新的 WLAN 認證弱點之偵防機制

曹偉駿* 李哲維
大葉大學資訊管理學系
*E-mail: wjtsaur@yahoo.com.tw

摘要

WLAN(Wireless Local Network)由於規格上的設計有別於傳統的 802.3 乙太網路架構，使得使用者面臨異於以往的資訊安全風險。現階段仍未有較為良好的工具可支援一般使用者自我檢測 WLAN 認證弱點；另一方面，網路管理人員在使用這些工具軟體進行弱點檢測普遍會面臨以下兩個問題：一、弱點偵防與檢測的工作需要耗費組織中大量的系統資源與稽核人力成本；二、WLAN 環境下之 Client 端節點變動頻繁，使得無線存取點(Access Point；AP)及使用者端稽核的工作面臨相當大的考驗。因此，本研究提出一新的 WLAN 認證弱點之偵防機制，可同時兼顧 WLAN 環境中的節點異動頻繁特性、簡化並降低未經授權之 AP 於稽核過程時所需的網路專業門檻及人力物力、自動化檢測無線網路服務使用者之合法使用期限。

關鍵詞：無線網路安全、弱點檢測、WLAN 認證機制、IEEE 802.11、橢圓曲線公開金鑰密碼系統。

1. 前言

微奈米製造技術的提升暨資訊個人化、行動化的需求，直接促成了無線網路技術的問世，使得人們逐漸將部份作業由桌上型電腦移至可移動式裝置進行處理，如此的發展，對於企業組織、軍事用途、教育學習等層面均帶來相當大的助益。

然而，WLAN(Wireless Local Network)由於規格上的設計有別於傳統的 802.3 乙太網路架構，使得使用者在享受無線網路便利性的同時，也面臨異於以往的資訊安全風險，更可能在不自覺的情況下將自身設備的弱點曝露於開放式的無線網路環境下。基於這些弱點，駭客可針對這些系統中軟硬體或是傳輸上的漏洞發動攻擊，進而竊取一些機密資料或進行破壞性行為來損害系統的正常運作。由於安全漏洞的攻擊程式容易取得或是根本不需要使用任何攻擊程式，使得這些安全漏洞非常容易被駭客當作入侵攻擊的管道。

根據 NIST[8]對於「Vulnerability」一詞的定義：其為系統在安全之程序上、設計過程中、進行實作時，甚至是內部控管不良而暴露出來的缺陷，此類缺陷的發生通常是無預警的被觸發，或是經由駭客等有心人士以某些工具或入侵手法所導致。

為了對於 WLAN 環境下的系統安全弱點進行系統化的檢測，ISECOM 組織提出適用於無線網路環境下之安全測試方法論，例如 Open-Source Security Testing Methodology Manual-Wireless Security Testing Section(OSSTMM WIRELESS)[5]，截至 2007 年 1 月為止的版本為 2.9.1。學者 Corral 等人[2]更基於此方法論，進行 WLAN 環境下，系統弱點檢測的實作；然而，該研究並同時指出，針對未經授權之設備搜尋(Unauthorized devices search)以及認證形態(Authentication type)等兩項 WLAN 弱點偵防需求，現階段仍未有較為良好的工具可支援一般使用者自我檢測。另一方面，使用者在使用這些軟體進行弱點檢測普遍會面臨以下幾個問題[2,4-5]：

一、使用者需於檢測過程中缺乏簡易而明確的步驟，如欲判讀檢測結果亦需具備較高度的網路專業知識，使得組織若有人員的異動，弱點偵測的作業程序無法維持一定的品質。

二、弱點檢測工作通常需要耗費組織中大量的系統資源與稽核人力成本。

三、WLAN 環境由於其網路拓蹼的特性，Client 端節點變動頻繁，增加使用者權限稽核工作之困難度。

有鑑於現有之研究僅能對弱點檢測之單項功能提出個別的解決方案，因此本研究為克服上述三項問題，將以多伺服器環境下之單一登入相關機制為基礎[13, 1]，設計一基於橢圓曲線公開金鑰密碼系統[12]之新的 WLAN 認證弱點偵防機制。本機制可同時兼顧 WLAN

環境中的節點異動頻繁特性、簡化並降低未經授權之 AP 於稽核過程時所需的網路專業門檻及人力物力、自動化檢測無線網路服務使用者之合法使用期限。亦即本研究除了可降低組織中的無線設備異動成本外，更不會因為設備的異動而使得現有組織中的設備遭受安全威脅。

本文由第 2 節開始，首先將針對 WLAN 架構、目前主流之 WLAN 安全認證機制及其弱點進行探討；第 3 節則分別經由建置階段、註冊階段、登入階段、檢測階段、變更使用者密碼等步驟，提出新的認證弱點偵防機制；第 4 節將對本文所提之機制，與目前主流之無線網路安全機制 EAP-TLS[9, 14, 15]、EAP-MD5[7, 9]、EAP–LEAP[9]等知名業界標準進行分析與討論，最後，將於第 5 節提出結論與未來發展方向。

2. 文獻探討

在本節中，本研究首先將於 2.1 節探討 IEEE 所制定之 WLAN 標準，之後將於 2.2 節探討現階段 WLAN 認證之現有解決方案及其存在之弱點。

2.1 802.11 WLAN 標準

IEEE (Institute of Electrical and Electronic Engineers；電機電子工程協會)在 1997 年首度公佈經由全球產官學界一致認可之 WLAN 標準。在此標準中規範了兩種網路架構[6, 10-11]，以下將逐一介紹：

- Infrastructure Mode

在此架構中，每個已安裝無線網路卡的無線裝置 (Workstation： WS)，必須透過 AP 以連線到有線區域網路，進行網路資源的存取，而 AP 所及的範圍便形成了基本服務集合(Base Service Set，BSS)。屬於不同 BSS 的無線裝置之間的溝通，則可先經由各自的 AP 連接上分散系統後，再透過彼此所屬之 BSS AP 進行資料交換，構成一個擴充服務集合(Extended Service Set, ESS)，使其架構更為完善。如圖 2-1 所示。

- Ad Hoc Network Mode

透過此架構，無線裝置之間的連線毋須透過 AP 即可進行資料的傳輸，其資料傳輸的方式採用點對點 (Peer to Peer)的方式，然而，此架構的缺點在於其無法連接有線區域網路，較適合臨時性質的無線區域網路應用，如圖 2-2 所示。

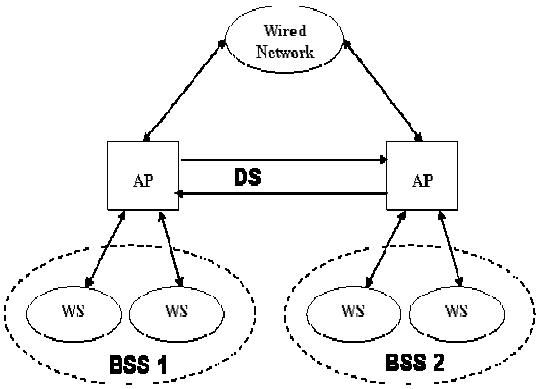

圖 2-1 Infrastructure Mode

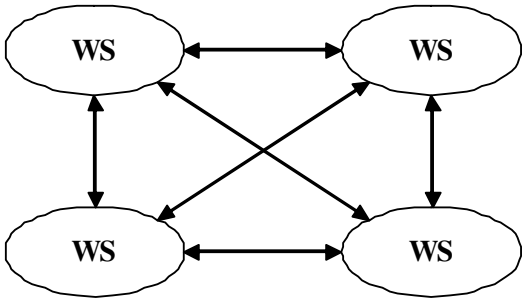

圖 2-2 Ad Hoc Network Mode

由於 Infrastructure Mode 型式的 WLAN 其通訊設備不僅包含無線裝置，更與有線網路端相連接，故安全上之顧慮相對的也比 Ad Hoc Network Mode 來得高，因此，本研究於 2.2 節開始，將針對 Infrastructure Mode 型式的 WLAN 認證安全機制進行探討。

2.2 WLAN 認證安全之現有解決方案及其存在之弱點

本研究已於 2.1 節論述 IEEE 所提出之 WLAN 技術規範，由於其網路架構及協定的設計有別於 802.3 乙太網路，使得 WLAN 的安全性絕大部份集中於認證之相關議題，針對這些議題，IEEE IETF 工作小組提出 EAP(Extensible Authentication Protocol)[9]之相關建議規範，以保障無線網路認證安全，本小節將針對較具代表性之數種 EAP 相關安全

機制進行探討。

(1) EAP–MD5

此機制搜集使用者的名稱以及密碼，經由 MD5 訊息雜湊函數轉換成訊息摘要後，針對此訊息摘要進行認證，在運算上相當快速，然而，此種認證方式無法滿足 Client 端與 AP 端之間的雙向認證，且此一弱點使得此機制容易遭受中間人攻擊 (Man-in-the middle attacks)[9]。

(2) EAP–TLS

EAP－TLS (Transport Level Security)認證機制定義於 RFC 2716 之中，此方法採用證書為基礎之公開金鑰密碼系統進行認證程序，改善了 EAP-MD5 僅能單向認證的缺點，提供 client 端與驗證端一良好的雙向認證程序，然而，此機制在認證的過程中除需耗費大量運算資源以產生證書外，其傳輸證書時產生的通訊成本亦相當可觀。

(3) EAP–LEAP

EAP-LEAP(Lightweight Extensible Authentication Protocol)由網路設備大廠Cisco Systems所開發，此方法基於使用者名稱/密碼的機制，亦可達成通訊雙方之雙向認證，就產生session key的功能而言，LEAP可為每一個獨立的session重新產生金鑰。然而，此種基於密碼的方法，通訊雙方的對談過程皆未受已加密的通道保護，同時也容易遭受字典攻擊[9]。

有鑑於本節所提之現存WLAN安全認證機制皆存在其弱點，本研究將於第3節提出新的WLAN認證弱點之偵防機制，此機制除了滿足現行近似方法之功能外，更進一步提供使用者權限稽核與非法AP檢測等功能。

3. 新的 WLAN 認證弱點之偵防機制

在第 2 節中，本研究已分別論述 WLAN 之網路架構、現行之主流 WLAN 認證機制及其。以下將分別於 3.1 節至 3.6 節，提出機制架構，以及建置階段、註冊階段、登入階段、檢測階段、變更使用者密碼等步驟，以有效解決現存認證弱點問題。

3.1 機制架構

本研究之機制如圖 3-1 所示，參與本機制的主要成員有使用者、AP 以及系統中心。

在使用者端的部份，本機制基於 Smart Card 技術，設計使用者特徵運算模組以及 AP 檢測模組以進行後續之資料運算與特徵檢測工作。

在 AP 端的部份，本機制所設計之 AP 特徵運算模組，可供其運算自身之特徵資訊，而使用者權限檢測模組除了可驗證使用者的身份，更可檢測使用者於該台 AP 的合法使用期限及資料傳輸時的完整性。

本機制中的系統中心其主要工作在於針對參與本機制之各項個體成員，於運算時所需之系統參數進行定義與初始化。

以下於 3.2 小節開始將針對本機制的運作流程進行論述。

3.2 建置階段

本階段主要針對參與本機制之各項個體成員於運算時所需之系統參數進行定義與初始化。首先將符號定義如下：

(1) p：大質數。

(2) 橢圓曲線方程式 $E(a,b)$：$y^2=x^3+ax+b$，滿足 $4a^3+27b^2 \neq 0 \pmod p$。

(3) q：p-1 的大質因數，長度 160 位元。

(4) Fp：為一有限場，且 Fp 為 (x,y) 滿足方程式 E，$E(Fp)$表示 $E \cup \{O\}$ ，其中 O 為無窮遠方的一個點。

(5) B：序為 q 的點，亦即橢圓曲線上的生成點。

(6) K_{pi}：使用者 U_i 的公鑰。

(7) K_{si}：使用者 U_i 的私鑰。

(8) S_{ca}：系統中心的私鑰。

(9) P_{ca}：系統中心的公鑰，其中

$$P_{ca} = S_{ca} \cdot B \pmod p \qquad (3.1)$$

(10) $h()$：單向雜湊函數 (One-way hash function)，其輸出為一整數，長度為 160 位元。

(11) w_i：使用者 U_i 的公鑰證明(Witness)。

(12) P_{ix}：點 P 其 X 座標軸上的值。

(13) S_SK_j：AP_j 的私鑰

(14) S_ID_j：AP_j 的公鑰，其中

$$S\_ID_j = \left(B \cdot S\_SK_j\right) (\mathrm{mod}\ p) \qquad (3.2)$$

且 $1 \leqq j \leqq m$

其次系統中心把各個 AP_j（$1 \leqq j \leqq m$）的 S_ID_j 其 X 軸之座標及 S_SK_j 作為點 X_j 的 X,Y 座標，把 X_1，X_2， X_3，...，X_m 各點內插於 $f(x)$，基於牛頓內插多項式的公式[3]可以得到以下式子:

$$f_i(X)=\sum_{j=1}^{m}\left[\sum_{j=1}^{m}\frac{(U\_ID_i)\dfrac{(X-U\_ID_i)}{S\_SK_j-U\_ID_i}}{\prod_{\substack{k=1\\k\neq j}}^{m}\left(S\_SK_j-S\_SK_k\right)}\times\prod_{k=1}^{m-1}\left(X-S\_SK_k\right)\right]$$

$$+V_i\prod_{y=1}^{m}\frac{X-S\_SK_y}{U\_ID_i-S\_SK_y}(\mathrm{mod}\ p) \qquad (3.3)$$

$$=a_mX_m+a_{m-1}X_{m-1}+...+a_1X+a_0\ (mod\ p)$$

系統建置完成後，系統中心將 $f_i(x)$ 傳給各 AP，如圖 3-1 之流程(1)所示，並公佈 E,B,P_{ca}。

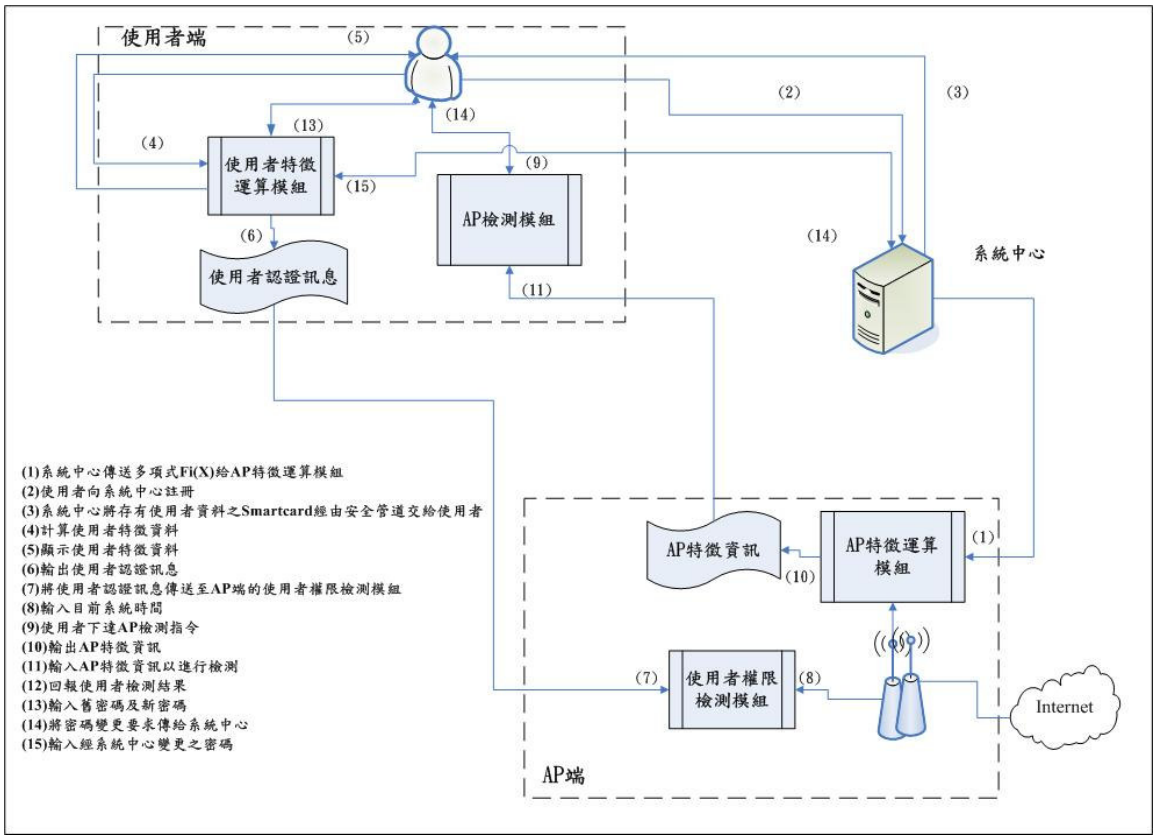

圖 3-1 新的 WLAN 認證弱點之偵防機制架構

3.3 註冊階段

當使用者欲登入至各 AP(AP_1,AP_2,.. ,AP_m)，須先向系統中心註冊，以利使用者獲取公鑰與私鑰。此外，其步驟如下:

Step 1 使用者 U_i 所進行的運算程序：

(1). 選擇一個代表自己身份的 U_ID_i。

(2). 隨機選擇一個為整數的亂數 Pw_i 為密碼。

(3). 計算 V_i，其中

$$V_i=h(Pw_i||U\_ID_i)\cdot B(mod\ p)$$

$$=\left(V_{ix},V_{iy}\right) \qquad (3.4)$$

(4). 傳送自己的身份 U_ID_i 及 V_i 給系統中心，如圖 3-1 流程(2)所示。

Step 2. 系統中心所進行的運算程序:

(1). 隨機選擇一個不同的整數 k_i。

(2). 系統中心經由使用者所提供之 V_i 與 U_ID_i，搭配自己所選的 k_i，與使用者協力運算使用者公鑰 K_{pi} 及公鑰證明 w_i:

$$K_{pi} = V_i + (k_i - h(U\_ID_i)) \cdot B (\mathrm{mod}\, P) \quad (3.5)$$
$$= (P_{ix}, P_{iy})$$

$$w_i = k_i + S_{ca} \cdot \left(P_{ix} + h\left(U\_ID_i\right)\right) (\mathrm{mod}\, p) \quad (3.6)$$

Step 3.建構具檢測使用者之使用期限功能之多項式方程式

(1). 將 V_i 代入在建置階段建立好的多項式方程式（3.3）中，算出 a_t 值。

$$f_i(x) = a_t + \sum_{k=1}^{m} a_k \prod_{j=0}^{k-1} (x - V_t) \quad (3.7)$$

(2). 將上述所求出之 a_t 值與各台 AP 的編號相加，得到 a_t+1, a_t+2…a_t+m 等數值

(3). 設定使用者 U_i 在每台 AP_i 可使用之有效期限(令其為 ST_{i1}, ST_{i2},.., ST_{im})

(4). 根據（a_t+1, ST_{i1}）,（a_t+2, ST_{i2}）,.....,（a_t+m, ST_{im}）等點，建構內插多項式為

$$f_m'(x) = a_m X^m + a_{m-1} X^{m-1} + ... + a_1 X + a_0 \quad (3.8)$$

系統中心將 $f_i(x)$、U_ID_i、K_{pi}、w_i 存在 U_i 的 Smart card 機密保護區中防止竄改，經由安全管道將 Smart card 發給使用者 U_i，如圖 3-1 流程(3)所示。

經由使用者特徵運算模組，使用者可計算自己的私鑰，作為個人之特徵，如圖 3-1 流程(4)與(5)所示

Step 4.使用者 U_i 收到 Smart card 後，根據內附資訊計算自己的私鑰 K_{si}

$$K_{si} = w_i + h(Pw_i \| U\_ID_i) (mod\ p) \quad (3.9)$$

Step 5.驗證公鑰 K_{pi} 的有效性是否成立：

$$K_{si} \cdot B = K_{pi} + h(U\_ID_i) \cdot B + [P_{ix} + h(U\_ID_i)) (\mathrm{mod}\, p)] \cdot P_{ca} \quad (3.10)$$

若驗證成功，則使用者 U_i 的私鑰為 K_{si}，公鑰為 K_{pi}。

3.4 登入階段

當已註冊使用者 U_i 要登入到 AP_j（$1 \leqq j \leqq m$）時，使用者首先插入 Smart card 至讀卡機中，之後輸入密碼 PW_i，其後之運算流程如下：

Step 1. Smart card 隨機選擇二整數 r_v 及 r_u，並計算下式:

$$V_i = h(Pw_i \| U\_ID_i) \cdot B (\mathrm{mod} p) = (V_{ix}, V_{iy}) \quad (3.11)$$

$$C_0 = r_v \cdot B (\mathrm{mod}\, p)$$

$$C_1 = r_u \cdot B (\mathrm{mod}\, p)$$

$$C_1' = C_1 + r_v \cdot S\_ID_j (\mathrm{mod}\, p) \quad (3.12)$$

$$h(Pw_i \| U\_ID_i) + K_{si} \cdot w_i (\mathrm{mod}\ p) \quad (3.13)$$

Step 2. Smart card 從系統中取得時間 t，並運用網路時間協定使得傳輸雙方之時間得以同步。

Step 3. Smart card 使用第 j 台 AP 的 S_ID_j 來計算

$$S = \left((r_u)(t) \cdot S\_ID_j\right) (\mathrm{mod}\, p) \quad (3.14)$$

Step 4. Smart card 建構並輸出認證訊息 M，如圖 3-1 流程(6)，其中，

$$M = \left\{U\_ID_i, t, S, C_0, C_1', C_2, V_i, U_{pi}, f_{m+1}(x), f_m'(x)\right\}$$

，之後傳送給隸屬於 AP_j 的使用者權限檢測模組，如圖 3-1 流程(7)。

3.5 檢測階段

在收到登入使用者 U_i 的認證訊息 M 後，AP_j 經由使用者權限檢測模組執行以下步驟來驗證使用者 U_i 的登入請求：

Step 1. AP_j 檢測使用者 U_i 的身份識別 U_ID_i 格式是否符合，不合則拒絕登入請求。

Step 2.AP_j 檢測下式是否成立，其中，AP_j 提供其目前日期時間 t_{now}，如圖 3-1 流程(8)，t 為使用者登入時間，ΔT 為系統預先設定的合理時間延遲參數。

$$t_{now} - t > \Delta T \quad (3.15)$$

若式(3.15)成立，則代表認證訊息在傳遞的過程中可能遭到不法的篡改，則此驗證將被終止。

Step 3. AP_j 從認證訊息 M 中的 C_0 及 C'_1 計算並還原 Smart 端所計算的 C_1

$$C'_1-(S\_SK_j \cdot C_0) \bmod p$$
$$= C_1 + ((r_v \cdot S\_SK_j) \bmod p) \cdot B - S\_SK_j (r_v \cdot B) \bmod p$$
$$= C_1$$

Step 4. AP 端在還原 C_1 後，利用使用者所傳來的登入時間資訊，t，與 AP_j 的私鑰等資訊計算出 S'值：

$$S' = (t) S\_SK_j \cdot (C_1) (\bmod p)$$
$$= \left[\left((r_u)(t) S\_SK_j \right) (\bmod p) \right] \cdot B$$
$$= \left((r_u)(t) \cdot S\_ID_j \right) (\bmod p)$$

若 S'與 S 不相同時，則拒絕登入。

Step 5. AP_j 利用 U_i 傳來的 $f_{m+1}(x)$與自己本身的多項式 $f(x)$，重建一個完整的多項式，亦即把方程式(3.3)與方程式(3.8)相加，得到多項式

$$f_i(x) = a_{m+1} X^{m+1} + a_m X^m + ... + a_1 X + a_0 (\bmod p) \quad (3.16)$$

Step 6. AP 端將 U_ID_i 代入方程式（3.15）中，求出 U_i 的 V_{ix}，如果 $f_i(U\_ID_i)=V_{ix}$，則接受 U_i 的登入請求，否則拒絕登入。

Step 7.為了防止 V_{ix} 被偽冒，所以 AP_j 再驗證以下方程式，如成立則接受 U_i 的登入請求，否則拒絕。

$$(C_2 \cdot B)(mod\ p) - K_{pi} \cdot w_i (mod\ p)$$
$$= ((h(Pw_i || U\_ID_i) + K_{si} \cdot w_i)(mod\ p)) \cdot B - K_{pi} \cdot w_i (mod\ p)$$
$$= (h(Pw_i || U\_ID_i) \cdot B(mod\ p) + K_{si} \cdot w_i \cdot B(mod\ p) - K_{si} \cdot w_i \cdot B(mod\ p)$$
$$= V'_i = (V'_{ix}, V'_{iy})$$

若 $V_{ix}=V'_{ix}$ 則接受登入。

Step 8. 檢測使用者於該台 AP_j 的登入有效期限:

(1). AP_j 用 U_i 的V_i 代入方程式（3.3）中，求出 a_t，接著將 a_t+j 代入方程式（3.7）中，計算 U_i 的登入有效期限如下：

$$f'_i (a_t + j) = ST_{ij}$$

(2). AP_j 比對經由 Step 8 流程(1)所計算出來的 ST_{ij} 與目前系統時間 t_{now}，若 $ST_{ij} \leqq t_{now}$ 成立，則代表使用者於該台 AP 的合法使用期限已過，AP_j 將終止使用者 U_i 的登入服務。

Step 9. AP 檢測及交談金鑰產生階段

在接受使用者登入後，使用者 U_i 下達檢測 AP 指令給 AP 檢測模組，如圖 3-1 流程(9)進一步驗證 AP_j，以確認對方確為欲登入之 AP，並產生交談金鑰，步驟如下：

(1).使用者驗證 AP 階段:

AP_j 任選一整數 $C_r \in \{2, q-2\}$，並經由 AP 特徵運算模組計算並輸出 AP 特徵資訊 C_{s1}，C_{s2} 如圖 3-1 流程(10)

$$C_{s1} = C_r \cdot B \ (\bmod\ p) \quad (3.17)$$

$$C_{s2} = C_1 + C_r . K_{pi} (\bmod p) \quad (3.18)$$

使用者在收到圖 3-1 流程(11)所傳來的訊息後，將經由 AP 檢測模組計算 C_1，並比較是否與使用者於登入階段時傳出的 C_1 值相同，若相同則表示 AP_j 確實為所欲登入的 AP，若不同則代表該 AP 為偽冒 AP，並回傳相關資訊給使用者，使用者將其中斷連線如圖 3-1 流程(12)。

$$C_{s2} - U_{si} \cdot C_{s1} (\bmod p)$$
$$= C_1 + C_r \cdot U_{pi} - C_r \cdot U_{si} \cdot B (\bmod p)$$
$$= C_1 + C_r \cdot U_{si} \cdot B - C_r \cdot U_{si} \cdot B (\bmod p)$$
$$= C_1$$

(2). 產生雙方之交談金鑰

Smart card 隨機選擇一個整數 x_a，計算

$T_a=x_a \cdot B\ (mod\ p)$，並傳送給 AP_j

AP_j 隨機選擇一整數 x_b，計算

$T_b=x_b \cdot B\ (mod\ p)$，並將$(S_ID_j, T_b)$傳送給 U_i。

使用者 U_i 運用式(3.19)計算其交談金鑰

$$SK = x_a \cdot S\_ID_j + K_{si} \cdot T_b \quad (3.19)$$

$$= x_b \cdot S\_SK_j (\text{mod } p) \cdot B$$
$$+ K_{si} \cdot x_b (\text{mod } p) \cdot B$$

AP_j 收到 x_a 後計算

$$V_u = K_{pi} + h(U\_ID_i) \cdot B$$
$$+ [(K_{pix} + h(U\_ID_i)) \bmod p] \cdot P_{ca} \quad (3.20)$$

並運用式(3.20)求出之 V_u 計算出 AP 端的交談金鑰 SK，如式(3.21)

$$SK = x_b \cdot V_u + S\_ID_j \cdot T_a$$
$$= x_b \cdot K_{si} (\text{mod} p) \cdot B + S\_SK_j \cdot x_a (\text{mod} p) \cdot \quad (3.21)$$

雙方得到相同的交談金鑰 SK，完成交談金鑰的建立。

3.6 變更使用者密碼

本小節將論述本機制的變更使用者密碼功能，其步驟如下:

Step 1.使用者端的運算步驟

(1). 使用者 U_i 輸入舊密碼 PW_i 及新密碼 PW_{in}，如圖 3-1 流程(13)

(2). 使用者特徵運算模組計算下列資訊

$$CV_i = h(Pw_i \| U\_ID_i) \cdot B (\text{mod } p)$$
$$CV_{in} = h(Pw_{in} \| U\_ID_i) \cdot B (\text{mod } p)$$
$$C_2 = h(Pw_i || U\_ID_i) + K_{si} \cdot w_i (mod\ p)$$

(3). 使用者特徵運算模組將 $U\_ID_i, CV_i, CV_{in}, C_2$ 傳送給系統中心，如圖 3-1 流程(14)

(4). 使用者特徵運算模組收到新公鑰 K'_{pi} 及公鑰證明 w'_i 及新的 $f'(x)$ 多項式後，計算使用者的私鑰 K'_{si}

$$K'_{si} \cdot B$$
$$= K'_{pi} + h(U\_ID_i) \cdot B$$
$$+ [(P_{ix} + h(U\_ID_i)) (\text{mod } p)] \cdot P_{ca}$$
$$K'_{si} = w'_i + h(Pw_{in} || U\_ID_i) (mod\ p)$$

並驗證公鑰 K'_{pi} 的有效性是否成立：

$$K'_{si} = w'_i + h(Pw_{in} || U\_ID_i) (mod\ p)$$

若驗證成功，則更新 Smart card 中資料，將使用者 U_i 的私鑰改為 K'_{si}，公鑰改為 K'_{pi} 完成密碼變更。

Step 2.系統中心的運算步驟

(1). 系統中心收到後計算驗證是否為原使用者 U_i

$$(C_2 \cdot B) (mod\ p) - K_{pi} \cdot w_i (mod\ p)$$
$$= ((h(Pw_i || U\_ID_i) + K_{si} \cdot w_i) (mod\ p)) \cdot B$$
$$- K_{pi} \cdot w_i (mod\ p)$$
$$= (h(Pw_i || U\_ID_i) \cdot B) (mod\ p)$$
$$+ K_{si} \cdot w_i \cdot B) (mod\ p) - K_{si} \cdot w_i \cdot B (mod\ p)$$
$$= CV'_i$$

(2). 在完成(1)的驗證後，系統中心選擇一個不同的整數 k_{in}，並計算新公鑰 K'_{pi} 及公鑰證明 w'_i 及新的 $f'(x)$，傳送給使用者特徵運算模組，如圖 3-1 流程(15)

$$K'_{pi} = CV_{in} + (k_{in} - h(U\_ID_i)) \cdot B (modp) = (P_{ix}, P_{iy})$$
$$w'_i = k_{in} + S_{ca} \cdot (P_{ix} + h(U\_ID_i)) (\text{mod } p)$$

(3). 系統中心亦將 CV_{in} 代入在建置階段建立好的多項式方程式（3.3）中，算出一個 a_t 值。利用 (a_t+1, ST_{i1}) (a_t+2, ST_{i2}),... (a_t+m, ST_{im}) 等點來建立牛頓內插多項式為

$$f'_m(x) = a_m X^m + a_{m-1} X^{m-1} + ... + a_1 X + a_0$$

4. 分析與討論

本文已於第 3 節詳述所提之機制運作流程，以下將於 4.1 節針對研究成果進行安全性分析，之後於 4.2 節與現行之 WLAN 主流安全機制 EAP-TLS、EAP-MD5、EAP-LEAP 進行分析與討論。

4.1 安全性分析

本文所提之機制，其安全性主要是基於解橢圓曲線離散對數問題的困難度。以下分別經由系統中心、使用者、攻擊者等角度，分析本研究之安全性：

(1) 系統中心

- 系統中心無法取得使用者密碼

本研究假設系統中心是可信賴的，然而，若系統中心存有惡意，欲取得使用者的密碼，除非系統中心能破解使用者在註冊階段所生的 V_i，此一破解手法將面臨橢圓曲線離散對數困難度。

- 可防止系統中心造假及達到雙向認證

本機制在註冊及登入時，可達成系統中心與使用者 Ui，使用者 Ui 與 AP 間的相互認證，增加使用上的安全性；此外，註冊階段採用自我驗證公開金鑰密碼系統之機制，此種機制的使用者公鑰是由系統中心與使用者共同產生，系統中心若欲假造使用者公鑰將會於註冊階段的式 3.10 中被偵測出來。

(2) 使用者:

- 使用者無法得知其他使用者的機密資料

使用者無法經由本身之多項式推出其他使用者的 V_i，因為使用者本身之多項式是由 $(at+1, ST_{i1})$, $(at+2, ST_{i2})$,....., $(at+m, ST_{im})$ 等點所構成，而根據牛頓內插法的特性，不同的點會產生不同的多項式，所以使用者無法得知其他使用者的機密資料。

- 可防範使用者自行延長使用期限

合法使用者無法從自己的Smart card所儲存之資訊中延長自己的使用有效期限，因為在本機制的註冊階段中，每台 AP 對使用者 U_i 的使用期限，是利用使用者 U_i 的 V_i 值，代入 AP 與系統中心才有的多項式內，經算出 a_t 後，再以牛頓內插法，將 U_i 的使用期限隱含於在多項式內。使用者只有檢查用的 $f'(x)$ 多項式，並無 $f(x)$ 多項式，所以無法得知 a_t，也就無法取得 ST_{ij}，所以本機制可防範合法使用者想自行延長使用期限，另外系統也可自動刪除過期使用者。

(3) 攻擊者:

- 安全的雙向認證

在檢測階段 Step 9 之使用者驗證 AP 階段，用來進行認證的 C_1 是包含在 C'_1 中且已用 AP 的公鑰加密，同時 r_u 及 C_r 為隨機選擇，為大於 160 位元的亂數，每次登入所選的均不相同，就算被攔截或破解，下一次登入也不會遭受安全威脅。

- 攻擊者無法取得使用者的私鑰與系統中心的私鑰

攻擊者可以取得的資料為 U_ID_i 與 K_{pi}，但經由註冊階段式(3.5)的分析可知，攻擊者無法從 K_{pi} 獲取 K_{si}；而 Wi 是由系統中心所產生的公鑰證明，攻擊者並無法從 W_i 獲取 S_{ca}。因此，任何攻擊者皆無法取得 K_{si} 與 S_{ca}。

- 可偵測偽冒攻擊

(1)偽冒認證訊息 M:

攻擊者可能偽冒一個認證訊息 M，但若系統時間由原本使用者產生的 t，變更為攻擊者產生的 t'，則在檢測階段 Step 4 中，原本的訊息 S 也變更為 S'，因此偽冒者無法通過認證。

(2)偽冒訊息 S:

攻擊者由於無從得知 C_1 及 r_u，所以偽冒 S 是不可行的。

(3)偽冒 V_i:

訊息 V_i 由使用者密碼 Pw_i 及 K_{si} 構成，皆於 Smart card 上計算，攻擊者無從得知，所以偽冒 V_i 無法通過驗證階段。

- 可防範重送攻擊

(1)攻擊者攔截登入者的認證訊息，未作修改內容，冒充傳送者重送訊息:

此種方式的重送攻擊將於檢測階段的式 3.15 被檢查出來，因此攻擊無法成功。

(2)攻擊者攔截訊息後進行偽造並重送:

攻擊者若欲進行此種攻擊，必須更改系統時間 t，以迴避式 3.15 之檢測，然而即使 t 值被改變，檢測者無法隨之更改 C_1 及 r_u，以迴避檢測階段 Step 4，因此攻擊無法成功。然而，式 3.15 中，參數 $\triangle T$ 的設定值需考慮網路壅塞程度進行調整，以免系統誤判，拒絕合法使用者登入。

- 攻擊者無法從攔截到之認證訊息中截取機密資料

認證訊息 M 中包含了以下資料:

$M=\{U\_ID_i, t, S, C_0, C'_1, C_2', V_i, K_{pi}, f_{m+1}(x), f'_m(x)\}$

其中，攻擊者若想經由 S, C_0, C_2, V_i, K_{pi} 等參數中獲取使用者的私鑰 K_{si} 及 r_u、C_1、Pw_i，均將面臨橢圓曲線離散對數困難度，而多項式 $f_{m+1}(x)$ 是方程式（3.16）的一部份，無法直接

用來求得 V_i 值，而 $f'_m(x)$是經由註冊階段 Step 3 程序(1)至程序(4)二次運算轉換得來的，無法直接利用。

- 可抵擋惡意 AP 從事偽冒攻擊

AP 管理者若具有惡意，欲於驗證階段經由 $f_i(U\_ID_i)=V_i$ 取得 V_i，並據以從事偽冒攻擊，推導出使用者密碼是不可行的，因為 $V_i=h(Pw_i||U\_ID_i)\cdot B(mod\ p)$， Pw_i 受到赫序函數及基於橢圓曲線離散對數問題之困難度所保護，所以具有惡意的 AP 無法達成偽冒攻擊。

- 可抵擋字典攻擊

攻擊者若欲經由攔截認證訊息 M，並從中擷取訊息 V_i，以進一步經由字典攻擊破解 V_i 內含的使用者名稱及密碼，將面臨橢圓曲線離散對數問題之困難度以及赫序函數單向的特性，使得本機制得以抵檔此種攻擊。

- 確保交談金鑰的安全性

在檢測階段 Step 9 中，驗證完後產生的交談金鑰值，每次均不同，若要從傳送中取得的 $T_a=x_a\cdot B(mod\ p)$ 及 $T_b=x_b\cdot B(mod\ p)$中，計算出 xa 及 xb，亦將面臨橢圓曲線離散對數困難度，可確保交談金鑰安全性。

4.2 討論

本文已於第 1 節中論述現今使用者進行弱點檢測時所面臨的問題，分別為:

一、缺乏簡易而明確的步驟可依循。

二、需耗費大量的人力物力。

三、在 WLAN 環境中，Client 端變動頻繁，增加弱點檢測難度。

以下將討論本文針對此三類問題所獲致之研究成果:

(1) 在第 3 節圖 3-1 中，本研究經由模組化的架構以簡易的方式詮釋所提機制之步驟流程，降低使用者於 WLAN 認證弱點偵防時的網路專業知識門檻，就偵防結果而言，則可藉由明確的認證訊息以輔助使用者進行判讀，使得弱點偵防之作業程序可維持一定的品質。

(2) 本研究所提之機制可協助使用者與 AP 雙方達成雙向認證，降低組織中的網路管理者於檢測組織網域內，非法架設及具惡意之 AP 時，所耗費組織中大量的系統資源與稽核人力成本。

(3) 為了因應 Client 端節點變動頻繁的特性，本研究可檢測 WLAN 服務使用期限已過期之使用者，有效降低使用者權限稽核工作之困難度。

表 4-1 機制功能比較

	EAP-MD5	EAP-TLS	EAP-LEAP	本機制
可檢測非法 AP	否	否	是	是
需要使用者帳號及密碼	是	否	是	是
使用者可更改密碼	否	否	否	是
是否需數位證書	否	是	否	否
可雙向認證	否	是	是	是
可建立交談金鑰	否	是	是	是
防止重送攻擊	否	是	是	是
防止字典攻擊	是	是	否	是
防止偽冒攻擊	是	是	是	是
可自動刪除過期使用者	否	否	否	是
防止使用者自行延長使用期限	否	否	否	是

此外，如表 4-1 所示，相較於 EAP-MD5、EAP-TLS、EAP-LEAP 等其它機制，本機制除了承襲現今主流 EAP 系列協定所提供之功能，亦可偵防 WLAN 常見之認證安全性弱點，諸如重送攻擊、偽冒攻擊、字典攻擊。此外，相較於現有機制更增加了變更密碼、使用者權限管理、偵測偽冒 AP 等功能，由此可知，本機制實為一功能完備且方便使用者使用之 WLAN 認證弱點偵防機制。

5. 結論

本研究提出一新的 WLAN 認證弱點之偵

防機制，可同時兼顧 WLAN 環境中的節點異動頻繁特性、簡化並降低未經授權之 AP 於稽核過程時所需的網路專業門檻及人力物力、檢測無線網路服務使用者之合法使用期限，未來可進一步延伸本研究所提之機制於 Ad Hoc Network 及 3G-WLAN 雙網整合之應用情境下，使得使用者無論在點對點式或整合式行動通訊等不同網路拓蹼下，均能受到高度認證安全機制之保障。

參考文獻

[1] 謝燦榮，"適用於多伺服器環境之兼具效率與安全的身份認證機制"，***大葉大學資訊管理系碩士班***, 2005.

[2] Corral, G., Cadenas, X., Zaballos, A. and Cadenas, M.T., "A distributed vulnerability detection system for WLANs". in ***Proceedings of First International Conference on Wireless Internet,*** pp.86-93, 2005.

[3] Curtis Gerald and Patrick Wheatley," Applied Numerical Analysis**",** ***Pearson Education*****, 2003**

[4] H.S. Venter and J.H.P. Eloff., "Vulnerability forecasting-a conceptual model". ***Computers & Security***, Vol. 23, Issue 6. pp. 489-497, 2004

[5] Herzog, P. "Open-source security testing methodology manual-wireless security testing section (OSSTMM WIRELESS)", ***The Institute for Security and Open Methodologies***, 2003.

[6] IEEE 802.11," Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ***IEEE Standard***, 1999.

[7] Il-Gon, Kim, and Jin-Young, C., "Formal verification of PAP and EAP-MD5 protocols in wireless networks: FDR model checking". in ***Proceedings of 18th International Conference on Advanced Information Networking and Applications. AINA 2004.*****,** pp. 264-269, 2004

[8] John Wack, Miles Tracy, and Murugiah Souppaya.," Guideline on network security testing. Technology",***Recommendations of the National Institute of Standards and Technology***, 2003.

[9] Ram Dantu, Gabriel Clothier and Atri, "A. EAP methods for wireless networks". ***Computer Standards & Interfaces***, ARTICLE IN PRESS. pp.1-13., 2006

[10] Sharma, S., Ningning, Z. and Tzi-cker, C. ,"Low-latency mobile IP handoff for infrastructure-mode wireless LANs". ***IEEE Journal on Selected Areas in Communications*****,** Vol. 22, Issue 4, pp. 643-652., 2004

[11] Tom Karygiannis and Owens, L. "Wireless network security 802.11, Bluetooth and handheld devices". , ***NIST Special Publication***, 2002.

[12] Woei-Jiunn Tsaur,. "Several security schemes constructed using ECC-based self-certified public key cryptosystems". ***Applied Mathematics and Computation***, Vol. 168, No. 1. pp. 447-464, 2005

[13] Woei-Jiunn Tsaur, Chia-Chun Wub and Lee, W.-B. "A smart card-based remote scheme for password authentication in multi-server Internet services". ***Computer Standards & Interfaces*****,** Vol. 27, No. 1. pp. 39-51., 2004

[14] Urien, P., Badra, M. and Dandjinou, M., "EAP-TLS smartcards, from dream to reality". in ***Proceedings of 4th Workshop on Applications and Services in Wireless Networks,*** *. ASWN 2004.* , pp 39-45., 2004

[15] Yue, M. and Xiuying, C., "How to use EAP-TLS authentication in PWLAN environment". in ***Proceedings of the 2003 International Conference on Neural Networks and Signal Processing*** .pp. 1677-1680 , 2003