第一章

緒論

1.1 研究背景

隨著網路與科技的普及，資訊與生活密切地整合，刺激人們對於網際網路之應用。網路使用趨勢從傳統的撥接、寬頻至現階段無線通訊的應用，已經成功地融入人們生活中。根據台灣網路中心(TWNIC)在2006年2月發表的台灣寬頻網路使用報告調查書中指出，在05年間，國內民眾無線上網使用人數達356萬人，佔總人口數18.3%；相較於04年7月的15.9%及05年1月的12.4%有明顯增加的趨勢。因此會有更多的人，無論在任何時間或是在戶外、行走中、車子上等任何地方，可直接透過手機、PDA等工具來進行資料的交換、共享與散播，使用網路來存取資料，達到行動上網的目標。無線網路環境的核心特性就是具備「可移動性(mobility)」，行動用戶可以直接在兩個不同的網域內移動，即使改變目前的工作環境，但透過基地台的無限延伸，享受漫遊上網的樂趣。

行動通訊的新技術，帶給目前資訊時代更多科技創新的機會，改變了人們資訊與服務的存取方式，也提高對於資訊服務之需求。同時服務提供者也希望透過更好的服務品質與個人化服務的提供，來追求利潤與市佔率的成長。電腦運算能力日漸強大的今日，結合著無所不在的網路建設，帶動了普及運算(pervasive computing, ubiquitous

computing)[1]的發展，成為現今技術發展的一個新領域，個人化、需求導向、適切與適地性的商業模式也隨之出現。

1.2 研究動機

行動通訊技術的進步與無線網路環境的普及，帶給生活上更多的便利與科技創新的機會，但同時也產生許多衝擊與威脅。資訊安全過去一直都是學者專家所研究的重點之一，然而隨著網路攻擊等安全事件層出不窮，無線網路與其他網路基礎建設成為下一波首要的攻擊目標。過去針對資訊安全所做的事前防護措施：建立政策管理的機制、存取控制、帳號與密碼之驗證等，這些安全防護觀念與行為隨著通訊科技的改變而顯得更不足，更多安全性的漏洞被破壞與攻擊。

行動化使得使用者在存取資源時，不必再侷限於傳統的實體地點或固定的網路，反而擴展到任何時間、地點與隨身的手持設備上。這類型寬頻無線式撥接(Broadband Wireless Access, BWA)、遊牧式的環境(nomadic environment)也因為行動網路移動性的特性，使之與過去穩定式的環境(static environment)產生很大的差異。在移動式的環境中，有關網路架構、行動用戶目前的地點、時間、資源的可得性、行動裝置或執行環境等變數都必需加以考量，要能隨時地針對這些變動因子的改變，做出彈性地調整，給予適當的回應。

由IETF(The Internet Engineering Task Force)所制定的驗證、授權與計價的AAA架構(Authentication, Authorization and Accounting, AAA Architecture)，可以用作為驗證使用者身份、決定網路存取授權及資源使用計費程序的一個標準。這類型傳統的網路存取系統，僅透過帳號/密碼的機制來驗證不同使用者的連線要求，用以作為限制網路存取機制的

[1]普及運算：電腦運算技術之拓展，可創造一個無所不在的計算環境。目的要能了解使用者意圖來提供最適切的服務，同時還要做到對使用者最少的干擾。

基礎。在穩定式的環境中或許能有安全防護的作用，不過如果在游牧移動式的環境中，還是存在著許多需要被克服的困難：

1. 行動用戶的可移動性，不僅使用者的位置常發生非預期的改變，且會造成與資源之間的信任關係產生變化。

2. 僅利用帳號/密碼來做為網路使用者身份的辨識與授權，會產生安全性的漏洞(被盜用的可能)。網路上有關資源存取的限制，還必須考量到其他個人(角色)或環境上(時間、地點)的屬性。

3. 過去資安防護的行為上，透過定義存取控制清單(access control list)來限制資源的存取。不過隨著網路複雜性、移動性逐漸增加，服務提供者或網路業者無法事先完整地定義出所有可能會存取資源的個體與存取行為。

4. 無法保証最初所授予的網路存取權限，會在整個連線對話過程中，不論地點、時間或是其他的變動，都仍適用。

在如此動態的無線漫遊網路中(roaming network)，不論是外在環境變化或是使用者的移動，都會造成個人相關屬性的改變，而如何動態地調整安全政策、有效回應使用者需求、保障無線網路的安全正是目前AAA架構所必需解決的問題。另外一方面，傳統的存取政策從自由裁決型(Discretionary Access Control)、強制存取型(Mandatory Access Control)甚至延伸至角色定義型(Role-based Access Control)，將使用者依其屬性分類成不同的角色來限制資源的使用，已不足以滿足現今行動網路上多變且複雜的需求。要如何設計一個彈性的存取政策，根據目前環境來推論出適當的安全機制來實行，也是管理者在設計安全政策時必需考量的。

1.3 研究目的

由上述描述的問題可以發現到，在未來行動網路的趨勢下，傳統的AAA架構適必要作出調整與改變。為了滿足無縫漫遊(seamless roaming)環境的需求，不同網域內的AAA伺服器之間必須建立互信的關係，彼此溝通、傳遞有關使用者資訊，進而驗證身份並做出授權決策。另外在資源存取、授權的安全政策之定義與設計上，必須達到充分的動態性與彈性，藉以改善網路環境中的安全性問題。因此一個安全系統，能夠動態地根據週遭環境與持續變動的使用者資訊來執行授予或撤回資源存取權，具備重新調整系統的安全政策(reconfiguration)與適應新環境(adaptation)的能力。

本研究即以AAA架構為基礎，在漫遊與虛擬企業網路的環境(virtual private network, VPN)中，發展一個能滿足行動網路動態性要求的安全授權系統，做為無線網路安全之解決方案。主要目的描述如下：

1. 在分散式、移動式的行動網路中，系統能夠自動地蒐集有關目前服務環境、網路環境與使用者特性等資訊。這些動態改變的資訊會被定義為「情境(context)」。情境會隨著時間、地點或其他因素改變，而系統也要能偵測這些變動，進而調整系統的安全設定。

2. AAA架構中，會由AAA伺服器根據事先定義好的政策來執行身分驗證、存取授權與服務計時計費的程序。但是在傳統的系統中，這些安全政策都是預先針對固定的使用行為或身分來定義的，無法動態地去適應新的行動用戶行為或改變的環境資訊。因此在定義AAA架構中的存取控制的政策(access control policy)時，必須以動態的情境做為設計考量。根據不同的情境組合，來定義可允許的授權範圍。一旦情境發生變動，就會自動地驅動存取控制程序，重新評估新的環境條件來決定接受或拒絕資源的存取。

1.4 研究程序

本論文章節如下圖所示，主要分為三大階段來進行。第一階段先根據研究問題，找出相關的文獻來探討要如何解決在AAA架構與無線行動網路中所存在的安全性議題。第二階段會基於相關的理論基礎與假設，提出一個建立在AAA架構下的情境感知系統，並以情境作為存取政策設計之考量，並詳細地描述各元件功能與元間之間的溝通流程。最後則設計一個情境感知的存取政策，並描述相關的測試情境。

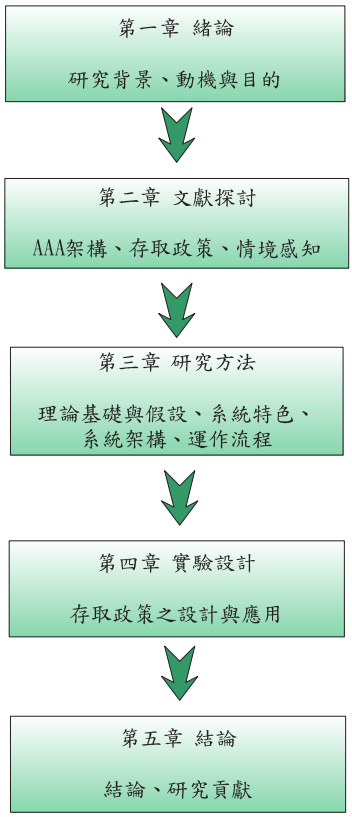

圖 1.1: 研究程序