行政院國家科學委員會專題研究計畫　成果報告

—個針對無基礎行動網路的代理簽章機制

計畫類別：個別型計畫
計畫編號：NSC94-2416-H-009-017-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：國立交通大學資訊管理研究所

計畫主持人：羅濟群

計畫參與人員：黃俊傑、周士宏、林彥紹

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 95 年 10 月 26 日

行政院國家科學委員會專題研究計畫成果報告

一個針對無基礎行動網路的代理簽章機制

A Proxy-Signature Scheme for Mobile Ad-Hoc Networks

計畫編號：NSC 94－2416－H－009－017－
執行期限：94 年 8 月 1 日至 95 年 7 月 31 日

主持人：羅濟群　　國立交通大學資訊管理研究所
計畫參與人員：黃俊傑、周士宏、林彥紹　　國立交通大學資訊管理研究所

中文摘要

無基礎行動網路它是由一群有線無線設備的所組成的通訊平台。它可以在任何地方或時間，可依其需要建立起一個互連的網路架構，由於它具有不需藉由無線擷取器等設備提供通訊服務，而是藉由自我組成之能力以構成路由環境，因此，它非常適用於災難救助、軍方作戰演訓及辦公室會議環境使用。但由於它具有動態拓樸及無線網路環境所形成的弱連結現象，使得它在實際應用面所遇到的安全問題較傳統的有線網路及無線網路環境更為複雜。

在此網路平台上雖具有上述的優點，但由於具有動態拓樸，使得資訊安全問題及其服務提供方式，與無線網路所討論的架構有所不同。本研究將針對資訊安全之代理簽章問題，設計一個符合無基礎行動網路環境所需的架構。所謂代理簽章指的是，若原始簽章者若無法執行簽章服務，亦可以指定一位代理人來幫他執行簽章的動作以產生有效的數位簽章。

基於上述概念，本研究提出一個稱之為分散式提名代理簽章機制。於此機制下，原始簽章者可以指定簽章的驗證者，以避免代理簽章者誤用之情形。另外，為保證網路上有節點可以執行上述之角色，本文提出具門檻機制的代理簽章者及驗證者，如此，可確保在無基礎行動網路架構下代理簽章執行的可行性及提供分散處理機制，以解決無線網路設備的問題。最後，藉由安全性分析與效率分析，說明本研究所提的架構之安全性與可行性。

關鍵字：無基礎行動網路、代理簽章、分散式提名代理簽章

Abstract

A mobile ad-hoc network, MANET, is a kind of communication network, and is composed of wireless devices. In this network, the mobile nodes, such as PDA, notebook, mobile phone, etc., can construct communication network and provide routing ability by self-organized without the help of access point in wireless network. Hence, it is more suitable in emergency, battle network, and conference environment. However, the security issues are the big problems in these networks because of its dynamic topology and weak link in wireless network. Security services, like authentication, data encryption/decryption, digital signature, etc..

According to the above conception, we will propose a new proxy signature scheme, called distributed nominative proxy signature in MANET. In our scheme, we can prevent proxy signer from the proxy key misuse. In addition, we will introduce threshold scheme into our system to provide multi-proxy signers and multi-verifiers. Therefore, the flexibility and the ability of distributed processing will be guaranteed in this network. We make proxy signature scheme more efficient and secure under the restriction of the dynamic topology, infrastructureless and wireless network constraints in the MANET environment. Finally, security analysis and complexity analysis present the scheme we proposed is more secure and efficient than the others.

Keywords: Mobile Ad Hoc Network, Proxy Signature, distributed nominative proxy signature

一、緣由與目的

無基礎行動網路，它是屬於無線網路的一種。它與一般的無線網路不同之處，在於它不需一個無線擷取器(Access point)的存在，而是藉由該網路節點彼此間構成路由架構，以建構此無線區域網路。換句話說，在此環境中由於節點間的通訊並不須預存一個基礎網路的設置，它們彼此間能自我組成(Self-Organize)完成構連，建立起通訊管道，而當兩個節點間已超過無線電電波範圍，則另一個節點立即具有路由功能，藉此搭起此兩通訊機間通訊通道。因此，它是一個具有多階性、動態拓樸與不可信賴的通訊通道。故在此架構下，資訊安全問題顯得特別複雜且重要。例如，認證機制、資料加解密及數位簽章等服務之提供。其中又以數位簽章服務為本研究探討之重點。該服務可以確保原始簽章者所簽署文件之有效性、可驗證性及確保原始簽章者與簽章的接收者之不可否認性。但由於在無基礎行動網路下，每個節點均呈現動態的移動，因此，無法提供數位簽章的服務；而需藉由代理簽章的服務以滿足此目的。

所謂代理簽章機制，它是一種特殊的數位簽章機制，亦即是說，簽署者可委託某一個人，代理它完成文件的簽署，且驗證者能驗證此簽章之有效性與來源性。藉由此機制可以確保原始簽章者達到簽章之目的。故本研究基於此架構下，提出一個稱之為分散式提名代理簽章機制。於此機制下，原始簽章者可以指定簽章的驗證者，以避免代理簽章者誤用之情形。另外，提名式代理簽章十分適合用在行動通訊的環境。在行動通訊中，使用者就像是原始簽章者，代理者則像是代理簽章者，由於提名式代理簽章只能由被提名者來驗證，因此使用者及代理者的身份都可以被保密。除了保密性的優點，一般的行動裝置本身的計算能力及電力都較為缺乏，透過代理簽章的方式，原始簽章者就可以把簽章原本要執行的大量計算，例如大量的模數與指數計算，交付給代理簽章者來做，以節省電力。另外為解決現行以提名為基底之代理簽章機制，在無基礎行動網路環境下，由於節點移動快速且沒有無線擷取器提供路由導致路由中斷，也使得無法提供代理簽章之服務，本研究試圖提出一個具門檻機制之以提名為基底之代理簽章機制，以滿足分散式及動態移動之無基礎行動網路的環境要求。

本研究之章節架構如下：第二章我們將藉由文獻探討，來熟悉無線網路架構上的差別，並介紹現有的代理簽章機制；第三章為本研究之方法，將說明分散式提名代理簽章機制及其演算法。此外，藉由安全性分析與效率分析，說明本研究所提的架構之安全性與可行性；第四章為本研究之結論與建議；最後，於第五部分就本研究提出計畫成果自評。

二、文獻探討

本小節將就無基礎行動網路環境做介紹，及就現有的代理簽章機制做概略性文獻討論。

2.1 無基礎行動網路環境

在無基礎行動網路環境中，節點間可以做直接的通訊，也能隨意移動，並繼續保持節點間連線的狀態。無基礎行動網路是由無線裝置自行建立的區域網路環境，其中並無無線擷取器或橋接器，它是一種能夠在沒有事先建置基礎架構的環境下，讓各個節點透過彼此點對點連結所臨時組成的網路，使得節點間彼此之間能夠互相傳送資料。

而無基礎行動網路最主要的特色包括動態拓樸及具有自我組織的能力[4] [12] 。由於具有動態拓樸的特性使得各個連結設備可以任意移動位置，且還能繼續和其他節點做溝通；而因具有自我組織，使得一方面它不但可以簡化網路的管理，提高其強健性(robustness) 和彈性，另一方面，它更能在處於動態的狀況下，像位置移動、不定的連結、和無法預測的流量負載的既定基礎結構下，作最理想的資源有效使用。

2.2 代理簽章機制分類與特性

代理簽章是源始於數位簽章的觀念而來。數位簽章，它是一種無法被偽造的資料，它代表了原始發訊者同意了附有其數位簽章的電子文件。數位簽章比起手寫的簽名字跡提供更高的安全。收到具有數位簽章訊息的人也可以用簽章來得知發訊者的身分，進而確認訊息的內容在經過簽章後是否遭受故意或是意外的竄改。另外，由於數位簽章具有不得否認的特性，所以若使用者在訊息上使用了數位簽章，則他將無法狡辯其簽章遭到偽造而逃避曾經撰寫過此訊息的事實。簡單的說，數位簽章在數位訊息中所扮演的角色為 鑑別 。它可以讓收訊者對於訊息的來源及其完整性更有信心。但由於在無基礎行動網路下，每個節點均呈現動態的移動，因此，對節點而言很難提供數位簽章的服務；有鑑於此，我們必須設計滿足此作業環境，但仍具有簽章效果的機制。此機制即為代理簽章。

所謂代理簽章機制，它是一種特殊的數位簽章機制，亦即是說，簽署者可委託某一個人，代理它完成文件的簽署，且驗證者能驗證此簽章之有效性與來源性，其架構如下圖 一。

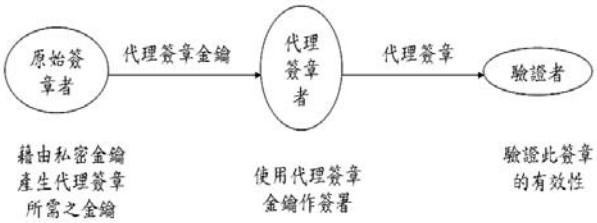

圖 一：代理簽章架構

最早討論代理簽章是由 Mambo 等學者於 1996 年所提出[6] ，他們所提的概念是原始簽章者可以指派一個代理人來代為簽章，而此代理人所簽署文件的效力就等同原始簽章者一樣。之後，陸續有學者提出新的代理簽章機制，例如：門檻式代理簽章(Threshold Proxy Signature)[8] [9] [11] 與多重代理簽章[1] 等等。於代理簽章機制，原始簽章者授予代理簽章者之授權方式大致而言，可區分下述幾種：

- 完全授權：所謂完全授權可以想成代理簽章者就是原始簽章者，亦即是說原始簽章者將其簽章所需的私密金鑰交給代理簽章者，此時代理簽章者就如同它的分身。此種授權方式非常危險，因為代理簽章者擁有它的私密金鑰，所以它可以隨意簽署任何文件，而原始簽章者無法約束，且驗證者無法從所簽署之文件辨別是由原始簽章者所簽署或是由代理簽章者所簽署，故無法滿足上述之特性。
- 部份授權：原始簽章者授予代理簽章者權力時，並非將個人的私密金鑰直接送給代理簽章者，而是利用個人的私密金鑰經過一系列的計算而產生代理金鑰，然後再將此代理金鑰送給代理簽章者。因此，代理簽章者可利用此金鑰產生代理簽章。由於原始簽章者所持的金鑰與代理簽章者所持代理金鑰不一樣，因此，驗證者可以區別此簽署文件是由誰所簽署。而在此授權模式下，又可區分成兩種狀況：第一種，代理簽章者直接使用原始簽章者所產生代理金鑰，然後對文件作簽署，此種方式雖可區別原始簽章與代理簽章之不同，但對代理簽章者而言並不公平，因為假若原始簽章者利用此代理金鑰對文件簽署，對驗證者而言，它會認定此文件是由代理簽章者所簽署，所以代理簽章者必須概括承受，故有第二種方式。第二種方式，即代理簽章者收到原始簽章者送過來的代理金鑰，並非直接使用它，而是將它與自己的私密金鑰再經過一系列的計算，以產生新的代理金鑰，當有文件需要簽署時，則使用新的代理金鑰加以簽署，當然此架構仍需滿足代理簽章機制之要求，但它也解決了公平性問題，亦即是說，原始簽章者由於沒有代理簽章者之代理金鑰，故無法假冒代理簽章者對文件作簽署。
- 授權憑證：此種授權方式即由原始簽

章者產生一個授權憑證給代理簽章者，而此授權憑證乃利用原始簽章者之私密金鑰簽署後產生，此憑證內容除了包括代理簽章者有權力代為執行簽章外，還需包括代理權限與期限及可簽署文件的類型等等。代理簽章者拿到此憑證之後，即可利用自己的私密金鑰簽署所代簽之文件，並將憑證一起送給接收者。而驗證者它除了需驗證此簽署文件的正確性外，還需檢查此憑證之合法性，以確保是否由原始簽章者授權給此代理簽章者簽署此份文件。

- 結合授權憑證之部份授權：此授權機制是將第二種與第三種的授權機制結合起來。原始簽章者先設定代理簽章者所應具有的權力，例如上述的代理權限與期限、可簽署文件的類型等等，然後再利用自己的私密金鑰連同所規範的簽署權力加以計算，再將結果送至代理簽章者。代理簽章者收到此訊息後，即利用此訊息與自己的私密金鑰加以計算，以產生代理金鑰，而代理簽章者所簽署的文件中亦須包含原始簽署者所規定的簽署權力，因此，只有符合此簽署權力的簽署文件才具有合法性。

此外，採用代理簽章機制必須滿足下述特性：

- 可區別性：驗證者它可以驗證被簽署之文件，到底是由原始簽章者所簽署或是由代理簽章者所簽署；若為多重代理簽章，除了需符合上述之要求外，還需要分辨是由那位代理簽章者所簽署。
- 不可偽造性：只有原始簽章者所指派代理簽章者，才可產生有效的代理簽章文件，沒有任何人可偽造此代理簽章。
- 可驗證性：驗證者可以從代理簽章者所送過來的公開訊息中驗證此簽章之合法性，且需能驗證此簽署文件是由原始簽章者所授權。
- 識別性：從代理簽章資訊，原始簽章者可識別代理簽章者的身份。
- 不可否認性：其效果就和一般數位簽章一樣，即代理簽章者不可否認曾經簽署過此份文件。
- 公平性：代理簽章者不能將代理簽章的權力轉移給它人使用，否則對原始簽章者是不公平。

2.3 提名式代理簽章

最早提出提名式簽章機制是由 Kim 等學者在 1995 年提出[2] [3] ，而後由 Park 等學者將其觀念應用在代理簽章機制[7] ，後續有學者基於此機制下做部分修改[10] 。提名式代理簽章(Nominative proxy signature)與一般的代理簽章最不同的地方，在於它必須透過第三者，亦即被提名者(Nominated verifier or Nominee)的幫忙，才可以驗證簽章是否有效，訊息接收者是不能自己驗算的。藉由上述特性，它比一般的代理簽章機制更適合用在行動通訊(Mobile communication)的環境。在行動通訊中，使用者就像是原始簽章者，代理者則像是代理簽章者，由於提名式代理簽章只能由被提名者來驗證，因此原始簽章者及代理者的身份都可以被保密。除了保密性的優點，一般的行動裝置本身的計算能力及電力都較為缺乏，透過代理簽章的方式，原始簽章者就可以把簽章原本要執行的大量計算，例如大量的模數與指數計算，交付給代理簽章者來做，以節省電力。

依據驗證者被提名的方式，提名式代理簽章可分為－原始簽章者提名式(Original-nominative proxy signature)，其驗證者是由原始簽章者所提名。另一種則是由代理簽章者來提名驗證者(Proxy-nominative proxy signature)，由代理簽章者來負責提名驗證者。其中 Original-nominative proxy signature 較適合訊息接收者是由原始簽章者決定的無線通訊環境；而 proxy-nominative proxy signature 則較適合用於行動電子商務環境。另外，提名式代理簽章機制必須滿足下述特性：

- 必須滿足所有簽章與代理簽章的特性。

- 只有原始簽章者(或代理簽章者)，可以提名驗證者。
- 原始簽章者與代理簽章者不可否認他們所產生的簽章。
- 只有被提名者可以直接驗證代理簽章是否有效。
- 如果有必要，只有被提名者可以向第三方證明某個簽章是否有效。

三、研究方法

本研究是基植於無基礎行動網路環境下，因其特殊架構的需求所提的分散式提名代理簽章機制，以達到代理簽章之目的。並藉由安全性分析與效率分析，說明本研究所提的架構之安全性與可行性。以下即就本研究之機制與安全性分析做描述。

3.1 符號定義

以下就本研究所需之符號做定義：

- p, q:兩個大質數；其中 q 必須滿足 $q \mid p-1$
- g：它是在模 p 下之原根(primitive root)，其 order 為 q。
- O：原始簽章者。
- PG：一群代理簽章者；其中 $PG = \{p_1, p_2, ..., p_n\}$。
- VG：一群簽章驗證者；其中 $VG=\{v_1, v_2, ..., v_m\}$。
- $h(.)$：為一個不可逆的單向雜湊函數。
- (x_0, y_0)：原始簽章者之私密金鑰與公開金鑰。
- (x_{p_i}, y_{p_i})：代理簽章者 p_i 之私密金鑰與公開金鑰。
- (x_{v_j}, y_{v_j})：驗證者 v_j 之私密金鑰與公開金鑰。
- y_{PG}：PG 之公開金鑰
- pg_0：PG 之私密金鑰
- y_{VG}：VG 之公開金鑰
- vg_0：VG 之私密金鑰
- k_1, k_2：隨機亂數是由代理簽者共同合作產生

3.2 分散式提名代理簽章機制

本機制是以提名代理簽章機制為基礎，並加入門檻機制，所形成的分散式提名代理簽章機制。換句話說，原始簽章者可以指定一群人為代理簽章者及另一群人為簽章驗證者，而任一個簽章接收者若不屬於驗證者的成員，無法執行簽章驗證的工作，以達到保護原始簽章者及代理簽章者之私密性。另外，藉由門檻機制可以分散簽章的運算與驗證的工作。因此，非常適用於無基礎行動網路的環境。

本機制共分成五個階段，以完成代理簽章之目的：

- Proxy group share generation phase: 此一階段，proxy group 成員會透過 secret sharing 的方式，合力產生 proxy group 的 group public key(y_{PG})與 group private key(pg_0)。
- Verifier group share generation phase: 同上，verifier group 成員會透過 secret sharing 的方式，合力產生 proxy group 的 group public key(y_{VG})與 group private key(vg_0)。
- Proxy key generation phase: 原始簽章者 O 首先產生一把 proxy key，交給該 proxy signer group，而 proxy signer group 在收到金鑰之後，再產生屬於屬群組的 proxy signing key，以防止 original 的偽造。
- Proxy signature generation and issuing phase: proxy signer group 透過合作的方式為 original signer 執行代理簽章，並藉由*(t,n)*門檻機制完成；換句話說，其中至少要有 t 個以上的 proxy signers 願意合作才能完成簽署動作。
- Verification phase: verifier group 透過合作的方式來為第三方驗證簽名是否有效，並藉由*(l,m)*門檻機制完成；換句話說，其中至少要有 l 個以上的 verifier 願意合作才能驗證簽章的真偽。

下述為各階段之演算法內容：

- Phase 1: Proxy group share generation

i. 每個代理簽章者 p_i 選擇兩個參數 $a_{p_i}, b_{p_i} \in_R Z_q^*$；然後計算下列式子：

$r_{p_i} = g^{a_{p_i}} \bmod p$

$b_{p_i} \equiv x_{p_i} \cdot r_{p_i} + a_{p_i} \cdot c_{p_i} \bmod q$

$\Rightarrow y_{p_i}^{'} = g^{b_{p_i}} = y_{p_i}^{r_{p_i}} \cdot r_{p_i}^{c_{p_i}} \bmod p$

ii. p_i 將 $Sign(h(b_{p_i}), r_{p_i}, c_{p_i})$ 作為自己的簽章，並計算下述維度為 t-1 的多項式：

$f_i(z) = b_{p_i} + e_{i,1} z + e_{i,2} z^2 + \cdots + e_{i,t-1} z^{t-1} \bmod q$

iii. 依照上述多項式為所有的其他代理簽章者 p_j 產生 $f_i(j)$。換句話說，

$f_i(j) = b_{p_i} + e_{i,1} j + e_{i,2} j^2 + \cdots + e_{i,t-1} j^{t-1} \bmod q; \forall j = 1,...,n; j \neq i$

並將 $f_i(j)$ 藉由安全的通道送給 p_j

iv. p_i 廣播 $g^{b_{p_j}}, g^{e_{i,1}}, ..., g^{e_{i,t-1}} (\forall j = 1,2,...,n; and\ j \neq i)$

v. 同理其他的代理簽章者 p_j 執行相同的工作。

vi. 每一個 p_i 可以驗證其他代理簽章者 p_j 送來 $f_j(i)$ 是否正確：

$g^{f_j(i)} = g^{b_{p_j}} \cdot (g^{e_{j,1}})^i \cdot (g^{e_{j,2}})^{i^2} \cdots (g^{e_{j,t-1}})^{i^{t-1}} \bmod p$

$= g^{b_{p_j}} \cdot A_{j,1}^{i} \cdot A_{j,2}^{i^2} \cdots A_{j,t-1}^{i^{t-1}} \bmod p$

where $A_{j,k} = g^{e_{j,k}}; \forall k = 1,...,t-1$

vii. 如果上述檢查正確，p_i 產生

$s_{p_i} = \sum_{j=1}^{n} f_j(i)$

當成自己的 share

viii. 由上述多項式我們可以計算出此代理簽章群組之群組秘密金鑰與公開金鑰，如下：

$pg_0 = \sum_{j=1}^{n} b_{p_j}$

$y_{PG} = g^{pg_0} \bmod p = g^{\sum_{j=1}^{n} b_{p_j}} \bmod p = \prod_{j=1}^{n} g^{b_{p_j}} \bmod p = \prod_{j=1}^{n} y_{p_j}^{'} \bmod p$

- Phase 2: Verifier group share generation

i. 每個簽章驗證者 v_j 選擇兩個參數 $a_{v_j}^{'}, b_{v_j}^{'} \in_R Z_q^*$；然後計算下列式子：

$r_{v_j}^{'} = g^{a_{v_j}^{'}} \bmod p$

$b_{v_j}^{'} \equiv x_{v_j} \cdot r_{v_j}^{'} + a_{v_j}^{'} \cdot c_{v_j}^{'} \bmod q$

$\Rightarrow y_{v_j}^{''} = g^{b_{v_j}^{'}} = y_{v_j}^{r_{v_j}^{'}} \cdot (r_{v_j}^{'})^{c_{v_j}^{'}} \bmod p$

ii. v_j 將 $Sign(h(b_{v_j}^{'}), r_{v_j}^{'}, c_{v_j}^{'})$ 作為自己的簽章，並計算下述維度為 *l*-1 的多項式：

$\psi_j(z) = b_{v_j}^{'} + e_{j,1} z + e_{j,2} z^2 + \cdots + e_{j,l-1} z^{l-1} \bmod q$

iii. 依照上述多項式為所有的其他簽章驗證者 v_i 產生 $\psi_j(i)$。換句話說，

$\psi_j(i) = b_{v_j}^{'} + e_{j,1} i + e_{j,2} i^2 + \cdots + e_{j,l-1} i^{l-1} \bmod q; \forall i = 1,...,m; i \neq j$

並將 $\psi_j(i)$ 藉由安全的通道送給 v_i

iv. v_j 廣播 $g^{b_{v_j}^{'}}, g^{e_{j,1}}, ..., g^{e_{j,l-1}} (\forall i = 1,2,...,m; and\ i \neq j)$

v. 同理其他的簽章驗證者 v_i 執行相同的工作。

vi. 每一個 v_j 可以驗證其他簽章驗證者 v_i 送來 $\psi_i(j)$ 是否正確：

$g^{\psi_i(j)} = g^{b_{v_i}^{'}} \cdot (g^{e_{i,1}})^j \cdot (g^{e_{i,2}})^{j^2} \cdots (g^{e_{i,l-1}})^{j^{l-1}} \bmod p$

vii. 如果上述檢查正確，v_j 產生

$s_{v_j} = \sum_{i=1}^{m} \psi_i(j)$

當成自己的 share。

viii. 由上述多項式我們可以計算出此簽章驗證者群組之群組秘密金鑰與公開金鑰，如下：

$vg_0 = \sum_{i=1}^{m} b_{v_i}$

$y_{VG} = g^{vg_0} \bmod p = g^{\sum_{i=1}^{m} b_{v_i}} \bmod p = \prod_{i=1}^{m} g^{b_{v_i}} \bmod p = \prod_{i=1}^{m} y_{v_i}^{''} \bmod p$

- Phase 3: Proxy key generation

i. 原始簽章者 *O* 選擇一個參數 $k \in_R Z_q^*$；然後計算下列式子：

$K = g^k \bmod p$

$e_h = h(M_w \| T \| K \| y_{VG})$

其中 M_w 是授權憑證，T 是時間戳記

ii. 原始簽章者 *O* 產生代理金鑰(proxy key) σ，產生方式如下：

$\sigma = x_0 \cdot e_h + k \bmod q$

iii. 原始簽章者 *O* 依照下述多項式，幫群組內的代理簽章者 p_i 產生代理金鑰的部分資訊 σ_{p_i}，並傳送給 p_i。換句話說，

$f^{'}(z) = \sigma + d_1 z + d_2 z^2 + \cdots + d_{t-1} z^{t-1} \bmod q$

$\sigma_{p_i} = f^{'}(i); \forall i = 1,...,n$

iv. 原始簽章者 *O* 廣播 $(M_w \| T \| K \| y_{VG})$

v. 群組內的代理簽章者 p_i 收到 σ_{p_i} 後，依下式可以驗證其合法性：

$$\begin{cases} e_h = h(M_w \| T \| K \| y_{VG}) \\ g^{\sigma_{p_i}} \stackrel{?}{=} y_0^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{j^j} \bmod p \end{cases}$$

vi. 群組內的代理簽章者 p_i 若都完成驗證工作，則表示此階段之代理金鑰產生成功。最後，每個 p_i 將收到的 σ_{p_i} 經過下式的運算，以產生新的 proxy share σ'_{p_i}，作為代理簽章之簽章金鑰。

$$\sigma'_{p_i} = \sigma_{p_i} + s_{p_i} \cdot e_h \bmod q$$

vii. 未來只要有 t 個代理簽章者共同合作，可以幫簽章者簽署文件 M。

- Phase 4: Proxy signature generation and issuing

i. 此階段之目的是由群組內任意 t 個代理簽章者共同為原始簽章者簽署文件 M。

ii. 代理簽章者 p_i 產生下述式子，並將 ξ_{p_i} 藉由安全的通道傳送給其他的代理簽章者 p_j：

$$\xi_{p_i} = k_{2,p_i} - \sigma'_{p_i} \cdot e'_h \bmod q; where\ e'_h = h(M \| M_w \| T \| K \| y_{VG})$$

iii. 同理，p_i 亦收到其他代理簽章者 p_j 之 ξ_{p_j}，並藉由下述式子驗證其正確性：

$$g^{\xi_{p_j}} \bmod p = g^{k_{2,p_j} - \sigma'_{p_j} \cdot e'_h} \bmod p$$

$$\Rightarrow g^{\xi_{p_j}} \bmod p = (g^{k_{2,p_j} + q_1 \cdot j + q_2 \cdot j^2 + \cdots + q_{t-1} j^{t-1}}) \cdot (g^{\sigma'_{p_j}})^{-e'_h} \bmod p$$

$$= (y_{k_{2,p_j}} \prod_{i=1}^{t-1} Q_i^{j^i}) \cdot (g^{\sigma_{p_i} + s_{p_i} \cdot e_h})^{-e'_h} \bmod p$$

$$= (y_{k_{2,p_j}} \cdot \prod_{i=1}^{t-1} Q_i^{j^i}) \cdot [y_0^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{j^i} \cdot (y_{PG} \cdot \prod_{i=1}^{t-1} A_i^{j^i})^{e_h}]^{-e'_h} \bmod p$$

iv. 如果上述式子驗證通過，則 p_i 可以計算出 k_1，k_2，$R = g^{k_1 - k_2} \bmod p$ 及 $Z = y_{VG}^{k_1} \bmod p$。

v. 代理簽章者 p_i 完成上述程序後，即可對文件 M 進行簽署，並產生簽章 S：

$$S = k_2 - \sigma' \cdot e''_h \bmod q$$

$$= f'''(0) - (f'(0) + f(0) \cdot e_h) \cdot e''_h \bmod q$$

$$where\ e''_h = h(M \| M_w \| K \| T \| y_{VG} \| R \| Z)$$

vi. p_i 傳送 $S, M, M_w, K, T, y_{VG}, R, Z$ 給簽章驗證者。

- Phase 5: Verification

i. 此階段之目的是由群組內任意 l 個簽章驗證者共同為簽章驗證者驗證簽署之文件 M 之有效性。

ii. 首先，這 l 個簽章驗證者需藉由共同合作，以產生此驗證群組的私密金鑰 vg_0，並驗證下述的式子：

$$(g^S \cdot y_{ps}^{e''_h} \cdot R)^{b'_0} \bmod p \stackrel{?}{=} Z \bmod p$$

$$where\ y_{ps} = g^{f'(0) + f(0) \cdot e_h} \bmod p$$

$$= g^{\sigma} \cdot (y_{PG})^{e_h} \bmod p$$

$$= (g^{e_h \cdot x_0 + k}) \cdot (y_{PG})^{e_h} \bmod p$$

$$= y_0^{e_h} \cdot K \cdot (y_{PG})^{e_h} \bmod p$$

$$= K \cdot (y_0 \cdot y_{PG})^{e_h} \bmod p$$

iii. 若簽章驗證者完成上述的動作，則代表此簽章之合法性。

3.3 安全性分析

本小節將針對本研究所提的分散式提名代理簽章機制進行安全性分析。於[5] [6]即就一個安全的代理簽章之安全需求做完整性的描述，包括：unforgeability、nonrepudiaty、identifiability、verifiability、prevention of misuse。因此，我們將就上述項目做安全分析，以說明本研究滿足上述特性：

- Proxy signers' deviation：其目的是確認代理簽章機制是否能抵擋由代理簽章者誤用代理金鑰，而去產生一個合法且有效的代理簽章。

i. 假設代理簽章者握有 σ、K 以及原始簽章者 O 的公開金鑰 y_0 等資訊。因此，只要代理簽章者能夠藉由上述資訊計算 x_0 或是 k，即可製造出 Proxy signers' deviation 的效果；或是代理簽章者產生出一個新的且有效的 $(\tilde{\sigma}, \tilde{K})$ 並滿足 $\tilde{\sigma} \equiv x_o \cdot \tilde{e}_h + \tilde{k} \bmod q$ 及

$\tilde{K} = g^{\tilde{k}} \bmod p$ ，亦可達到上述效果。

ii. 若代理簽章者要能產生上述之一的效果，它必須找出原始簽章者O的私密金鑰x_0。因此，只要原始簽章者O的私密金鑰能保護好，對代理簽章者來說要做這種攻擊幾乎不可能。

- Unforgeability：此條件之目的是為了保證除了原始簽章者，或是被授權的代理簽章者能替它產生有同等效力的簽章外，其他人無法偽造出和原始簽章者有同等效力的簽章。事實上這種攻擊要比上一種還更為艱難，因為它不屬於代理簽章群組的成員，它必需先試著解出$\tilde{\sigma} \equiv x_o \cdot \tilde{e}_h + \tilde{k} \bmod q$這個多項式，但它只擁有部分公開的資訊：原始簽章者的公開金鑰y_o以及K。
- Secret key's dependence：代理簽章者的代理金鑰σ是由原始簽章者的私密金鑰x_o計算出來，因此，若沒有原始簽章者的私密金鑰，攻擊者是無法產生出σ。
- Verifiability：驗證者必需有能力確認原始簽章者確實授權給代理簽章者。我們可以藉由K來達成，因為當原始簽章者在授權給不同的代理簽章者之群組時，都會產生不同的K，而在驗證時，原始簽章者的公開金鑰y_o就會是它授權給代理簽章者的證據。
- Distingushiability：驗證者必需有能力能區別出該簽章是由原始簽章者或是代理簽章者所簽署；因為我們採用的是 protected partial delegation 的簽章技術，兩者可以很容易區別出來。
- Identifiability：原始簽章者必需要有能力藉由代理簽章者所簽署的簽章，辨認出這個簽章是哪個群組的代理簽章者所簽。這點可以很容易就達成，因為除了原始簽章者之外，沒有人可以產生有效的σ、K和e_h組合，也只有被給與這些參數的代理簽章者才能替原始簽章者產生有效的代理簽章；此外，因為當原始簽章者在授權給不同的代理簽章群組時，都會產生不同的K，所以不同代理簽章群組所產生的簽章是可以被辨認出來的。
- Nonrepudiaty：一但一個有效的代理簽章被產生後，做出該簽名的代理簽章者就無法否認是由它所產生。由於代理簽章者在進行簽章時，使用了自己產生的ξ_{p_i}來簽署文件，因此它無法否認所產生的簽章。

藉由上述的安全性分析，證明了本研究所提的分散式提名代理簽章機制，符合代理簽章機制對於安全的基本需求。此外，由於本研究將[10] 方法中幾個重要參數用一些運算給取代掉，讓攻擊者得花更多的精力在破解這些參數上，所以相較之下更為更安全。

3.4 效能分析

本小節將針對本研究所提的分散式提名代理簽章機制進行效率分析。本分析方式採 Kaliski 學者所提出的評估方式進行。他針對數位簽章計算過程所需花費的計算量提出了一個方法，其概述如下：

- $WM(b)$：執行 b-bit 模數乘法所需耗費的計算量。
- $WS(b)$：執行 b-bit 平方所需耗費的計算量。
- 基本的計算法則如下：

  i. $WS(b) = 0.75WM(b)$

  ii. $\frac{WM(b_1)}{b_1^2} = \frac{WM(b_2)}{b_2^2}$

依據上述法則，我們可以試著找出一個執行指數次方與模數計算所需的計算工作量。例如： $g^s \bmod p$，其所需的計算量，W，為 $|s|WS(|p|) + 0.5|s|WM(|p|)$，再搭配上述基本法則後，可得到 $W = 640WM(512)$ (其中 s, p 都是 512-bit)。

因此，本研究於效能分析採用此模式，將本研究所提的方法 Zuo-Wen Tan 與 Zhuo-Jun Liu 的方法做比較：

- 符號定義：如下表 一

表 一：符號定義

符號	意義
H_1	$H(m_w \| T \| r \| y_C)$
H_2	$H(M \| m_w \| y_C \| R \| Z)$
H_3	$H(M \| m_w \| T \| r \| y_C \| R)$
e_h	$H(M_w \| T \| K \| y_{VG})$
$e_h^{'}$	$H(M \| M_w \| T \| K \| y_{VG})$
$e_h^{''}$	$H(M \| M_w \| K \| T \| y_{VG} \| R \| Z)$

以下我們就幾種情境做說明：

- Zuo-Wen Tan 與 Zhuo-Jun Liu 的方法

  i.所需的計算量：

  $3848+3\cdot WH(H_1)+WH(H_2)+WH(H_3)$

- 分散式提名代理簽章機制(一個代理簽章者與一個驗證者)

  i.所需的計算量：

  $5771+3WH(e_h)+WH(e_h^{'})+2WH(e_h^{''})$

- 分散式提名代理簽章機制(t 個代理簽章者與 l 個驗證者)

  i.所需的計算量：

  $640\times(6t^2+2l^2+4t)+(t+2)\ WH(e_h)+t\times WH(e_h^{'})+2\ WH(e_h^{''})+t\cdot WH(b_{p_i})+l\cdot WH(b_{v_j}^{'})+3t^3-2t^2+8t+l^3-2l^2+3l+3$

由上述之結果可以得知，本研究所提之分散式提名代理簽章機制，在一個代理簽章者與一個驗證者請況下並不會較其他的提名式代理簽章之效能來的差，另外我們提供了更有彈性的代理簽章者與簽章驗證者個數的彈性，更適用於無基礎行動網路的環境。

四、結論與建議

無基礎行動網路，已經成為無線網路架構主流之一；因為它具有動態拓樸與自我組織之特性，使得它有別於其他無線網路架構，故使得它可應用的範圍更廣，例如應用戰場、緊急醫療與車機系統上。而通訊過程的私密性、資料完整性、身份驗證及數位簽章均是無基礎行動網路所需具備的安全機制。本研究希望在通訊架構下，提出依個可行的簽章機制。由於無基礎行動網路環境，節點移動頻繁，故需藉由代理簽章機制的觀念，方能完成簽章之目的。

本研究試圖提出一個可解決的方法，稱之為分散式提名代理簽章機制。於此機制下，原始簽章者可以指定簽章的驗證者，以避免代理簽章者誤用之情形。另外，為保證網路上有節點可以執行上述之角色，本文提出具門檻機制的代理簽章者及驗證者，如此，可確保在無基礎行動網路架構下代理簽章執行的可行性及提供分散處理機制，以解決無線網路設備的問題。藉由本演算法五個步驟的執行，可以確保原始簽章者可以指定簽章的驗證者；代理簽章者藉由群組合作可以正確產生代理簽章；簽章的接收者可以藉由簽章的驗證者確認此簽章之有效性；最後，簽章的驗證者可以驗證此簽章之合法性。最後，藉由安全性分析與效率分析，說明本研究所提的架構之安全性與可行性。

五、計畫成果自評

本計畫在無基礎行動網路環境下共完成(1)無基礎行動網路架構之研究(2)現有數位簽章與代理簽章機制之研究(3)分散式提名代理簽章機制之設計(4)安全性與效能之分析。以上四項均滿足本計畫之目標。由於具有提名機制與門檻機制，使得原始簽章者可以順利指派簽章的驗證者，並可透過一群代理簽章者，執行文件簽署之工作，因此，非常適用於無基礎行動網路架構的環境。另外，從安全性分析，可以確認本研究所提之機制滿足代理簽章機制安全性之需求；並藉由效能之分析之結果，確認本研究之機制在一個代理簽章者與一個驗證者請況下並不會較其他的提名式代理簽章之效能來的差，另外我們提供了更

有彈性的代理簽章者與簽章驗證者個數的彈性，更適用於無基礎行動網路的環境。故本研究機制具有後續研究價值。

參考文獻

[1] S.J. Hwang and C.H. Shi, “A simple multi-proxy signature scheme,” Proc. Of the tenth National Conference on Information Security, pp.134-138, 2000.

[2] S.J. Kim, S.J. Park, and D.H. Won, “Nominative Signatures,” Proc. ICEIC’95, pp.68-71, 1995.

[3] S.J. Kim, S.J. Park, and D.H. Won, “Zero-knowledge nominative signature,” Proc. of Pragocrypt’96, International Conference on the Theory and Applications of Cryptology, pp.380-392, 1996.

[4] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks,” IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.

[5] B. Lee, H. Kim, and K. Kim, “Strong proxy signature and its applications,” *In Proceedings of SCIS*, 2001.

[6] M. Mambo, K. Usuda, and E. OKamoto, "Proxy Signatures for Delegation Signing Operation," Proc. Third ACM Conf. on Computer and Communications Security, 1996, pp. 48-57.

[7] H.U. Park and I.Y. Lee, “A digital nominative proxy signature scheme for mobile communication,” Proc. of ICICS 2001, International Conference on Information and Communications Security, Springer-Verlag, Lecture Notes in Computer Science 2229, pp.451-455, 2001.

[8] H.M. Sun, “An efficient nonrepudiable threshold proxy signatures with known signers,” Computer Communications, 22(8), pp.717-722, 1999.

[9] H.M. Sun, N.Y. Lee, and T. Hwang, “Threshold proxy signatures,” IEE Proc. Computers and Digital Techniques, Vol. 146, Issue. 5, pp.259-263, Sept. 1999.

[10] Z.W. Tan and Z.J. Liu, “Nominative Proxy Signature Schemes”, Institute of Systems Science , AMSS, Chinese Academy of Sciences, State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, 2004.

[11] K. Zhang, “Threshold proxy signature schemes,” 1997 Information Security Workshop, Japan, pp.191-197, 1997.

[12] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network , pp.24-30, Dec, 1999.

[13] 羅元琮，”一個適用於 Ad-hoc 網路環境下的分散式提名代理簽章機制”，國立交通大學資訊管理研究所，民國 95 年。