可動態更新金鑰之 Mobile IP 安全註冊協定[1]

A Secure Mobile IP Registration Protocol with Dynamic Key Refreshment

黃明賢

中央大學資管所

s0433011@cc.ncu.edu.tw

陳奕明

中央大學資管所

cym@mgt.ncu.edu.tw

摘要

隨著無線網路存取需求增加，以 Mobile IP **提供使用者在** IP **網路下無縫隙漫遊**(seamless roaming)**的服務將是未來之趨勢，但近年來電腦網路安全威脅日深，** Mobile IP **此一協定亦有可能遭受如重送攻擊、會談盜用**(Session hijacking)**等惡意攻擊，因此近年來有越來越多的研究在探討如何設計一個安全的** Mobile IP **註冊協定（**registration protocol**）以防範此類攻擊。可是過去大部分的協定改進都要求行動節點（**Mobile Node, MN**）進行繁複的公開密鑰計算，未考慮到** MN **的計算能力有限的問題，以致在實用推廣上造成困難。為克服此問題，本文提出一套以對稱式加密法為基礎並以** Nonce **來達到相互認證同時可以動態變換通訊雙方通訊金鑰的安全註冊協定。和其他的類似研究比較，本協定具有以下特色：**(1)MN **註冊程序可與分配通訊金鑰的步驟結合，**(2)**通訊金鑰可動態更新，**(3)**可以防止重送及會談盜用等攻擊，**(4)MN **計算之軟硬體需求簡單，以及**(5)Scalability **較佳。為便於中英文之檢索，請務必填妥中英文對照之"論文題目"、"關鍵詞"及"摘要"。請於** 300 **字內，以中文或英文介紹本文之主要內容、目的、方法、結論等項目。**

關鍵詞：Mobile IP、**註冊協定、動態金鑰更新、重送攻擊、會談盜用**

Abstract

Along with the tremendous increase in the wireless network resource access, the mobile IP service which can provide user seamless roaming within IP network will be the future trend. However, as the threats to the computer network grow with time, the Mobile IP also becomes the attack target by malicious attackers. For example, during Mobile IP registration, if home agent is not able to authenticate the mobile node, the attacker may imitate legitimate user to freely use the network resource or prohibit the legitimate users to receive messages. So the registration protocol of Mobile IP need to be protected. Since mobile node's computation power is limited, we need to take into account the mobile node's computation power in designing a secure Mobile IP registration protocol. In consideration of these premises, in this paper, we propose a secure Mobile IP registration protocol which can dynamically refresh communication parties' session keys and achieve mutual authentication based on public-key based security scheme. Compare with others similar researches, our protocol has the following five features: (1) the mobile node's registration process can combine with the key distribution process, (2) session key can be refreshed dynamically, (3) it can prevent replay attack and session stealing attack, (4) the mobile node's hardware and software requirement is easy to meet, and (5) it has good scalability.

Key words: Mobile IP、Registration Protocol、Dynamic Key Refreshment、Replay Attack、Session Hijacking

一、簡介

近來無線網路設備成本降低，同時又提供比傳統有線網路更容易佈建之優點，愈來愈多支援無線網路標準之行動裝置(例如：PDA**、筆記型電腦、膝上型電腦、手機等)，對於利用無線網路存取** Internet **及** Intranet **資源之需**

[1]**本研究由國科會補助研究，為國家寬頻實驗網路（NBEN）研究計畫一部份，計畫編號：NSC-91-2219-E008-009**

求將更為增加，據 UMTS Forum所作的預測，到了 2010年，全球將有超過 17億以上的行動工作者[1]。這意味網際網路與電信網路技術兩者將整合，未來之網路環境將為全 IP(All IP)之環境，提供 IP 漫游(IP roaming)或 IP 行動性(IP mobility)將是未來之之趨勢[2]。但由於 IP Protocol 上之定址(addressing)及路由(routing)機制運作上之關係，通常假定電腦不會改變其網路接取點(point of network attachment) 。為了解決電腦移動位置又不失原先之網路連線，1996 年 Internet Engineering Task Force (IETF) 組織中之 Mobile IP 工作小組訂出名為 IP Mobility for IPv4[3] 此一機制，可克服原始 IP 定址模式對行動主機(Mobile Node，MN)移動時的限制，允許行動主機保留原來的位址。Mobile IP 的基本概念是無論行動主機移動到何處，它始終採用相同的ＩP 地址，並且維持處於 active 狀態的 TCP 連接，提供 MN 在不改變應用程式及 IP 的前提下，仍能夠漫遊於 IP 網路之中。當 MN 移動到另一個網路，該 MN 可以經由代理人（Agent）探索機制收聽代理人的廣播，或是主動送出訊息給代理人來取得一個臨時位址(Care-of Address，COA)，MN 漫游到外部網路(foreign network)，取得臨時位址後必須向其主代理人(Home Agent, HA)註冊其臨時位址，即將 Care-of Address 送回主網路上的 HA，用來連繫 MN 之永久位址(home address) 和 Care-of Address 之關係。而行動主機向 HA 註冊過程中，若註冊訊息未受到適當之安全機制保護，則會有若干安全威脅，例如重送攻擊(replay attack)、會談盜用(session hijacking)等攻擊[4]，為了確保註冊過程的安全，設計一安全的 Mobile IP 安全註冊協定有其必要性。

本文共分為五節，第一節為簡介，第二節針對 Mobile IP 的註冊協定相關研究作一回顧，並指出這些研究中其協定弱點，第三節對於前述協定缺點設計提出本文之可動態更新金鑰之 Mobile IP 安全註冊協定，第四節為此新協定與第二節所述各 Mobile IP 註冊協定在安全性及效率性上作一分析比較，最後第五節說明本文結論及未來研究方向。

二、Mobile IP 註冊協定相關研究

(一) Mobile IP 註冊協定

MN 雖然可以經由無線網路介面連上 Internet，但因為 MN 是可以隨意移動的，當它由一個網路接取點漫遊到另外一個網路接取點時，需要一個有效的機制來通知網路關於目前網路接取點改變的情形，此機制即為 Mobile IP 註冊協定，以便讓送給移動到目前網路接取點的 MN 之封包能夠完整的被 MN 所接收，其註冊程序如圖 1。雖然在 Mobile IP 中為避免註冊過程遭受重送攻擊使用了挑戰回應 (challenge/response) 機制及時戳(timestamp)兩種方法，但 Sufatrio 和 Lam認為 Mobile IP 註冊協定仍然容易遭受重送攻擊[4]。原始 Mobile IP 註冊協定的另一個缺點是其整個註冊過程中，當網路上有 m 個節點通訊時，就會有(m)* (m-1)/2 把金鑰之分配需求，這將造成通訊頻寬被佔用外，對於金鑰之管理也相當不易，故其延展性(Scalability)不佳。如果 MN-HA，MN-FA 及 FA-HA 間之共享秘密是經由事先約定並以手動方式預先設定好的話，則 Mobile IP 就不適合大範圍的漫游。為了解決 Mobile IP跨網域、大範圍漫游(即 Inter domain roaming)所需要的認證，於是便有各種針對 Mobile IP 金鑰分配之註冊協定出現，以下陸續加以介紹。

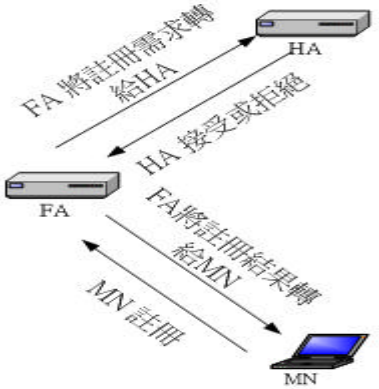

圖 1： 註冊程序

(二) Certificate-based 之 Mobile IP 註冊協定[5]

Ohzahata 將公開金鑰配合使用 Diffie-Hellman(D-H)金鑰交換法 [6] 應用到 Mobile IP 上，當 MN 於註冊過程中，MN、FA、HA 分別以 D-H 金鑰交換法算出 MN 與 FA 間，MN 與 HA 間及 FA 與 HA 間各自的通訊金鑰。Certificate-based 之 Mobile IP 註冊協定雖然解決了 Mobile IP 金鑰分配之問題，但此協定需有一公開金鑰基礎建設以便讓 MN、HA、及 FA 分別從 CA 獲得公開金鑰及 CA 之憑證，另外 MN 註冊過程所需之通訊金鑰係使用 Diffie-Hellman(D-H) 金鑰交換法來獲得，並未考慮到 MN 之運算資源是有限制的，而 D-H 金鑰交換法用到指數之運算，相對地會增加一些 MN 的負擔，安全性方面，此協定對於前面提到的重送攻擊亦無有效防止對策[5]。

(三) MinPub(Minimal Public Key Based)之 Mobile IP 註冊協定[4]

Sufatrio 及 Lam 提出的 MinPub 安全註冊協定多加了 FA-HA 間的挑戰回應機制，可以解決 Mobile IP 遭受重送攻擊之可能，同時 HA 還

可以當作金鑰分配中心(Key Distribution Center，KDC)來分配 MN-FA 間的通訊金鑰，該機制是以秘密金鑰(secret key)及公開金鑰(public key)互相結合為基礎，訊息驗證的方式在 MN 是使用秘密金鑰方式之訊息確認碼(MAC)驗證訊息，而在 FA 及 HA 端則是使用公開金鑰方式之數位簽章來驗證訊息，一來不會增加 MN 之運算負擔影響操作效率，二來 FA-HA 間可相互驗證，增加了 Mobile IP 註冊協定的安全性。

(四) MIP/AAA 之 Mobile IP 註冊協定[7][8]

由於 Mobile IP 機制中缺少對 Key 之分配管理，故 MN 僅適合於小範圍 (例如 Intranet) 內漫游（macro mobility）。

Certificate-based 之 Mobile IP 註冊協定雖可改進通訊金鑰之分配管理問題，但因為使用了 D-H 金鑰交換法來各自算出通訊所須之通訊金鑰，由於 D-H 金鑰交換法使用到指數之運算，相對地會增加一些 MN 的負擔，而 MinPub 之協定中，HA 作為金鑰分配中心，可改善通訊金鑰之分配問題，但因其需作 CRL (Certificated Revocation List) 之取得及驗證工作間接造成 HA 成為網路的瓶頸。在 MIP/AAA 之 Mobile IP 註冊協定中，Mobile IP 的註冊程序可以和分配通訊金鑰的步驟結合成一道程序，由 AAAH(Home Domain AAA Server)充當金鑰分配中心並以對稱式加密法來加密通訊金鑰，不會造成 MN 的運算負擔，可以加速 Mobile IP 註冊流程及分配通訊金鑰的步驟，不過此 MIP/AAA 之 Mobile IP 註冊協定仍易受重送攻擊及因通訊金鑰不經常變換容易被破解。

如上所述，Mobile IP 協定的基本安全弱點有下列幾項：

1. 沒有任何通訊金鑰分配機制
2. 易遭受重送攻擊
3. 易遭受會談盜用之攻擊
4. 通訊金鑰未能定期更新

而以上三種我們回顧的新 Mobile IP 註冊協定雖然設法改善這些弱點，但其設計本身也依然有缺點，這些缺點整理如表一所示：

表一： 三種新 Mobile IP 註冊協定之安全弱點列表

協定名稱	針對Mobile IP註冊協定改進之處	所使用之方法	缺點
Certificate-based 註冊協定	1.改進標準的Mobile IP 註冊協定之通訊金鑰分配	配合公開金鑰加密及 D-H 金鑰交換法	1. MN 運算負擔重 2.易遭受重送攻 3.易遭受會談盜用之攻擊
MinPub 註冊協定	1. 改進標準的Mobile IP 註冊協定之通訊金鑰分配	HA 當作金鑰分配中心	1. HA 成為網路的瓶頸 2.易遭受會談盜用之攻擊
	2.改進 MN 運算的負擔	訊息驗證的方式在 MN 是使用秘密金鑰方式之訊息確認碼(MAC)驗證訊息，而在 FA 及 HA 端則是使用公開金鑰方式之數位簽章來驗證訊息	
	3.改善重送攻擊威脅	挑戰/回應機制	
MIP/AAA 註冊協定	1.改進標準的 Mobile IP 註冊協定之通訊金鑰分配	使用現成之 AAA 並以 AAAH 作為金鑰分配中心	易遭受重送攻擊及會談盜用之攻擊
	2.改進 MN 運算的負擔	使用對稱式加密演算法	

三、可動態更新金鑰之 Mobile IP 安全註冊協定

為求研究之深入與減少複雜性，本研究作了以下幾項假設：

1. 行動主機的計算能力是有限制的，無法負擔複雜之運算。
2. 安全註冊協定架構中包括下列個體：MN (Mobile Node)、HA (Home Agent)、

FA(Foreign Agent)、AAAH(Home Domain AAA Server)、及 AAAL(Local Domain AAA Server)。其中 AAAH 及 AAAL 係利用 ISP 或網路運作者(Network Operators)現有之 AAA 伺服器(Authentication、Authorization and Accounting Server)，而 MN 與 AAAH 伺服器間 AAAH 與 AAAL 伺服器間、HA 與 AAAH 伺服器、FA 與 AAAL 伺服器間有一預先建立之信任關係(pre-established trust relationships)存在。

3. Mobile IP 未特別註明則專指 Mobile IP IPv4 (MIPv4)，MIPv6 專指 IPv6 版本之 Mobile IP。

根據上述假設的前提，為改善 Certificate-based、MinPub 及 MIP/AAA 之 Mobile IP 註冊協定之弱點，本文提出一套基於 MIP/AAA 機制並可以動態更新金鑰之 Mobile IP 安全註冊協定，我們所提的方法是以 MIP/AAA Mobile IP 註冊協定為基礎，再加上相互認證及動態變換 MN-HA 及 MN-AAAH 間之通訊金鑰之技術，可以避免重送攻擊、會談盜用等威脅，詳述如下：

(一) 可動態更新金鑰之 Mobile IP 安全註冊協定

我們的可動態更新金鑰之 Mobile IP 安全註冊協定其做法為：

1. 利用臨時訊息(Nonce)於 FA—AAAL、AAAL—AAAH、AAAH—HA 間及 MN—HA 間作挑戰與回應認證，來預防重送攻擊。
2. 利用前一次通訊金鑰作為部份參數，加上其他參數來產生本次的通訊金鑰，即 MN—HA 間之共享秘密(S_{MN-HA})可作為第一次 MN 註冊訊息(Registration Request Message)加密用之加密鑰匙 $SK_{MN-HA}=H(S_{MN-HA})$，第二次以後之加密鑰匙由下式導出：$SK_{MN-HA}^{+}=HMAC(SK_{MN-HA}, (N_{HA}^{-} \oplus N_{HA}))$，攻擊者就算破解了此次之通訊金鑰，除非亦同時破解前一次之 N_{HA}^{-}（N_{HA}^{-}是由前一次之通訊金鑰所加密），若不知道前一次之通訊金鑰，仍無法算出下一次之通訊金鑰。
3. 同樣地 MN—AAAH 間第二次以後之通訊金鑰($SK_{MN-AAAH}$)可由下式導出：$SK_{MN-AAAH}^{+}=HMAC(SK_{MN-AAAH}, (N_{MN} \oplus N_{MN}^{-}))$。

由於通訊金鑰經常動態更新，可以確保 Mobile IP 註冊協定的安全，以下詳述本協定。

A. 預先建立之信賴關係：

依 Mobile IP 之定義，MN 與 HA 間應有一信賴關係存在(圖 2)，故本文所提出之協定比 MIP/AAA 之 Mobile IP 安全註冊協定多了 MN 與 HA 間有一信賴關係存在之假設，預先建立之信賴關係如下：

1. MN 與 AAAH 間有一預先建立之信賴關係(pre-established static trust relationship)及 MN 與 HA 間有一預先建立之信賴關係(因為 MN 隸屬於該主網路(home domain))。
2. AAAL 與 AAAH 間有一預先建立之信賴關係(否則彼此間交換之認證訊息將不被雙方信賴)。
3. FA 與 AAAL 間有一預先建立之信賴關係(以便讓 FA 確信 AAAL 可以授權 FA 對 MN 提供本地資源給 MN 使用)。
4. HA 與 AAAH 間有一預先建立之信賴關係。

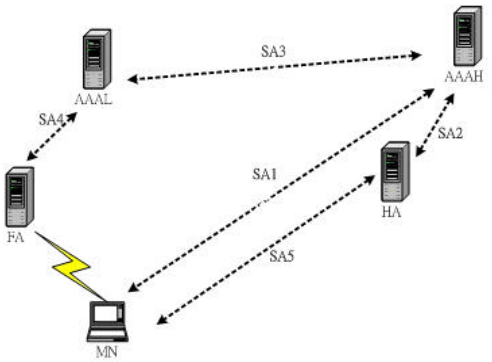

圖 2 ：可動態更新金鑰之 Mobile IP 安全註冊協定預先建立之信賴關係

B. AAA Server 主要任務：

1. 起始(initiate)與 致能(enable) Mobile IP 註冊之認證(Authentication of Mobile IP registration)。
2. 授權 MN 可以使用 Mobile IP 之服務。
3. AAAH 當作金鑰分配中心(KDC) 分配 MN-FA、FA-HA 間之通訊金鑰(Session Key)，而 K1 及 K2 這兩個通訊金鑰 (圖 3)，將被用於後續 Mobile IP 註冊訊息認證之用。

B. 挑戰與回應認證機制：

可動態更新金鑰之 Mobile IP 安全註冊協定使用了挑戰與回應機制，在 MN 與 HA 間使用了挑戰與回應相互認證機制，而其他參與個體間則只用到單向認證(挑戰與回應認證機制其挑戰亂數參見圖 4)，使用此挑戰與回應機制使『可動態更新金鑰之 Mobile IP 安全註冊協定』可以用來預防攻擊者重送(Replay)

之攻擊。

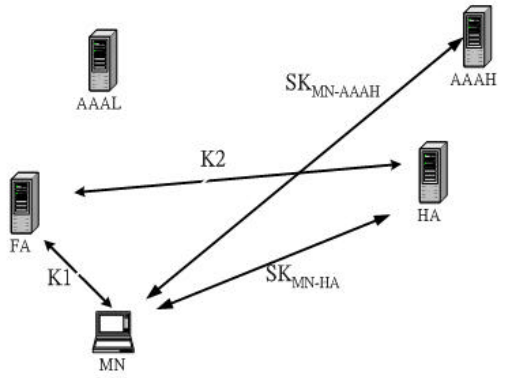

圖 3：可動態更新金鑰之 Mobile IP 安全註冊協定動態建立之信賴關係

C.可動態更新金鑰之 Mobile IP 安全註冊協定訊息流程：

訊息流程：為說明方便，本協定所用符號意義如下(表二)：

1.FA→MN： **(Advertisement｜N_{FA})**

FA 規律持續地送出廣播訊息(包含表明自己身份的 NAI_{FA} 及由 FA 產生之 Nonce(N_{FA}).

2. MN→FA： **A2= (M2｜<M2>$SK_{MN-AAAH}$)**

其中 M2=({M2a}SK_{MN-HA} ｜NAI_{MN}｜N_{FA}｜{N_{MN}}$SK_{MN-AAAH}$).

M2a =(RQ｜NAI_{MN}｜N_{MN}｜N_{FA}).

而 N_{MN} 為 MN 對 HA 之挑戰亂數(Challenge). 另外

$SK_{MN-AAAH}$= H($S_{MN-AAAH}$) ⊕ $S_{MN-AAAH}$

SK_{MN-HA}= H(S_{MN-HA}) ⊕ S_{MN-HA}

在 MN 送給 FA 之訊息中，MN 將包含註冊需求(RQ)之訊息(M2a)以 SKMN-HA 加密，然後再以 SMN-AAAH 再對訊息 M2 作 MAC 運算，最後將訊息 A2 送往 FA。FA 首先檢查 NFA 是否是最新的(Fresh)，如果不是則拒絕 MN 此次之註冊，否則接受 MN 此次之註冊並將此註冊需求之訊息轉給 AAAL.

3. FA→AAAL： **A3=(M3｜<M3>$S_{FA-AAAL}$)**

其中 M3=(Message in A2｜N_{FA1})而 N_{FA1} 為此次註冊 FA 對 AAAL 之挑戰亂數，當 AAAL 收到後先驗證 <M3>$S_{FA-AAAL}$ 之確認器(Authenticator)，如果驗證結果不正確表示該訊息可能已經被竄改了，如果驗證結果正確則繼續檢查 N_{FA1}，如果檢查結果正確就接受此訊息並並將此訊息轉給 AAAH.

4. AAAL→ AAAH：

A4=(M4｜<M4>$S_{AAAL-AAAH}$)

其中 M4=(Message in A2｜N_{FA1}｜N_{AAAL1}) 而 N_{AAAL1} 為此次註冊 AAAL 對 AAAH 之挑戰(Challenge)，當 AAAH 收到 AAAL 送過來之訊息後若 AAAH 一切驗證都沒問題則 AAAH 將 N_{MN} 解碼，並計算下一次通訊所須之通訊金鑰即 AAAH 下次 MN-AAAH 之通訊金鑰：

$SK_{MN-AAAH}^{+}$ = **HMAC($SK_{MN-AAAH}$，(N_{MN} ⊕ N_{MN}^{-}))**，其中 N_{MN}-為上一回合 MN 對 HA 所送出之挑戰 (Challenge) 亂數。

5. AAAH→ HA：

A5=(M5｜<M5>$S_{AAAH-HA}$)

其中 M5= (Message in A2｜N_{FA1}｜N_{AAAL1} ｜ N_{AAAH1} ｜ {K2}$S_{AAAH-HA}$ ｜ {K1}$SK_{MN-AAAH}$)而 N_{AAAH1} 為此次註冊 AAAH 對 HA 之挑戰亂數, K2 為 AAAH 分配給 FA-HA 間之通訊金鑰並以 $S_{AAAH-HA}$ 加密，K1 為 AAAH 分配給 MN-FA 間之通訊金鑰並以 $SK_{MN-AAAH}$ 加密。當 HA 收到 AAAH 送過來之訊息後採取之行動如圖 5，若 HA 一切驗證都沒問題則 HA 將接受 MN 此次的註冊，並計算下一次 MN，HA 間之通訊金鑰即

SK_{MN-HA}^{+} = **HMAC(SK_{MN-HA}，(N_{HA}^{-} ⊕ N_{HA}))**，而 N_{HA}^{-}為上一回合 HA 對 MN 所送出之挑戰亂數.

6. HA→AAAH： **A6=(M6｜<M6>$S_{AAAH-HA}$)**

其中 M6={M6a ｜ <M6a>SK_{MN-HA} ｜ N_{AAAH1}｜N_{AAAL1}｜N_{FA1}} 且

M6a=(Result ， {Result ｜ RP ｜ {N_{HA}}SK_{MN-HA} ｜ {N_{MN}}SK_{MN-HA} ｜ {K1}$SK_{MN-AAAH}$})而 N_{HA}為預備下一次MN 註冊時 HA 對 MN 之挑戰亂數，N_{AAAH1}為此次註冊 HA 對 AAAH 之挑戰回應(Response)。

7. AAAH→AAAL：

A7=(M7｜<M7>$S_{AAAH-AAAL}$)

其中 M7={M6a ｜ <M6a>SK_{MN-HA} ｜ N_{AAAL1}｜N_{FA1}}｜{K1｜K2} $S_{AAAH-AAAL}$).

而 N_{AAAL1}為此次註冊 AAAH 對 AAAL 之挑戰回應(Response)，在 AAAH 送給 AAAL 之訊息中包含了 MN 之註冊結果以及用 $SK_{MN-AAAH}$ 加密之 K1 和以 $S_{AAAH-AAAL}$加密之(K1｜K2) $S_{AAAH-AAAL}$，當 AAAL 收到 AAAH 送過來之訊息後若 AAAL 一切驗證都沒問題則將加密 之 K1 及 K2 解密(如圖 6)，並將訊息轉給 FA。

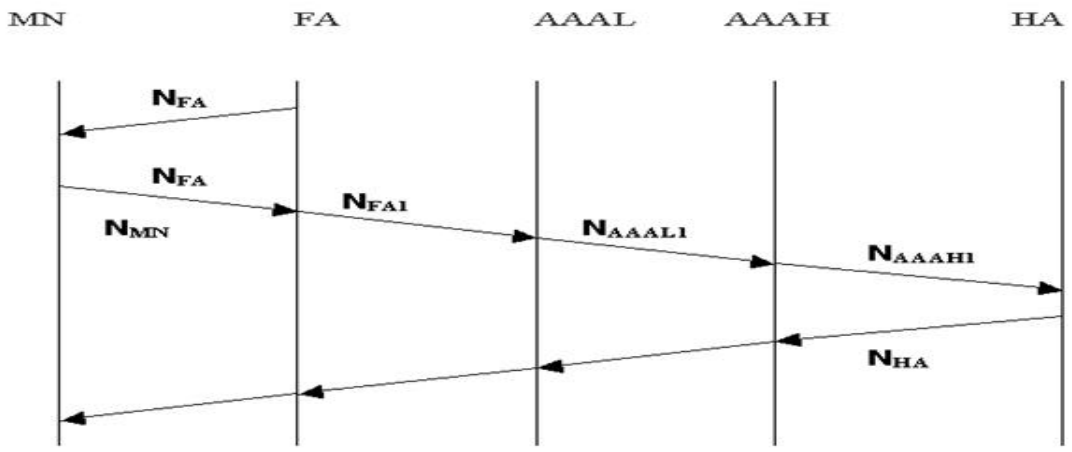

圖 4： 可動態更新金鑰之 Mobile IP **安全註冊協定挑戰與回應訊息流程**

表二：可動態更新金鑰之 Mobile IP **安全註冊協定符號意義**

符號	**代表意義**	**符號**	**代表意義**
AgentAd	**用來表示**Agent **的廣播訊息**	RQ	MN **的註冊需求訊息**
Request	**註冊需求訊息內代表註冊需求之欄位**	Result	MN **註冊結果**
RP	MN **的註冊回應**	MN	Mobile Node
FA	Foreign Agent	HA	Home Agent
AAAL	Local Domain AAA Server	AAAH	Home Domain AAA Server
<M>K	**訊息**M**用** Key K**所產生的訊息確認碼**	{M}K	**訊息**M **用**key K **來加密**
$\{K_A \mid K_B\}S$	**以**S**加密** K_A **及** K_B	(M ｜ N)	**包含**M,N**的訊息**
X→Y	X**將訊息傳送給**Y	$(m,n\ldots..)_K$	**以**key K**對序列**m,n…..**加密**
N_X	X**的**Nonce(**例如：** N_{FA}**為**FA **的**nonce).	NAI_X	X**的**Network Access Identifier
S_{X-Y}	**為**X-Y **間共享之秘密鑰匙** (**例如** S_{FM}**、** S_{HM}**、** S_{FH} **分別為**FA-MN,HA-MN **及** FA-HA**間共享之秘密鑰匙**).		
SK_{X-Y}	**為**X-Y **間之通訊金鑰(例如**SK_{MN-FA}**：**MN**、** FA**間之通訊金鑰**)		
HMAC(K，M)	**以**K**對訊息**M**所作之**HMAC**運算**		

```
HA_ Action ( )
        {
         Check the Authenticator;
            If Authenticator is invalid then return a code indicating messages is modi-
                                fied ;
           Else Check N_AAAH1 ;
            If N_AAAH1 is not fresh then reject the registration request ;
                  Else Binding the MN COA、 Home address、lifetime ;
                                compute next time MN-HA'Session key ;
                                Reply the registration request ;
                               go to the next step;
        }
```

圖 5：可動態更新金鑰之 Mobile IP **安全註冊協定**-HA **採取行動**

8. AAAL→ FA： A8= (M8 ｜ <M8> $S_{AAAL-FA}$)

其中 M8={M6a ｜ <M6a>SK_{MN-HA} ｜ N_{FA1} ｜ {K1 ｜ K2} $S_{AAAL-FA}$)

而 N_{FA1} **為** MN **此次註冊過程中** AAAL **對** FA **之回應**(Response)**，當** FA **收到** AAAL **送過來之訊息後，如果** MN **此次註冊成功則** FA **將已加密之** K1 **及** K2 **解密，並將結果轉給** MN**。**

9. FA→ MN： A9=M9

其中 M9={M6a ｜ <M6a>SK_{MN-HA} }

而 N_{MN} **為此次註冊** HA **對** MN **之挑戰回應**(Response)**，當** MN **收到** FA **送過來之訊息後所採取之行動如圖** 7**，如果** MN **此次註冊成功則** MN **將已加密之** K1 **解密，並計算下一次通訊** MN **與** AAAH **間之通訊金鑰和下一次通訊** MN **與** HA **間之通訊金鑰，即：**

$SK_{MN-AAAH}^{+} = HMAC(SK_{MN-AAAH}, (N_{MN} \oplus N_{MN}^{-}))$.

$SK_{MN-HA}^{+} = HMAC(SK_{MN-HA}, (N_{HA}^{-} \oplus N_{HA}))$

```
AAAL_Action1 ( )
  {Check the Authenticator ;
        If Authenticator is invalid then return a code indicating messages is modified;
        Else check N_AAAL1 ;
              If N_AAAL1 is invalid then return a code indicating replay attack;
                    Else read the registration result ;
                          If result =1 then accept the reply ;
                                Decrypt K1& K2 ;
                                go to the next step;
                              Else go to the next step ;
                    }
```

圖 6**：可動態更新金鑰之** Mobile IP **安全註冊協定**-AAAL **採取行動**

```
MN_ Action1 ( )
    {Check the Authenticator ;
      If Authenticator is invalid then return a code indicating messages is modified ;
        Else check N_MN ;
          If N_MN is invalid then return a code indicating replay attack ;
              Else read the registration result ;
              If result =1 then Decrypt RP;
                    Decrypt K1;
                  compute next time MN-HA'Session key ;
                  compute next time MN-AAAH' Session key ;
                      Else exit ;
    }
```

圖 7**：可動態更新金鑰之** Mobile IP **安全註冊協定**-MN **採取行動**

四、安全性及效率比較分析

本文提出的協定在安全性及效率上與其他 Mobile IP **註冊協定比較起來擁有諸多優點，此處分別對我們提出的協定與其他** Mobile IP **註冊協定做一比較分析，並描述** MN **在不增加計算負擔下，如何防範其他** Mobile IP **安全註冊協定所不能防範的攻擊**

(一) Mobile IP 安全註冊協定之安全性比較分析

A. **重送攻擊：首先就防範重送攻擊來討論，傳統的** Mobile IP **註冊協定無法抵擋重送攻擊，**MinPub **之** Mobile IP **註冊協定考慮到此一安全威脅，故** MinPub **之方法可以防範重送攻擊，**Certificate-based **之** Mobile IP **註冊協定並沒有此防範重送攻擊之機制，**MIP/AAA **之** Mobile IP **註冊協定雖考慮到重送攻擊之可能，故在註冊協定中使用了挑戰與回應機制，但發出挑戰亂數者其對應之回應，並非由發出此一挑戰亂數者所驗證，**MIP/AAA **之** Mobile IP **註冊協定仍有可能遭受重送攻擊。我們的可動態更新金鑰之** Mobile IP **安全註冊協定於註冊過程當中亦使用了挑戰與回**

應機制，且發出挑戰亂數者，對方之回應，就由發出此一挑戰亂數者所驗證，並全程於 MN—FA、FA—AAAL、AAAL—AAAH、AAAH—HA 及 MN—HA 間作挑戰與回應認證，可以確保註冊需求是最新的註冊需求，故可以達到預防重送攻擊之要求。

B. 註冊訊息是否可能遭受竄改或被冒名頂替：關於註冊過程當中，註冊訊息是否可能遭受竄改或被冒名頂替？由於在我們的協定中，使用了對稱式加密之訊息確認碼(MAC)，可以確認收到之訊息沒有遭到更動。如果攻擊者更動了訊息但未更動 MAC 則攻擊者計算出來之 MAC 會與收到之 MAC 不同，訊息被攻擊者竄改後很容易被對方偵測到，故訊息之完整性可以獲得確保，而且因為攻擊者不知道通訊雙方之共享金鑰，無法算出正確之 MAC，故可以確定訊息的確是來自合法之通訊端點，不怕通訊雙方被冒名頂替。

C. 通訊金鑰動態變換：為了加強協定之安全性，通訊金鑰應該經常變換，以免遭受攻擊者以離線字典法(off-line dictionary)之方法破解，在與我們的協定做比較的各種方法中，並未考慮動態變換通訊金鑰的機制，我們提出的協定中，MN 與 AAAH 間之通訊金鑰是由前一次之通訊金鑰運算所推導出的即 $SK_{MN\text{-}AAAH}^{+} = HMAC(SK_{MN\text{-}AAAH}, (N_{MN} \oplus N_{MN}^{-}))$，而 MN 與 HA 之通訊金鑰亦是由前一次之通訊金鑰加上部分參數(N_{HA}，N_{MN})運算所推導出的即 $SK_{MN\text{-}HA}^{+} = HMAC(SK_{MN\text{-}HA}, (N_{HA}^{-} \oplus N_{HA}))$，其中參數，像 N_{HA}，N_{MN} 是經過加密過的，更不容易被取得。而且本次使用的通訊金鑰是(Session Key)由上次註冊過程中，由雙方各自先行計算出來的，在前次通訊中並沒有公開傳遞，攻擊者更加不易取得此通訊金鑰，因此整個通訊金鑰的安全性是比前幾種方法可靠。

D. 會談盜用(Session hijacking)：會談盜用是一種主動形的資訊竊取方式，其他幾種方式因為未對註冊訊息加密，攻擊者可能偽造註冊被拒絕之訊息(例如 home agent unreachable、home network unreachable、insufficient resources 等偽造之訊息)給合法之 MN，因未對註冊訊息及回應加密，此種會談盜用之攻擊仍有可能成功。針對此一攻擊的有效解決方法為對訊息加密，我們的機制對 MN 的註冊訊息以 $SK_{MN\text{-}HA}$ 來加密，可以有效地防止此種攻擊。

(二) Mobile IP 安全註冊協定之效率分析比較

MN(Mobile Node)：由於計算上非對稱式密碼系統較對稱式密碼系統所須之運算資源、運算複雜度及速度為高，MN 註冊過程若使用對稱式密碼系統來運作，不僅不需要增加額外軟、硬體需求，整體的運作效能也更為提高。我們的協定使用了對稱式密碼系統，由於計算之軟硬體需求簡單，效率自然比 MinPub 之 Mobile IP 註冊協定、Certificate-based 之 Mobile IP 註冊協定等 Mobile IP 註冊協定效率上要來的好。以下對各種安全註冊協定之安全性及效率做一綜合比較如表三：

五、結論與未來研究方向

因 Mobile IP 本身並沒有任何通訊金鑰分配機制，且 MN-FA 間、FA-HA 間之認證並非強制性的，這對 Mobile IP 之延展性及安全有不良之影響。Sufatrio[4] Ohzahata[5]、Perkins[7]等針對此缺失提出解決方法，但這些方法大都要求行動節點進行繁複的公開密鑰計算，未考慮到 MN 的計算能力有限的問題，以致在實用推廣上造成困難。為克服此問題，我們在本文提出的方法是以 MIP/AAA 之 Mobile IP 註冊協定為基礎並加以改良，我們的方法具有下列優點：

1. MN 註冊程序可與分配通訊金鑰的步驟結合，簡化 Mobile Node 註冊過程及分配通訊金鑰的步驟。
2. 通訊金鑰可動態更新，如此可避免過程中遭受通訊金鑰的洩漏之危險，避免 Mobile IP 安全註冊協定可能遭受之攻擊。
3. 可以防止重送及會談盜用等攻擊。這是因為我們在協定裡使用了挑戰/回應之認證機制及註冊訊息使用加密處理故可以防止重送及會談盜用等之攻擊。
4. MN 計算之軟硬體需求簡單。本協定中的 Mobile Node 註冊過程因使用對稱式密碼系統來運作，不需要增加額外軟、硬體需求，整體的運作效能也更為提高。
5. 延展性（Scalability）佳。由於本協定中 MN-HA、MN-FA、FA-HA 間為動態建立之信任關係，解決大部分人工建立信任關係之缺點（人工建立信任關係適合在小區域範圍內施行），故本協定之延展性佳。

在未來研究方面，我們認為本協定的安全性未來可以朝向使用 BAN Logic[9]來加以驗證，另外在此協定中，雖然在計算上使用的是運算資源需求及運算複雜度較低而運算速度較快的對稱式加密系統，但未來可以朝

向減少 Mobile Node 註冊過程當中訊息交換個數及簡化分配通訊金鑰的步驟上繼續加以研究探討。

表 三： Mobile IP 安全註冊協定的比較

項目	Mobile IP 安全註冊協定	Certificate-based 之 Mobile IP安全註冊協定	MinPub之 Mobile IP 安全註冊協定	MIP/AAA之 Mobile IP安全註冊協定	可動態更新金鑰之 Mobile IP安全註冊協定
MN 的密碼系統	Secret Key	Public Key	Secret Key	Secret Key	Secret Key
MN 的計算負擔(指數運算數)	輕 0	重 10	輕 0	輕 0	輕 0
HA 和FA 的密碼系統	Secret Key	Public Key	Public Key	Secret Key	Secret Key
訊息驗證機制	MAC	MAC+ Digital Signature	MAC+ Digital Signature	MAC	MAC
通訊金鑰分配方式	手動設定	D-H 金鑰交換	由 HA 當 KDC	由 HA 當 KDC	由 AAAH 當 KDC
防止重送攻擊	否	否	否	否	是
防止會談盜用	否	否	否	否	是
通訊金鑰更新	否	否	否	否	是
Scalability	差	佳	中等	佳	佳

六、參考文獻

[1] http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/MultiMedia_PDFs_Reports_report08executive-summary.pdf. (2 Feb., 2003).

[2] B. Stiller, L. Kacnelson, C.E. Perkins and P. Dini, "Mobility in a future Internet." Proceedings of 26th Annual IEEE Conference on Local Computer Networks, LCN 2001, 2001, Page(s): 24 –30.

[3] C.E. Perkins, "Mobile IP Support for IPv4." IETF RFC 3344, Aug. , 2002

[4] Sufatrio and Yan Lam Kook, "Mobile IP registration protocol: a security attack and new secure minimal public-key based authentication." Proceedings of Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN '99), Perth/Fremantle,Australia,23-25,Jun.,1999,Page(s): 364 –369.

[5] Satoshi Ohzahata, Shigetomo Kimura and Yoshihiko Ebihara,"A Fast Authentication Method for Secure and Seamless Handoff. "6th International Conference on Information Networking, 30 Jan.-2 Feb., 2002.

[6] W. Diffie and M. Hellman, "New Directions in Cryptography." IEEE Transactions on Information Theory, November 1976.

[7] C.E. Perkins, "Mobile IP joins forces with AAA." IEEE Personal Communications [see also IEEE Wireless Communications], Aug. 2000.

[8] G. Schaefer, A. Festag and H. Karl, "Current Approaches to Authentication in Mobile and Wireless communications." Technical University Berlin, Telecommunications Network Group, Version 1.0, 26 Mar., 2001.

[9] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication." 1990.