得，因此此系統架構是安全的。而且這個架構對非法攻擊者和 VLR 都有達到匿名的目地。
4. 不受攻擊影響：我們使用 timestamp 來避免 reply attack，同時在各步驟都可以相互認證，可預防 man-in-the-middle attack。

以下我們針對匿名與否，計算匿名的複雜度，安全性考量等幾方面，對GSM系統，Traveling alias(改進GSM)的系統，及我們的架構做一個比較，比較結果詳見表一。

五、結論

在無線及行動通訊中提供使用者隱私是個很重要的需求。而現存的 GSM 和 CDPD 的系統在提供使用者的匿名並不夠完整，在[11]中 Traveling alias(改進 GSM)系統的作法雖然可以達到匿名性，但是會遭受到攻擊，造成架構上安全性不足。因此我們提出了一個新的匿名作法，又提出可達到匿名又具安全性的架構，不但改進了其餘系統的缺失，在比較之下也具有較高的安全性。而我們的架構未來或許還可以試著在 remote logi 上實作，這是我們目前努力的目標。

無線及行動通訊的蓬勃發展，許多在有線已很完備的安全性需求，在無線系統中都需要重新考量。因此不只要考量匿名的安全，還有許多如加解密演算法(因爲行動主機計算能力較低)，認證機制(無線系統需透過 visit domain)等等，都是可以再重新設計；因此資訊安全在無線及行動通訊上還有很大的發展。

致謝

本論文爲中華民國行政院國科會補助之研究計畫 NSC89-2213-E-005-005 的部份成果，僅此致謝。

	GSM 系統	Traveling ali a 系統	我們的系統
是否達成匿名	是 IMSI 直接傳送	是 Ph(Na, Na⊕Uid)	是 $A_i = H(A_{i-1}, K_{i-1} \oplus K_{uh})$
匿名分類要求	C1,(C2)	C1,C2,(C3)	C1,C2,(C3)
計算複雜度	不需計算	XO 計算	XO 及 Hash functio 計算
匿名安全性	無安全性可言	會遭受外界攻擊(reply attack 和 man-in-the-middle attack 混合如第三節所述)	類似 traveling ali a 系統的攻擊無效，取得 session k e 也無法破解匿名
效率(加解密時間)	匿名無需加解密運算	匿名加解密快，只需做 XO 的運算	匿名已事先計算，加密時不需再計算匿名 ，解密只需查看資料庫；因此加解密更快

表一、各系統比較結果

參考文獻(Reference)

[1]B. Askwith, M. Merabti, Q.Shi, K.Whiteley, *Achieving User Privacy in Mobil Networks*, Computer Security Applications Conference, 1997. Proceedings.,13th Annual , 1997 , pp. 108 –116

[2]N. Asokan, *Anonymity in a Mobile Computing Environment*, Mobile Computing Systems and Applications, 1994. Proceedings.,Workshop on , 1995 pp. 200 –204

[3]M. Beller, L. Chang and Y. Yacobi, *'Privacy and Authentication on a Portable Communication System*, IEEE JSAC, Special Issue on Wireless Personal Communications, August 1993, pp. 821-829

[4]A. Herzberg, H. Krawczyk and G. Tsudik, *On Travelling Incognito*, Mobile Computing Systems and Applications, 1994. Proceedings.,Workshop on , 1995, pp. 205-211

[5]L. Jianwei, W. Yumin, *Authentication of Mobile Users in Personal Communication System*, Personal, Indoor and Mobile Radio Communications, 1996. PIMRC'96 ., Seventh IEEE International Symposium on Volume: 3 , 1996 , pp. 1239 -1242 vol.3

[6]J.Kim, M.Oh, T. Kim, *Security Requirements of Next Generation Wireless Communications*, Communication Technology Proceedings, 1998. ICCT '98. 1998 International Conference on , 1998 , pp. 6 pp. vol.1

[7]R. Molva, D. Samfat and G. Tsudik, *Authentication of Mobile Users*, IEEE Network, March/April 1994, pp. 26-34

[8]R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, *KrytoKnight Authentication and Key Distribution Systems*, Proceedings of ESORICS'92, November 1992.

[9]S. Patel, *Weaknesses of North American Wireless Authentication Protocol*, IEEE Personal Communications Volume: 4 3 , June 1997 , pp. 40 –44

[10]M. Rahnema, *Overview of the GSM system and protocol architecture*, IEEE C ommunications Magazine, April 1993, pp. 92-100

[11]D. Samfat, R. Molva, *A Method Providing Identity Privacy to Mobile Users during Authentication*, Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on, 1995, pp.196-199

[12]V. Varadharajan and Y. Mu, *Preserving Privacy in Mobile communications: A Hybrid Method*, Personal Wireless Communications, 1997 IEEE International Conference on,1997, pp. 532-536

[13]曾志嘉、曾文貴， *Certificate-Based Security Protocols in Wireless Networks*, 第九屆全國資訊安全會議 Session4C Group-Oriented System, 1999,pp.340-347

[14]賴溪松、韓亮、張真誠，*近代密碼學及其應用*，松崗電腦圖書資料股份有限公司，1995。

[15]顏嵩銘、李中銘、何良台、李訓育，PayFair：A prepaid internet micropayment scheme promising customer fairness, 第九屆全國資訊安全會議 Session1C Electric Commerce, 1999,pp.74-82