高效率GSM相互鑑別機制

Efficient Mutual authentication Scheme of GSM

呂崇富
中國海事商業專科學校資訊工程科
延平北路9段212號
台北市111士林區
peter@mail.ccmtc.edu.tw

Chung-Fu Lu
Department of Computer Science and Information Engineering,
China College of Marine Technology and Commerce
212, Sec 9, Yan-Pin N. Rd.
Taipei 111, Taiwan, R.O.C.

摘要

數位化的全球行動電話(GSM, Global System for Mobile Communication)系統已廣泛地使用在歐洲及其他全球各地，目前已有超過190個國家總計10億人口在使用GSM系統。但是現行GSM系統的鑑別機制卻存在著一些安全性威脅，例如MS(Mobile Station)與VLR(Visitor Location Register)間無法相互鑑別、增加HLR(Home Location Register)與VLR間傳遞鑑別資訊的通訊頻寬負擔及VLR額外儲存負擔等。本論文將提出一個能夠同時解決上述缺點的GSM相互鑑別機制，我們提出的方法並不須改變現行GSM系統架構，且相當有效率。

關鍵詞：鑑別、單向雜湊函數、加密、解密

Abstract

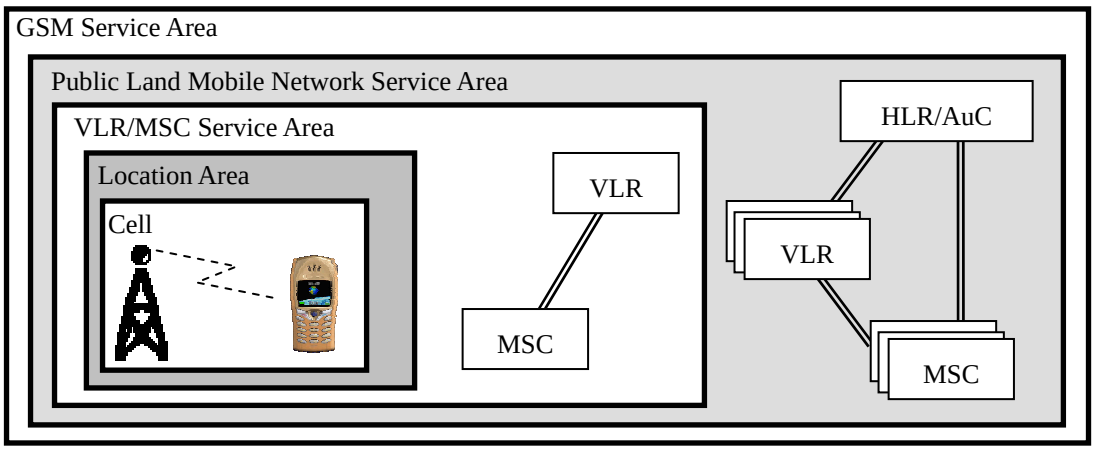
GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM has over one billion users worldwide and is available in 190 countries. There are several drawbacks found in the existing authentication protocol of GSM, such as the property that VLR cannot be authenticated, communication bandwidth consumption between VLR and HLR, and storage overhead in VLR. In this paper, we propose a novel mutual authentication protocol which can not only solve those drawbacks but also make the authentication more efficient.

Key words: authentication, one-way function, encryption, decryption

壹、引言

從第一代行動電話跨越到第二代行動通訊的分野是從類比進展到數位調變，第二代行動通訊具有較高的保密性、系統服務容量增加、傳輸數據資料等優點，促使世界各國陸續將第一代行動電話升級到第二代行動通訊。因應資訊服務合法性與使用存取權限管理之需求，當使用者需要某些資訊服務時，服務提供者之資訊系統須先驗證使用者是否具備合法身份後，才會提供合法使用者所需之相關服務。然而系統大多經由公開網路傳輸媒介來傳送資料，但各網路轉接節點間可能存在著系統所無法掌控的區域，所以可能遭受其他通訊的干擾、攔截、竊聽與欺騙之威脅（Aziz & Diffie 1993；ETSI-2 1993；Rahnema 1993；Hwang 19999；Lin & Harn 1999），有鑑於此，系統便需要有一些安全機制來達到資訊保密、訊息或身份鑑別，及訊息完整性之保護目的。

根據GSM聯盟(GSM Association)資料顯示，現今GSM可橫跨190個以上的國家，行動用戶人口數已達10億，並成爲歐洲及亞洲的工業上的標準(de facto standard)，可謂是第二代行動通訊中使用率最廣的一個規格。GSM系統是由基地台子系統、交換機子系統、管理維護子系統所共同組成，當建設GSM系統時，必須將各個子系統安置在通訊區域內，以使各個地區的子系統彼此間能夠相互配合來完成各項功能，這種將地理位置由小到大劃分爲若干區域的觀念就是GSM系統的地理階層(Hierarchy)，詳如圖一所示，從最小的微細胞(Cell)到整個GSM網路的服務區域(Service Area)。GSM系統經由在各個區域內的信號傳遞與交換等程序，提供人們無線通訊的商業應用便利性，但也面臨到無線通訊環境下的相關安全性威脅（Kumar & Zahn 2003），其中以身份鑑別安全議題最受矚目，雖然GSM系統已提供相關的保密及鑑別演算法來加以防制相關威脅，但現行GSM鑑別機制仍存在著一些有待改善的缺點。本論文將提出一個高效率相互鑑別機制，其能簡易地運用於現行GSM架構中，並有效改善現行GSM鑑別機制的缺點。本論文接下來將於第二節中簡單介紹現行GSM鑑別機制與所面臨的問題，並在第三節提出一個有效解決現行GSM鑑別缺失的相互鑑別機制，第四節則針對我們所提出之相互鑑別機制的安全性及效率評估加以探討，最後陳述我們的結論。



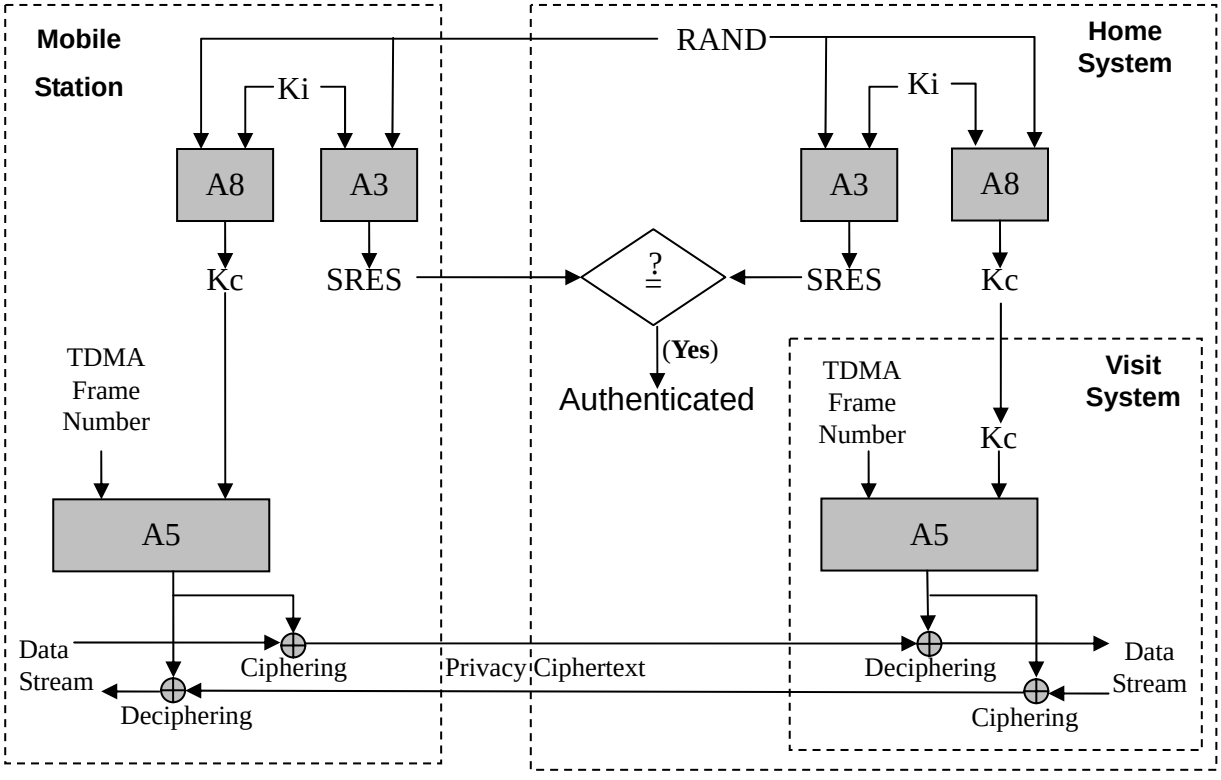
圖一：GSM系統的地理階層

貳、現行GSM鑑別機制簡介

第一代行動通訊系統在手機發話時會將個人資料(電話號碼、序號等)經由無線電波傳送至基地台後，再進行手機用戶身分鑑別，此種身分鑑別程序很容易讓惡意人士從空中攔截用戶資料並進行盜拷，造成合法使用者遭受一號多機的盜打損失。

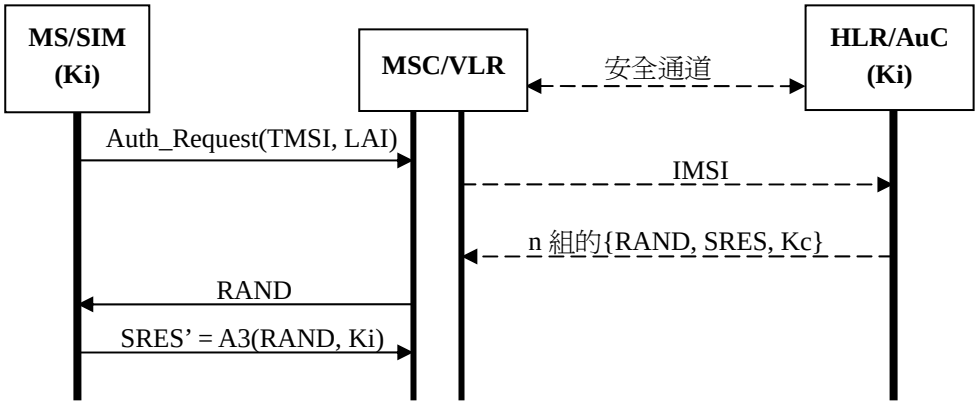
針對第一代行動通訊系統的上述鑑別缺失，第二代行動通訊GSM系統則改變了上述鑑別程序，在資料經由無線電波的傳輸途中，並不會直接將電話號碼等個人資料發射到空中，而是先核對用戶與呼叫用戶身份後，再將資料加密成亂碼後才加以傳送，並經過MS與HLR雙向的鑑別程序，有效降低了遭受盜拷與盜打的可能性。現行GSM系統中，直接與身份鑑別相關的安全參數說明如下：

- 行動用戶之全球唯一識別碼IMSI（International Mobile Subscriber Identity）：在用戶申請註冊時，存於HLR/AuC (Authentication Center)並燒錄於SIM卡中。IMSI長度不可超過15碼，我國使用15碼，即IMSI=466-920-xxxxxxxxx。
- MS的SIM卡之區域性臨時識別碼TMSI（Temporary Mobile Subscriber Identity）：長度不可超過32位元。TMSI由VLR產生，只在同一個VLR服務區內有效。主要用於保護用戶身份之機密性。
- 用戶鑑別金鑰Ki（Individual Subscriber Authentication）：用戶申請登記時，由系統產生之私密鑑別金鑰。Ki產生後，即被儲存在AuC內，並燒錄於用戶之SIM卡上。所以Ki是MS及HLR所共享的秘密金鑰。
- 加密金鑰Kc（Ciphering Key）：在每次無線通訊中，對資料進行加密時所使用之金鑰。
- 服務區識別碼LAI（Location Area Identity）：提供系統識別行動台之位置。



圖二：GSM安全架構

GSM安全措施主要是基於手機鑑別及訊息加密等兩個方向來考量，相關安全架構如圖二所示，GSM身分鑑別及加密使用A3、A5及A8等三個演算法，Ki及Kc等兩個金鑰，一個RAND亂數挑戰和SRES簽署回應，其中金鑰Ki和A3、A5及A8演算法都不會在網路上傳送。而A3是鑑別MS身分所使用的單向雜湊函數，A5爲串流加密器(stream cipher)之金鑰流產生器(key stream generator)，A8則是產生Kc的單向雜湊函數（ETSI-1 1993；Rahnema 1993；Molva et. al. 1994；Harn & Lin 1995；Al-tawil et. al. 1998；Hwang et. al. 2000）。



圖三：現行GSM系統的身分鑑別程序

圖三所示爲現行GSM鑑別機制的程序示意圖，雖然GSM提供了手機鑑別及訊息加密的功能，但仍會面臨到下列五項安全性之威脅：

- 僅能提供網路端對手機用戶之單向鑑別，所以MS容易遭受仿冒BTS的攻擊。
- 相關鑑別參數均未提供完整性之保護，無法有效偵測出鑑別參數是否遭惡意竄改。
- 手機用戶與網路端之間的相關鑑別參數均以明文方式傳送，易遭受攻擊者截收之威脅。
- A3、A5及A8演算法均未公開檢驗，有安全之疑慮。
- 加密演算法之金鑰長度太短，有被破解疑慮。

本論文提出一個GSM的高效率相互鑑別機制，可以有效減少HLR與VLR間傳遞鑑別資訊的通訊負擔及VLR額外的鑑別資訊儲存量。我們的機制並不是一個解決所有上述GSM五項安全性威脅的方法，我們主要是針對GSM鑑別機制的相關問題加以改善。

參、我們提出的GSM相互鑑別機制

假設GSM網路端的傳輸通道是安全通道，檢視現行GSM鑑別機制後，我們可以發現其仍存在著一些缺失尚待改善，例如：

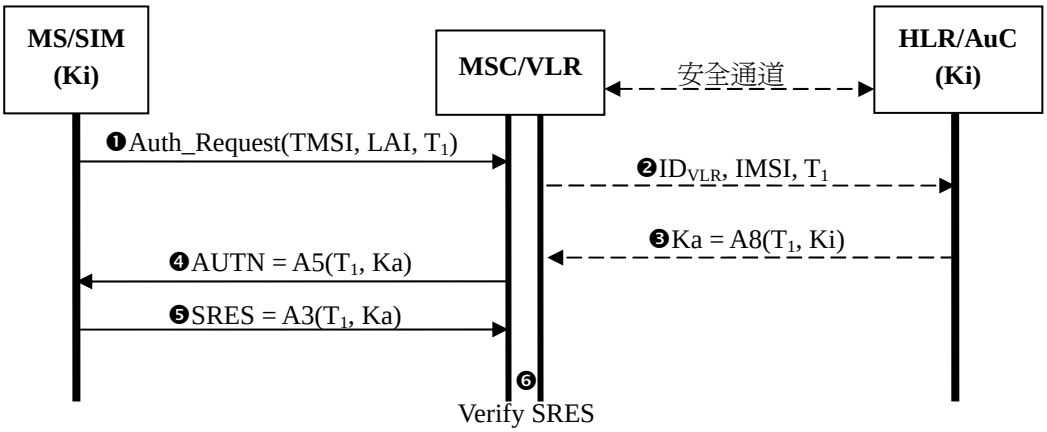
- 僅有VLR對MS單向的身分鑑別，MS與VLR間並無相互鑑別，所以MS無法對VLR加以鑑別，致使MS易遭受仿冒BTS攻擊之威脅。
- VLR針對每個MS均須儲存相關的n組鑑別參數{RAND, SRES, Kc}，容易造成VLR額外的儲存負擔。

- 若MS長期停留在同一個VLR進行通訊，致使n組的鑑別參數均已被使用掉時，則VLR就必須向HLR重新要求n組新的鑑別參數，會造成HLR與VLR間的通訊與頻寬的負擔。
- 若MS在通訊期間內快速的轉移多個VLR，則每個新的VLR均會向HLR要求n組鑑別參數，會造成VLR與HLR間的通訊與頻寬的負擔。

針對上述的現行GSM鑑別缺失雖已有學者提出相關研究的改進方法，但是均僅限於解決上述的部份問題或是需要改變現行GSM架構（Harn & Lin 1995；Al-tawil et. al. 1998；Lee et. al. 1999；Lee et. al. 2003）。我們所提出的方法則在不改變現行GSM架構下，可以直接利用現有GSM演算法來同時解決所有上述的幾項現行GSM鑑別缺失。我們所提出的方法依據通訊的時機，可以區分爲第一次及第j次(j>1)通訊等兩個相互鑑別的程序階段。

一、第一次通訊的身分鑑別

當MS剛加入一個新的VLR後，在進行第一次通訊時，因爲先前MS與新的VLR間尚未經過任何的相互身分鑑別程序，所以此時會啓動第一次的相互鑑別程序，有關第一次通訊時的身份鑑別程序如圖四所示，相關步驟說明如下：



圖四：我們的方法於第一次通訊時的身分鑑別程序

step1： 當MS加入一個新的VLR並要求提供通訊服務時，MS必須先送出一個包含TMSI、LAI及時間標籤T_1等資訊的身份鑑別請求給新的VLR。

step2： 新VLR會依照所收到的LAI資訊到舊VLR處，並依據TMSI取回該MS的IMSI後，新VLR再將自己的身分識別碼ID_{VLR}連同所取回的IMSI及T_1送給HLR，並將T_1儲存起來。

step3： HLR收到VLR所傳送的相關訊息後，首先會檢查ID_{VLR}的有效性，若爲合法有效的ID_{VLR}才會計算$Ka = A8(T_1, Ki)$，並將計算的結果Ka送給新VLR。若ID_{VLR}的檢查結果爲無效則中止鑑別程序。

step4： VLR儲存來自HLR的Ka後，計算$AUTN = A5(T_1, Ka)$及並將AUTN傳送給MS，作爲鑑別VLR身分之依據。

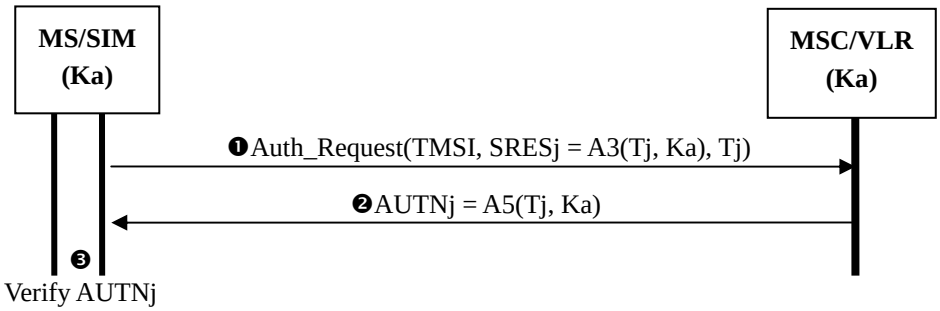
step5： 當MS接收到AUTN後，首先須計算$Ka' = A8(T_1, Ki)$及$AUTN' = A5(T_1, Ka')$並與所接收到的AUTN相比較，若兩者相同即表示MS成功地鑑別VLR的合法身分，MS

隨即計算SRES = A3(T_1, Ka')後，並將SRES送給VLR，以作爲鑑別MS身分之依據。若AUTN與AUTN'不同則中止身分鑑別程序並結束此次之通訊要求。

step6： VLR根據所收到的SRES後，首先須計算SRES' = A3(T_1, Ka) 並與所接收到的SRES相比對，如果兩者相同即表示該MS是合法使用者，否則便表示MS的身分鑑別失敗並結束此次之通訊要求。

二、第j次通訊的身分鑑別，j>1

當MS在未轉移VLR情況下，如果MS先前已與該VLR成功地進行過相互的身分鑑別程序並獲得通訊服務，則表示MS與VLR間已存在一把共同分享的秘密金鑰Ka，所以MS在同一個VLR進行第j次通訊時(j>1)，將會啓動如圖五所示的第j次相互鑑別程序，相關相互鑑別步驟說明如下：



圖五：我們的方法於第j次通訊時(j>1)的身分鑑別程序

step1： MS首先計算SRESj = A3(Tj, Ka)後，隨即送出一個包含TMSI、SRESj及時間標籤Tj等資訊的鑑別請求給同一個VLR。

step2： VLR根據所收到的SRESj後，首先須自行計算SRESj'= A3(Tj, Ka) 並與所接收到的SRESj相比對，如果兩者相同即表示該MS是合法使用者，隨即VLR必須計算AUTNj = A5(Tj, Ka)，並將AUTNj送給MS。若SRESj與SRESj'不同，則表示MS的身分鑑別失敗，將中止鑑別程序並結束此次之通訊要求。

step3： 當MS接收到AUTNj後，必須先計算AUTNj' = A5(Tj, Ka)並與AUTNj相比較，若兩者相同即表示MS成功地鑑別VLR身分，否則中止身分鑑別程序並結束此次之通訊要求。

肆、安全性與效能評估

本論文所提出的方法可以提供MS與GSM網路間完整的相互鑑別功能，且更具效率，本節將針對我們所提出方法的相關安全性及效能評估加以探討。

一、安全性分析

假設網路端之間的有線傳輸通道是安全通道，在不改變現行GSM系統架構的前提下，我們所提出的方法使用現行GSM的安全演算法(A3、A5及A8)來達到MS與GSM網路間相互鑑別的目的，在現行GSM系統仍繼續使用這些安全演算法情況下，且網路端之間的有線傳

輸通道是安全通道的前提下，我們的方法將可視爲是安全且可行的，相關安全性分析說明如下：

- MS與VLR間在進行每次通訊服務時，提供相互身分鑑別的程序。
  - SRESj = A3(Tj, Ka)，其中Ka = A8(T_1, Ki)爲合法MS與VLR所共同分享的鑑別金鑰，而Ki被儲存在AuC內，並燒錄於用戶SIM卡上。假冒的MS因爲無法獲得Ki的任何資訊，無法製造出Ka及能夠通過VLR鑑別的SRESj”，所以我們的方法藉由SRESj的傳送與驗證，可以避免VLR遭受假冒MS的欺騙威脅。
  - 因爲AUTNj = A5(Tj, Ka)，假冒的VLR並無法獲得Ki的任何資訊，無法製造出Ka及能夠通過MS鑑別的AUTHj”，所以我們的方法藉由AUTNj的傳送與驗證，可以避免MS遭受假冒VLR的欺騙威脅。
- 在每次的鑑別請求中加入不同的時間標籤Tj，且每次通訊的相互鑑別資訊SRESj及AUTNj的結果均與Tj相關且不同，即使攻擊者攔截到鑑別請求與相關身分鑑別資訊，但因爲攻擊者並未握有金鑰Ki或Ka，且Tj於每次通訊時均不同，所以攻擊者無法經由重送SRESj或AUTNj來冒充成MS或VLR來欺騙對方，可以有效避免遭受重送相關身分鑑別資訊的攻擊威脅。

二、效率評估

與現行GSM系統的鑑別機制相較之下，我們所提出的相互鑑別機制具有較佳的執行效率，可以減少鑑別資訊的計算量、儲存量與通訊量。我們使用現行GSM的A3、A5及A8演算法來達到相互鑑別的目的，相關演算法之執行次數如表一所示，其他相關效率評估說明分述如下：

- 在我們的方法中，在MS與VLR進行第一次通訊時，HLR並不需要計算n組不同的鑑別參數傳送給VLR，HLR僅需要計算AUTN及Ka，並僅須傳送AUTN及Ka給VLR，如此可以有效地減少HLR的鑑別資訊計算量及HLR與VLR間的鑑別資訊通訊量。
- 在MS與VLR進行第j次通訊時(j>1)，並不需要HLR參與此次的身分鑑別程序，VLR可以直接利用Ka來自行計算AUTNj與驗證SRESj，如此可以有效地減少HLR的鑑別資訊計算量及HLR與VLR間的鑑別資訊通訊量。
- 針對每個MS而言，VLR不再需要儲存n組不同的鑑別參數，僅需要儲存Ka與Tj，如此可以有效地減少VLR的鑑別資訊儲存量。
- MS與VLR(及HLR)所分享的秘密金鑰Ka可以取代現行GSM系統的Kc，並配合A5演算法作爲加密/解密資料的金鑰，所以在我們的方法中，雖然HLR須計算Ka並傳送Ka給VLR，但卻不會造成系統的額外計算量與儲存量之負擔。

表一：我們的方法與現行GSM鑑別機制之演算法執行次數比較

	現行 GSM 系統			我們的方法				
	改變 VLR 時之單向鑑別			第一次通訊之相互鑑別			第 j 次通訊(j>1)之相互鑑別	
	MS	VLR	HLR	MS	VLR	HLR	MS	VLR
執行 A3 次數	1		n	1	1		1	1
執行 A5 次數				1	1		1	1
執行 A8 次數	1		n	1		1		

伍、結論

隨著行動通訊用戶及網際網路的快速成長，將促使電子商務的快速成長，但是未來通訊系統容量將會出現明顯的不足，所以全球一致期望未來第三代行動通訊(3G)能夠將電信網路與網際網路相互連接，成爲以IP封包爲基礎的核心網路，同時可以支援語音與數據傳輸，而手機與基地台間也能享有更高速的數據傳輸速率。但是3G標準目前全球尚未統一，且GSM系統已普及超過190個國家，使用人口數更高達10億，所以短期內3G尚無法全面取代GSM，有鑒於此，爲顧及安全性與置換更新之成本考量，如何在不改變現有GSM系統架構下，持續加強現有GSM系統安全性是值得關注之議題。

我們所提出的方法與其他GSM鑑別機制相較，在各方面均具有相當不錯的表現，相關比較結果詳如表二所示。在不改變GSM系統架構下，我們的方法雖然無法解決現行GSM系統的所有安全缺失，但卻可以同時解決現行GSM鑑別機制中有關MS與VLR間無法相互鑑別、增加HLR與VLR間傳遞鑑別資訊的通訊頻寬負擔及VLR額外鑑別資訊儲存負擔等三項缺失，能夠有效提高現有GSM系統鑑別機制的安全性與效率，雖然爲了獲得上述利益所付出之代價是VLR的計算量增加，但此計算負擔僅是從原本的HLR轉移至VLR，且在第j次通訊時(j>1)的身分鑑別程序中，VLR僅須額外負擔一次的A5(Tj, Ka)計算量，然而由VLR負擔這樣的計算量應該是可以接受的。

表二：我們的方法與其他GSM鑑別機制比較表

	我們的方法	現行GSM系統	參考文獻（Harn & Lin 1995）	參考文獻（Al-tawil et. al. 1998）	參考文獻（Lee et. al. 1999）	參考文獻（Lee et. al. 2003）
改變現行GSM架構	No	--	Yes	Yes	No	No
第1次通訊時須相互鑑別	Yes	No	No	No	No	Yes
第j次通訊(j>1)時須相互鑑別	Yes	No	No	No	No	No
解決現行GSM系統鑑別資訊儲存負擔	Yes	No	No	No	Yes	Yes
解決現行GSM系統鑑別資訊通訊負擔	Yes	No	No	No	Yes	Yes

雖然在我們提出的方法中，A5須處理之資料可能是鑑別資料或一般使用者資料，然而在既有之GSM系統中，當正式進行通訊前，必須先經由信號交換及驗證程序後，才能進行一般使用者資料的傳送，且信號交換及驗證程序所須之控制資料是在控制頻道(Control Channels)上傳送，而一般使用者資料則是在運輸頻道(Traffic Channels)中傳送，所以兩者並不會混雜傳送，因此，我們可以直接利用現有傳送機制或稍加修改相關演算法，便可將鑑別資料及一般使用者資料分別由控制頻道及運輸頻道傳送。本論文僅提出方法論與理論的驗證，所以未來研究之方向則可以利用模擬軟體或其他實作方式來產生相關數據，以強化並實際驗證我們提出方法之安全性與效能。

參考文獻

1. Al-tawil K., Akrami A., and Youssef H., “A new authentication protocol for GSM network,” *Proceedings of IEEE 23rd Annual Conference on Local Computer Networks*, October 1998, pp.21-30, Boston.
2. Aziz A. and Diffie W., “Privacy and authentication for wireless local area networks,” *IEEE Personal Communications*, July 1993, First Quarter, pp.25-31.
3. ETSI-1. “Recommendation GSM 02.09: Security aspects,” *Technical Reports, European Telecommunications Standards Institute, ETSI*, June 1993.
4. ETSI-2. “Recommendation GSM 03.20: Security related network functions,” *Technical Reports, European Telecommunication Standards Institute, ETSI*, June 1993.
5. Harn L. and Lin H. Y., “Modification to enhance the security of the GSM protocol,” *Proceedings of the 5th National Conference on Information Security*, May 1995, pp.416-420, Taipei, Taiwan.
6. Hwang M. S., ”Dynamic participation in a secure conference scheme for mobile communication,” *IEEE Transaction on Vehicular Technology*, 1999, Vol. 48, pp.1469-1474.
7. Hwang M. S., Tang Y. L., and Lee C. C., ”An efficient authentication protocol for GSM networks,” *Proceedings of AFCEA/IEEE EuroComm’2000*, May 2000, pp.326-330.
8. Kumar S. and Zahn C., “Mobile communications: evolution and impact on business operations,” *Technovation*, 2003, Vol. 23, No. 6, pp.515-520.
9. Lee C. H., Hwang M. S., and Yang W. P., “Enhanced privacy and authentication for the global system for the mobile communications,” *Wireless Networks*, 1999, Vol. 5, pp.231-243.
10. Lee C. C., Hwang M. S., and Yang W. P., “Extension of authentication protocol for GSM,” *Proceedings of IEE on Communication*, April 2003, Vol. 150, No. 2, pp.91-95.
11. Lin H. Y. and Harn L., “Authentication protocol with nonrepudiation services in personal communication systems,” *IEEE Communication Letters*, August 1999, Vol. 3, pp.236-238.
12. Molva R., Samfat D., and Tsudik G., “Authentication of mobile users,” *IEEE Network*, 1994, Vol. 8, Issue. 2, pp.26-34.
13. Rahnema M., “Overview of the GSM system and protocol architecture,” *IEEE Communication Magazine*, 1993, Vol. 31, No. 4, pp.92-100.