行政院國家科學委員會專題研究計畫　成果報告

子計畫一:虛擬家網路環境之異質網路交談管理機制(I)

計畫類別： 整合型計畫
計畫編號： NSC92-2213-E-002-094-
執行期間： 92 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立臺灣大學資訊工程學系暨研究所

計畫主持人： 林風

計畫參與人員： 鄭欣明，張桓鳴，陳威豪

報告類型： 精簡報告
報告附件： 出席國際會議研究心得報告及發表論文
處理方式： 本計畫可公開查詢

中　華　民　國 93 年 9 月 30 日

行政院國家科學委員會專題研究計畫成果報告

計畫編號：NSC 92-2213-E-002-094-
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日
主持人：林 風　台灣大學資訊工程系
計畫參與人員：鄭欣明、張桓鳴、陳威豪 台灣大學資訊工程系

一、中文摘要

由於無線裝置的多元化發展，使用者往往擁有不只一個隨身的無線裝置。當使用者擁有越來越多不同的無線裝置，在享受便利的同時，也伴隨資料分散保存而造成存取不便。因此我們發展了智慧型閘道器（Intelligent Gateway）平台，除了整合異質型態網路讓使用者方便利用異質裝置使用網際網路外，更提供議程（session)管理機制以實現個人化的服務，讓使用者在不同的智慧型閘道器移動時，能夠保留個人的操作環境，達到虛擬家網路的環境。

我們也探討使用者終端裝置在無線異質網路環境中移動時會遭遇到的安全性問題。我們設計並實作出一具漫遊機制的多功能「智慧型閘道器」（Intelligent Gateway）平台提供使用者終端裝置一智慧型的行動計算環境。此平台由智慧型閘道器所組成，提供使用者藉由各式各樣終端裝置，透過智慧型閘道器在網際網路中擷取任何資訊服務、並且在服務過程中可以切換到不同個人隨身終端裝置。此外，此平台具備漫遊能力，使用者可以漫遊到外部智慧型閘道器（Visitor Intelligent Gateway; VIG），透過外部智慧型閘道器的漫遊機制連回家智慧型閘道器（Home Intelligent Gateway; HIG）繼續使用服務。當使用者終端裝置由 HIG 漫遊到 VIG 時，原來在家智慧型閘道器中屬於使用者終端裝置的個人行動計算環境必須由家智慧型閘道器遷移 (Migrate) 至外部智慧型閘道器，HIG 與 VIG 間需建立一地道 (Tunnel) 來為此遷移傳送所需的資料。並且, HIG 與 VIG 間必須有保密的協定以確保使用者終端裝置個人資料的安全性。

關鍵詞：安全性（Security）、虛擬家環境（Virtual Home Environment; VHE）、代理人（Agent）、異質網路（Heterogeneous Network）

Abstract

Because of the rapid development of the mobile devices, the users often have more than one kind of mobile devices. However, with the increasing number of devices, the users are harder and harder to maintain their diverse personal data. Hence, we developed an Intelligent Gateway platform to integrate heterogeneous networks for users to access the Internet with different kinds of devices more conveniently, and to realize the personal mobility by providing session management mechanism. This platform maintains the personal operating environment of the user to realize the goal of virtual home environment.

We also study the issue of the Security Management for the mobile user when roaming among heterogeneous networks. A personal and intelligent computation environment (that helps users to manage the information in the Internet and acts for the users to access Internet applications) should be considered. In this project, we will design

and implement a platform that provides the mobile user the intelligent personal computation environment. This platform consists of Home Intelligent Gateways (HIGs) that act as the agents of the mobile user in the Internet. The HIG is the IG which the mobile user registers to. Due to the limited capabilities (e.g., small storage), instead of storing the personal information on the mobile device, the mobile user stores the personal information on the HIG. When the mobile user leaves the service area of the HIG, he may connect to the VIG. At this moment, VIG is the agent of the mobile user. This process is referred as “Roaming”. When the mobile user roams from the HIG to the VIG, the following two steps are performed; a tunnel is created between the HIG and VIG. Besides, a security negotiation is performed between VIG and HIG to ensure the security of the personal data of the call agents.

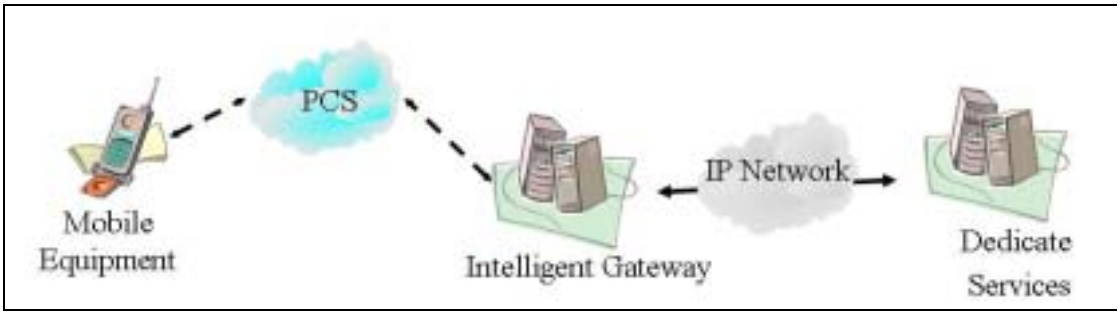
Keywords: Security, Virtual Home Environment; VHE, Agent, Heterogeneous Network

二、緣由與目的

無線通訊行動化，已經是全球科技產業近年來極為重視的部份。隨著行動裝置的蓬勃發展、無線技術的進步，裝置間的溝通方式以及連線能力更形多元：從傳統有線網路，到無線的紅外線（Infrared）[7] 傳輸、藍牙無線網路 [8]、GPRS/UMTS [9] 網路、與 IEEE 802.11 [10] 系列無線技術，這些都是希望能夠為人類生活帶來方便、更有效率的資料溝通與傳輸能力。再者，經由個人數位助理（PDA, Personal Digital Assistant）連線能力的發展、或是行動通訊器材（諸如手機）個人資料運算功能的日益強大之中發現：「個人化的資料處理」與「行動裝置的連線溝通能力」將會是未來行動裝置研究發展的重點目標。

然而，雖然行動裝置的功能日趨強大，但仍然存在幾項問題，如：(1) 使用者隨著使用裝置的不同，資料的維護也隨之複雜，聯絡人的資料在不同的裝置上存放不同的版本而無法同步，或是重要資料因為行動裝置的更替而無法隨使用者移動。(2) 當使用者在不同裝置間移動，外界傳訊，如 Email 之傳送，很有可能無法將訊息正確的繞送到使用者正在使用中的裝置。(3)使用者能常用的功能與一些基本的應用程式，如行事曆與電話簿，隨裝置的功能不同而受限制甚至完全沒有。(4) 使用者切換裝置的時候無法保持連線不中斷，而導致服務被中斷。無論行動裝置再新穎、功能再強大，都必然會面臨以上的問題，且當使用者的行動裝置越多，情形就越明顯。

因此，我們相信必須有新的系統、新的架構從底層來改善問題。希望藉由新的系統，能夠相容既有的通訊裝置（如功能陽春的手機），亦能兼顧發展性相容於功能更強的設備（如具上網能力的 PDA），使個人化的資料不因裝置的不同而遺失或無法存取；讓使用者不因裝置不同而無法接收重要訊息；更能夠讓使用者透過不同裝置享受如同使用個人電腦般的強大功能。我們希望運用代理人（Agent）的觀念、異質性網路的溝通能力、以及低廉成本且安全的架構，針對使用者個人為導向，提供具擴充性的個人化計算（Personalization

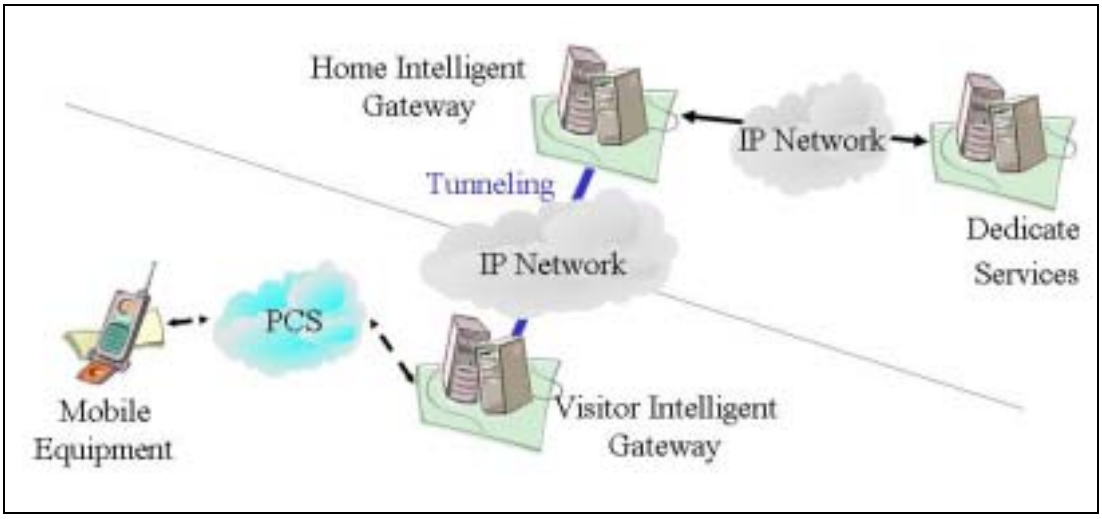


（圖一）使用者透過智慧型閘道器連接到 IP 網路上的伺服器使用服務

Computing）服務平台，為使用者管理重要資料、提供異質裝置上網使用一般服務之能力、以及維持使用者可存取（Accessibility）。我們亦提供使用者漫遊環境，讓使用者在安全性的前提下，還能夠在不同的智慧型閘道器上使用服務。而漫遊所容易引發的安全性議題，我們則是研究與分析現行適用於本系統的公開金鑰基礎建設(PKI) [18]安全保護機制，並將之實作於此平台上。而詳細的 PKI 機制內容請參考[18]。

三、研究方法與平台介紹

圖一為實驗虛擬家網路環境所開發的智慧型閘道器系統的使用情形與概念示意圖，使用者終端裝置（Mobile Equipment）透過網路連線到智慧型閘道器，並對智慧型閘道器下適當的指令，使其代理使用者連線到 Internet 上使用服務，如電子郵件（E-mail）、檔案傳輸（FTP）、瀏覽網頁（WWW）等。智慧型閘道器接著將擷取到的資訊做適當的呈現轉換（Adaptive-Presentation），以符合使用者終端裝置顯示能力，隨後傳到使用者終端裝置上。若資料量太大時，智慧型閘道器也會先行將資料暫存，等到使用者具備較佳的連線能力，或是使用較佳計算能力的終端裝置時再下載。本系統實作了代理人（Agent）的觀念，當使用者的終端裝置離開的時候，或是切換傳輸媒介的時候，智慧型閘道器系統會繼續保持使用者正在進行的工作，例如幫使用者繼續接收尚未接收完的檔案，或是使用者遠端登入的服務（Telnet）。而當使用者重新登入回系統時，系統依然能夠讓使用者持續先前的議程（Session）。舉例來說，假如使用者透過智慧型閘道器使用遠端登入服務連線到 IP 網路上的伺服器，而此時使用者必須離開，或是想切換到更佳的連線媒介，如 WLAN，就可以使用暫時停止的功能來做暫時登出的動作，待切換完或是漫遊到外部智慧型閘道器時，都可以藉由重新登入的動作來恢復工作的進行。縱使使用者使用不同的裝置透過不同的網路連線到智慧型閘道器，都能夠接續使用進行中的服務，對於使用者而言，就如同持續使用同一網路與裝置般沒有分別，形成一虛擬家網路環境。



（圖二）使用者漫遊到外部智慧型閘道器

圖二表示使用者漫遊到外部智慧型閘道器時，外部智慧型閘道器會依據使用者所給的資訊連回使用者的家智慧型閘道器進行安全性檢查的動作，倘若驗證成功，外部智慧型閘道器會與使用者的家智慧型閘道器建立地道，替使用者把正執行於家智慧型閘道器的程式資料轉送給使用者，使用者就能透過外部智慧型閘道器繼續使用家智慧型閘道器正進行中的服務，而此地道的安全性是由公開金鑰基礎建設(PKI)的安全機制所保護。當使用者在不同的外部智慧型閘道器間漫遊的同時，透過建立地道轉送資料的議程管理機制來達成虛擬家網路的功能，無論是個人的資料或是正進行中的服務，都能夠藉由地道的建立來達到轉移的功能。使用者如同在家網路般，無論在任何智慧型閘道器上，個人的資料與服務環境都與家網路一樣，在該智慧型閘道器上形成一虛擬家網路環境。

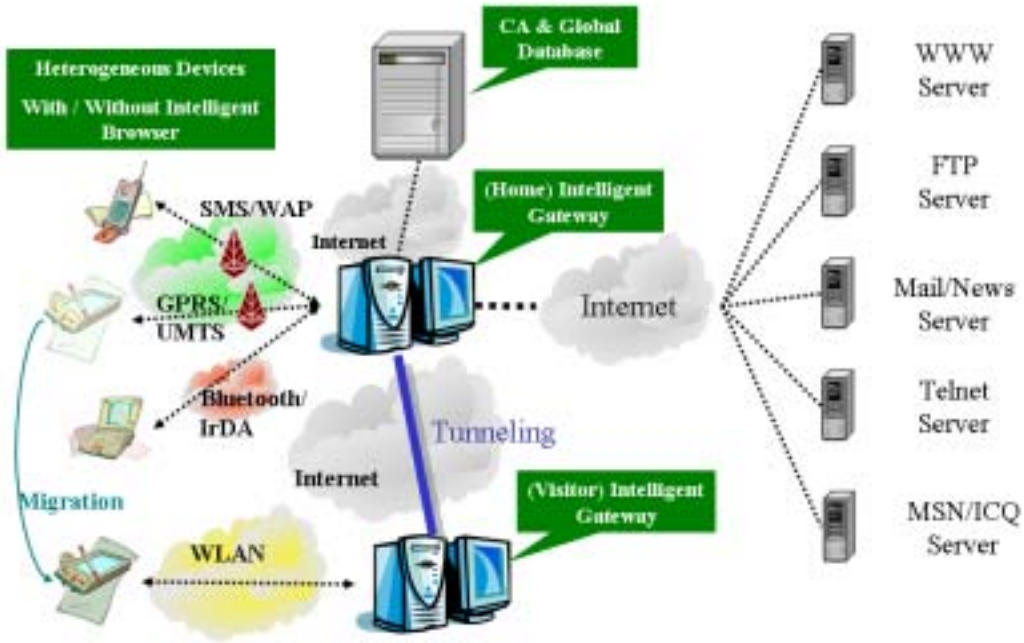
四、文獻探討

使用者行動計算（User Mobility）[1,4,13,14]是近年來相當熱門的一個學術研究主題。簡單地說，即是讓使用者能夠在同一個 Session 的過程中，能夠自由的「行動」，並利用手邊所能接觸到的工具繼續控制 Session。而使用者行動計算若再細分，可以分為以「機器」為主的裝置移動性（Device Mobility）和以「人」為主的個人化移動性（Personal Mobility）。已經有許多學術研究組織在進行這個主題，細節請查詢我們的參考文獻[2,3]。而我們著重的重點，在於個人化的移動性，針對個人化的可存取性（Accessibility）與個人化資料管理（Personalization）兩大功能作為平台的主軸，並搭配容納異質型網路終端裝置，以及安全機制、資源管理機制、代理人的概念，以實現安全的虛擬家網路環境。

不過，目前大部份的研究以及產品採取「將代理人放在代理人伺服器」的作法。此種作法通常是在公網的網域上建立一個代理人伺服器，然後所有使用者的代理人都放置在這個位於遠端網路的代理人伺服器上。我們挑選幾個性質相近功能相若的國外計畫分述如下：

Mobile People Architecture [4]

此架構主要是設計提供使用者從任何



（圖三）系統網路架構圖

地方透過任何連線資訊媒體來與另一使用者進行溝通，使用的資訊媒體可以是電子郵件、即時通訊軟體（如：ICQ）等。溝通的同時能夠確保使用者所在地的隱密性，提供隱私權保障，不同的通訊媒介系統也能夠提供轉換的動作，如：電子郵件的訊息轉換成即時通訊訊息，反之亦然。藉由 Personal Layer 的引入，以及固定的個人代理器（static personal proxy），系統能夠保持使用者的蹤跡，將訊息正確的繞送到使用者。同時藉由固定的個人代理器，使用者的行蹤不會被其他人所知，確保個人的隱密性（privacy）。

問題。

NetChaser [1]

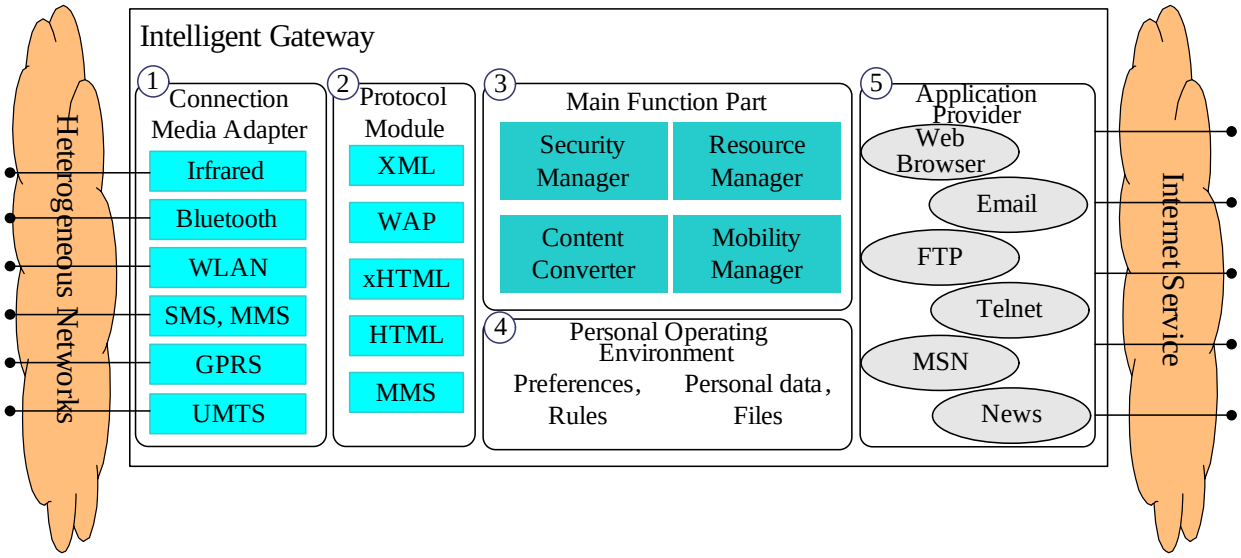
此計畫主要的架構核心是運用行動代理人替使用者進行狀態的維持，如同本平台的方法。此計畫提供的服務以及架構較為固定，目前僅提供 HTTP、FTP 與電子郵件代理人的服務。同樣強調個人資料的維持，但是缺乏使用者間的溝通機制。

IPMoA [2]

IPMoA（Integrated Personal Mobility Architecture）同樣是為了提供使

ICEBERG [3]

此計劃是由加州柏克萊大學所主持，用者藉由不同裝置使用 IP 網路服務的架構，主要提供一個整合電信網路與資料網路的也提供了個人化的功能，運用的技術如同本計架構，此計畫由多個子計畫所組成，讓電畫與 NetChaser，即為代理人的方式。但是與信網路與資料服務間得以溝通。此系統較本計畫相異之處在於其代理人會隨著使用者少強調個人化資料的維持，但同樣強調不的移動而遷移到使用者所在的 IPMoA 伺服器，同異質裝置間的溝通。同時提供一套命名但是本計畫的解決方式是透過建立地道。在效機制來解決電信網路與資料網路間對應的能也許 IPMoA 較佳，但是對於無法移動的服



（圖四）智慧型閘道器系統架構

務(如:部份的服務會需要固定的 IP 位址,或是重要連線無法使用中斷再重新連線的方式）。因此本計畫所犧牲的部份效能相信能夠換取較佳的使用方式與彈性。

五、智慧型閘道器平台架構說明

如圖三所示，智慧型閘道器系統主要由三個部分所組成：

- **Intelligent Browser：** 使用者上的智慧型瀏覽器，負責與智慧型閘道器網路進行溝通。此外能夠自動幫使用者偵測可使用的連線媒介，對 Intelligent Gateway 的內容做適性式的呈現（Adaptive-presentation）。
- **Intelligent Global Database：** 負責智慧型代理器網路的憑證核發，此外也負責使用者所在位址的維護。
- **Intelligent Gateway：** 智慧型閘道器個人服務平台。為異質網路與 Internet 的溝通橋樑，能讓使用者透過異質性終端裝置，使用網際網路上一般性的服務，以代理人的方式維護使用者的議程（session），並提供個人化資料的存取。此外並具備閘道器之間交談功能，使用者能利用異質終端裝置透過不同的外部智慧型閘道器連回家智慧型閘道器形成一虛擬家網路環境；當使用者從一閘道器漫遊至另一閘道器時，交談機制亦能確保服務不中斷與個人資料的正常存取。

六、智慧型閘道器軟體架構圖

圖四中顯示智慧型閘道器系統內部組成主要分為五個部份，由此五個部分互相搭配完成系統功能。以下我們針對每個部份、及其間互相搭配的流程進行說明。

連線媒介轉換器（Connection Media Adapter）：參照圖四(1)。連線媒介轉換器包含連線實體模組，如紅外線 [7]收發器、藍牙 [8]收發器、網路卡等，以及其對應的伺服器聆聽程式。異質裝置透過此模組建立實體連線，對智慧型閘道器下指令與收發訊息。連線媒介轉換器的設計盡可能以模組化、訂定統一介面的方式，如此對於未來新的連線媒介，能夠有較佳的擴充性支援。

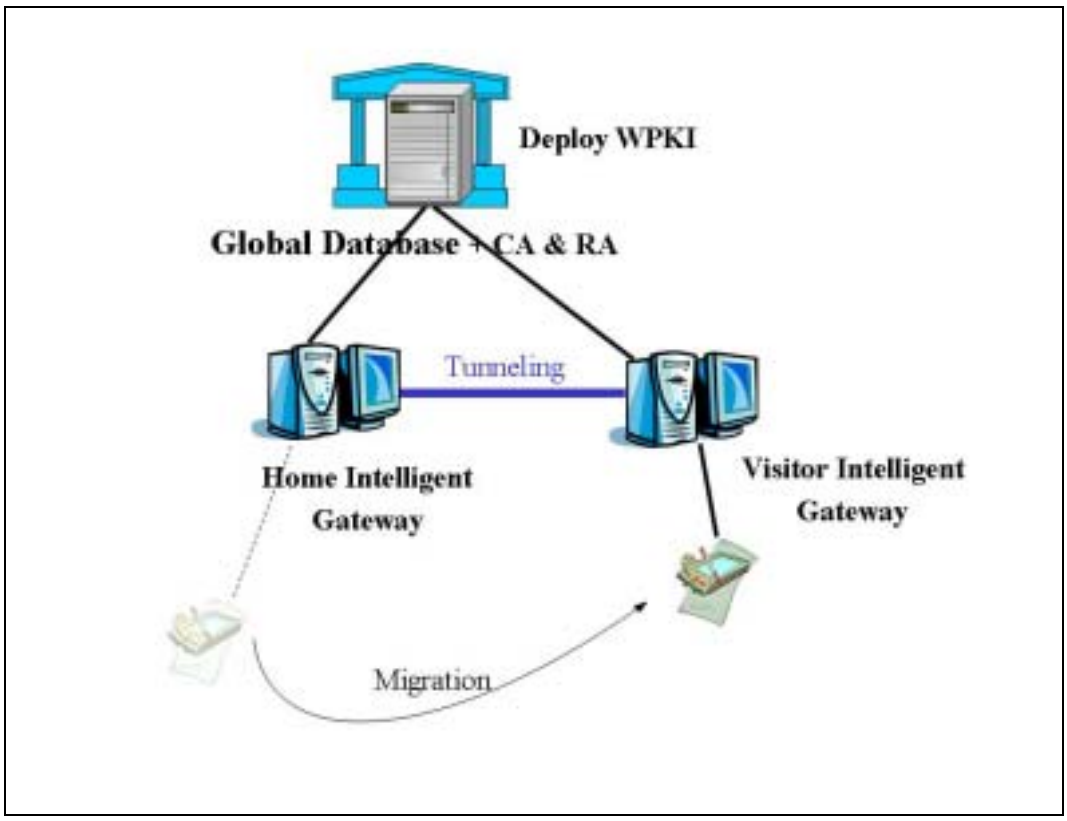
通訊協定模組（Protocol Module）：參照圖四(2)。通訊協定模組提供上層的通訊協定溝通模組，由於異質網路所用的網路通訊協定不盡相同、種類繁多，如：

HTML、xHTML、WAP 等，因此為了提供異質多樣溝通管道，必須針對每個通訊協定實作對應的通訊協定模組，作為包裝與解譯通訊協定之用。此模組同樣必須具備可擴充性，容易延伸，以方便開發、加入未來的通訊協定模組。

主要功能元件組（Main Function Part）：參照圖四(3)。主要功能元件組包含本平台主要功能的核心元件，配合其他的模組來達成系統的主要特性。核心元件為：安全性管理者（Security Manager）、資源管理者（Resource Manager）、內容轉換器（Content Converter）、移動性管理者（Mobility Manager）。安全性管理者負責安全機制的維護以及提供必備安全的功能，例如認證（Authentication）、授權（Authorization）等。使用者登入智慧型閘道器時，首先認證使用者是否為合法的系統使用者，然後根據使用者的身分（漫遊的使用者（visitor user）或是家使用者（home user））來給予對應的權限：家使用者能夠啟用服務、存取該智慧型閘道器的個人化環境與檔案；而對於漫遊的使用者，外部智慧型閘道器(VIG)僅給予轉送訊息至家智慧型閘道器（HIG）的權限與功能。除此之外應用程式所需的加解密程式、公私金鑰讀取等，也由安全性管理者提供。資源管理者負責智慧型閘道器上資源的分配，由於異質裝置能力不同，因此所需的計算能力也不同；此外異質網路的頻寬需求不同，當使用者人數較多的時候，資源管理者便根據使用者的裝置、及其所在網路的特性，在智慧型閘道器上給予適當的計算能力以及頻寬，當使用者要求服務時，也根據智慧型閘道器上資源使用情形給予使用權。內容轉換器則是針對使用者裝置，給予適當的顯示內容或是過濾內容，初步的內容轉換以過濾大型的檔案使其能夠適合小型裝置的顯示為主，後續的議題可以是動態內容轉換，例如對於圖片方面，將大圖動態改為小圖等。移動性管理者負責使用者位址的追蹤與管理，維持使用者所在的網路位址與裝置資訊，將訊息正確地繞送到使用者所在位址。當使用者漫遊至 VIG 時, VIG 的移動性管理者會與 HIG 的移動性管理者交換訊息，進行彼此身份的認證, 隨後建立安全通道由 HIG 替使用者將訊息經由 VIG 繞送至正確的網路與裝置位址。倘若使用者不在智慧型閘道器系統上，亦即無登入至系統或是離開 VIG 所服務範圍, 則負責繞送訊息之移動性管理者將替使用者暫存於個人資料庫，待使用者登入後轉送給使用者。移動性管理者為實現個人的可及性（Reachabitity），強調不論在任何網路或是裝置，系統都能夠正確地將訊息繞送至使用者。

個人作業環境（Personal Operating Environment）：參照圖四(4)。個人作業環境包含個人檔案儲存空間，具備如同一般作業系統的檔案系統，讓使用者透過異質裝置存取個人資料，透過主要功能元件組內的內容轉換器，則可以將資料以較適合於裝置的型態顯示出來。個人作業環境亦用於儲存個人資料，或是該使用者的應用程式資料，如下載的檔案、我的最愛、通訊錄、使用的服務等。這部分主要實現跨異質網路以及異質裝置，仍能夠保持喜好設定、個人資料的機制，強調個人化的重要特性。

應用程式提供組件（Application Provider）：參照圖四(5)。此部分主要為應用程式所在的模組，應用程式的客戶端（client）皆實作為元件（component）存放於此，亦為應用程式的執行環境。使用者透過 Call Agent 經由智慧型閘道器對此處的應用程式模組下達命令，應用程式則



（圖五）智慧型閘道器安全機制示意圖

將執行的結果送回至 Call Agent，而將永續資料（Persistent data）儲存在個人作業環境，如此介面與資料的分離，將簡化異質裝置上所需的開發，而將重要資料、應用程式存放與執行於智慧型閘道器中也能強化家環境的概念。

七、建置 PKI 環境保護的安全機制

我們選擇在智慧型閘道器平台建置公開金鑰基礎建設（PKI）（如圖五）的安全機制環境以保護節點間的溝通以避免竊聽竄改等攻擊，我們將在 Intelligent Global Database 上架設 PKI 中的憑證處理中心（CA 與 RA），負責審核與發放憑證（certificate）給各個節點，如智慧型閘道器或是使用者終端裝置，而每個憑證中包含公開金鑰和該節點的身分。當使用者終端裝置連接至 Home Intelligent Gateway 時，Home Intelligent Gateway 即可前往 Intelligent Global Database 比對 Client 輸入的使用者帳號和密碼是否為合法的使用者，以此確保應用層（application layer）的安全，亦即防止非合法智慧型閘道器使用者的入侵；再上公開金鑰演算法，透過加解密、數位簽章的機制來保證對談層（session layer）的安全。發送端利用接收端的憑證中的公開金鑰加密，而接收端利用本身的私密金鑰解密，以此保障資料在網路傳輸時不被竊聽。而憑證的觀念納入，可保證連線的雙方都是合法非偽造的，提供節點與節點間的相互認證，進一步保障網路的安全。

使用者終端裝置漫遊至 Visitor Intelligent Gateway 時（參照圖五），為確保使用者的身分，要先比對使用者的帳號密碼進行身分的認證。而認證成功後使用者所在的外部智慧型閘道器將 Home Intelligent Gateway 上所進行的議程（session），利用地道的機制移轉至使用者，於外部智慧型閘道器處形成一虛擬家網路環境。此地道的資料傳輸則是利用前

述的公鑰私鑰加解密演算法加以保護。

八、結論

隨身裝置的多元化與連線媒介的發展，雖然為人們帶來方便，卻增加了使用電腦的複雜度。因此本系統希望能夠藉由透過單一的使用入口—智慧型閘道器，代理使用者連線到網際網路使用各項服務，替使用者維持議程（session），讓使用者切換裝置、漫遊在不同的智慧型閘道器的同時，能夠盡量不會感受到裝置與連線間的差異性與複雜度，藉以實現虛擬家網路環境。同時，安全化、個人化資料的管理讓使用者能夠放心地在任虛擬家環境中都能安心的存取個人化資料。本計劃的研究，加強了目前其他研究較為薄弱的安全議題，也實作了虛擬家網路環境的功能，拓展目前對於個人化移動性的研究。

九、參考文獻

[1] Antonella Di Stefano and Corrado Santoro, *"NetChaser: Agent Support for Personal Mobility"*, *IEEE Internet Computing*, vol.4, issue 2, Mar/Apr 2000.

[2] B. Thai and A. Seneviratne, *"IPMoA: Integrated Personal Mobility Architecture"*, *Mobile Networks and Applications*, Vol.8, Issue 1, 2003.

[3] Helen J. Wang, et al., *"ICEBERG: An Internet-core Network Architecture for Integrated Communications"*, *IEEE Personal Communications 2000 special issue on IP-Based Mobile Telecommunication Networks*.

[4] Maniatis Petros, et al., *"The Mobile People Architecture"*, *ACM Mobile Computing and Communication Review*, July 1999.

[5] Eric Gamma, et al, *"Design Patterns – Elements of reusable Object-Oriented Software"*, 1994.

[6] Jeffrey Undercoffer, et al, *"A Secure Infrastructure for Service Discovery and Access in Pervasive Computing"*, *Mobile Networks and Applications*, Vol.8, Issue 2, 2003.

[7] http://www.irda.org/

[8] http://www.bluetooth.org

[9] http://www.3gpp.org

[10] http://www.ieee802.org/

[11] http://www.wapforum.org

[12] http://www.ietf.org/rfc/rfc3261.txt

[13] http://iwork.stanford.edu/

[14] http://ninja.cs.berkeley.edu/pubs/pubs.html

[15] http://www.w3.org/XML/

[16] *"Wireless Application Protocol Public Key Infrastructure Definition"*, WAP Forum (Wireless Application Protocol Forum) WAP-217-WPKI Version 24-Apr-2001.

[17] *"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 6)"*, 3GPP TS 23.107

[18] R. Housley et al., *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*, RFC 3280, Internet Engineering Task Force, April 2002.