基於模糊邏輯技術之無線交談金鑰安全預測機制

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

摘要

無線區域網路(Wireless Local Area Network, WLAN)技術其分散式運作的特性，提供今日使用者於機動性與便利性之資訊應用需求。然而，其通訊節點之間的安全亦充滿許多的不確定性，通訊節點的稽核工作也更為困難，使得使用者必須面臨異於以往的資訊安全風險。自1990年代末期以來至2007年，雖陸續有學者應用模糊邏輯技術其善於處理不確定性問題之能力以設計網路安全等級之預測機制，但現有方法仍無法兼顧使用者其機密性、便利性與節省系統運算資源等需求。因此，本研究提出無線交談金鑰安全預測機制，透過此機制之運作將可使同一使用者於每次登入時，無需皆更換交談金鑰，以節省系統運算資源。使用者可視交談金鑰之風險預測結果，以評估是否需重新更換交談金鑰，如此一來除了可降低系統於產生交談金鑰時所耗費的運算資源，更可免除使用者須時常更新交談金鑰的困擾。相信本機制可提供使用者一兼具高安全性、便利性與低成本之無線交談金鑰安全解決方案。

關鍵詞：無線區域網路安全、模糊邏輯、交談金鑰、橢圓曲線密碼系統

Abstract

Wireless Local Area Networks (WLAN) provide the demand for information application in the mobility and the convenient capital for users. At the same time, users must to face the variance in the former information security risk. Since 1990s to 2007, although there were scholars applying fuzzy logic technology to design the schemes for network security forecasting schemes cause it well at processing ability of the uncertainty question, but the existing method was still unable to give dual attention to user its confidentiality, the convenience and saves demands and so on system operation resources. Therefore, this research proposed the wireless session key security forecasting mechanism in order to let user does not need all to replace the session key when they login the system every time, in order to save the system operation resources. Especially, users could estimate if he needs to regenerate a session key, depending on the forecasting result of the risk of rank for it. In such a case, this schemes cannot only reduce the operation resources of key generating, but also avoid the user to renew session key frequently. We affirm that the proposed schemes can provide the enterprise to achieve a highly secure, convenient and low-cost solution for WLAN.

Keywords：Wireless Local Area Network Security, Fuzzy logic, session key, Elliptic Curve Cryptosystem

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，網路技術其分散式運作的特性，使得通訊節點之間的安全充滿不確定性，通訊節點的稽核工作也更為困難。此種特性在無線區域網路環境下更趨嚴重。為解決上述問題，自1990年代末期以來至2007年，陸續有學者應用模糊邏輯技術其善於處理不確定性問題之能力以設計網路安全等級之預測機制，包含：基於模糊邏輯(Fuzzy Logic)技術之通行碼驗證(Password Authentication)機制[10]、蠕蟲(Worm)傷害預測機制[7]、適用於行動隨意網路(Mobile Ad hoc Network；MANETs)之路由(routing)安全等級推論機制[5]。然而，上述方法仍無法兼顧無線區域網路環境下，使用者的機密性、便利性與節省系統運算資源等需求。因此本研究提出基於模糊邏輯技術之無線交談金鑰安全預測機制，經由駭客的角度，透過交談金鑰破解軟體 Aircrack-ng [3]或 Airsnort [6]等工具，搜集 WLAN 通訊雙方之封包資訊、傳輸時

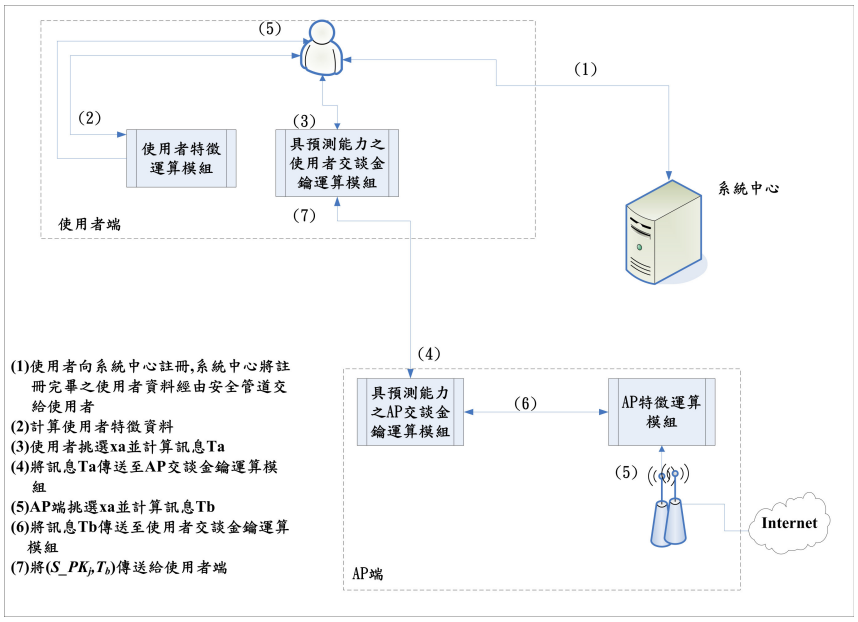

圖2-1　無線交談金鑰建立流程

間與金鑰長度等參數，探討在上述不同參數之組合下，其交談金鑰破解時間與輸入參數之間的關連性。以進一步進行模糊推論程序，最終可輸出交談金鑰安全等級。使得使用者可視交談金鑰之風險等級預測結果，以評估是否需重新更換交談金鑰，如此一來除了可降低系統於產生交談金鑰時所耗費的運算資源，更可免除使用者須時常更新交談金鑰的困擾。

本研究由第2章開始，將敘述所提之機制其運作流程。之後於第3章將針對所提機制其預測功能進行系統實作與模擬 。最後於第4章討論本研究之成果與結論。

2. 兼具高安全性與便利性之無線交談金鑰預測機制

本研究已於第1章中敘述模糊邏輯應用於資訊系統安全之研究現況。以下首先將於2.1節敘述使用者與無線存取點(Access Points, AP)間之無線交談金鑰建立流程，包含交談金鑰參數定義、註冊階段、交談金鑰產生階段。之後於2.2敘述所提機制之各步驟之運作，包含系統初始設定、輸入參數進行模糊化、推論程序、解模糊化。

2.1. 無線交談金鑰建立流程

本研究之機制架構如圖2-1所示，主要成員有使用者、AP 以及系統中心。

在使用者端的部份，本機制設計具預測功能之使用者交談金鑰運算模組[8]，除了可與使用者端的對應模組共同協商出一把交談金鑰外，更提供交談金鑰安全等級之預測功能，而使用者特徵運算模組則可供其運算自身之特徵資訊。就 AP 端而言，亦提供具預測功能之 AP 端交談金鑰運算模組，除了可與使用者端的對應模組共同協商出一把交談金鑰外，更可進一步對所產生的交談金鑰進行安全性之預測。AP 特徵運算模組則可供其運算自身之特徵資訊。

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。以下將於2.1.1至2.1.3節依序定義交談金鑰之相關參數、註冊階段之運作，以及通訊雙方其交談金鑰之建立流程。

2.1.1. 交談金鑰參數定義

(1) p：大質數。
(2) 橢圓曲線多項式 $E(a,b)$：$y^2=x^3+ax+b$，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) 滿足多項式 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 座標值。

(13) s_sk_j：AP_j 的私鑰

(14) S_PK_j：AP_j 的公鑰，其中

$$S\_PK_j = s\_sk_j \cdot B(\mathrm{mod}\, p) = (S\_PK_{jx}, S\_PK_{jy}) \quad (3.2)$$

(15) U_ID_i：Client 端 i 的 ID

系統建置完成後，系統中心公佈 E, B, P_{ca}。

2.1.2. 註冊階段

當使用者 U_i 欲登入至各 AP_j，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:

步驟 1.使用者所進行的運算程序：

(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

$$V_i = h(pw_i || U\_ID_i) \cdot B(mod\, p) = (V_{ix}, V_{iy}) \quad (3.3)$$

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

步驟 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:

$$\begin{aligned} K_{pi} &= V_i + (k_i - h(U\_ID_i)) \cdot B \ (\mathrm{mod}\ p) \\ &= (P_{ix}, P_{iy}) \end{aligned} \quad (3.4)$$

$$w_i = k_i + s_{ca} \cdot (P_{ix} + h(U\_ID_i))(\mathrm{mod}\ p) \quad (3.5)$$

步驟 3.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 2-1 流程(2)所示

步驟 4.使用者 U_i 收到系統中心所核發之資訊後，根據內附資訊計算自己的私鑰 k_{si}

$$k_{si} = w_i + h(pw_i || U\_ID_i) \quad (3.6)$$

步驟 5.驗證公鑰 K_{pi} 的有效性是否成立：

$$k_{si} \cdot B = K_{pi} + h(U\_ID_i) \cdot B + [P_{ix} + h(U\_ID_i)] \cdot P_{ca} (\mathrm{mod}\ p) \quad (3.7)$$

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

2.1.3. 交談金鑰產生階段

步驟 1.使用者交談金鑰產生模組首先隨機選擇一個整數 x_a，之後計算 $T_a = x_a \cdot B\ (mod\ p)$，如圖 2-1 流程(3)，接著將訊息 T_a 傳送給 AP_j，如圖 2-1 流程(4)

步驟 2. AP_j 經由 AP 特徵運算模組隨機選擇一整數 x_b，如圖 2-1 流程(5)，經由 AP 端交談金鑰產生模組計算 $T_b = x_b \cdot B\ (mod\ p)$，如圖 2-1 流程(6)，並將$(S_PK_j, T_b)$傳送給 U_i，如圖 2-1 流程(7)，此時，雙方皆已各自持有計算交談金鑰所需之資訊。

步驟 3.使用者 U_i 運用式(3.8)計算其交談金鑰

$$\begin{aligned} SK &= x_a \cdot S\_PK_j + k_{si} \cdot T_b \\ &= x_b \cdot s\_sk_j \cdot B\ (\mathrm{mod}\ p) \\ &+ k_{si} \cdot x_b \cdot B\ (\mathrm{mod}\ p) \end{aligned} \quad (3.8)$$

AP_j 收到 x_a 後計算

$$\begin{aligned} V_u &= K_{pi} + h(U\_ID_i) \cdot B \\ &+ [(K_{pix} + h(U\_ID_i)) \bmod p] \cdot P_{ca} \end{aligned} \quad (3.9)$$

並運用式(3.9)求出之 V_u 計算出 AP 端的交談金鑰 SK，如式(3.10)

$$\begin{aligned} SK &= x_b \cdot V_u + s\_PK_j \cdot T_a \\ &= x_b \cdot k_{si} \cdot B\ (\mathrm{mod}\ p) \\ &+ s\_sk_j \cdot x_a \cdot B\ (\mathrm{mod}\ p) \end{aligned} \quad (3.10)$$

至此，雙方得到相同的交談金鑰 SK，完成交談金鑰的建立。

2.2. 無線交談金鑰預測機制

本研究已於2.1.3節中敘述使用者端與AP端雙方建立交談金鑰之流程。然而，由於交談金鑰之建立過程仍需耗費頗多系統運算資源。因此，本機制所具備之交談金鑰運算模組，亦提供基於模糊邏輯技術之交談金鑰安全等級預測功能，使得同一使用者於每次登入時，無需皆更換交談金鑰，以節省系統運算資源。換句話說，本預測功能將透過模糊技術的處理不確定性資訊的優越能力，以簡單明瞭的方式預測目前所使用的交談金鑰，在傳輸多少封包資訊以及經歷多少傳輸時間後，是否存在被破解的風險及其隸屬之安全等級。使用者可視交談金鑰之風險預測結果，以評估是否需重新更換交談金鑰，如此一來除了可降低系統於產生交談金鑰時所耗費的運算資源，更可免除使用者須時常更新交談金鑰的困擾。以下將敘述本小節所提之預測機制其運作方式。本機制基於學者 Sanguanpong 等人[7]與 Jing 等人[5]所提之模糊邏輯推論機制，設計適用於預測 WLAN 交談金鑰安全等級之模式，主要經由法則推論的程序以達成預測之功能，其模式架構如圖2-2所示，以下將敘述此模式其相關參數的運作流程。

步驟一、系統初始設定

此步驟主要在於建立輸入端、法則庫、輸出端之間的關聯性，如圖 2-3 所示，本研究透 fuzzyTECH[4]模擬軟體，首先定義三項輸入參數，亦即金鑰長度(key_length)、已傳輸之封包數量(packet_num)、已連線之時間(trans_time)，接著定義輸出端之金鑰安全等級(security_level)，最後經由畫面左邊之導覽列拖曳“法則庫(Rule_Base)方塊”

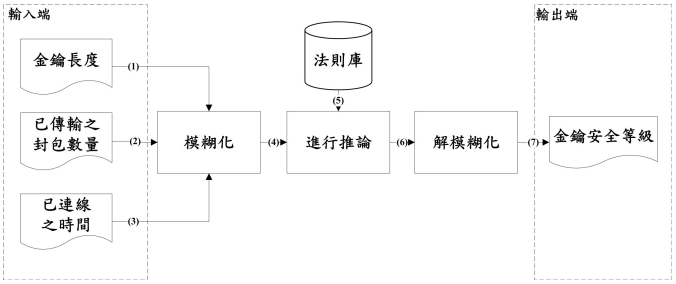

圖 2-2　適用於預測無線區域網路交談金鑰安全等級之模式架構

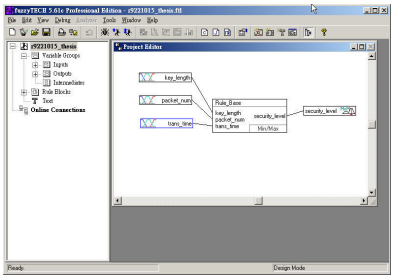

圖 2-3　交談金鑰預測模式初始化設定

至圖中之 Project Editor 視窗中，再設定法則庫與輸入端及輸出端之間的關連性，經由輸入端之交互關係，即可產生系統初始之法則庫，供後續步驟運作。

步驟二、輸入使用之金鑰長度、已連線之時間、已傳輸之封包數量等資訊，進行模糊化

在此步驟，本研究首先定義三個輸入參數，分別為金鑰長度、已傳輸之封包數量及使用者已持續連線之時間。由於 Jing、Sanguanpong、Wilfred [9]等多位學者已分別將梯形隸屬函數及三角隸屬函數應用於網路通訊之相關研究中，由此可知此兩類之函數可適用於 WLAN 以及 LAN 等網路通訊應用情境下，因此本研究亦結合梯形與三角形等兩種隸屬函數進行模式之設計：

步驟 2-1:

就金鑰長度之設定而言，本研究除基於學者 Jing 等人的設定值，分別以 64bits 與 128bits 之金鑰長度為基準進行調整外，更進一步針對此兩數值進行模糊分割處理，之後轉換成語意變數，以利後續之模糊化程序，如圖 2-2 流程(1)所示；其隸屬函數示意圖如圖 2-4 所示。

圖 2-4　交談金鑰長度之模糊隸屬函數
(單位：bits)

步驟 2-2:

本步驟於封包傳輸數量之參數設定則參考 Corral 等人[3]所述，以一百萬個封包量為基準進行調整，亦對此數值進行模糊分割處理，之後轉換成語意變數以利後續之模糊化程序，如圖 2-2 流程(2)所示；其隸屬函數示意圖如圖 2-5 所示。

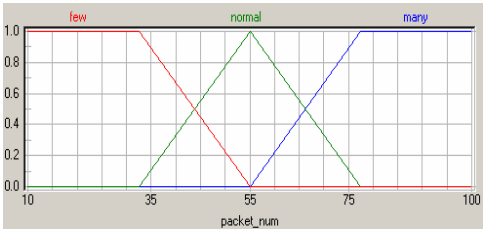

圖 2-5　封包數量之模糊隸屬函數
(單位：萬封包數)

步驟2-3:

根據學者 Bitttau 等人[2]的研究，駭客在破解無線交談金鑰時的關鍵參數，除了金鑰長度、封包傳輸數量外，資料的持續傳輸時間亦為另一重要指標，當駭客持續搜集封包資訊的時間越長，使用者金鑰被破解的可能性越高，因此本研究在設計金鑰預測模式時，亦考慮封包資訊的持續傳輸時間，以 40 分鐘至 200 分鐘為範圍進行調整，如圖 2-2 流程(3)所示；其隸屬函數示意圖如圖 2-6 所示。本步驟最後將可輸出金鑰長度、封包傳輸數量、封包持續傳輸時間所個別對應的隸屬函數 *u(key_length)*、*u(packet_num)*、*u(trans_time)*，如圖 2-2 之流程(4)。

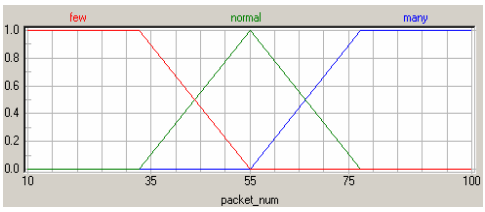

圖 2-6　封包持續傳輸時間
(單位：分鐘)

表 2-1　交談金鑰安全等級預測法則

輸入端			輸出端
金鑰長度	**封包數量**	**傳輸時間**	**安全等級**
短	少	低	中
短	少	中	中
短	少	高	低
短	中	低	中
短	中	中	低
短	中	高	低
短	多	低	低
短	多	中	低
短	多	高	非常低
中	少	低	高
中	少	中	中
中	少	高	中
中	中	低	中
中	中	中	中
中	中	高	中
中	多	低	中
中	多	中	中
中	多	高	低
長	少	低	非常高
長	少	中	高
長	少	高	高
長	中	低	高
長	中	中	高
長	中	高	中
長	多	低	高
長	多	中	中
長	多	高	中

步驟三、進行推論程序

步驟 3-1:

首先定義以下之交談金鑰安全等級預測法則參數：*m* 代表法則之數目

$X_{1.....}X_m$ 代表輸入端之參數敘述；例如“key-length、packets”

$A_{1.....}A_m$ 代表輸入端之語意變數；例如“short、long、low、normal、high”

$Y_{1.....}Y_m$ 為輸出端之結果敘述；例如“security-level”

$B_{1.....}B_m$ 為輸出端之語意變數；例如“short、long、low、normal、high”

根據上述之法則定義，可建立以下之法則型式: *If* ***key-length*** *is* ***short*** *and* ***packets*** *is* ***low*** *and* ***trans_time*** *is* ***low*** *then* ***security-level*** *is* ***medium***，其可能之法則組合列表，如表 2-1 所示。其中，就金鑰長度等級的設定而言，“短”的範圍設定為 40~84 bits；“中”的範圍設定為 62~106 bits；“長”的範圍設定為 84~128 bits。就封包數量的範圍設定而言，將“少”的範圍設定為 10~55 萬個；“中”的範圍設定為 32~77 萬個；“多”的範圍設定為 55~100 萬個。就傳輸時間的範圍而言，將“低”的範圍設定為 40~120 分鐘；“中”的範圍設定為

80~160 分鐘；“高”的範圍設定為 120~200 分鐘。此外，若未來系統參數範圍有所變化，例如金鑰長度或封包數量，本研究亦可視使用上之需求，以動態更新等級範圍並調整法則，快速反應最新之無線網路使用情境。

步驟 3-2:

在法則定義完畢後，接著比對輸入值與表 2-1 內所列之語意變數，若相符則代表該法則成立，如圖 2-2 之流程(5)。由於同樣一組輸入變數有可能同時觸發多條法則，使得推論結果的集合亦存在多個可行解:，因此需進一步進行推論程序。本研究採用最為普遍之 Mamdani 最小模糊推論法[10]進行模糊推論，如圖 2-2 之流程(6)。其公式如下：

$$u(\text{sec}urity\_level) = \min[u(key\_length), u(packet\_num), u(trans\_time)] \quad (3.11)$$

其中，

u(key_length)：金鑰長度之隸屬程度

u(packet_num)：封包傳輸數量之隸屬程度

u(trans_time)：封包傳輸時間之隸屬程度

u(security_level)：金鑰安全等級隸屬程度

步驟四、解模糊化

步驟 4-1:

就金鑰安全等級模糊語意變數之定義而言，本研究主要延伸學者 Bittau 等人的實驗成果，以金鑰被破解的時間範圍為基礎，透過表2-2將交談金鑰之安全性劃分為五個等級，其模糊隸屬函數如圖2-7所示。

步驟 4-2:

針對本小節步驟3-2所求得之金鑰安全等級隸屬程度進行解模糊化程序，以推論出目前所使用之交談金鑰其安全等級，如圖2-2之流程(7)。本研究所採用的解模糊化方法為最大平均法；此方法具有高合理性以及高計算效率等特性[1]。

表 2-2　金鑰安全等級-破解時間對照

金鑰安全等級		金鑰破解時間(單位：分鐘)
1	非常低	<48
2	低	48-96
3	中	96-144
4	高	144-192
5	非常高	>192

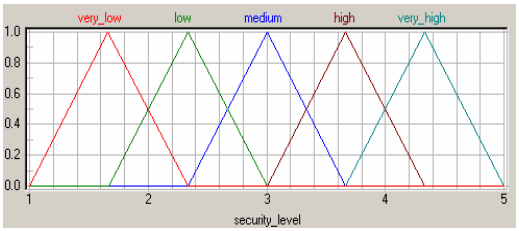

圖 2-7　交談金鑰安全等級之模糊隸屬函數

以下將經由一範例進一步說明本小節所提之交談金鑰安全等級預測模式其運作方式，在此範例中，將使用者的金鑰長度設定為 65bits、已傳輸之數量為 100 萬個封包、已持續連線的時間為 80 分鐘；其流程如下：

(1) 將金鑰長度設定為 65bits，則可分別計算隸屬程度為“low”以及“medium”之數值，如圖 2-8 所示。

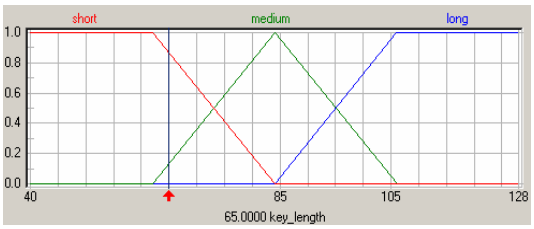

圖 2-8　交談金鑰長度為 65bits 時之隸屬程度

(2) 將已傳輸之封包數量設定為100萬個，則可分別計算隸屬程度為“normal”以及“many”之數值，如圖2-9所示：

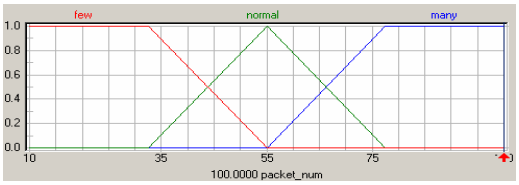

圖 2-9　封包傳輸數量為 100 萬個之隸屬程度

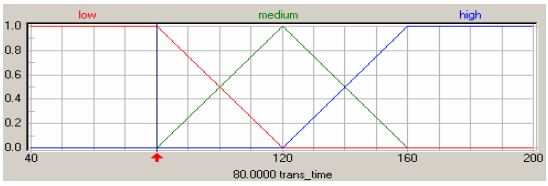

圖 2-10　封包傳輸時間為 80 分鐘之隸屬程度

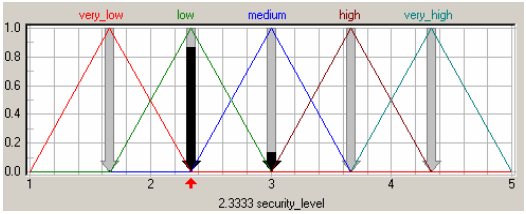

圖2-11　已解模糊化之金鑰安全等級

表 2-3　符合輸入端語意變數組合之法則集合

金鑰長度 (隸屬程度)	封包傳輸量 (隸屬程度)	傳輸時間 (隸屬程度)	安全等級 (隸屬程度)
短(0.86)	中 (0.54)	中 (0.6)	低 (0.54)
短(0.86)	中 (0.54)	高 (0.4)	低 (0.4)
短(0.86)	多 (0.46)	中 (0.6)	低 (0.46)
短(0.86)	多 (0.46)	高 (0.4)	非常低 (0.4)
中(0.14)	中 (0.54)	中 (0.6)	中 (0.14)
中(0.14)	中 (0.54)	高 (0.4)	中 (0.14)
中(0.14)	多 (0.46)	中 (0.6)	中 (0.14)
中(0.14)	多 (0.46)	高 (0.4)	低 (0.14)

(3) 將已持續傳輸封包之時間設定為 80 分鐘，則可分別計算隸屬程度為“medium”以及“high”之數值，如圖 2-10 所示。

(4) 經由本小節範例內容中(1)-(3)的計算程序，推論出與計算結果相符之模糊法則集合如表 2-3。

(5) 經由計算表 2-3 中各語意變數之隸屬程度，配合式 3.22 之計算，可得到 Security_level 對應於各層級之隸屬程度 *u(security_level)*，最後輸入表 2-3 中之各項數值進行解模糊化，可得到輸出值為 2.33，如圖 2-11 所示。

由此可得知在此一範例中，該名使用者所面臨之安全等級為“中”，此等級進一步對映至表 2-2 可得知，其可能被破解的時間範圍約為 96 分鐘至 144 分鐘，其安全性為中等。

經由本小節所提之交談金鑰安全等級預測模式，一般使用者毋需記憶繁複且具高度專業的網路術語，諸如交談金鑰、封包等，僅需參考本機制所輸出的安全等級預測警訊，即可防患於未然，主動更新交談金鑰，同時也免除了時常更換金鑰的麻煩，故本方法實為一兼具安全性與便利性之交談金鑰安全等級預測機制。

3. 系統實作與模擬

本研究已於第2章敘述所提機制之運作流程，經由2.1.1節之參數定義可得知，本研究所具備之交談金鑰運算模組可產生基於橢圓曲線離散對數困難度且長度為160位元之高安全性交談金鑰。然而，站在使用者的角度，本研究亦考量在不同的使用情境下，使用者對資通安全等級之需求亦有高有低。例如，當使用者於餐廳用餐時、短期造訪企業組織，甚至是參加學術研討會等需要短暫使用無線網路服務的場合，其無線交談金鑰的使用時間及封包傳輸量亦相對較少，針對此類不同使用情境，若千篇一律均產生160位元的無線交談金鑰，則所耗費的系統資源亦相當可觀。因此，在分別敘述本研究所提之高安全交談金鑰產生方式及其安全性分析後，本章以下將以所設計出來的無線交談金鑰，使用長度64/128位元為例進行系統實作與模擬，以證明本研究所提之機制除了可產生高安全性的交談金鑰，並在較短交談金鑰、較少封包傳輸量及較低傳輸時間的應用情境下，亦可降低無線網路攻擊行為所帶來的安全威脅。首先於3.1節描述本研究之實驗環境，之後於3.2節敘述所提機制其具備的無線交談金鑰預測功能之實驗步驟。

3.1. 實驗環境描述

如圖3-1所示，在本研究之實驗環境中，共存在三項網路通訊個體，分別為封包傳送方、封包接收方、無線存取點。特別一提的是，由於本研究所採用的無線交談金鑰破解軟體需特定晶片才可支援，因此本實驗所採用的無線網路卡其晶片為Atheros，此類型之晶片已證實確可順利與無線金鑰破解軟體 aircrack-ng-0.9-win 協同運作。

此外，存在於本實驗環境之三項網路通訊個體皆已事先設定無線網路交談金鑰；為符合目前實務上之資通應用需求，本研究將分別以64位元及128位元之金鑰長度進行實驗，未來若無線網路卡、無線存取點，以及無線金鑰破解軟體所支援之金鑰長度增加，本研究所提之預測功能亦可隨之彈性調整金鑰長度。

3.2. 實驗步驟

本研究之實驗步驟主要可分為五大項，分別為：一、設定無線交談金鑰；二、無線網域資訊偵蒐；三、蒐集無線網路封包；四、破解無線交談金鑰；五、無線交談金鑰安全等級預測。以下將敘述本研究之實驗步驟細節。

步驟一、設定無線交談金鑰

經由圖 3-2 可看出，目前所設定的 WEP 無線交談金鑰長度為 128 位元，其值為 26 個 16 進位的字元: 014842d480b571495a4a036379。

步驟二、無線網域資訊偵蒐

網路入侵者在面對一全然陌生之攻擊目標網域時，首先需針對攻擊目標進行資訊之探測與偵蒐。在此步驟中，本研究採用 NetStumbler 做為無線網域資訊偵搜之工具軟體；其畫面如圖 3-3 所示。經由圖中可得知，在鄰近之無線網域內，僅有一台運作中之無線存取點，其 MAC address 為 00-90-CC-E6-95-18；SSID 為“home”；使用之通訊頻道為 6；且已採用 WEP 加密機制。

步驟三、蒐集無線網路封包

在使用 NetStumbler 蒐集目標網域資訊後，接著便可針對所蒐集到的資訊，諸如 SSID、頻道、MAC address，配合 Airodump-ng 開始蒐集無線網路封包。然而，由於在一般使用情境下，無線網域內的封包流量較為緩和，因此入侵者通常會透過各式各樣的手法，以產生疑似合法的網路流量，以縮短無線封包的蒐集時間。

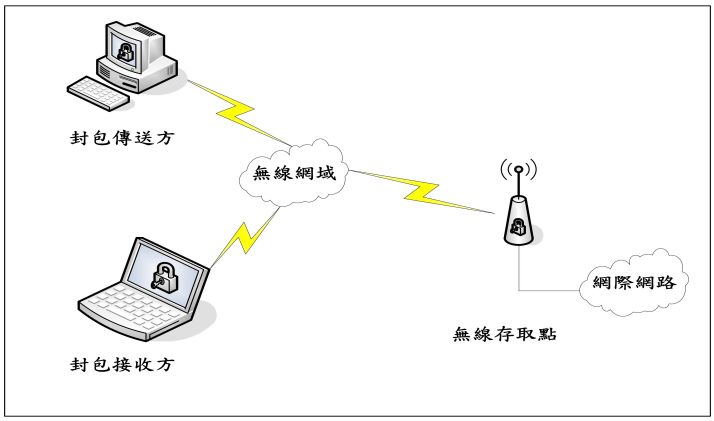

圖 3-1　本研究之實驗環境

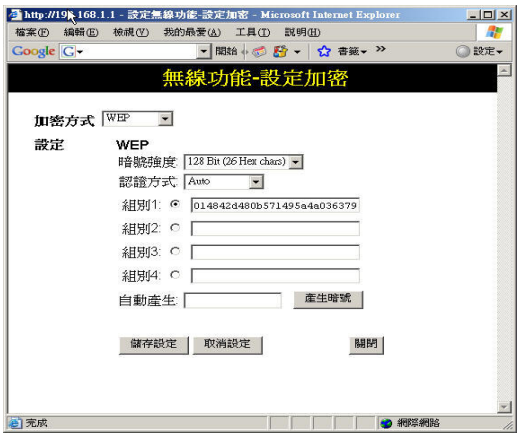

圖 3-2　無線存取點 WEP 金鑰設定

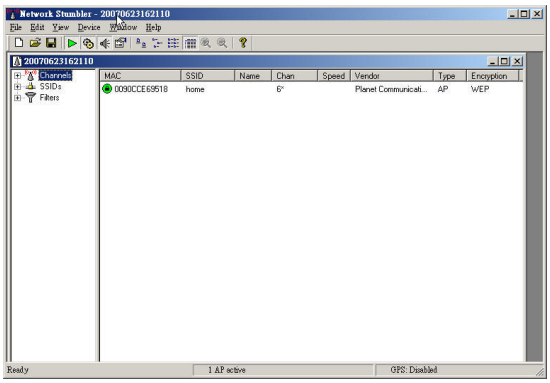

圖3-3　NetStumbler 主畫面

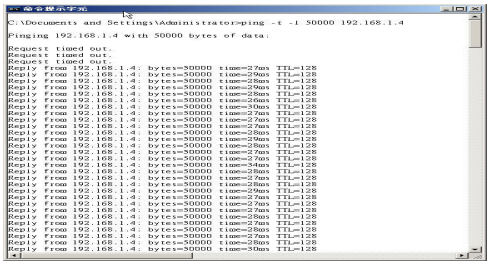

圖 3-4 產生無線網路封包

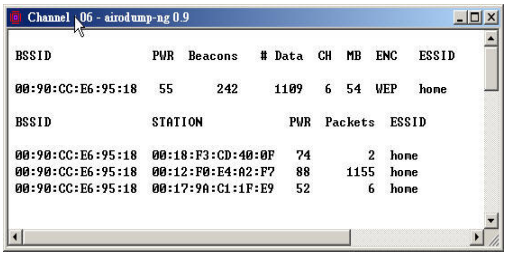

圖 3-5　使用 Airodump-ng 蒐集無線網路封包

在此步驟的一開始，本實驗首先經由封包傳送端之個人電腦執行 ping 指令產生封包流量，之後將無線網路封包傳送至封包接收端之筆記型電腦其內建之無線網路卡介面，如圖 3-4 所示。當無線網路流量漸漸增加後，進入 Airodump-ng 主畫面即可看到目前網域內之通訊個體等相關資訊，如圖 3-5 所示，圖中列出所有經由 ESSID 為“home”的無線存取點連線之網路介面，包含 MAC address 分別為 00-17-9A-C1-1F-E9 、 00-12-F0-E4-A2-F7 、 00-18-F3-CD-40-0F 三項無線網路介面，圖中亦可得知，00-12-F0-E4-A2-F7 之介面，亦即 IP 為 192.168.1.4 所接收到的網路流量已遠高於其他網路介面，當傳輸之封包數量達到所欲測試之數值(EX:30 萬或 50 萬)，即可按下 ctrl+c 終止此步驟。

步驟四、破解無線交談金鑰

經由圖 3-6 中可得知，在此次破解程序中，Aircrack 一共嘗試了 123 支交談金鑰，100%破解出本研究於實驗步驟一所設定之交談金鑰：014842d480b571495a4a036379，此次實驗總計監聽了 510196 個封包，持續傳輸時間由 2007 年 6 月 23 日 21:23 起至 2007 年 6 月 24 日 00:06 分，共約歷時 142 分鐘。

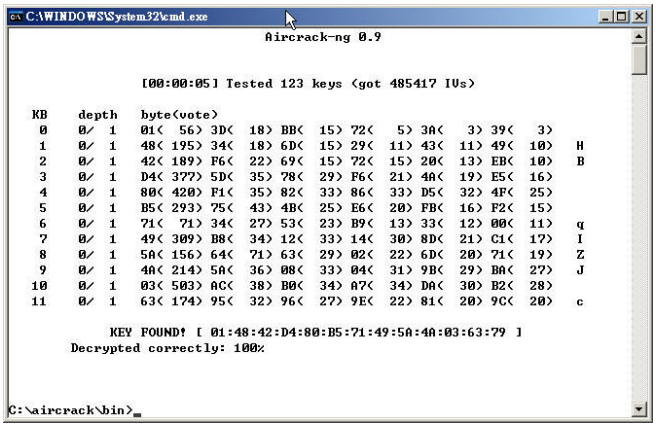

圖3-6　使用 Aircrack-ng 破解交談金鑰

表 3-1　測試個案

測試項目	金鑰長度 (單位：位元)	封包傳輸量 (單位：萬)	平均封包傳輸量 (單位：萬)	傳輸時間 (單位：分鐘)	平均傳輸時間 (單位：分鐘)	交談金鑰安全等級
1	64	16	15	96	98	中
		14		97		
		15		101		
2	64	72	70	94	94	低
		71		93		
		67		95		
3	128	33	35	149	150	高
		35		148		
		37		153		
4	128	49	51	144	142	中
		51		143		
		53		139		

步驟五、無線交談金鑰安全等級預測

經由本研究實驗步驟一至實驗步驟四，可得知若將 WEP 交談金鑰設定為 128 位元之長度，且其值為 014842d480b571495a4a036379，則在傳輸 510196 個封包，歷時 142 分鐘後，即遭破解。因此，在此步驟將輸入實驗結果之數據於本研究應用 fuzzyTECH 軟體所建構之 WLAN 交談金鑰安全等級預測機制，進行模擬，如圖 3-7 所示，圖中可看出解模糊化之後的安全等級數值為 3.6667，之後再進一步對照表 2-2 之金鑰安全等級-破解時間對照，可得知此次實驗結果所對應之安全等級為「中」，對應之金鑰破解時間大約落在 96-144 分鐘之區間內，使用者可自行決定是否需更新交談金鑰。

如表 3-1 所示，除上述所提之測試個案(表中之測試項目 4)外，本研究亦蒐集並統計在不同應用情境下，其金鑰長度、封包傳輸量與傳輸時間等參數之間的交互關係及其對應的交談金鑰安全等級；如表 3-1 中之項目 1 至項目 3。就項目 1 之應用而言，其所輸出的安全等級為「中」，使用者可自行決定是否需更新交談金鑰。而根據項目 2 所顯示之推論結果，其所輸出的安全等級為「低」，建議使用者應儘速更換交談金鑰。從項目 3 之推論結果可得知，其所輸出的安全等級為「高」，使用者暫時毋須更換交談金鑰。

經由本節實驗可得知，本研究所設計之交談金鑰安全等級預測功能，符合實務上之無線網路應用情境，為一兼具安全性與便利性之無線交談金鑰安全等級預測機制。

4. 討論與結論

4.1. 討論

綜觀現今進行無線區域網路安全防護所面臨的問題，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，增加安全稽核難度。

而且，在本研究之緒論中亦提及，現有研究仍無法兼顧無線區域網路環境下，使用者的機密性、便利性與節省系統運算資源等需求。因此，以下將陳述本研究針對上述問題所獲致之成果:

一、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 弱點檢測時的網路專業知識門檻，就模糊推論結果而言，則以明確的等級表示目前所使用的交談金鑰其安全性，以輔助使用者進行判讀，使得無線區域網路安全防護之作業程序可維持一定的品質。

二、使用者可視交談金鑰之風險等級預測結果，以評估是否需重新更換交談金鑰，以同時滿足使用上的便利性及安全性需求。

三、在檢測階段步驟 9 中，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 x_a 及 x_b，亦將面臨橢圓曲線離散對數困難度[8]，可確保交談金鑰安全性。

4.2. 結論

本研究提出兼具高安全性與預測能力之 WLAN 弱點檢測機制，將可同時避免 WLAN 環境中的節點異動頻繁所造成之安全性衝擊、簡化並降低企業組織於稽核未經授權之 AP 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、預測並評估目前所使用的交談金鑰之風險等級。相信透過本機制之建立，將可提供企業組織一兼具高安全性、便利性與低成本之 WLAN 安全解決方案。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，使得企業組織在面對瞬息萬變的經營環境下，均可兼顧 WLAN 之安全性與便利性。

5. 參考文獻

[1] C. V. Altrock, *Fuzzy Logic & Neuro Fuzzy Applications In Business & Finance*. Upper Saddle River，NJ:Prentice Hall PTR, 35-43, 1996.

[2] A. Bittau, H. Mark, & L. Joshua, “The Final Nail in WEP’s” Coffin, *Proceedings of 2006 IEEE Symposium on Security and Privacy* (pp. 386-400), USA：California., 2006.

[3] G. Corral, X. Cadenas, A. Zaballos, & M. T. Cadenas, “A Distributed Vulnerability Detection System for WLANs.” *Proceedings of First International Conference on Wireless Internet* (pp. 86-93), Budapest：Hungary, 2005.

[4] FuzzyTECH, *FuzzyTECH Features Overview* Available:http://www.fuzzytech.com/e/ftpo.html [2007, March 15]

[5] N. Jing, J. Wen, J. Luo, X. He, & Z. Zhou, “An Adaptive Fuzzy Logic Based Secure Routing Protocol in Mobile Ad Hoc Networks.” *Fuzzy Sets and Systems,* Vol.157, No. 12, 1704-1712., 2007.

[6] N. T. Anh, & R. Shorey, “Network Sniffing Tools for WLANs: Merits and Limitations,” *Proceedings of the 2005 IEEE International Conference on Personal Wireless Communications* (pp. 389-393), India：New Delhi, 2005.

[7] S. Sanguanpong, & U. Kanlayasiri, “Worm Damage Minimization in Enterprise Networks,” *International journal of Human-Computer Studies*, Vol. 65, NO. 1, 3-16., 2006.

[8] W. J. Tsaur, “Several Security Schemes Constructed using ECC-Based Self-Certified Public Key Cryptosystems,” *Applied Mathematics and Computation*, Vol. 168, 447-464., 2005.

[9] L. Wilfred, W. Allan, & T. S. Dillon,. “Application of Soft Computing Techniques to Adaptive User Buffer OverflowControl on the Internet”. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Review*s, Vol. 36, No. 3, 397-410., 2006

[10] G. Willem, D. Ru, & J. H. P. Eloff, “Enhanced Password Authentication through Fuzzy Logic,” *IEEE expert magazine*, Vol.12, 38-45.,1997.

[11] Y. Xie, & K. Burnham, Fuzzy decision support system for demand forecasting with a learning mechanism. *Fuzzy Sets and Systems*, Vol. 157, No.(12), 1713-1725., 2006.