國立交通大學

資訊管理研究所

碩士論文

一個針對衛星通訊的使用者認證機制

A Novel Authentication Mechanism for Satellite Communications

研究生：林友義

指導教授：羅濟群博士

中華民國 九十五 年 六 月

一個針對衛星通訊的使用者認證機制

A Novel Authentication Mechanism for Satellite Communications

研 究 生： 林 友 義　　Student: You-Yi Lin

指導教授： 羅 濟 群　　Advisor: Chi-Chun Lo

國立交通大學

資訊管理研究所

碩士論文

A Thesis

Submitted to Institute of Information Management

College of Management

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science in Information Management

June 2006

Hsinchu, Taiwan, the Republic of China

中華民國　九十五　年 六 月

一個針對衛星通訊的使用者認證機制

研究生：林友義　　指導教授：羅濟群 教授

國立交通大學資訊管理研究所

摘要

隨著網路通訊環境的成熟，行動通訊在現有的網路架構已結合了既有的網路環境，包含有線與無線網路，構成嚴密的網路拓樸。在 IMT-2000 通訊架構下，不僅提供陸上行動通訊的通訊架構，且提供衛星通訊進而構成完善的通訊環境。由於衛星通訊之涵蓋區域範圍非常廣泛，且不受地面之地型情況所影響，因而更能提供足夠的頻寬。此外，在衛星通訊架構下結合陸上行動通訊及有線與無線的網路環境，尤其是新一代通訊衛星的星載處理(On Board Processing, OBP)，使得衛星網路的功能更加強大。目前行動通訊的環境下已有數種認證機制，卻不適合於衛星環境下。因此本研究著重於針對衛星的特性，提出一套適合用於衛星通訊之認證機制。並以理論分析與系統模擬進行安全性分析，以此證明此機制兼具安全與適用於衛星通訊之特殊環境。

關鍵字：衛星通訊、星載處理、IMT-2000、認證機制

A Novel Authentication Mechanism for Satellite Communications

Student：You-Yi Lin　　Advisor：DR. Chi-Chun Lo

Institute of Information Management
Nation Chiao Tung University

Abstract

Because of the improvement of network technology, mobile communication system has combined wired and wireless networks to form complete network topology. It provides the communication architecture for terrestrial mobile communication and an environment for satellite communication system under the architecture of IMT-2000. As the result of widely coverage brought by satellite, it is possible to building up the vision of globular communication network. However, in the environment where satellite communication architecture combine wired and wireless network, a new satellite technology, On Board Procession(OBP), makes utilities of satellite communication more powerful. Although, there are several user authentication machines for mobile communication systems, they are not entirely compatible with satellite communication environment. Therefore, in this thesis, we focus on features of satellite communication system and proposed a novel authentication scheme which fits for satellite systems. Besides, we improvement a system to prove this scheme is a secure system and suit for satellite communications.

Keyword：Satellite Communication、OBP、IMT-2000、Authentication Scheme

誌 謝

碩士班兩年的時間一下子就過了，在完成這篇論文的同時，也就是離開校園的時候。回想兩年前剛進研究所，對於論文一點概念也沒有。兩年後的現在，順利通過論文口試，首先要感謝羅濟群教授，他自由卻又不失嚴謹的教學方式，深深在我心中刻劃了做研究應有的態度，並讓我享受到當個研究生應有的樂趣，所有的知識全都靠自己去鑽研。還要感謝陳文賢教授、楊亨利教授和陳瑞順教授在論文口試時所給予珍貴的建議，讓我的論文更趨於完善。

這段日子走來，要感謝的人實在太多了。除了父母和家人的支持，讓我可以全心投入於研究生活。還要感謝網路實驗室的夥伴們，俊龍學長、俊傑學長和鼎元學長在寫論文的過程中，提醒我應該注意的地方，讓我的思路更加實際。完成初稿後，感謝宗智學長仔細地字字校稿，建議我寫論文的技巧和人生哲理。宇哲、小德子和立群學長組成的八卦研究單位，帶給我碩士班生活更多的歡笑，使得沉重的課業壓力得以解放。感謝所有碩二的同學，尤其是愛帶正妹來實驗室，行事不低調的小欽欽，做事認真負責的超哥和個性樂觀灑脫的仁哥，能認識你們為了我的人生帶入更多色彩。再感謝碩一的學弟，為我們實驗室帶來不少歡樂，特別是小郭和宏爺的脫線演出，真的是笑死哥哥了，哥哥永遠愛你們。

一樣感謝菸鬼每次到台北都出來陪我，讓我暫時放掉學校煩心的事。還有肥達和 X 晏這對戀人的浪漫愛情故事。撞球小神童老驢，讓我的球精進不少。當然，還有當時在圖書館和我一起打拼的 ELVA，此生此景永難忘，再苦的日子都有你在，永遠感謝。最後，則是可愛的小美女，因為你讓我的努力有了目標，我相信一定會再見到心中最美的彩虹。

目 次

中文摘要 ..... **I**

英文摘要 ..... **II**

誌 謝 ..... **III**

目 次 ..... **IV**

圖目次 ..... **VI**

表目次 ..... **VII**

第一章 緒論 **1**

1.1 研究背景 1
1.2 研究動機 2
1.3 論文架構 3

第二章 文獻探討 **4**

2.1 衛星通訊概論 4
2.1.1 衛星通訊系統架構 5
2.1.2 衛星的分類 5
2.1.3 衛星通訊頻段 7
2.1.4 衛星的通訊方式 7
2.1.5 衛星的網路傳輸架構 8
2.1.6 著名的寬頻衛星系統 9
2.1.7 衛星多重存取(Multiple Access) 10
2.1.8 衛星的傳輸 13
2.2 行動通訊認證技術 16
2.2.1 行動通訊簡介 17
2.2.2 身份認證機制 19
2.2.3 GSM 認證機制 20
2.2.4 IS-95 CDMA 認證機制 22
2.2.5 UMTS 認證機制 24
2.3 衛星通訊認證 27

第三章 針對衛星通訊的認證機制 **31**

3.1 問題定義 31
3.2 解決方法 31
3.3 系統架構與目標 33

3.3.1 系統架構 33
3.3.2 系統目標 33
3.4 認證機制 34
3.4.1 註冊階段 35
3.4.2 本地端使用者認證階段與金匙更新階段 36
3.4.3 使用者漫遊身份認證機制與金匙更新 38
3.4.4 使用者相互認證與產生 session key 40
第四章 系統實作 43
4.1 系統設計 43
4.2 系統架構 43
4.3 系統實作環境介紹 44
4.4 系統運作流程 47
4.4.1 註冊階段 47
4.4.2 認證階段 47
4.4.3 產生 end-to-end session key 階段 48
4.5 系統實際運作畫面 49
4.6 總結 51
第五章 安全性與效率分析 52
5.1 安全性分析 52
5.2 效率分析 55
第六章 結論與未來展望 57
6.1 結論 57
6.2 未來展望 57
參考文獻 59

圖目次

圖 1　衛星通訊架構 5
圖 2　同步衛星示意圖 6
圖 3　bent-pipe 衛星架構 9
圖 4　OBP 及 ISL 的技術 9
圖 5　傳輸控制協定的送件格式 16
圖 6　改良 TCP/IP 協定示意圖 16
圖 7　在 ITU 下 IMT-2000 標準制定的機構 18
圖 8　IMT-2000 願景 19
圖 9　GSM 認證機制 21
圖 10　IS-95 認證機制 23
圖 11　IS-95 漫遊認證機制 24
圖 12　UMTS 認證流程圖 26
圖 13　Hwang et al. 衛星通訊架構 28
圖 14　註冊階段程序 29
圖 15　認證階段程序 29
圖 16　衛星通訊認證系統架構 33
圖 17　使用者註冊階段 36
圖 18　本地端使用者認證與金匙更新階段 37
圖 19　使用者漫遊之認證與金匙更新階段 39
圖 20　使用者相互認證與產生 session key 41
圖 21　系統架構圖 44
圖 22　Mobile User 45
圖 23　Fixed User 45
圖 24　註冊流程圖 47
圖 25　認證流程圖 48
圖 26　產生 session key 流程圖 49
圖 27　伺服器執行畫面 50
圖 28　用戶端執行畫面 51

表目次

表 1　著名衛星系統 10
表 2　GSM 符號說明 20
表 3　IS-95 符號說明 22
表 4　UMTS 符號說明 25
表 5　現行認證機制比較表 27
表 6　Hwangs'Scheme 符號說明 29
表 7 各項認證協定比較表 30
表 8 系統符號說明 35
表 9 系統硬體需求 46
表 10 系統軟體需求 46
表 11 安全分析比較表 55
表 12 率比較表 56

第一章　緒論

1.1　研究背景

提起電腦網路，在現代可說是家喻戶曉，但不只是目前當紅的網際網路(Internet)，實際上網路的應用在現代的生活中比比皆是。舉凡最普遍的電話、有線電視、郵局自動提款機、信用卡刷卡消費，及網路下單，報稅等，都是網路所提供的便利。基於網際網路的蓬勃發展與資訊科技的精進，網路能做的事已經不單單只是檔案的傳輸或瀏覽網頁而已。在未來，網路的應用的主流為多媒體視訊與行動通訊兩方向。多媒體視訊的應用像是隨選視訊(Video on Demand)、遠距教學(Distance Learning)、遠距醫療(Distance Medicine)和視訊會議(Video Conference)等。為滿足即時性的需求，更需要廣大的網路頻寬和資料壓縮技術。而行動通訊帶給人們的便利是不論何時何地都能夠使用網路的資源。因此，除了寬廣的頻寬以及普及的網路建設之外，更需要克服異質性網路之間的整合問題。

以現階段全球衛星通訊發展之方向而言，網際網路之盛行賦予衛星通訊一個全新的發展空間。例如：透過衛星的寬頻網路來連接各地區之網際網路骨幹網路(Internet Backbone)、衛星直播到府之網際網路服務(Direct Internet)，甚至結合影像、聲音、數據等多項應用之衛星多媒體服務亦方興未艾。展望未來，衛星通訊服務將善用其寬頻、非對稱以及點對點之特性，在國際之間的通訊服務市場將演非常重要的角色。

一般而言，衛星通訊有以下幾個特性：

1. 衛星涵蓋範圍無遠弗屆，通訊距離遠，涵蓋面積廣大。同步衛星的波束可涵蓋 42.4%的地表面。

2. 衛星系統的開發迅速，無纜線的架設與規劃問題。因此，用戶可於短時間內

裝設完成。

3. 衛星傳輸價格不受距離影響，不像線纜傳輸由距離決定。衛星的傳輸價格是取決於頻寬、頻道數與傳輸速率。

4. 因為衛星通訊的地面設施較少，也較為單純。縱使受地震、颱風等天災影響，也能迅速恢復通訊。

5. 衛星具有多點通訊導向系統，與目前地面通訊系統單點對單點通訊模式相較之下，只要透過衛星便可輕易地做到多點通訊網。

因為衛星有上述這些優點，於是在網際網路未來的發展上，扮演著舉足輕重的角色。甚至有學者提出將網際網路搬上太空的構想(Internet over Sky)[15]，此為行動衛星通訊的延伸。其透過為數眾多的行動通訊衛星所建構而成的網路，得以快速地將一方的資料傳送到地球上的另一方。又因為衛星所具有的特性，於是網路將無遠弗屆地延伸下去，使用者也可享受到網路所帶來的服務，屆時網際網路又將進入另一個新的里程碑。

1.2 研究動機

任何通訊系統的關鍵性成功因素可分為兩個層面。首先是技術層面，不外乎是系統的效率和可用性。其關係到演算法的好壞，採用適合的編碼系統和基地台的涵蓋率等。另一為管理層面，例如：使用者最在意的是個人隱私的侵害，或者是非法盜用身份之類的安全問題。而服務的提供者最在意的是系統的安全性，以及計費，收費和非法盜用等議題。不論是使用者關心的隱私或是系統提供者所在意的收費問題，都是屬於在使用者認證(User Authentication)的議題之下。

在眾多廠商的推動下，數個衛星通訊系統的建構計畫已如火如荼進行著。截至目前為止，數百顆衛星在地球軌道上運行著。如此可見其受重視之程度，因此

不少研究行動通訊衛星系統應用與協定的議題已被討論著，但有關衛星通訊安全這方面的議題仍尚未有一套完善的機制。

目前在於無線通訊系統上的認證機制已行之多年。但是不禁自我反問，現在所使用的認證機制適用於衛星通訊的環境上嗎？經過研究現有的行動通訊和衛星認證機制後，發現目前的認證機制並不完全適用於衛星通訊系統。本論文將針對衛星通訊的安全議題，試著提出一套更適用於衛星環境下的身份認證機制。

1.3 論文架構

本論文共分成六章。第一章為緒論，介紹本文的研究背景、動機和論文架構。第二章為文獻探討，探討衛星通訊系統，包括衛星通的特性和各種衛星通訊系統與目前行動通訊系統的認證機制。第三章提出改良方法和流程。第四章則是系統實作的部份，進一步介紹系統的設計、架構和模擬方式。第五章為安全與效率分析，探討系統執行的效能和結果。第六章為結論以及未來的研究方向。

第二章　文獻探討

本章內容主要分成三大部份，首先介紹衛星通訊系統的架構和特性。對於衛星通訊系統具備通盤的認知之後，隨即則是目前行動通訊的認證機制，如：GSM、UMTS 等。之後介紹衛星通訊目前所提出相關的認證機制。本章節最後分析上述機制對於衛星通訊環境的適用性。

2.1　衛星通訊概論

所謂衛星通訊是指利用人造衛星為中繼站，轉送無線電訊號波以進行兩個或多個通訊站之間的通訊。進一步來說，衛星通訊是利用衛星地面站將欲傳送之資料訊號以高頻無線電傳送至太空中之衛星本體，再藉由衛星網路下傳至衛星訊號接收站。藉此方式構成單向傳播或雙向通訊的衛星體系。

一般而言，衛星通訊有以下幾個特點[16]：

1. 衛星涵蓋範圍無遠弗屆，通訊距離遠，涵蓋面積廣大。同步衛星的波束可涵蓋 42.4%的地表面。

2. 衛星系統的開發迅速，無纜線的架設與規劃問題。因此，用戶可於短時間內裝設完成。

3. 衛星傳輸價格不受距離影響，不像線纜傳輸由距離決定。衛星的傳輸價格是取決於頻寬、頻道數與傳輸速率。

4. 因為衛星通訊的地面設施較少，也較為單純。縱使受地震、颱風等天災影響，也能迅速恢復通訊。

5. 衛星具有多點通訊導向系統，與目前地面通訊系統單點對單點通訊模式相較之下，只要透過衛星便可輕易地做到多點通訊網。

2.1.1 衛星通訊系統架構

衛星通訊系統的組成分為「地面站系統」與「空中系統」。地面站系統由 gateway stations (GSs)、network control center (NCC)與 operation control centers (OSSs)組成。NCC 與 OSSs 負責網路資源管理、衛星操作及衛星軌道控制；GSs 則扮演衛星網路與地面各種不同網路的介面，同時也執行協定(protocol)、網路位址(network address)和格式(format)的轉換。而空中系統則由衛星組成，可區分為同步衛星(geostationary orbit, GSO)與非同步衛星(nongeostationary orbit, NGSO)。而非同步衛星又依其運行軌道的高低分為中軌衛星(medium earth orbit, MEO)及低軌衛星(low earth orbit, LEO)

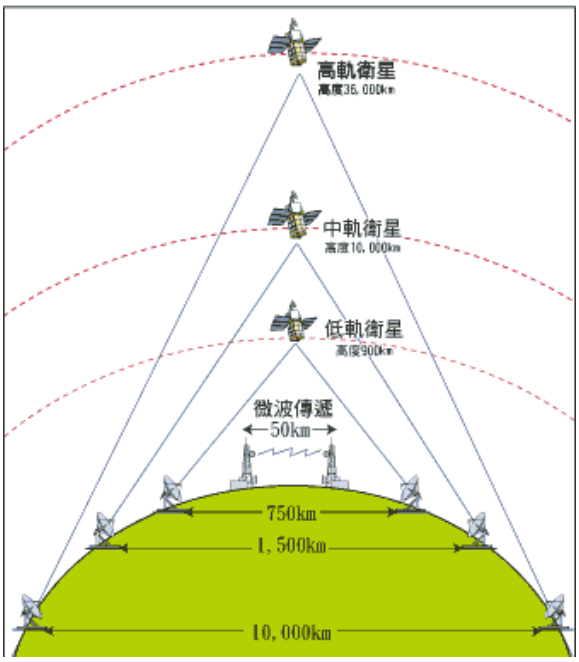

圖 1　衛星通訊架構

2.1.2 衛星的分類

一、同步衛星(geostationary satellite)

通訊衛星依其運行的軌道，可分為同步衛星和非同步衛星。所謂同步衛星，

即是固定於地球上空某個位置的衛星。一顆衛星要能永遠固定在地球軌道的相同位置上，先決條件就是其繞行地球的週期和地球的自轉週期相同都是 24 小時，因此從地球上看它，好像是靜止的。同步衛星的高度約為 35,860 公里。訊號的覆蓋區可達地球表面 1/3 區域，因此只需要三顆同步衛星，訊號便可覆蓋全球(圖 2)。雖然同步衛星的涵蓋範圍廣，且不會產生 Doppler 頻移 [1] 的問題。但是，卻有一個影響通訊功能的主要缺點：由於距離地球太遠，使得無線電波來回時間增長而造成訊號延遲。一般而言，訊號延遲時間大約介於 250-280 ms 之間，因此不適合即時性的傳輸。

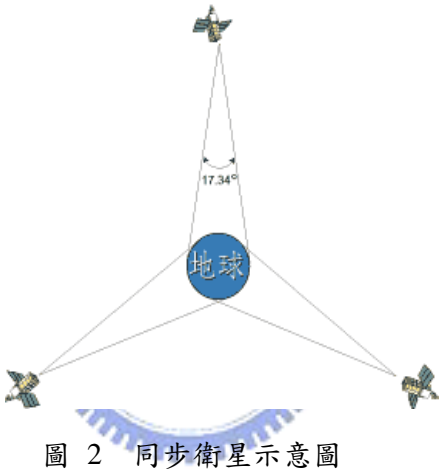

圖 2　同步衛星示意圖

二、中軌衛星(MEO)與低軌衛星(LEO)

MEO 位於地球上方 3,000~15,000 公里的地方，訊號延遲時間大約介於 110-130ms；LEO 則是位於地球上方 200-3,000 公里的地方，訊號延遲時間大約介於 20-25ms 之間。相較於 GSO，MEO 及 LEO 的體積較輕、較小。發射升空的價格也較便宜。因為高度低，訊號傳送時間較短，地面發射站天線和發射機輸出功率不必太強。不過軌道較低造成訊號涵蓋範圍較小，所以需要的衛星數目較多。

[1] 當訊號源向接收端前進時，接收端所測得之頻率較高。反之則較低，此為 Doppler 頻移。

2.1.3 衛星通訊頻段

在目前的衛星系統頻段中，一般多使用 C 頻、Ku 頻及 Ka 頻。其頻率範圍分別為 4 -8GHz、10-18GHz，及 18-31GHz。頻率越高波長越短，所需的天線面積相對較小。

使用 C 頻的衛星系統其天線直徑約為 2-3 公尺，不過由於 C 頻的波長較長，所以雨衰[2]情形不會像高頻段訊號嚴重，常用於全球廣播、半球廣播及越洋中繼廣播。

使用 Ku 頻的衛星系統其天線的直徑約為 18 英吋，多半運用在區域廣播、點對點廣播、直播衛星播送及 SNG(Satellite News Gathering)中繼傳送等。

在 C 頻與 Ku 頻的頻道日漸不敷使用的情況下下，許多衛星公司開始研究利用 Ka 頻提供服務。因此，系統頻寬較高的 Ka 頻成了近年來發展寬頻衛星通訊的主要頻段。然而，雨衰與大氣雲層等干擾是目前 Ka 頻亟待克服的問題。此外，在訊號傳輸中，Doppler 頻移效應與天線追蹤的問題仍待進一步解決。

2.1.4 衛星的通訊方式

以衛星為基礎的通訊網路，其架構因衛星的設計方式不同，而有多重的選擇。主要可將衛星通訊可依下列方式分類：

- ✓ 按衛星運行軌道分類：同步衛星(GSO)、中軌道衛(MEO)、低軌道衛星(GEO)。
- ✓ 依 Payload 的不同可分為：bent pipe、星載處理(OBP) 。
- ✓ 是否具有跨衛星連線(ISL)能力。

---

[2] 當衛星信號到達天線前，行進的途徑如有烏雲或雨水的阻擋而形成信號衰減。

衛星網路可做為網路骨幹及高速接取網路。使用衛星來做為通訊骨幹及接取網路可解決網路通訊中最後一哩的問題(last mile problem)，亦即衛星網路可連接使用者端至網路接取點(Network Access Point)。主要利用的技術則是小型衛星地面站(VSAT，Very Small Aperture Terminal)系統。

2.1.5 衛星的網路傳輸架構

傳統的衛星尤其是 GSO 大多是使用 bent-pipe 的方式，做為地面兩個溝通點的 repeater，並無星載處理(onboard processing，OBP)的能力，因 bent-pipe 的方式是較為簡單可行的。不過較先進的衛星具備 OBP 的能力，它包含了 demodulation/remodulation、decoding/recoding、transponder/beam switching， 和 routing 的功能，使得通道的利用能更有效率。OBP 也支援跨衛星連線(Intersatellite Links, ISLs)。藉由使用跨衛星連線(ISLs)的技術，衛星與衛星在空中的通訊傳輸不需要透過地面即可完成，這可降低地面站台的數目。

一、bent- pipe 衛星架構

一般傳統的衛星通訊網路主要是採用 bent-pipe 衛星架構(圖 3)，此種架構可採用 GSO、MEO 或 LEO 等任一種衛星。它可提供網路接取和資料中繼服務。衛星網路和地面網路之間的介面則是地面上的 gateway stations(GWs)。在沒有其它的連接方式時，衛星網路可能成為少數使用者的唯一接取模式（如圖 3 中的 user A）。此外，它也可能成為多數使用者於傳統網路之外的另一種選擇（如圖 3 中的 user B）。不過由於 bent-pipe 的衛星架構不具備跨衛星連線能力，不能在空中直接連接傳輸。在訊號下傳後必需經由地面線路再上傳才能到達另一顆衛星，故需較多的地面站台，這使得資料之間的傳輸缺乏效率。

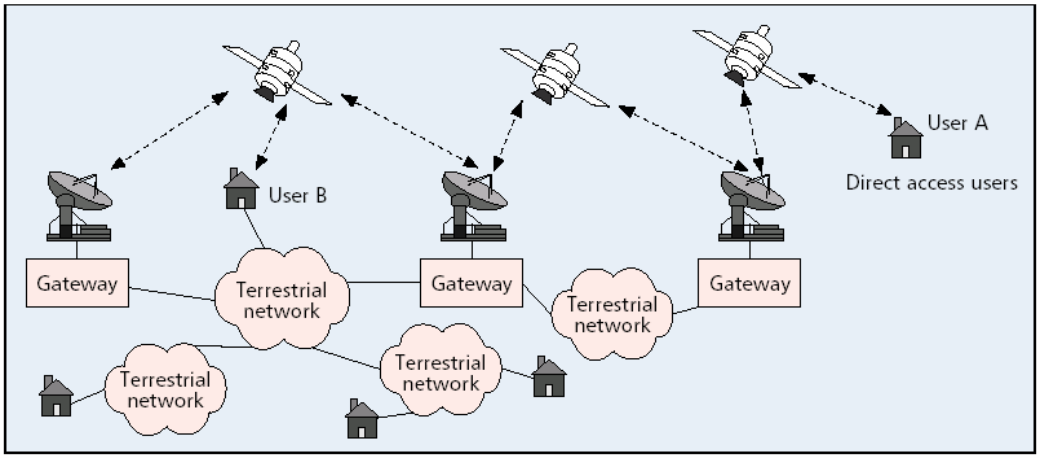

圖 3 bent-pipe 衛星架構[20]

二、OBP 及 ISL 的技術

為了改善 bent-pipe 不具跨衛星連線的缺點，部份衛星系統使用 OBP 及 ISL 的技術來達成衛星的空中連結（如圖 4）。例如：Teledesic 衛星計劃使用了 288 枚可跨衛星連結的 LEO，組成了一個空中的衛星網路，讓衛星之間可彼此通訊。這使得衛星網路通訊能更有彈性，不過也帶來了複雜的 routing 問題。

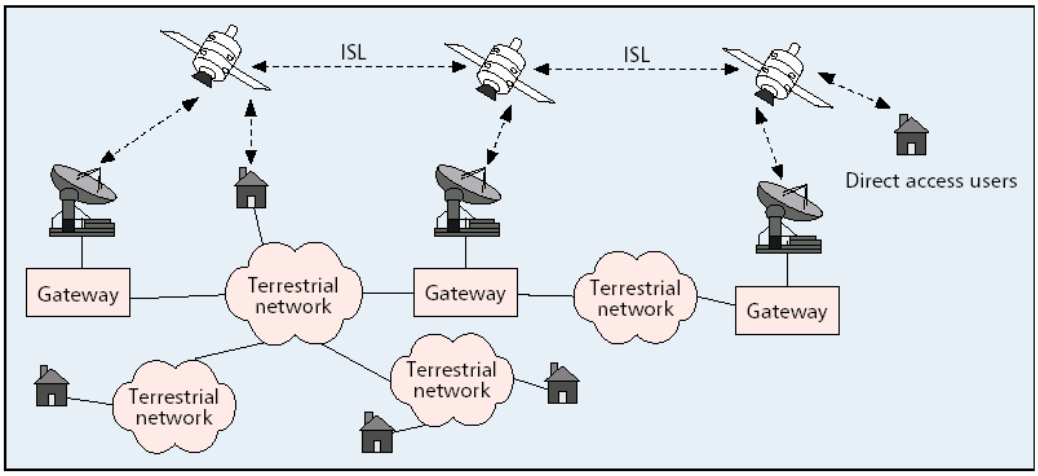

圖 4 OBP 及 ISL 的技術[20]

2.1.6 著名的寬頻衛星系統

表 1 整理了世界上較著名的寬頻衛星系統，主要提供高速的網路服務。不

過其中並未包含於 1998 年開始營運的銥計劃（Iridium）[17]。因為它的設計主要是用來做語音的傳輸，而不是為了數據的傳輸而設計。

表 1　著名衛星系統 [20]

System	Major sponsors	Constellation	Satellite payload	Frequency band	Data rate	Service date
Astrolink	Lockheed Martin	Up to 9 GSO satellites	OBP and ISLs	Ka	Up to 200 Mb/s downlink Up to 20 Mb/s uplink	2003
Skybridge	Alcatel Espace, Loral Space	80 LEOsatellites at 1469 km	Bent-pipe	Ku	16 kb/s–20 Mb/s downlink 16 kb/s–2 Mb/s uplink	2002
Spaceway	Hughes	4 GSO satellites (ultimately 21 satellites)	OBP and ISLs	Ka	Up to 92 Mb/s downlink 16 kb/s–6 Mb/s uplink	2002
Teledesic	Motorola, Lockheed Martin	288 LEO satellites at 1375 km	OBP and ISLs	Ka	16 kb/s–64 Mb/s downlink 16 kb/s–2 Mb/s uplink	2004

2.1.7 衛星多重存取(Multiple Access)

由於衛星在傳輸時的頻寬有限，因此要在眾多的等候傳輸的競爭者中適當地分配頻寬，成為一件很重要的工作。主要的分配方式可分為三種模式：固定分配（Fixed Assignment）、隨機存取（Random Access）及需求分配（Demand Assignment）

一、固定式分配（Fixed Assignment）

對固定式分配衛星的溝通方式而言，可分為分時多工(Time-Division Multiple Access, TDMA)、分頻多工(Frequency-Division Multiple Access, FDMA)及分碼多工(Code-Division Multiple Access, CDMA)三種方式。這可用宴會中多人溝通的方式來比擬。分時多工是指每個人利用不同時段，但同一時段只能有一人說話。分頻多工是指每個人的頻率都有些許的不同，因此可清楚區分。分碼多工則類似第一個人講英文，第二個人講中文，而第三個人講日文，由於各種語言互相垂直易辨別而可清楚辨識，每個人用不同的語言講話。例如：全球定位系統(GPS)即是採用分碼多工方式。

(1) 分頻多工(FDMA)

如果衛星系統使用此種接取方式,所有地面傳送站可同時共享衛星所提供的頻道,彼此有個別的傳送頻帶。也就是說,將衛星的有效頻寬分割成多個次頻帶,再配置給各個發射站使用。不過 FDMA 技術有下列幾項缺點:

- ✓ 為了避免相鄰頻道的干擾,頻道間需保留安全頻帶(guard band),因此浪費一些有效頻寬。
- ✓ 若傳送站無經常使用,頻道處於閒置狀態這些頻道視同無用而浪費。
- ✓ 當衛星轉頻器同時使用多個載波傳送資料時,由於轉頻器之非線性特性會產生相互干擾。為避免干擾,轉頻器需做反減補償(back -off)使得發射功率降低。

(2) 分時多工(TDMA)

TDMA 技術係以時間座標為基礎,每一傳送站分配一個小時槽(time slot),只允許在時槽內傳送資料,所有 TDMA 系統均是數位化的,因此 TDMA 系統有不少優於 FDMA 系統的優點。

- ✓ TDMA 技術易於重新規劃,以適應資料流量及抵抗雜訊干擾。
- ✓ 轉頻器只使用一個載波,因此不會有互調干擾雜訊,衛星轉頻器之傳送訊號功率可到達最大極限。
- ✓ 可更改每一地面站之脈衝訊號發出時間,由於脈衝訊號時間,因此每一地面站之容量可更改。

為了達到 TDMA 傳送方式,傳送站將資料規劃成資料訊框(frame)來傳送,資料封包含一個同步化參考訊息(reference signal)以及多位使用者資料。參考訊息的目的在使所有地面站校正時間,以便使用正確的時槽。參考訊息後面跟著使用

者的原始資料，每位使用者僅能使用一個時槽，為了確保資料安全，時槽之間預留一些安全時間(guard time)，時槽前端附加前序編碼(Preamble)，當資料傳送完畢後再加上一個後序編碼(Postamble) 。

(3) 分碼多工(CDMA)

分碼多工技術，使用者全部時間均可使用衛星轉頻器的全部頻寬。使用者的訊號必須經過編碼處理，唯有知道傳送站所使用的編碼方式與解碼方式，才能接收其訊號。此種技術提供一種分散式衛星網路環境，接收站皆有個自的編碼，稱為地址，傳送站以接收站的地址來調變訊號，再把資料傳送給衛星即可。

二、 隨機存取（Random Access）

採用隨機存取式傳輸技術的衛星系統，如 VSATs 和 USATs(Universal Satellite & Antenna Tripod)，可隨時傳送資料，但在傳送時可能會有碰撞的情發生。

隨機存取式傳輸最主要的接取方式有 ALOHA 進接。使用 ALOHA 接取技術，使用者可隨時傳送資料，在頻道上的進出並未受到時間或頻率限制，當兩使用者傳送的資料再空中碰撞時，原資料會受到破壞，原傳送站得重送資料，此種進接方式為純 ALOHA。為了改善資料訊框的碰撞，發展出了另一種槽式(slotted) ALOHA 法，地面站需與衛星建立共同時序，等到地面站的時間同步，所有通訊站在時槽(Time Slot)開始時傳送資料，其他時間則不送出。槽式 ALOHA 亦會發生碰撞，但碰撞受損之時間比純 ALOHA 方式減少許多。

三、需求式分配（Demand Assignment）

即使隨機存取的方式可容納較多人同時傳輸，但並不能提供 QoS(Quality of Service)的保證，這使得傳輸的品質不穩定。為了解決這方面的問題，目前的衛星傳輸科技，提出了依需求指定多路接取(Demand Assigned Multiple Access,

DAMA)的傳輸方式。透過衛星管道，根據數據解法進行網路服務， DAMA 提供多個地面之間聯繫，是具彈性和節省的複數通路技術。因為 DAMA 可對眾多用戶提供直接聯繫、減少費用， DAMA 使新用戶有機會透過較小地面站達到全球性聯繫。

DAMA 可用於大大小小的地面站，就每通電話自動傳達也可支持許多不同的介面，以及通訊規則，此傳達和切換的聯合，DAMA 對不同目的地 trunks 不須預先設定路線，DAMA 會把來話繞送到目的地，因連接到 DAMA 的 trunk circuits 可分用不同目的地之 trunks 而改進服務的可行性，採用 DAMA 可設立直接聯繫，省卻傳達費用。

有了低價格的地面站、裝置、維修和調換都非常簡易，客戶將能迅速擴大其服務，若干國內地區和國際應用可獲得 DAMA 的 彈性所支援，用戶的使用包括國際網路，以及部署救災的迅速通訊，從事商業應用廣泛使用於各行業，如銀行、證卷、報業、連鎖店、加油站等，而偏遠地區如高山、沙漠、小島亦是最好應用場合。

2.1.8 衛星的傳輸

在目前的網路上傳輸協定一般都使用 TCP/IP 及 UDP/IP，而目前的衛星傳輸也仍然使用 TCP 及 UDP 的協定。但這兩種協定的效能，由受到衛星系統的高錯誤率及延遲特性影響而成效不佳。針對這樣的問題美國 NASA 的 ACTS 衛星及 IETF 機構進行研究，希望能改善 TCP/IP 在衛星網路上的效能[9]。以下將分為兩部份來介紹 TCP 在衛星網路上的效能問題，第一部份討論 TCP 在衛星網路上的限制，第二部份則針對目前 TCP 效能提昇的研究議題做整理。

一、TCP 在衛星上的效能

TCP 使用正向回饋機制來控制傳輸達成率及可靠度。高延遲時間的問題增加

了 TCP 端對端(end-to-end)的傳輸延遲及回應的遲緩，不但會使傳輸效率低落，也可能會引起網路的擁塞。另外動態拓樸(dynamic topology)也會引起大幅變動的封包來回傳送時間。封包來回傳送時間（Round Trip Time, RRT）則是另一項影響網路品質的重要因素。通常來回傳送時間愈長，資訊傳送速率愈慢，途中所遭遇的壅塞也可能愈嚴重。因此，如果能夠嚴格維持網路中（指其自有節點間或至與其他網路接續點）的封包遺失率與封包來回傳送時間這兩項服務品質指標，不分尖峰、離峰情況均達到要求，則對網路所有應用的服務品質提供基本的保障。

TCP 在一開始傳輸時是以緩慢的方式開始，即使這時資料量成指數方式成長，TCP 仍是以緩慢的方式增加其資料傳輸量，這使得頻寬無法獲得充份的利用。這時可能採取的解決方法是增加一開始的 window size，TCP 允許一開始最大的 Window size 為 64kbytes，但這可能會增加資料傳輸延遲的問題。因此目前 IETF 在其網路規格文件 1323 中[12]，已對於 window size 的設定做了一些定義及規定。

衛星傳輸可能會產生高位元錯誤率(Bit-Error Rate；BER)，即使利用較先進的更正調整技術如：coding schemes 及 forward error correction 向前除錯等技術，在某些環境下仍可能會有高的位元錯誤率。另外，TCP 並不能辨別錯誤資料所引起的傳輸錯誤及網路封包所引起的擁塞。此外，當天候不佳時由於傳輸效果差，也會使得網路傳輸錯誤大量出現。所以空中通訊標準-傳輸協定(SCPS-TP)[19] 規定了這兩種不同錯誤的差別及其回應方式的差異。

由於衛星網路的不對稱性也會減弱 TCP 的效能，衛星網路的不對稱性的發生可能有下列兩種原因：第一個原因可能是因為之前所提過的，衛星直播網路存取架構所引起的；而另一個原因可能是由於上傳及下傳的頻寬的速度並不相同所引起的。此外，TCP 在面對不同的 RTT 時，並不能針對不同的 RTT 給予不同的頻寬，這使得傳輸的效率不能被有效提升。

二、效能的提昇

最近 IETF 的 TCP 部門衛星事務委員會在其網路規格文件中，對衛星連結的 TCP 效能提升問題做了一些建議：

- ✓ RFC2018 給予 TCP 選擇性回應 selective acknowledgment-(SACK)的權力。
- ✓ RFC1644 的 T/TCP 試圖減少連接時的 hand-shaking 動作，讓 hand-shaking 由兩個 RTT 降為一個 RTT，這能有效減短傳輸時間。
- ✓ RFC2068 支援 HTTP1.1 的 TCP 持續連結功能。
- ✓ 最大可傳送量路徑的發現機制，允許 TCP 使用儘可能較大的封包大小，這可避免 IP 切割的問題，可減少網路的負擔及資料重組的問題。
- ✓ FEC 可改善資料傳輸錯誤的問題，以提昇傳輸品質，但不能解決人工干擾所造成的噪音問題

擴充後的 TCP 相較於標準 TCP，可解決以上部份問題，不過仍存在著一些和網際網路連線的技術挑戰。

因為衛星網路的運作是建立在封包的傳送上並採用 TCP/IP 通訊協定溝通，封包的送件規格置於封包標頭處如圖 5 所示。由圖可看出封包容量是由滑動視窗(sliding window)寬度來規定，其最大值為 16 位元或代表封包容量上限是 64KB。由於同步衛星的距離非常遠，前面的分析可知其傳送遲延為單程 250ms，考慮來回距離後可知每秒只可傳送兩個封包。

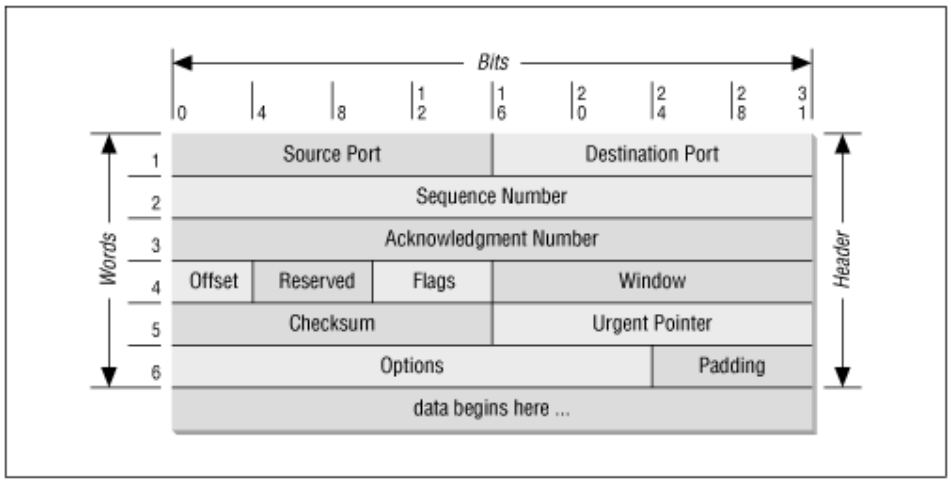

圖 5 傳輸控制協定的送件格式[8]

目前已發展出資料鏈結層(Data Link Layer)、端對端(End-to-end)及代理設備(Proxy)三種網路技術來克服人造衛星低資料傳送量的方法。對資料鏈結層而言，這是修改資料鏈結層中收到資料的確認通知(Acknowledgement)方式來增加每秒傳送的封包數。對端對端而言，這是修訂 TCP/IP 通訊協定使得滑窗寬度可達 30 位元。對代理設備而言，這是把網路以連線分割(Connection Splitting)方式拆成圖 6 中 C1、C2 及 C3 三段；而封包在建立連線後，第一個的封包從 H1 到達 G1 處就由 G1 發回應並請 H1 繼續傳第二個封包。此方式可解決人造衛星因距離而產生的傳送延遲問題。

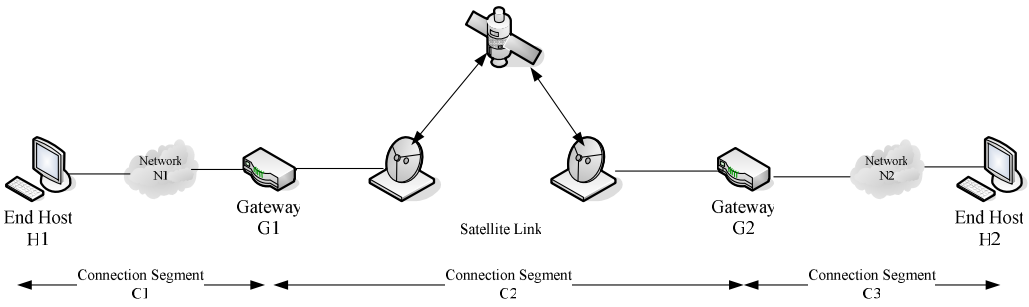

圖 6 改良 TCP/IP 協定示意圖

2.2 行動通訊認證技術

無論任何通訊環境，皆需在安全的通訊環境中完成，包括通訊通道不應受

到干擾或截聽，行動設備彼此之間應可做身份確認，以免遭受偽冒或重送攻擊。另外，使用者身份認證亦為重要一環，以下將探討行動通訊和身份認證的相關議題。

2.2.1 行動通訊簡介

行動通訊的演變由第一代(1G)只傳遞語音，如 AMPS(Advanced Mobile Phone Service)；至第二代(2G) GSM(Global System for Mobile communication)系統或美洲體系的 CDMA One(IS-95A)，其中 GSM 結合語音與數據通訊的能力，於數據傳輸上可達 9.6Kbps，但為提升傳輸速率故發展 GPRS(General Packet Radio Service)。此外 IS-95A 演變成 IS-95B，即俗稱的第 2.5 代的行動通訊；但為了提供行動用戶傳輸多媒體與即時影音資料，並且支援網際網路的 All-IP 高速服務，故有了第三代行動通訊系統(3G)的研發。第三代無線通訊系統，從 1985 年開始，由國際電信聯盟 ITU[10]所提出，最初的名稱為「未來陸地移動通訊系統 FPLMTS (Future Public Land Mobile Telecommunication System」，到了 1996 年正式更名為 IMT-2000。

IMT-2000 主要整合陸上細胞系統(Terrestrial Cellular system)、無線系統、無線接取和衛星系統為單一家族式標準系統。在 ITU 下整個 IMT-2000 標準是由 ITU-R 及 ITU-T 兩部門制定，其中 ITU-R 負責無線電及系統方面標準的制定；而 ITU-T 負責網路方面標準的制定，包括服務、管理、安全機制、訊號與協定及編碼、壓縮等，其架構如圖 7。

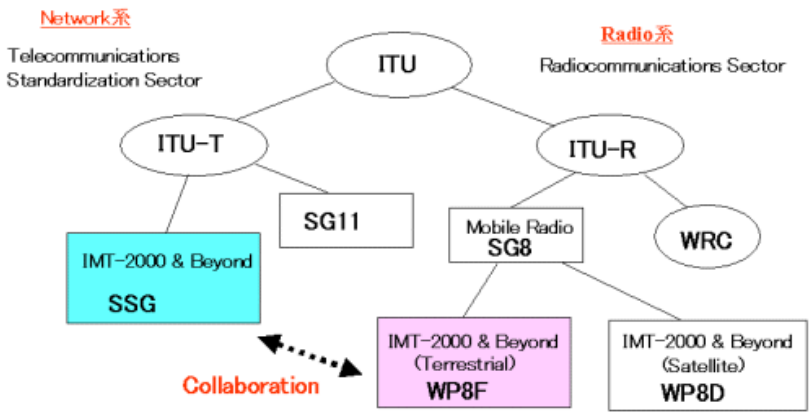

圖 7　在 ITU 下 IMT-2000 標準制定的機構[4]

IMT-2000 發展之目的是希望以寬頻技術整合各類服務需求，達到多媒體行動通訊的理想，以提供更好的通話品質，更多樣化的服務. 同時藉由衛星行動通訊的技術使得服務區域更廣泛，真正實現一機走天下的理想。因此，依據 ITU-R 的規劃，未來的用戶，只要透過一個輕薄短小的通訊設備，在任何時間、在世界的任何地點都可獲得需要的通訊服務。而整個網路環境則是涵蓋了低功率無線電系統、蜂巢式行動電話、衛星系統、及有線（電話/電腦）網路等，整合成單一通訊介面的全球性通訊網路. 系統會自動依照用戶要求的服務項目及當地的網路環境，選擇適當的連線方式。圖 8 為 IMT-2000 之願景。目前 ITU 已經核定在歐洲及大部分亞洲(含日本)的 IMT-2000 系統使用 2 GHz 的載波頻率(規劃的頻段為 1885~2025MHz，2100~2200MHz，其中 1980~2010MHz 及 2170~2200MHz 指定給衛星行動使用)的通訊系統；另主要接取技術為 Wide-Band CDMA(3GPP)、CDMA2000(3GPP2)及 TD-SCDMA。

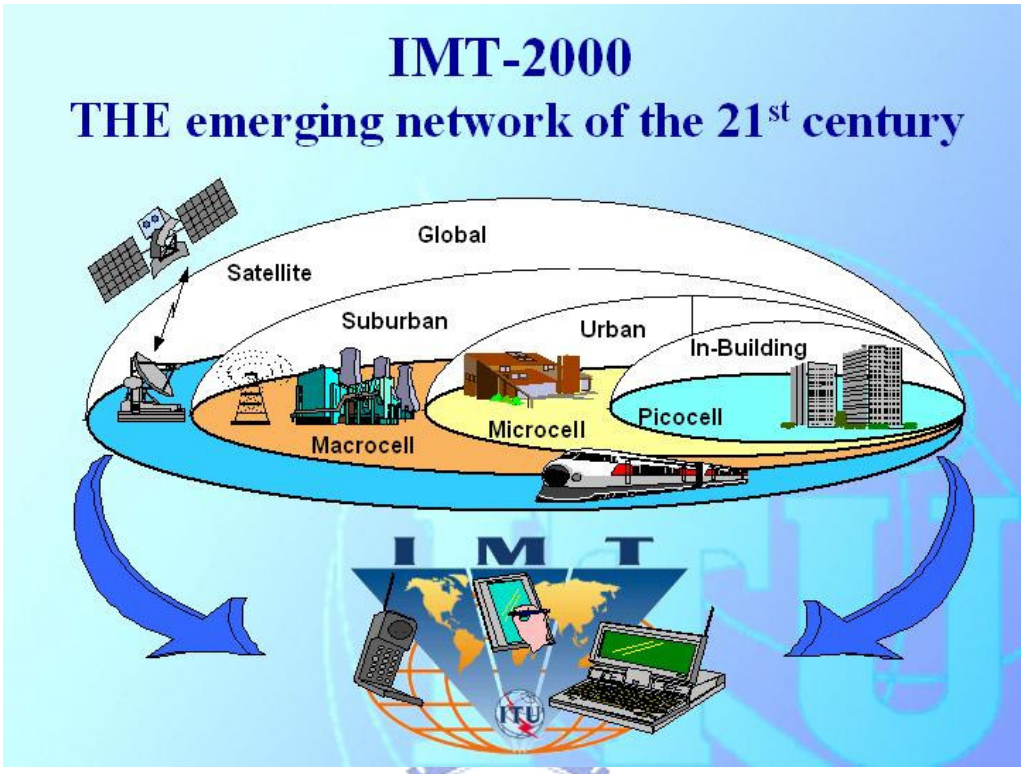

圖 8　IMT-2000 願景[21]

2.2.2 身份認證機制

由於不同以往傳統的電腦網路是利用線材傳送資料，行動通訊將訊息曝露於空中，相對的，行動通訊傳送的資料易遭截取。因此，在安全上必須有相當程度的考量，身份認證即成為重要的議題。身份認證可包括使用者認證及基地端認證兩方面來討論：

一、使用者認證：由於行動通訊的開放環境，使得冒用合法的使用者相當容易，造成提供服務的廠商常常損失大量的金錢。而除了來自系統以外的非法使用者之外，系統內部的人員也可能因不想誠實付費或想從中獲利，而私自更改資料，因此對於使用者的認證是不可或缺的。

二、基地端認證：基地端有可能是由有心人士所惡意假扮的，為了防止這樣的情形發生，於是對於基地端也需要認證。

2.2.3 GSM 認證機制

在介紹 GSM[11]之前，列舉了在 GSM 常見的符號並做大略的說明。每一個使用者都有屬於自己的私有金匙（secret key）和唯一的身份（International Mobile Subscriber Identity，IMSI），其為註冊初期由母系統(HLR)的認證中心（Authentication Center）所發給，藉此證明此為合法用戶。

表 2 GSM 符號說明

符號	說明
HLR	Home Location Register
VLR	Visited Location Register
MS	Mobile Station
IMSI	MS 的身份識別碼，由 HLR 的認證中心發給，證明這是合法的使用者
K_i	MS 和 HLR 共享的 secret key
K_c	此次通訊的通訊金匙(session key)
RAND	隨機亂數，challenge/response 中的 challenge
SRES	challenge/response 中的 response
TMSI	VLR 分配給 MS 的暫時身份識別碼
A3	用來產生 HLR 的回應
A5	產生加解密函數
A8	產生 session key

GSM 認證的過程詳述如下：

(1) MS 將個人的 IMSI 傳給 VLR，要求 VLR 提供通訊服務。

(2) VLR 轉送給 MS 的 HLR，獲取相關的資料，以確定是否為合法之使用者。

(3) HLR 依據 K_i，產生一個亂數 RAND，利用 A3 演算法得到預期中的回應(response)，SRES。然後以 A8 得到 session key。K_c，將（RAND，SRES，K_c）回傳給 VLR。

(4) VLR 利用 RAND 當成一個挑戰(challenge)，要求 MS 送回正確的 SRES。

(5) MS 同樣根據 RAND、K_i，產生 SRES，並計算出通訊金匙 K_c，然後將 SRES 傳給 VLR。

(6) VLR 比對 SRES，若無誤，VLR 將挑選一個 TMSI 當成暫時 MS 的身份，並以 K_c 加密，回傳給 MS。

(7) 使用者利用 Kc 解開得到 TMSI，並且回傳 ACK 至 VLR 完成整個過程。

完整的 GSM 認證流程如圖 9 所示。

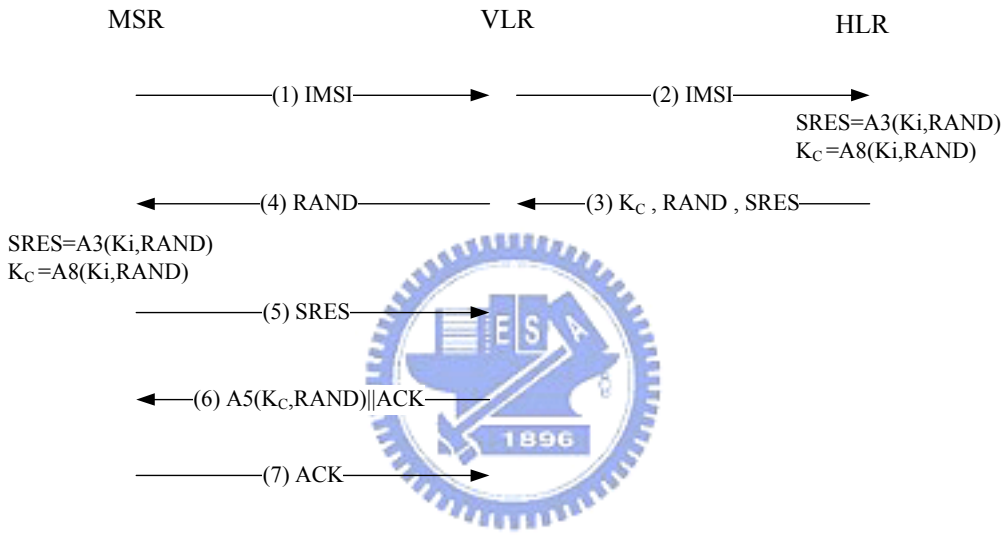

圖 9 GSM 認證機制

以上是 GSM 的認證過程，綜合以上所述，發現 GSM 的認證在安全性上較為不足之處共有以下幾點：

- ✓ 未經任何加密動作直接將 IMSI 傳給 VLR，違反了使用者匿名的原則。
- ✓ 未達成 MS、VLR 和 HLR 之間的相互認證。
- ✓ K_C 未經加密即在網路上傳送。
- ✓ 資料隱密性不夠完整。
- ✓ 記錄 RAND 和 SRES，日後可利用重送攻擊，騙取使用者信任，並破解 K_C 以竊取資料。

✓ 傳遞整組的(RAND、K_C、RES)給 VLR，由於 VLR 已知使用者的 IMSI，於是有機會可冒充使用者。

由於以上幾個攻擊點，因此認為使用者機密資料必需先經過加密才能在網路上傳送，並且不宜給 VLR 過多的資料。加強對 VLR 的身份認證，保證 VLR 和 HLR 之間連線的可用性，因為 GSM 認證必須借助於 HLR。

2.2.4 IS-95 CDMA 認證機制

CDMA 是成長最快的數位無線技術，在 1997 到 1998 這一年之中成長了三倍，並且約有五十多國使用 CDMA 標準，在此，以美國的 CDMA 標準，IS-95 為例。在認證的過程中，是憑藉著 MS、VLR 和 HLR 之間的 SSD(secret shared data)， 利用 SSD 產生一個亂數 RAND。MS 和 HLR 共同擁有一把私密金匙(A-Key)，A-Key 儲存於 MS 的記憶體中，並且只有 MS 和 HLR 持有這把 key。IS-95 中所有認證過程皆是利用 CAVE 函數所完成[18]。

表 3 IS-95 符號說明

符號	說明
MS	Mobile Station
HLR	Home Location Register
VLR	Visited Location Register
SSD、XSSD	Shared Secret Data
A-Key	MS 和 HLR 共享的 Secret Key
CAVE	Cellular Authentication and Voice Encryption，產生認證參數的函數(非公開)
R1、R2	隨機亂數，challenge/response 中的 challenge
XSSD、XAUT	challenge/response 中的 response
SSD、AUT	Authenticator，用以認證的參數

SSD 更新過程詳述如下：

(1) HLR 產生亂數 R1，利用 CAVE 函數求出新 SSD，傳給 MS 亂數 R1。

(2) MS 在收到 R1 之後，同樣以 A-key、R1 輸入 CAVE 函數，求得新 SSD，

XSSD。之後 MS 傳給 HLR 自己挑選的亂數 R2，利用 R2 和 XSSD 輸入 CAVE 計算 AUT。

(3) 以 R2 和 HLR 的新 SSD 輸入 CAVE 求出 XAUT，將回應 XAUT 傳回給 MS。

最後，MS 比對 AUT 和 XAUT，若正確，將傳送 ACK 訊息給 VLR，表示 SSD 更新和 MS 對 HLR 的認證完成。

IS-95 SSD 更新的過程如圖 10 所示：

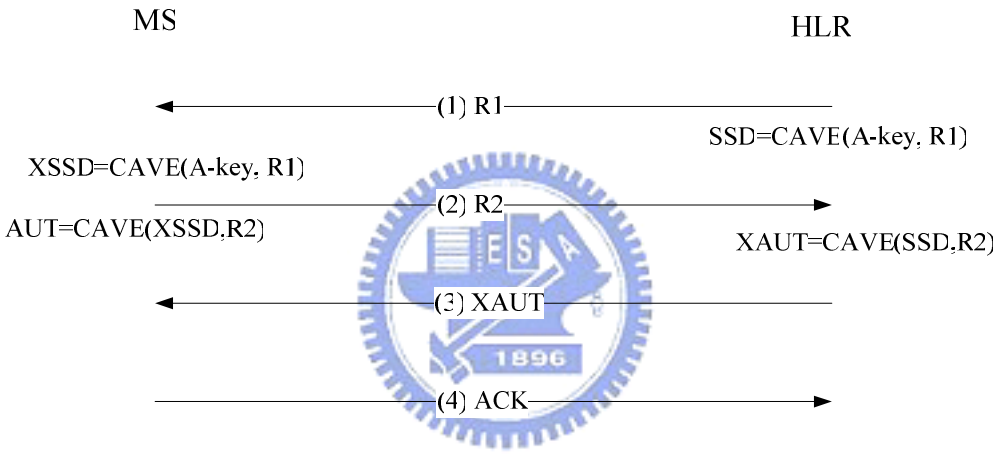

圖 10 IS-95 認證機制

當使用者漫遊到客系統時，程序詳述如下：

(1.) VLR 必須先從 HLR 得到認證所需的 SSD，再以 Challenge-Response 來驗證使用者。

(2.) VLR 產生一個亂數 R1，並算出對應的 AUT，將 RAND 傳給 MS。

(3.) MS 收到 RAND 後，計算出 XAUT，以回應 VLR 的挑戰，並回傳 XAUT 給 VLR。

(4.) VLR 核對 XAUT 和 AUT，若符合，傳送 ACK 給 MS，完成使用者認證。

流程圖如所示：

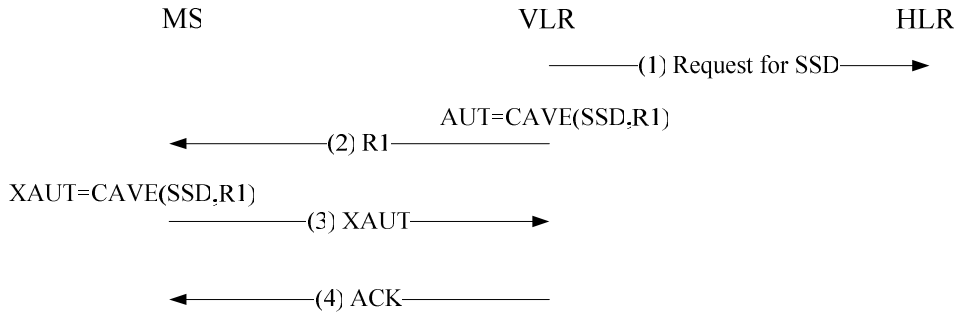

圖 11　IS-95 漫遊認證機制

經過分析之後，發現在主系統的服務範圍之內，MS 和 HLR 之間可達相互認證，並且不需經過大量運算，都是使用 CAVE 函數，並無將大量認證過程中所需的資料在網路上傳送。當漫遊到客系統時，由於 VLR 未持有 MS 的金匙，還需 HLR 的協助。在 SSD 從 HLR 傳送至 VLR 的過程中，應格外注意 SSD 的隱密性，避免被竊取。此外，在 IS-95 中皆是假設 VLR 是可信任的，未加以驗證 VLR。當 VLR 記錄下 SSD 之後，下次若再進行認證的過程時，便有機會騙取使用者的信任。因此，必需加強 VLR 的身份認證。相較於 GSM，IS-95 多了 HLR 認證和訊息私密性，但是未提供使用者匿名功能[5]。

2.2.5 UMTS 認證機制

本節將介紹第三代行動通訊[14]的 AKA (Authentication and Key Agreement) 機制，提供了資料的隱密性和相互認證。它可在 UMSI (UMTS SIM)和 HLR 之間建立 cipher key ，AKA 協定是使用對稱式密碼系統，並且 secret key 只有 UMSI 和 HLR 共享。

表 4 UMTS 符號說明

符號	說明
MS	Mobile Station
RAND	Random Number Challenge
AUTN	Authentication Token， AUTN =(SQN⊕AK ‖ AMF ‖ MAC)
XRES	Expected Response
CK	Cipher Key
IK	Integrity Key
AK	Anonymity Key
AMF	Authentication Management Field
AV	Authentication Vector，AV=(RAND ‖ XRES ‖ CK ‖ IK ‖ AUTN)
SQN	Sequence Number

認證的流程詳述如下：

(1) 收到從 VLR 送過來的連線請求之後，HLR 將回傳大小為 n 個 AV，並且排序過的陣列給 VLR。此 AV 是依據 SQN 排序。

(2) AV 包含有 RAND、XRES、CK、IK 和 AUTN，當 VLR 要初始化個認證和交換金匙協定時，VLR 從陣列中挑選出一個 AV (Authentication Vector)，並且傳送其中的 RAND 和 AUTN 給 MS(mobile Station)。

(3) 當 MS 收到 RAND 和 AUTN 時，MS 執行以下幾個運算：

- ✓ $AK=f_{5k}(RAND)$。
- ✓ $SQN=(SQN⊕AK) ⊕AK$。
- ✓ $XMAC=f_{1k}(SQN ‖ RAND ‖ AMF)$。
- ✓ 確認 XMAC 和 AUTN 中的 MAC 是否相同，並且確認 SQN 是否在正確範圍之內。
- ✓ $RES=f_{2k}(RAND)$ $CK=f_{3k}(RAND)$ $IK=f_{4k}(RAND)$。

(4) 最後，UMSI (MS)產生一個回應的 RES，並傳給 VLR，VLR 比對所收

到的 RES 和 XRES，若相同，則 VLR 認為此次的 AKA 協定已成功地完成。

UMTS 認證流程圖如下：

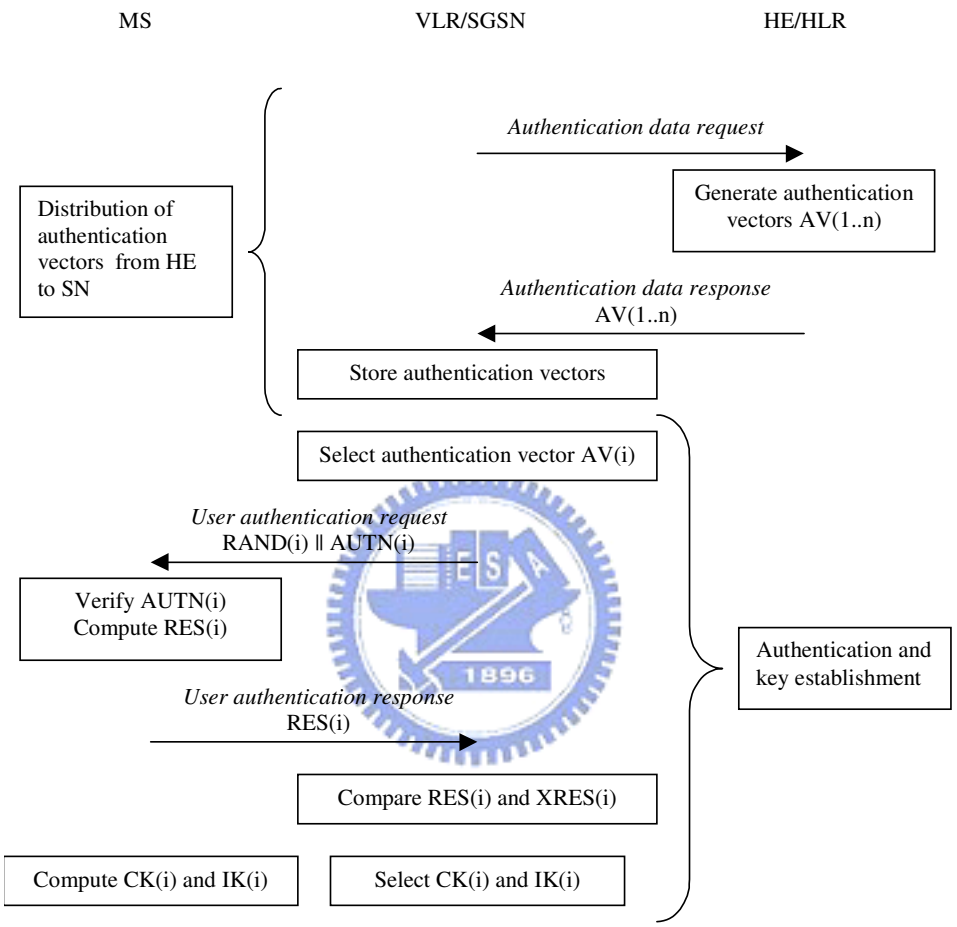

圖 12 UMTS 認證流程圖[2]

根據以上的分析，可得知 UMTS AKA 機制在安全上不足的地方：

- ✓ Challenge-Response Vectors 是未經加密就藉由網路來認證 MS 的身份。
- ✓ Authentication Vector 含有太多關於驗證使用者所需要的資訊，尤於 VLR 也知道使用者的真實身份，會導致 VLR 偽裝成使用者的風險。
- ✓ 假設所有的 VLR 都是可信任的。

✓ 資料的隱密性並不夠完整。

因此，UMTS 的安全性仍然有改進的空間，可藉由數位簽章的方式，達成三方之間的相互認證。並利用非對稱加解密系統，以提高資料的安全性，並達到不可否認性。

綜合上述三種認證機制，將其可能遭受之攻擊與缺點整理如下表：

表 5 現行認證機制比較表

	GSM	IS-95	UMTS
相互認證	N	*N/Y	Y
認證資料隱密性	N	N	N
使用者匿名	N	Y	N
HLR 認證 VLR	N	N	N
VLR 不宜掌握過多資料	N	N	N
預防重送攻擊	N	N	N

*依據情況能否防止攻擊。

2.3 衛星通訊認證

關於使用者認證協定，Hwang et al.[13]提出一個專為衛星環境設計的架構。此系統元件有衛星、使用者、閘道和網路控制中心(Network Control Center)，如下圖所示：

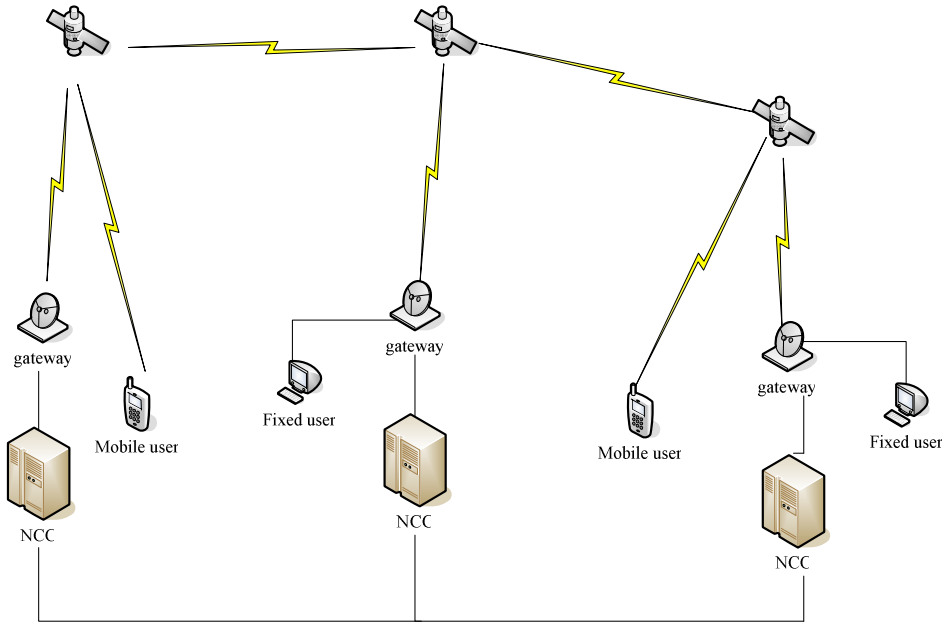

圖 13 Hwang et al. 衛星通訊架構

Mobile User 完成註冊之後即可直接和衛星進行通訊不需再經過 Gateway 的轉送。Gateway 的主要功能在於服務地面有線的使用者，由於有線的使用者無法直接和衛星連線，因此需藉由 Gateway 的協助將資料送出。此外，還連結當地的電信業者，創造出更多元化的服務。地面控制站(以下簡稱 NCC)，所擔任的工作是負責使用者的認證、註冊服務和衛星的監控。

在此協定中，分成為兩個階段：行動使用者註冊和使用者認證階段，並且在每次的通訊之中都將會自動產生一把新的 session-key 已供加密之用。

一、註冊階段

在使用衛星通訊系統服務之前，使用者必需先和向 Gateway 註冊一個帳號，如圖 14 所示，使用者將可得到一個永久的 U_{ID}，一個暫時的 T_{ID}，NCC 和 user 之間所共同持有的 secret key K_{md}，接著 gateway 將(U_{ID}，T_{ID}， K_{md})和使用者所屬衛星的 ID 一同傳到送 NCC，以做為日後認證之用，茲將符號說明如下表：

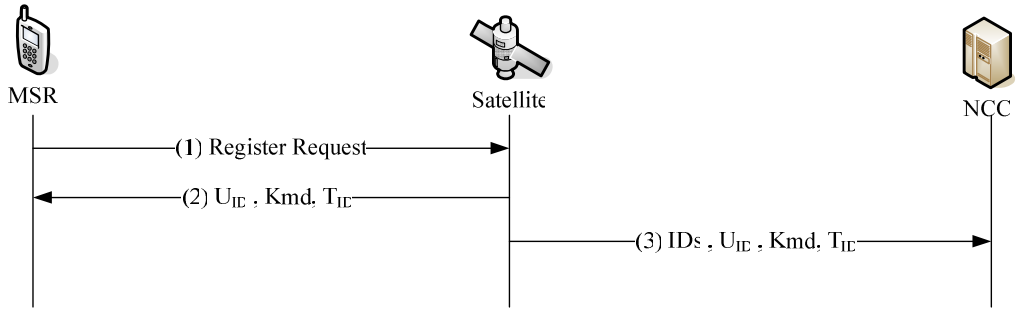

圖 14 註冊階段程序

表 6 Hwangs'Scheme 符號說明

符號	說明
U_{ID}	使用者永久不變的 ID
T_{ID}	使用者在系統中暫時的 ID
K_{md}	由使用者和 NCC 所共用持有的 secret key
ID_S	衛星的識別碼

二、認證階段

當使用者想和其他使用者進行通訊之前需先經過系統的認證，一個使用者的認證協定如圖 15 下所示：

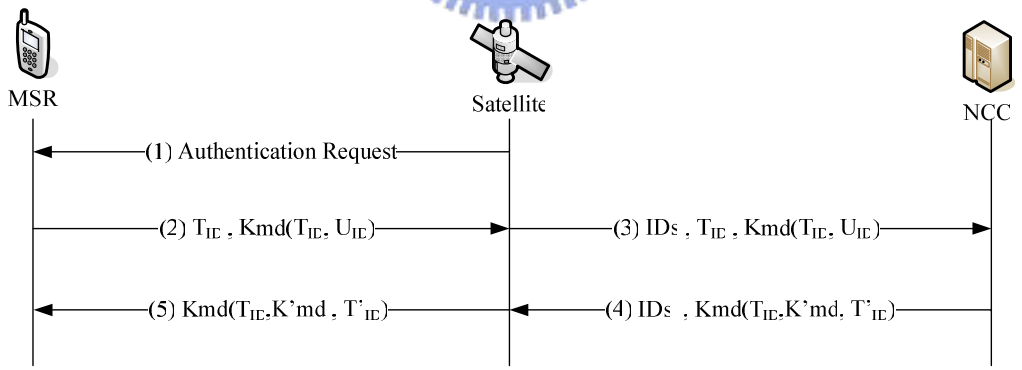

圖 15 認證階段程序

詳細資料流程說明如下：

(1) 由衛星送出認證請求到使用者，要求提供認證所需的相關資料。

(2) 當使用者收到認證請求後，使用者送出 T_{ID}，並以 shared key K_{md} 將(U_{ID},

T_{ID})加密送出。

(3) 衛星收到由使用者所送出之認證資料後，隨即將 ID_S 附加於資料後，送到 NCC。

(4) NCC 收到之後，先由使用者 T_{ID} 得到共用的私密金匙，將使用者所加密的資料解密，得到 T_{ID}，並和未加密的 T_{ID} 比對，若相同則代表使用者通過認證。NCC 產生一把新的 K'_{md} 和一個新的 T'_{ID}，再以舊的私密金匙加密(T_{ID}，T'_{ID}，K'_{md})，將資料送回。

(5) 衛星收到 NCC 所傳送的資料，將資料內衛星的 ID 去除，再回傳到使用者。

使用者利用舊 K_{md} 將 NCC 所傳送過來的資料解密，核對其中的 T_{ID}，若和原來的相同則使用者對 NCC 的認證成功，並更新 K_{md} 和新的 T_{ID}。

探討過前幾節現行的的認證系統之後，將其特性整理如下。

表 7 各項認證協定比較表

	GSM	IS-95	UMTS	Hwang et al. Scheme
密碼系統	對稱式	對稱式	對稱式	對稱式
訊息私密性	是	是	是	是
使用者認證	是	是	是	是
系統端認證	否	是	否	是
安全性	低	高	中	中
運算負擔	低	中	高	低
適用於衛星	否	否	否	是

第三章　針對衛星通訊的認證機制

3.1 問題定義

由於訊號是在公共且不安全的環境下傳送，於是訊號的安全會是本研究的重要議題。在傳送之前，必定加上加密的步驟。並且根據所收集到的資料都說明了衛星主要的功能在於訊號的傳播，是個訊號的中繼站。然而除了接到從使用者端所發送之信號外，還需判斷將訊號傳送到某一顆衛星，當成訊號的下一站中繼點，衛星並不具備強大的運算能力。因此，衛星通訊系統在使用者認證過程中所需要資料運算部份就落在收、發端和網路控制中心上。綜合相關文獻，將設計認證協定所需注意的特性整理如下：

- ✓ 延遲時間較長，容易遺失封包。
- ✓ 衛星本身不具備有強大運算能力。
- ✓ 由於低軌衛星是繞著地運轉，必定會 HAND-OFF 情形。
- ✓ 傳送使用者資料於空氣中，資料有被截取之虞。

3.2 解決方法

衛星本身先天上就具有上述特性，因此針對這些特點找出解決的辦法，茲說明如下：

一、目前有關於衛星上使用 TCP/IP 協定的相關文獻，會因為延遲而導致網路效能低落，封包遺失。即使是改良式的 TCP/IP 協定，雖有改善效能，但延遲和封包遺失的問題還在。為了解決因延遲或封包遺失而造成認證失敗，必須設定有效時間的門檻值。若在此時間內未收到回應，即認為封包遺失，重新

送出認證請求。而外在環境也可能使延遲時間更常，形成假性封包遺失的情形。因傳送端重傳的結果，造成接收端重覆收到封包。因此，需在訊息內加入時間戳記(time stamp)和隨機號碼(RAND nonce)，以區別先後先順序。

二、因為衛星和行動通訊設備不具有強大運算能力，於是傳接雙方和 NCC 需負責認證過程中資料核對和運算，並且在訊號傳送過程中加解密運算也是由傳接使用者和 NCC 來執行。受限於硬體技術，目前行動裝置所具有的運算能力也還不足以和一般電腦相抗衡，因此在設計協定的過程需達到理想的安全程度，另外運算能力的需求也以不佔用行動裝置太多系統資源為佳。

三、相同於 GSM 行動通訊系統，當發生 HAND-OFF 現象時，就像是在 GSM 環境下會有突然訊號接收不良的情況，甚至是斷線，將造成使用者或 NCC 因太久未收到回應而認證失敗。為補強此缺點，在認證的資料中，需加上足以識別是屬於不同次認證的資訊，例如隨機號碼、TIME-STAMP。並加強 NCC 之間傳送用戶換手資料的能力，快速完成換手程序。

四、若是資料未經保護就直接傳送，只需截取所傳送出來的訊號，即可得到關於使用者的相關資訊。為避免發生，所提出的機制將會於資料送出之前先進行加密，其中所使用的金匙在認證之後會產生。此外，為了提高安全性，每次所用之 session key 皆不相同。

基於上述幾點的條件之下，認證部份主要分成兩個面向，一是使用者端上線認證，衛星通訊屬於安全性需求較高的系統，所以需嚴格限定有權限的使用者上線權限。另一部份則是終端使用者之間的相互認證，清楚了解目前正在對話的另一方，以防重要資料被盜取。

3.3 系統架構與目標

3.3.1 系統架構

就身份認證而言，本研究主要提供端點對端點的使用者間雙向相互認證、行動用戶對 NCC 間雙向的相互認證，及固定用戶與地面接收站間雙向的相互認證。圖 16 為本研究所採用的認證系統架構，在此架構中，最上方為一認證伺服器，其主要功用在於促成 NCC 之間的相互認證。NCC 之下再獨自管理個自的用戶，NCC 和使用者持有秘密分享金匙(shared secret key)，可達成相互認證。

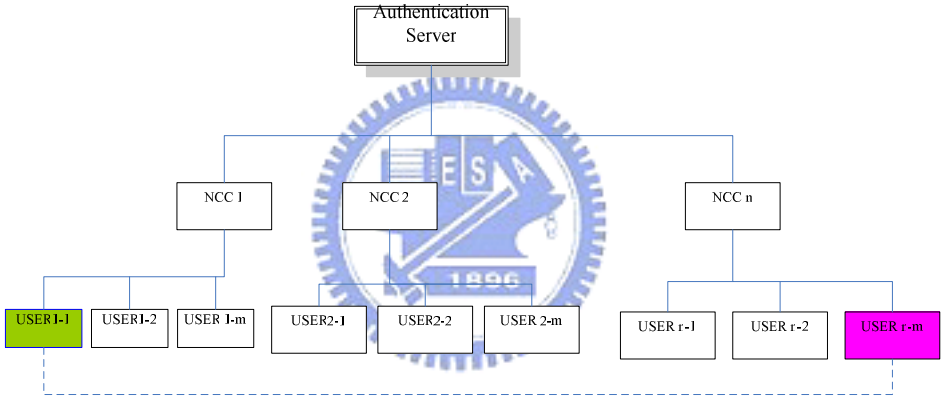

圖 16 衛星通訊認證系統架構

3.3.2 系統目標

於衛星通訊身份認證之設計必需滿足下列的要求：

1. Privacy of Communication Setup Information

在通訊建立之初，使用者會將與衛星通訊系統進行認證所需要的資料進行交換，例如使用者的身份、產生 session key 所需的資料，或是所要求的服務類型，這些資訊必須在絕對安全的前提下傳送，這項也是 GSM 協定最缺乏的。若以明文傳送，即可輕易得到使用者的重要資料，甚至是冒名和另一方進行

通訊。

2. Privacy of Speech

通訊雙方的通話內容必需先經過加密之後才能傳送到系統中。

3. Privacy of Data

雙方所進行的資料交換必需經過加密，以確保不被修改。

4. Privacy of User Location

當使用者在進行通訊時，使用者所在的位置必需保密，最常見的做法就是將使用者的 ID 加密。此外使用者的位置會被記錄在資料庫中，所以必須確保這些資料庫的安全，以避免被未經過授權的存取、破壞。

5. Privacy of User ID

當使用者在進行通訊時，使用者所在的真實身份必須保密。通常的做法都是當使用者欲進行認證時，其所使用的 TID 並不是系統內的固定 TID，而是產生以用於此次通訊所需，最安全的機制是每經過一次認證之後，就必需改變其認證所需的 TID。

6. Integrity of Data

於訊息之後加上 HMAC，若是訊息經過修改，可以訊速辨別。

3.4 認證機制

為方便介紹本研究所提的機制，茲表 8 就身份認證協定所需使用的符號作說明：

表 8 系統符號說明

符號	說明
IMSI	使用者的永久識別碼
TID	此次通訊所使用之暫時 ID
TID'	更新之後的 TID
IDs	衛星的 ID
SN	Subscriber Number(用以辨識另一通話端)
K1	user 和 NCC 之間共有的 secret key
K2	user 之 public key
K3	user 之 private key
K_{NCC}	NCC 間共有的 secret key，由認證伺服器所產生
X	g^a mod p(DH 演算法元素)
Y	g^b mod p(DH 演算法元素)
RADN	隨機變數，用於認證和辨識不同訊息
RAND'	RAND+1，認證過程中使用

本研究所提出的認證流程分為三個階段分別是：使用者註冊階段、認證與金匙更新階段及終端使用者之相互認證階段，其中認證階段又分為本地端和漫遊兩種模式。完成註冊後，此使用者即可成為系統用戶。每次上線時需再經過認證的程序才能真正使用系統。最後在和另一方通話時，系統會自動產生 session key 和完成用戶間的相互認證。

3.4.1 註冊階段

當不屬於衛星通訊系統的用戶欲使用這項服務之前，需要先和提供本系統服務之 NCC 取得合法的使用權。此為註冊階段，系統的流程如圖 17 所示。經過註冊之後，使用者會持有：

- ✓ 使用者和 NCC 所共用持有的 secret key，K_1，做為日後使用者和 NCC 之間傳遞資料時加解密之用。
- ✓ 非對稱式密碼系統中的 private key，K_3。
- ✓ 一個暫時性的 TID，其目的是為了避免在通訊過程中洩露行動用戶的位置，

以保障其通訊隱私，在通訊的過程中並不直接傳送用戶 IMSI，取而代之的則是 TID。。

NCC 將會持有：

- ✓ 註冊使用者的 IMSI 及 TID。
- ✓ 使用者和 NCC 所共同持有的 secret key，K_1。
- ✓ 非對稱密碼系統中使用者的 public key，K_2。
- ✓ 其他一些使用者的相關資訊。

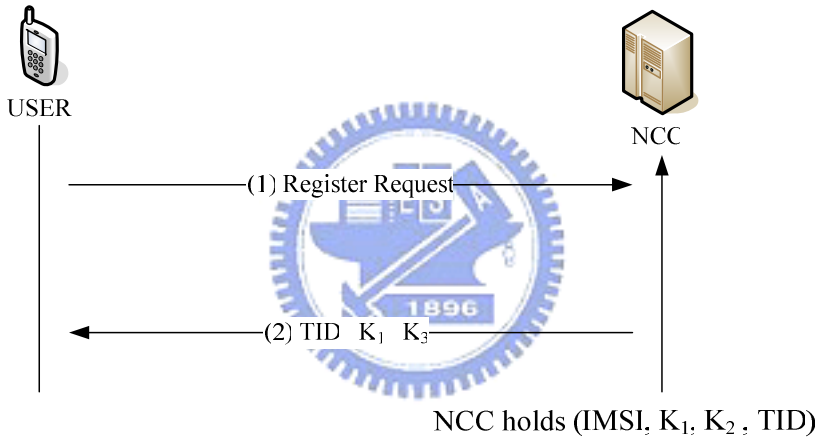

圖 17 使用者註冊階段

3.4.2 本地端使用者認證階段與金匙更新階段

註冊之後，在使用衛星通訊連線服務前，需再經過認證。所需資料傳送到 NCC，經過 NCC 確認無誤之後，方可使用系統服務。設計方向朝著提供最大的安全性，考量效能問題，且加入同步更新的功能。在此將使用者分成兩大類：一種為本地端的使用者，另一種為漫遊的使用者。先介紹第一種的身份認證方式，另外於身份認證完成之後，立即執行金匙更新，作為此次通訊所需之會議金匙。圖 18 為整個協定過程：

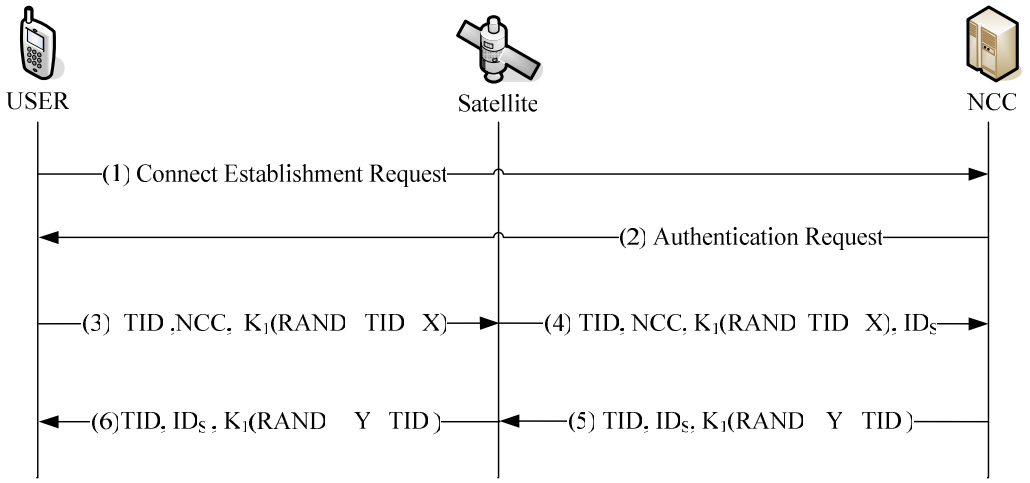

圖 18 本地端使用者認證與金匙更新階段

(1)使用者送出建立連線請求至 NCC 端。

(2)NCC 送出認證請求給使用者。

(3) 使用者端送 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 及將 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 以具有訊息認證碼(Message Authentication Code, MAC)的單向雜湊函數(One-way Hash Function)處理之，即 $HMAC\{TID, NCC, \{RAND \| TID \| X\}_{K_1}\}_{K_1}$，並將上述兩個訊息送至衛星。其中 RAND 代表隨機亂碼，其目的是為防止重送攻擊(Replay Attack)；由於 $\{RAND \| TID \| X\}$ 是用使用者與 NCC 預先分享的金匙 K_1 加密，故僅有雙方可將訊息解開；另外，在身份認證過程，亦藉著 DH 金匙交換協定，完成會議金匙的產生，而為了防止因使用 DH 協定所產生的中間人攻擊法，將 X 包在加密的訊息，而非以明文的方式傳遞。另外，藉由 HMAC 的使用，使得可確保整串訊息 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 在傳遞過程未被修改，以達完整性之目的。

(4)待衛星接收此訊息後，它將訊息不做任何修改，另外加入自己的 ID_S，送至 NCC 端。

(5)待 NCC 收到此訊息後，確認衛星、使用者之 ID 後，先藉由 HMAC 的計算，以確定在傳遞的過程資訊是否遭受修改。若遭受修改，則丟棄此訊息。否則，將訊息以與使用者共同分享的金匙 K_1 解開，以取得 RAND

及 X。其中，RAND 要儲存以防止攻擊者實施重送攻擊，而 X 要使用 DH 協定以產生此次通訊所需之會議金匙。同理，NCC 會計算 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 及使用 HMAC 將 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 處理之，即 $HMAC\{TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}\}_{K_1}$。其中 RAND 加 1 的目的，為防止重送攻擊，並讓使用者確認是由 NCC 送來此次通訊的訊息，且內含使用者下次通訊所需使用的 TID'。另外，Y 亦是作為 DH 協定所需的參數，同理，為了防止因使用 DH 協定所產生的中間人攻擊法，將 Y 包在加密的訊息，而非以明文的方式傳遞。另外，藉由 HMAC 的使用，使得可確保整串訊息 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 在傳遞過程未被修改，以達完整性之目的。

(6)待衛星接收此訊息後，它將訊息不做任何修改，送至使用者端。

使用者收到此訊息後，確認衛星之 ID 後，先藉由 HMAC 的計算，以確定在傳遞的過程資訊是否遭受修改。若遭受修改，則丟棄此訊息。否則，將訊息以與 NCC 共同分享的金匙 K_1 解開，以取得 RAND'及 Y。其中，使用者可藉由 RAND' 以確認是否重送攻擊，若為重送攻擊則不以予處理。此外，使用者可獲得下次通訊所需使用的 TID'。最後，使用者與 NCC 可藉由 DH 協定與收到雙方的 Y 與 X 計算出此次會議所需的會議金匙，新 $K_{MD} = Y^a \bmod p = X^b \bmod p$ 。

3.4.3 使用者漫遊身份認證機制與金匙更新

在使用者漫遊部份所提供的身份認證機制不同於本地端的身份認證機制，因為它必須藉由原先註冊的 NCC 幫忙，以達成身份認證之目的。因此，整個身份認證過程還必須考慮其他 NCC 是否為可信賴的 NCC，故要藉由認證伺服器達到雙向 NCC 之間的認證。下述為本協定內容：

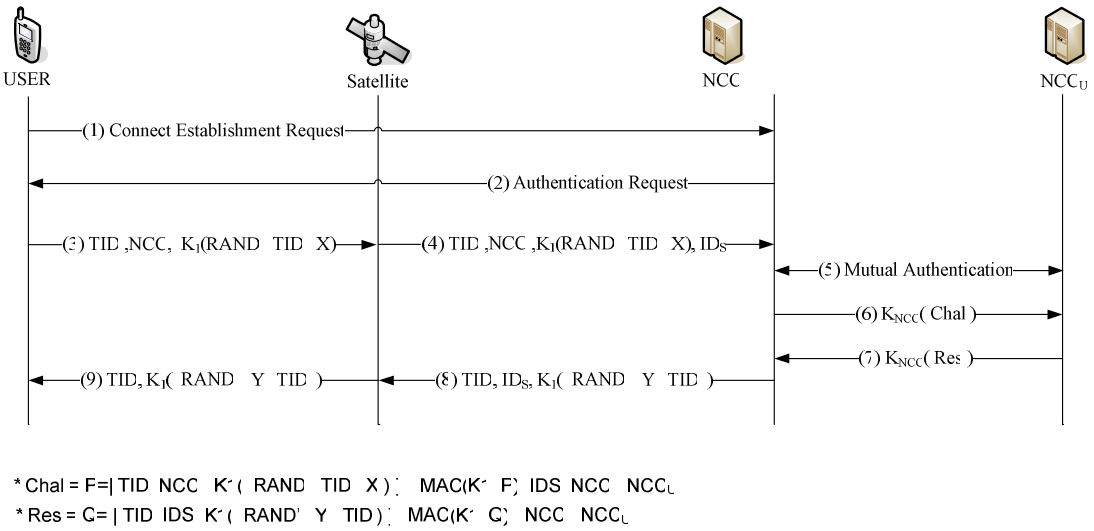

圖 19 使用者漫遊之認證與金匙更新階段

(1)使用者送出建立連線請求至 NCC 端。

(2)NCC 送出認證請求給使用者。

(3) 使用者端送 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 及將 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 以具有訊息認證碼(Message Authentication Code, MAC)的單向雜湊函數(One-way Hash Function)處理之，即 $HMAC\{TID, NCC, \{RAND \| TID \| X\}_{K_1}\}_{K_1}$，並將上述兩個訊息送至衛星。

(4)待衛星接收此訊息後，它將訊息不做任何修改，另外加入自己的 ID_S，送至 NCC 端。

(5)由於使用者漫遊端的 NCC 無使用者的註冊資訊，因此，它必須藉由原註冊的 NCC_U 協助方能完成身份認證事宜。故在此步驟，必須完成兩個 NCC 間的交互認證(Mutual Authentication)。此交互認證本研究採可信賴的第三者(Authentication Server)完成，並產生一把會議金匙 K_{NCC} 作為兩個 NCC 間使用。

(6) 待確認雙方身分後，NCC 將 NCC, NCC_U，
$\{TID, NCC, NCC_U, \{RAND \| TID \| X\}_{K_1}, HMAC\{TID, NCC, \{RAND \| TID \| X\}_{K_1}\}_{K_1}, ID_s\}_{K_{NCC}}$

送至原使用者註冊的 NCC_U 端。

(7)使用者原註冊端 NCC_U 拿到使資訊後，先用 K_{NCC} 將訊息解開，並藉由 HMAC 的計算，以確定在傳遞的過程資訊是否遭受修改。若遭受修改，則丟棄此訊息。否則，將訊息以與使用者共同分享的金匙 K_1 解開，以取得 RAND 及 X。同理，使用者原註冊端的 NCC 會計算 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 及使用 HMAC 將 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 處理之，即 $HMAC\{TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}\}_{K_1}$。最後，用 K_{NCC} 將整串訊息加密，即 $NCC, NCC_U, \{TID, NCC, NCC_U, \{RAND+1 \| TID' \| Y\}_{K_1}, HMAC\{TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}\}_{K_1}, ID_s\}_K$ 送至使用者目前漫遊的 NCC 端。

(8)待 NCC 收到後，用 K_{NCC} 將訊息解開後，將 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$ 及 $HMAC\{TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}\}_{K_1}$ 送至衛星。

(9)待衛星接收此訊息後，它將訊息不做任何修改，送至使用者端。

待使用者收到此訊息後，確認衛星之 ID 後，先藉由 HMAC 的計算，以確定在傳遞的過程資訊是否遭受修改。若遭受修改，則丟棄此訊息。否則，將訊息以與 NCC 共同分享的金匙 K_1 解開，以取得 RAND+1 及 Y。最後，使用者與原註冊地的 NCC 可藉由 DH 協定與收到雙方的 Y 與 X 計算出此次會議所需的會議金匙，$K_{MD} = Y^a \bmod p = X^b \bmod p$。

3.4.4 使用者相互認證與產生 session key

本協定需藉由第三方認證單位提供相關的使用者資料，在系統中是由 NCC 來扮演此項任務，由於在註冊完成之後，就可得到非對稱式加密系統中的 private key 和 public key。先假定 A、B 分別是發送者和接收者，A 先將自己的資料以自己的 private key 加密送出，B 收到之後再向 NCC 取得 A 的 public key 解密，證

明 A 是本人，B 也用相同方法之後 A、B 雙方即通過雙向認證。

待完成上述的身份認證後，透過此協定，讓終端使用者 USER A 與 USER B 間產生一把未來共同使用的會議金匙 K_{AB}。其步驟如下：

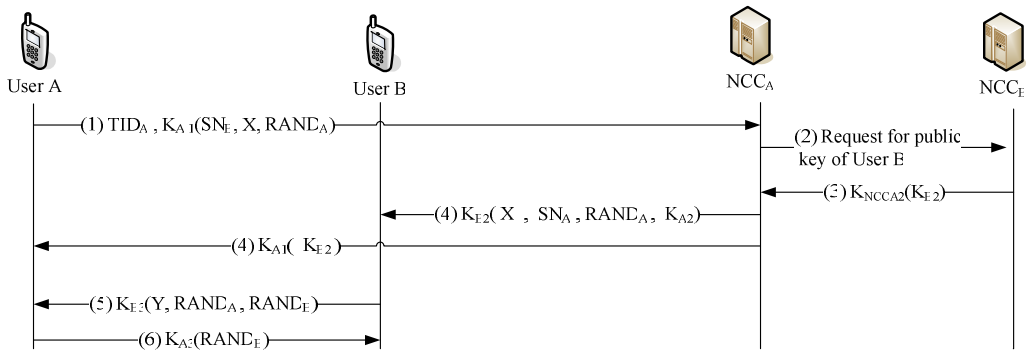

圖 20 使用者相互認證與產生 session key

(1)USER A 送 $NCC_A, TID_A, \{SN_B, X\}_{K_{A1}}, HMAC\{TID_A, \{SN_B, X\}_{K_{A1}}\}_{K_{A1}}$ 至 NCC_A。其中 K_{A1} 代表 USER A 與 NCC_A 間預先分享的金匙；而 SN_B 代表 USER B 的 subscriber number。

(2)待 NCC_A 收到後，即向 NCC_B 詢問 USER B 的公開金匙。

(3) NCC_B 回覆 USER B 的公開金匙給 NCC_A，即 $K_{NCC_{A2}}(K_{B2})$。其中 K_{B2} 代表 USER B 的公開金匙。

(4)待 NCC_A 收到後，將 $K_{A1}(K_{B2})$ 給 USER A，另外送 $K_{B2}\{X, SN_A, K_{A2}\}$ 給 USER B。

(5)待USER B收到後，它會送K_{B3}(Y, $RAND_A$, $RAND_B$)給USER A。

(6)USER A收到之後，核對$RAND_A$ 是否相符，若符合即回傳K_{A3}($RAND_B$)當成ACK用途。

USER B收到(6)送出的訊息，和步驟六進行相同動作。USER A與USER B各自藉由DH協定算出此次會議所須之會議金匙 $K_{AB} = Y^a \bmod p = X^b \bmod p = K_{BA}$。

另於本研究所設計的協定中，使用者所使用的身份都不是其真正的身份，因為達到了使用者的匿名性，更由於衛星所需的 RRT(round trip time)比陸地上的無線通訊系統更來得長，所以需在認證所需的資料內加上 random nonce 以防止重送攻擊，更由於每次的資料傳送或是對話，其內容都會由 session key 所加密，更因此達到了資料的隱密性，不會被非法的使用者所截取。

第四章　系統實作

4.1 系統設計

由於無法取得衛星資源，故本論文之實驗環境為交通大學學術學網路，並設定有關於衛星通訊特性的參數，以期更能完整表現系統可能會遇到的問題。因此本系統需符合下列功能特性：

- ✓ 以亂數產生封包遺失的情況。
- ✓ 模擬衛星延遲時間。
- ✓ 當使用者移動到其他衛星範圍內，需有快速換手(hand-off)的能力。
- ✓ 需有能力判斷何時重送資料，與辨別資料新舊的能力。

4.2 系統架構

本系統架構如圖 21 所示，提供一個使用者介面以利使用者和系統溝通之用。在系統核心內部有一解析引擎，在系統運作的過程中，解析引擎需先取得使用者和 NCC 相關的資料，如所在區域和加解密金匙。此後使用加解密演算法和系統訊息格式，取得由外部接收到的訊息內容，或是產生欲傳送出去的資料。此外還提供系統設定檔和例外處理程序其他功能，增加了系統運作的彈性。

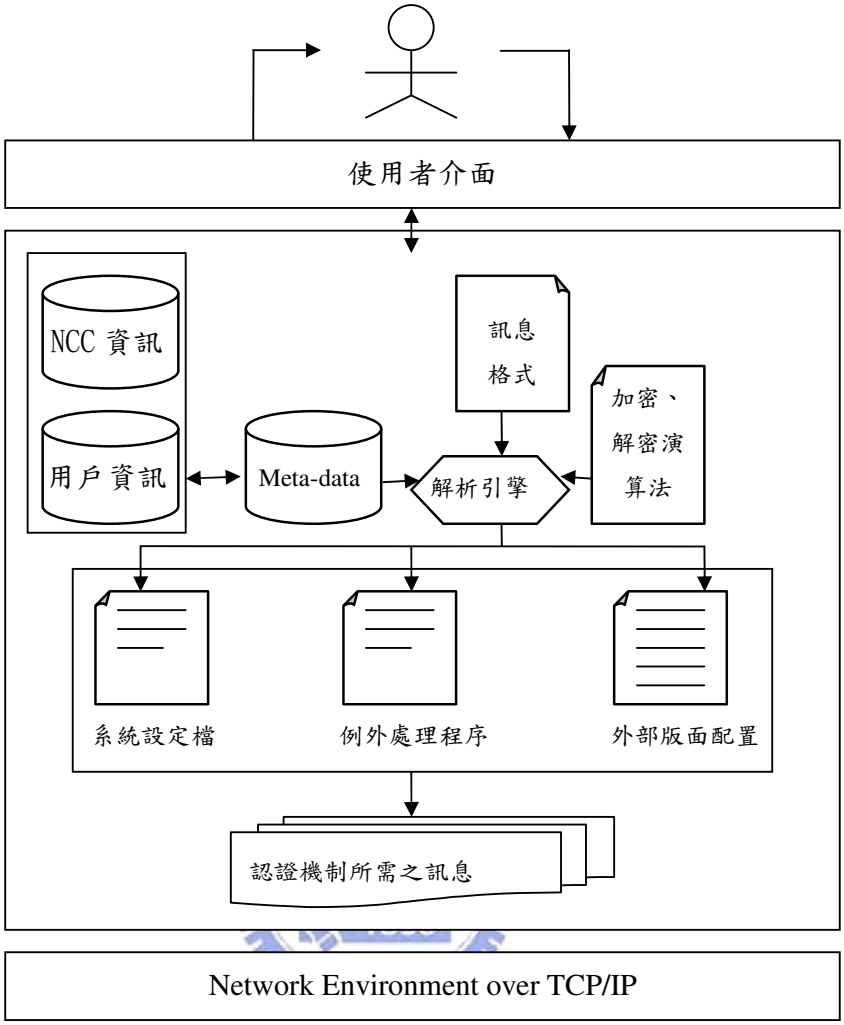

圖 21 系統架構圖

4.3 系統實作環境介紹

首先，在介紹所使用之軟、硬體設備之前，需先定義本論文模擬的環境。在衛星通訊系統下的使用者可分成 Mobile user 和 Fixed user。前者其傳送訊息流程如圖 22 所示：

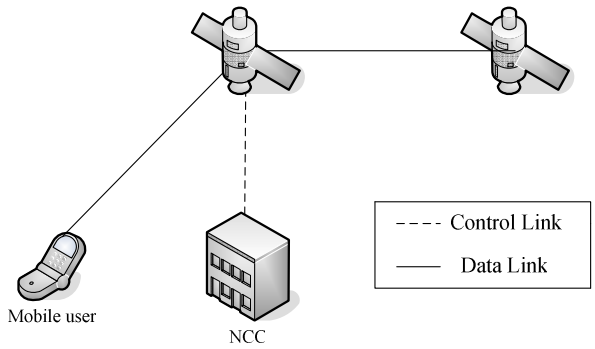

圖 22 Mobile User

如圖 23 所示資料直接由 Mobile user 送至衛星，經由衛星轉送到其他區域，NCC 在此為控制衛星是否幫使用者傳送資料的角色。後者為之訊息流程如下，Fixed user 因為不具備直接和衛星連線的功能，因此需藉由 NCC 所提供的閘道將資料傳送到衛星。

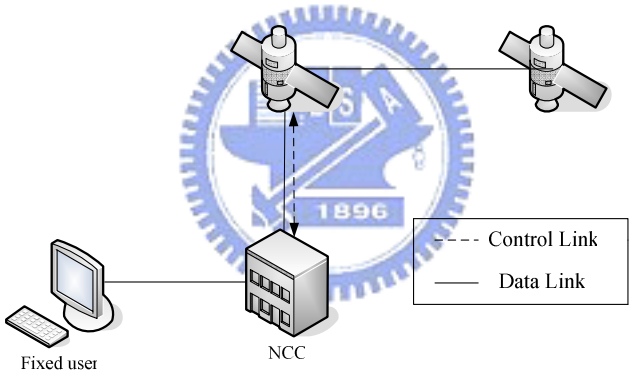

圖 23 Fixed User

在本實驗是採用 Mobile user 的模式，此兩種模式的差異只在於先傳至 NCC 或是直接傳送到衛星，並不影響本研究的安全性。因此，為了模擬衛星通訊的運作模式，在實作方面需六部電腦，詳細規格與所模擬的角色介紹如下表：

一、硬體環境：

表 9 系統硬體需求

	角色	CPU	RAM	功能
1	使用者_A	P3-933	128MB	傳送端
2	NCC_A	AMD 2.5G	1GMB	傳送端 NCC
3	衛星_A	P4-2.4	512MB	轉送資料
4	使用者_B	P3-933	128MB	接收端
5	NCC_B	K8-3G	1GMB	接收端 NCC
6	衛星_B	P4-2.4	1GMB	轉送資料

二、軟體環境：

表 10 系統軟體需求

軟體類別	軟體名稱與版本
作業系統	Windows XP、 Windows SERVER 2003
資料庫	MySQL 5.0.16-nt
程式語言	Sun Microsystems – java language J2DK-1.4.2

三、加密演算法：

(1)非對稱式密碼系統：實作所使用的加密系統為橢圓曲線(elliptic curve cryptosystem, ECC)。使用 192bits 金匙長度的 ECC 其安全性強度和使用 1024bits 之 AES 相同，適合用於記憶體不多的行動通訊設備。

(2)對稱式密碼系統：實作上使用 AES 為對本系統對稱式加密系統。AES 其版本有 AES-128、AES-192 和 AES-256，已取代 DES 成為美國加密標準系統，不需大量運算資源，並加強了加密系統的強度。

(3)DH(Diffie-Hellman)演算法：使用 DH 演算法時，產生加密金匙需和系統中對稱與非對稱加密演算法所使用之加密金匙長度相符(AES：128，192 或 256bits)。

(4)HMC：HMAC 主要用於保持資料的完整性，其演算法是為單向的雜湊函數。HMAC 所使用的演算法為 MD5 是 MD4 的更安全的版本，同時速度更快，產生 128 位元的摘要值，不會造成太高的額外的負擔，尤其適用於頻寬資源珍貴的衛星通訊上面。

四、模擬假設：

根據 Bo Ryu[6]所提出之衛星環境模擬方法，可以從以下幾點分析：

- ✓ RRT
- ✓ 封包遺失率
- ✓ 封包錯誤率
- ✓ 訊框大小

因此，系統實作將引入以上幾項，並以隨機亂數的機率發生。

4.4 系統運作流程

4.4.1 註冊階段

當使用者送出認證請求時，系統會將使用者的資料新增到資料庫，並送將使用者的 TID 和用戶號碼，連同日後認證和產生 session-key 所需要的金匙送回使用者。詳細的流程圖可參照圖 24。

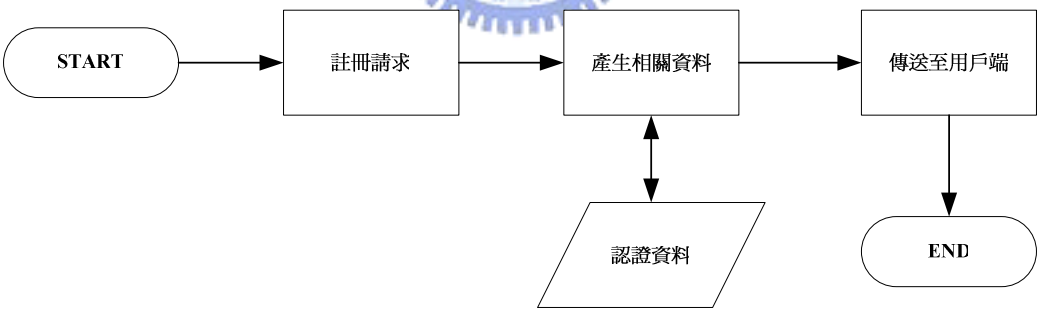

圖 24 註冊流程圖

4.4.2 認證階段

當使用者送出認證請求時，當地的 NCC 首先確認此使用者是否為其所屬之用戶。否則將這請求送到使用者所註冊的 NCC 代為處理，待另一 NCC 完成程序後，則將此用戶列為合法的使用者。若是此系統的用戶，則執行解密的動作，完成雙向認證的程序。成功認證之後，則列為合法用戶，並利用 DH 演算法更新 secret key。

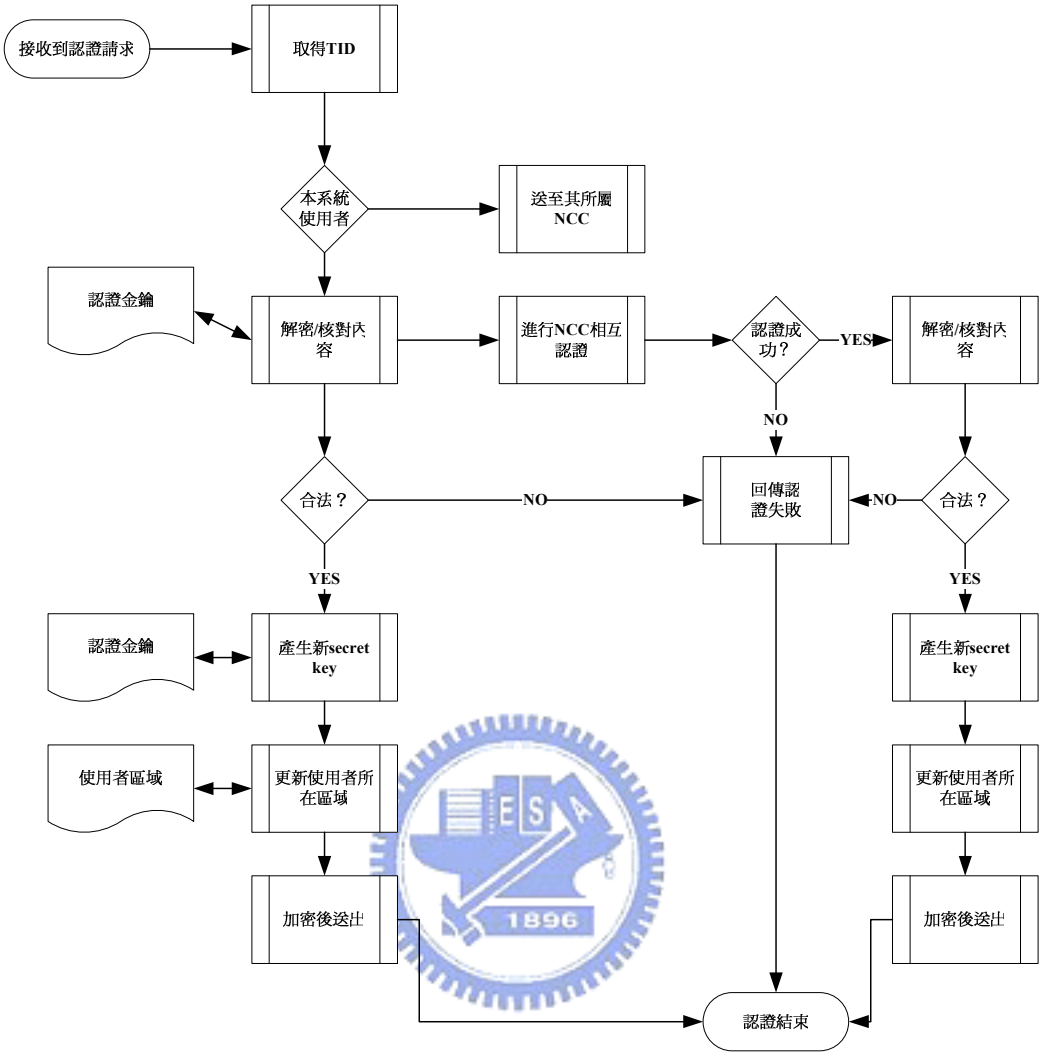

圖 25 認證流程圖

4.4.3 產生 end-to-end session key 階段

當 NCC 收到用戶發出的端對端認證請求後，先核對收話端的用戶是否為本系統的用戶，於是取出其公開金匙。若不是，則向另一 NCC 取得收話端的公開金匙。完成以後，將協定中必要的資訊以加密的方式送達兩方，完成端對端的認證和 session key 的產生。

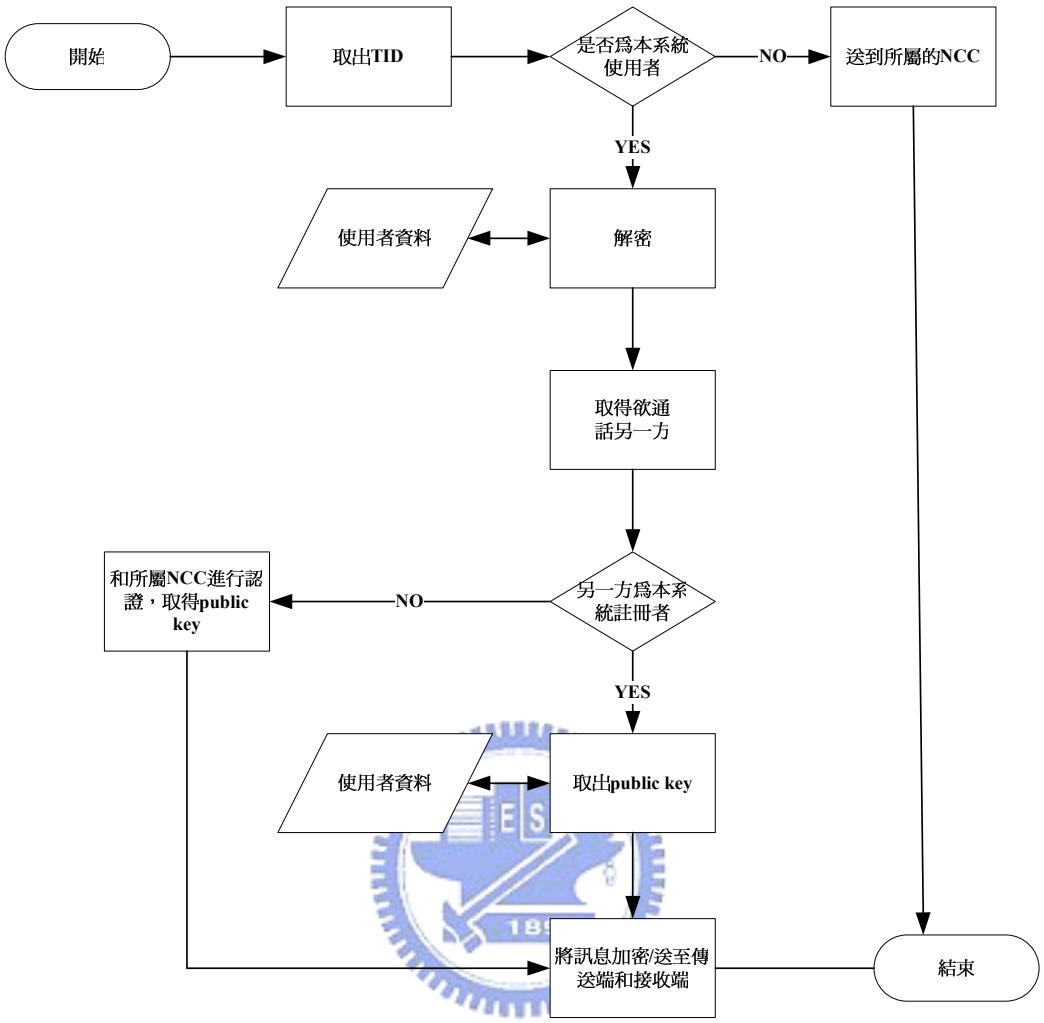

圖 26 產生 session key 流程圖

4.5 系統實際運作畫面

一、伺服器端

圖 27 為伺服器端介面，介面上可看到”location NO.”、”Server Name”、”Register User”、”Online User”和”Log File”，方便管理員監視系統的使用情況。

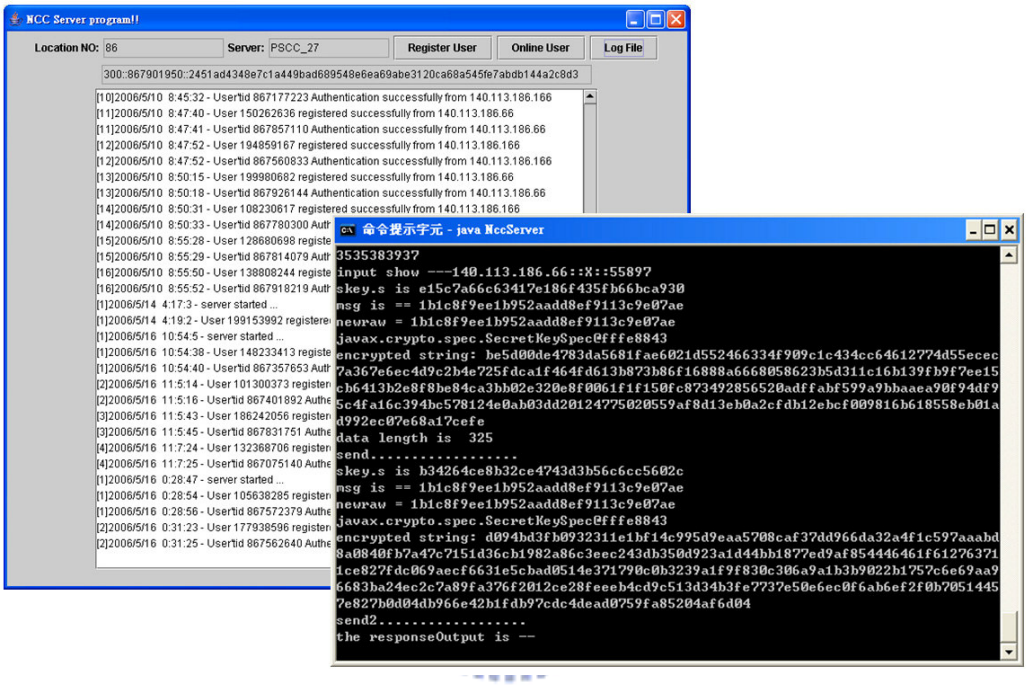

圖 27 伺服器執行畫面

二、用戶端

在畫面上選則註冊的 NCC，如圖 28，接著點選註冊之後，若資料無誤即可完成註冊程序。經過註冊之後，選取目前範圍內的 NCC。若和所註冊的 NCC 相同，則可在此 NCC 內部完成認證程序。若否，NCC 則會將請求送至原來註冊的 NCC。完成以後可看到畫面上會顯示用戶號碼和 TID。完成上述程序後，填選欲連線端的用戶號碼，按下”E2E Authentication”鍵後，和對方完成認證，並產生 session key，即可開始對談。

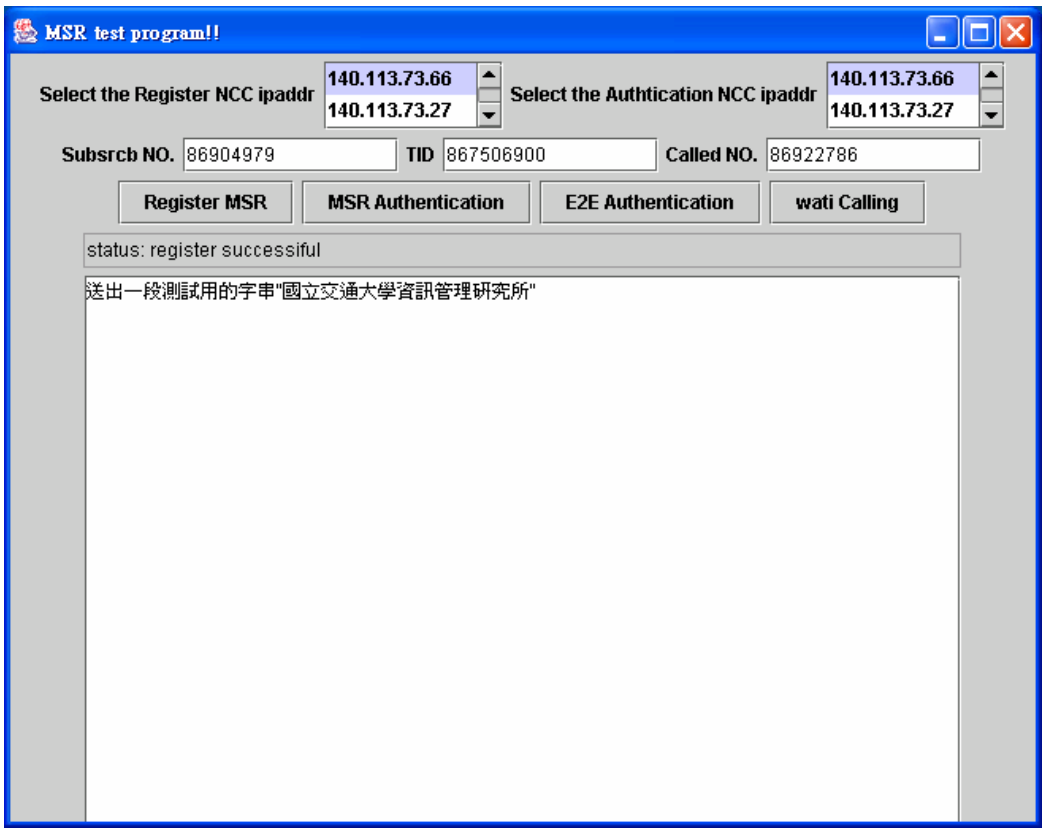

圖 28 用戶端執行畫面

4.6 總結

完成系統實作的過程之後，將進行認證機制和效能的比較。以系統實際運作的過程為基礎，進一步驗證理論分析的安全性。本研究將分析的結果於第五章內探討。並整理出比較表。

第五章　安全性與效率分析

5.1　安全性分析

為了證明所提出的機制是可行的，在此列舉了目前幾個較常見的攻擊模式，並說明如何克服這些問題。

一、竊取(Interception)

只有經過授權的人才能讀取所傳送的資訊。提出的機制中，不論是哪一階段，每次資料傳送的過程都會利用通訊雙方所共同持有的 shared key，K_1，或是此次資料交換所使用的 session key，來給予資料加密。因此，只有擁有此金匙的用戶方能將加密的資料解開，不會造成資料洩露出去，阻絕了資料遭竊取的風險。

二、竄改(Modification)

未經授權的第三者非法截取了所傳送的資料，不但取得存取某項資源的權力，並且竄改其中的內容。針對此一攻擊，於是在每筆資料的傳送過程中，都會在資料後段加上以 HMAC 作為資料完整性的確認，以防止資料被竄改。本研究所提的方法即是在接收端收到資料之後，先核對是否相符合，若不合，視為資料已經過竄改。即使攻擊者不知道訊息的內容，以達到不被竄改的目的。例如，將 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 以具有訊息認證碼的單向雜湊函數處理之，即 $HMAC\{TID, NCC, \{RAND \| TID \| X\}_{K_1}\}_{K_1}$，當接收端收到資訊後，以 shared key，$K_1$，再做一次 HMAC，即可驗證資料的完整性。因此，假如攻擊者竄改了使用者所送出的認證資料，由於攻擊者並未持有使用者和 NCC 所共同持有的 shared key，因此無法將竄改之後的訊息正確對應到相對的 HMAC。故 NCC 或使用者一收到訊息，即執行 HMAC 的比對，由於在中途已經被攻擊者竄改，HMAC 比

對結果絕對是不正確的，即將資料給丟棄，以達到防範資料被竄改的危險。

三、重送攻擊(Replay Attack)

未經授權的第三者在截收到資料之後，將資料儲存，並在之後偽裝成傳送端，把之前所儲存的訊息再送出，以騙取使用者的信任，此為重送攻擊。未了防此一情況發生，在認證的過程中每次所使用的 random nonce 並不會相同，並且通話過程每次所使用的 session key 也都不同，阻絕了重送攻擊的可能性。例如，使用者端送 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$，其中 RAND 即是為防止重送攻擊，而 NCC 端送 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$，其中 RAND+1 目的亦是一樣。

四、伺服器偽裝攻擊(Sever Spoofing Attack)

攻擊者偽裝成認證端，傳送訊息給終端使用者以騙取機密資料。由於認證機制是採行 shared key 的認證方式，並加上系統端和使用者的相互認證，使用者只要發現傳送出去的資料，和伺服器端加上認證所需的資之後不符合，立即當成伺服器端不是合法的伺服器。例如，在使用者身份認證過程中，假若有一個偽冒 NCC 的機器，待它收到使用者端的 $TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 資料後，由於它並無 shared key K_1，因此無法解出其中資訊，故無法回傳正確的 RAND'給使用者，因此，使用者可藉由 RAND'判斷是否為偽冒 NCC 的機器送出來的資訊。

五、中間人攻擊(Man-in-the-Middle Attack)

假設 A、B 是為通訊的雙方，而 C 是介於 A、B 之間的第三者，其任務可能只是負責轉送資料。所謂的中間人攻擊模式即是 C 將 A 所傳送的資料留住而不轉傳給 B，並自己發送一段訊息偽裝成是 A 所發出。同理，在 B 往 A 方向的通訊也採用相同手法。如此一來 C 即可清楚了解 A、B 之間所交換資料的內容。可能的情形也會發生衛星通訊系統上。因此，假設使用者所屬的 NCC 是可信賴的，

在最後 session key 產生階段，使用者需將產生的 session key 的資料以自己和自己所屬的 NCC 所共同持有的 shared key 加密，由 NCC 解開，並發起接下來的程序，以防止中間人攻擊。另外，有可能發生中間人攻擊的地方是使用 DH 協定所產生的攻擊，但由於本研究所採用的 DH 協定，其參數 X 與 Y 均用雙方分享的私密金匙加以包裝，例如，$TID, NCC, \{RAND \| TID \| X\}_{K_1}$ 及 $TID, ID_s, \{RAND+1 \| TID' \| Y\}_{K_1}$，故不會造成中間人攻擊的問題。

在 Hwang et al. 所提出的協定中，因缺少產生 session key 這階段。因此，若在雙方未握有彼此的資訊，如：public key、雙方共用的 secret key。於是在產生 session key 時，必需以明文傳送有關的資料。利用本論文所實作的系統，只需在 NCC 端截取此資料，即可竊取雙方的訊息內容，在通訊的過程將會有安全上的問題。

另外，本研究所提出的身份認證機制於每次認證成功之後，皆會更新使用者和系統端的 shared key，並且端對端的使用者其 session key 也都是只使用一次，提高系統的安全性。為避免在通訊過程中洩露行動用戶的位置，以保障其通訊隱私，在通訊的過程中並不直接傳送用戶的 IMSI，取而代之的是一個暫時的 TID。此外，於 NCC 間及使用者與使用者間的相互認證均可提高本機制之安全性及防止上述攻擊。

表 11 為本論文和 Hwang et al.所提出之認證機制的比較表，灰色部份為 Hwang et al.的機制所未探討的部份。在安全性上本論文之機制高過於 Hwang et al.的協定。關於衛星環境的考量，本論文所提出的方法也較完備。

表 11 安全分析比較表

	Hwangs' Scheme	Proposed Scheme
竊取	Y	Y
竄改	Y	Y
重送攻擊	Y	Y
伺服器偽裝攻擊	Y	Y
中間人攻擊	N	Y
End-to-end 認證	N	Y
產生 session key	N	Y
資料完整性	N	Y

5.2 效率分析

由於衛星通訊是屬於運算能力不強之通訊系統，然而對於安全性的需求又不得疏忽，於是在達到最高的安全性之餘，也在協定的設計上強調系統的效率性。效率上大致上可由三部份來分析分別為傳送訊息的次數、演算法的複雜度和金匙數量。

一、發送訊號次數：礙於運算能力的限制，於是將較複雜的運算過程留在系統端。在認證和產生 end-to-end session key 的過程中，終端用戶端只需發出兩次訊號，減少電力的浪費，加速認證所需的時間。

二、運算能力需求：系統中加密演算法為混合式，即是對稱與非對稱。非對稱演算法只有在最後產生 end-to-end session key 時，用來加密 DH 的元素之一，為了避免在傳送過程中被截取。除了非對稱式加密之外，其他皆為對稱式加密演算法，採用高效率與安全性強的 AES 演算法，因此，在演算法複雜度這部份具有高效率。

三、金匙數量：每用戶都有對應的四把金匙，分別是使用者的 public key、private key、和 NCC 共有的 shared key、end-to-end session key。和第二點相同，public key 和 private key 只用一次。shared key 用於認證使用者階段，最後使用者之間的通訊是使用 end-to-end session key。雖然金匙的數量多，不過最終目的都是為了達到最高的安全性。

表 12 效率比較表

	Hwangs' Scheme	Proposed Scheme
Key	1	4
Round	3	5
Computing	2AE+2AD	4AE+4AD+3EE+3ED

*AE：AES 加密運算

*AD：AES 解密運算

*EE：ECC 加密運算

*ED：ECC 解密運算

第六章　結論與未來展望

6.1　結論

綜合目前所使用的認證機制，皆是應用於陸上的行動通訊系統。若直接套用於衛星通訊上，將導致效果不彰，甚至是系統安全上的漏洞。針對衛星通訊上的使用者認證協定，有學者 Hwang et al.提出相關的認證方式，但關於安全性功能，還稍嫌不足。因此，本論文提出一套完整的認證機制，茲將本論文貢獻整理如下：

- ✓ 介紹衛星相關特性，提供一個快速入門的媒介。
- ✓ 依據衛星實際環境分析，設計符合衛星通訊環境之安全且完整的認證機制。
- ✓ 以系統模擬方式，驗證提出之機制的可用性。
- ✓ 解決了目前行動通訊上所可能遭遇的安全性問題。

在設計協定的過程中，從註冊、認證到終端使用者之間的相互認證，巧妙利用對稱式與非對稱式的加密演算法達到用戶資料的保密，提供一個安全的通訊環境。

6.2　未來展望

衛星通訊在目前網路占了一席之地，關於衛星通訊的研究與建構計畫正如火如荼進行。新一代的通訊衛星因其備有星載處理(onboard processing, OBP)，使得網路拓樸(Network Topology)，更為複雜，造成許多問題產生。如網路協定與網路管理的問題。其中網路協定問題即是如何將 TCP/IP 協定整合於衛星的網路環境中。而網路管理題，首先需探討在此通訊架構下，錯誤管理之錯誤識別方法，因其影響了衛星網路的效能。而後的研究可朝著衛星的網路協定和網路管理這兩

方向前進。

參考文獻

【中文部份】

[1] 林志興，「3G 行動通訊使用者認證協定之研究」，中原大學電機工程學系碩士學位論文，2002。

[2] 董乃仁，「改良 UMTS 認證機制之研究」， 中原大學電機工程學系碩士學位論文，2003。

[3] 楊松諺，「JAVA SECURITY 全方位解決方案」，碁峰，台灣，2003。

[4] 「 System Beyond IMT-2000 之 標 準 化 動 向 」， <http://www.moteco.co.jp/tech01_a02.html>。

【英文部份】

[5] "3G TS 21.133:Security Threats and Requirements," <http://www.etsi.org/>.

[6] Bo Ryu, "Modeling and simulation of broadband satellite networks. II. Traffic modeling," Communications Magazine, IEEE Vo 37, Issue 7, July 1999, pp:48-56.

[7] C.-K. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall PTR, New Jersey, 2002.

[8] Craig Hunt, "TCP/IP Network Administration," O'REILLY , 1997.

[9] Davide Astuti. Markku Kojo, "Simulation Study of TCP Performance in TRANSAT," 2003.

[10] ITU-R, "Principles and Approaches on Evolution to IMT-2000/FPLMTS,"1997.

[11] Lin H.Y., "Security and Authentication in PCS," Computers & Electrical Engineering, Vo 25, pp.225-248, 1999.

[12] M. Allman, D. Glover, L. Sanchez, "Enhancing TCP Over Satellite Channels using Standard Mechanisms," RFC2488, 2002.

[13] M.S. Hwang, C.C. Yang, and C.Y. Shiu, "An Authentication Scheme for Mobile Satellite Communication Systems," ACM SIGOPS Operating

Systems Review, Vol. 37, No. 4, October 2003, pp. 42-47.

[14] N Jefferies, “Security in third-generation mobile systems,” 1995.

[15] Prakash Chitre and Ferit Yegenoglu, “Next-Generation Satellite Networks:Architectures and Implementations,” IEEE Communications Magazine, pp.30-36, 1999.

[16] Priscoli, F.D, “Functional areas for advanced mobile satellite systems. Vehicular Technology Conference,” 1997 IEEE 47th Vol 1, pp.223-227, 1997.

[17] Raymond J.Leopold, “The IRIDIUM Communications System,” ICCS/ISITA, 1992.

[18] Sarvar Patel and Bellcore, “Weaknesses of North American Wireless Authentication Protocol,” IEEE Personal Communications, June 1997, pp.44-40.

[19] Wang,R.H.; Horan,S., ” Performance Evaluation of TCP and Its Extensions Over Lossy Links in a Small Satellite Environment Communications,” IEEE International Conference on Vol 3, pp:1478-1482, 2005.

[20] Yurong Hu and Victor O.K.Li, ” Satelliet-Base Internet,” IEEE Communications Magazine, 2001.

[21] “Mobile and Wireless Communications,” <http://www.iet.ntnu.no/groups/radio/newresearch/systems/mobile_telecommunications.htm.>.