新的高效率車載服務之安全架構

簡宏宇	劉晏辰	黃新睿	陳榮靜	李南逸
暨大資管系教授	暨大資管系碩士班	暨大資管系碩士班	朝陽資管系教授	南台資管系教授
hychien@ncnu.edu.tw	s98213527@ncnu.edu.tw	s98213543@ncnu.edu.tw	crching@cyut.edu.tw	nylee@mail.stut.edu.tw

摘要

由於車載網路(VANET)藉由無線通訊技術傳送資料於車輛及路邊存取站台(Access Point，縮寫AP)，因此攻擊者容易在無線電波涵蓋範圍內擷取封包，進行資料的竄改、重送攻擊或其他攻擊等，造成駕駛人的隱私資訊洩漏，嚴重的影響網路安全；此外，駕駛者也常需要於進行中存取網路服務。因此，本論文提出以高效能的 Three party Encrypted Key Exchange (3PEKE) 來建立車輛與路邊存取站台間的安全通訊；針對駕駛者部份，我們提出一以指紋認證搭配 3PEKE 方式來建立駕駛者與應用服務間的安全通訊及車輛移動間安全的換手(Hand-off)協定；如此不但效率高且可兼顧駕駛的安全。

關鍵詞：車載網路、3PEKE、指紋認證、換手。

Abstract

Vehicular Ad-Hoc Network (VANET) would become more and more popular, and it is imperative to design an efficient and secure VANET. This paper proposes a security framework for VANET. One of the framework is a highly efficient Three-party encrypted key exchange (3PEKE) protocol to build the secure channels between vehiculars and road side access points. For drivers's safety, we propose a fingerprint-based 3PEKE protocol to build secure channels between drivers and application servers, and a safety Hand-off protocol .

Keywords:VANET, 3PEKE, Fingerprint authentication, Hand-off。

1. 前言

近年來，資訊科技應用不斷創新，車載資訊系統逐漸受到重視並迅速發展，傳統智慧行車裝置僅能提供燃料、引擎、溫度檢測，以及駕駛座位依不同駕駛人自動調整…等功能。車載資訊系統結合智慧車輛安全、氣象預報、行車導航、車內資訊娛樂、電子收費、安全監控等系統。2009 年全球產值達 258 億美元，預估 2010 年，全球車載資訊系統市場規模有 1 千億美元的市場銷售價值。

目前車載網路尚未有一套安全標準，但在開發車載網路應用時，必須建立足夠的安全機制來保護傳送的資訊及認證使用者的合法性[1]，這樣一來才能使開發的系統實際使用。一個好的 VANET 安全架構需考慮車輛與 AP 間的安全通訊、車輛在 AP 間的換手(Handoff) 通訊安全、駕駛者使用上的方便及安全性、系統擴充性及高效率等等。

Hakjae-Kim [2] 等人提出車載認證方法，但他們忽略了一項威脅，那就是中間人攻擊(Man-in-middle attack)。由於傳統的使用者認證方式是經由密碼或是智慧型卡片做認證，但這些傳統認證是潛在許多弱點的，例如卡片遺失、遭偷竊，或是忘記密碼等；此外，駕駛者如果需要於駕駛中輸入密碼或金鑰也是極不方便，甚至帶來危險；加上近來，生物識別技術逐漸受到重視，生物識別技術是最可靠的身份認證方式，因生物識別直接使用人的物理特徵來表示每一個人的數字身份，不同的人具有不同的生物特徵，因此幾乎不可能被仿冒和

複製[3]。因此在本論文，我們提出以高效能的 Three party Encrypted Key Exchange (3PEKE) 來建立車輛與路邊存取站台間的安全通訊，並設計出高效率的 AP 間換手協定；針對駕駛者部份，我們提出一以指紋認證[4, 5]為基礎之 3PEKE 方式[6]來建立駕駛者與應用服務間的安全通訊，如此駕駛者在開車時就不用分心於輸入密碼或金鑰的動作；如此不但效率高且可兼顧駕駛的安全。

然而指紋影像對於多數的人而言是較隱私的，且所需的儲存量和比對的運算量，相較於密碼，是較為龐大和複雜的，所以指紋資訊必須以多封包的方式來傳送，因此我們必須考量車輛在移動時 AP(Access Point)間資料的傳遞，以及認證使用者的合法性和指紋資訊安全傳達的問題。

2. 環境介紹

在本論文所討論的 VANET 包含四種實體-認證伺服器(Authentication Server, AS)、車載服務伺服器(VANET Services Server, VSS)、車載電腦(client)、及使用者(User)。 AS 是整個系統的認證中心，提供對 APs、clients 及 Users 的認證；AS、AP、及 VSS 可透過既有的 Internet 形成一安全的網路層(可以是有線傳輸或無線傳輸[7])；車載電腦 (client)以無線通訊方式與 AP 通訊，在取得 AS 認證後即可透過 AP 存取 VANET (甚至 Internet)；然而車載電腦 (client)在車子行進間需存取不同 APs，

並在 APs 間進行換手協定；最後，使用者(User)為取得付費(或加值)服務，需進行使用者認證；當然 User 與 VSS 需架構在 client、AP 與 AS 所認證過所架起的網路通道上。其中，我們假設 AS 與 APs、AS 與 VSS 可利用現存的密碼安全機制 [8]建立安全通道；而 client 與 AP 間的無線通道安全及 User 與 VSS 間的安全通道建立是本論文的主題。

如圖 1 所示，車載電腦 (client)在進入 VANET 範圍內時會自動偵測路邊 APs，並透過 AS 與 AP 進行認證協定以建立與 AP 的安全通道；之後當車子行進間，需在 APs 間進行換手協定以保持通訊的安全；當 client 與 APs 間建立安全通道後，使用者便可透過所建立的通道選擇所需的車載服務(例如氣象預報、行車導航…等服務)。當然，有些服務是免費，而其中有些服務是必須要額外收費的，例如影音娛樂服務、電子收費；因此，User 與 VSS 間的認證是必需的。為考慮 Uesr 在行車間輸入金鑰(或密瑪)進行認證會分心甚至帶來危險，本論文提出以指紋取代密碼來做 User 認證。

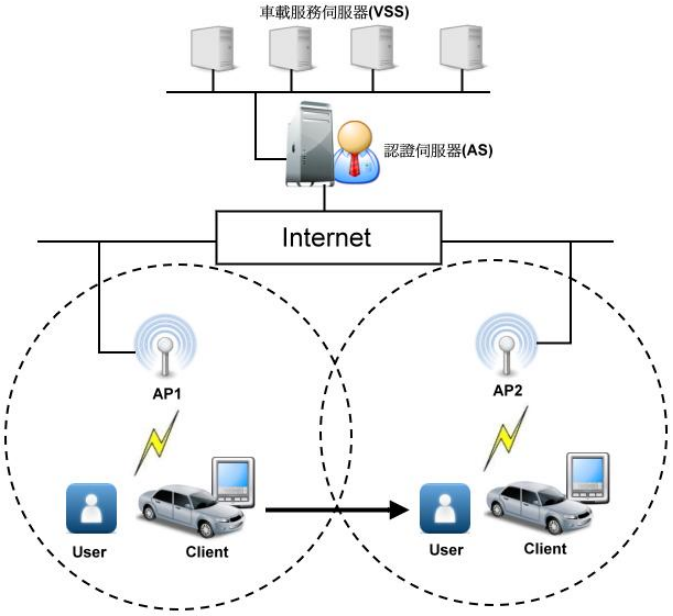

圖 1. 車載網路環境架構

3. 安全需求

由於行車間若要求使用者輸入密碼認證可能會有行車安全顧慮，本論文提出在行車間以使用者指紋認證可改善此缺點。

我們將車載電腦 (client)結合指紋感應器；指紋驗證分為指紋註冊和指紋認證兩個階段。首先，使用指紋感應器擷取指紋影像，再取出指紋影像的指紋特徵值，將特徵值存入認證伺服器(AS)中；但因考慮到使用者的隱私權，所以取出特徵值後，必須將原始的指紋影像刪除，完成指紋註冊手續。在指紋認證階段，駕駛者於指紋感應器按壓指紋，再透過指紋感應器的預處理，取出指紋特徵值並經由無線網路將特徵值傳送到鄰近的 AP，AP 再透過網路與認證伺服器比對先前註冊的指紋特徵值。以下我們討論此架構下 VANET 的安全需求。

需求 1：C 與 AP 間的認證金鑰。

需求 2：U 與 VSS 間的認證金鑰。

需求 3：C 在 AP 間的安全換手(Hand-off)

車載電腦 (client)在行進時需在 AP 間進行換手協定[10, 11]以建立安全通道。

4. 所提出的車載認證協定

概括以上系統環境敘述及安全需求，我們提出一安全的 VANET 架構。此架構的組成如第二節環境介紹；在本環境中 AS 是扮演公路監理所的角色，負責認證車輛、車載服務伺服器(VANET Services Server, VSS)及使用者；AS 擁有 public key KU_{AS}，並假設 AS 底下管轄的 APs、及 Clients 都預設了 KU_{AS}。每一 AP_i 與 AS 預先共享一把金鑰 K_{AP_i}；每一 VSS_j 預先與 AS 共享一把金鑰 K_{VSS_j}；每一車載電腦 C_x 與 AS 預先共享一把金鑰 K_{C_X}；每一使用者 U 預先在 AS 處註冊了其指紋摘要 $Figerprint_{minuitage}$。在底下的描述中我們假設 AS 與 AP、AS 與 VSS 可利用預先共享金鑰建立安全管道(例如利用 SSL 或 TLS 等機制[8])-它們之間的通訊是可認證及機密-所以底下描述中將直接表示它們之前傳輸的內容而不特別標示加密等動作。這章節要設計的協定包括：C 與 AP 間的認證金鑰協定(透過 AS)、C 在 APs 間的換手協定、及 U 與 VSS 間的認證金鑰(透過 AS)。

符號標記

$X||Y$：資料 X 串接資料 Y。

ID_A：A 的識別碼。

Sid：回合識別碼。

N_A, R_A：由 A 產生的隨機亂數(nonce)。

K_{AP_i}, K_{VSS_j}, K_{C_X}：AP_i 與 AS 預先共享一把金鑰，VSS_j 預先與 AS 共享一把金鑰，車載電腦 C_x 與 AS 預先共享一把金鑰 。

$fingerprint_{minuitage}$：U 預先在 AS 處註冊了其指紋摘要。

KU_{AS}：AS 的公開金鑰

$K_{A\text{-}B}$：A 與 B 間的會議金鑰

$E_{K_A}(X)$：使用 A 的祕密金鑰對資料 X 加密

$E_{KU_A}(X)$：使用 A 的公開金鑰對資料 X 加密

$E_{K_{A\text{-}B}}(X)$：使用 A 與 B 的會議金鑰對資料 X 加密

$h(X)$：使用單向雜湊函數對資料 X 雜湊

4.1 車輛(C)與 AP 認證協定

在[6]，簡等人已提出一高效率的 3PEKE 協定並已在正規化的模型下證明其安全；因此本論文將植基於簡等人的 3PEKE 設計一適用於 C 與 AP 間的認證金鑰協定。本機制與[6]不同處在於簡等人的 3PEKE 採用了共享密碼，而此處由於 AP 是設備，因而採用了安全性更高的金鑰。圖 2 是我們所提出的車輛與 AP 認證協定的資料傳遞過程：

步驟一. C→AP：

$$Sid||ID_C||ID_{AP}||D_C = g^{N_C}||$$
$$E_{KU_{AS}}(ID_C||ID_{AP}||K_C \oplus D_C||R_C)$$

C 發出通訊要求後，隨機產生亂數(N_C, R_C)，計算出 $D_C = g^{N_C}$，以 C 的祕密金鑰 K_C 與 D_C 作互斥運算(xor)，接著使用 AS 公開金鑰 KU_{AS} 將 $ID_C||ID_{AP}||K_C \oplus D_C||R_C$ 加密，並串接 $Sid||ID_C||ID_{AP}||D_C = g^{N_C}$ 後，將值傳送給 AP。

步驟二. AP→AS：

$Sid||ID_C||ID_{AP}||D_C = g^{N_C}||D_{AP} = g^{N_{AP}}$

$E_{KU_{AS}}(ID_C||ID_{AP}||K_C \oplus D_C||R_C)$

$E_{KU_{AS}}(ID_C||ID_{AP}||K_{AP} \oplus D_{AP}||R_{AP}||h(K_{C\text{-}AP}))$

AP 在收到 C 所提出的要求後，隨機產生亂數（N_{AP}，R_{AP}），使用雜湊函數 $h(Sid\|ID_C\|ID_{AP}\|g^{N_C*N_{AP}})$ 計算出 C 與 AP 間的會議金鑰 $K_{C\text{-}AP}$，計算 $D_{AP} = g^{N_{AP}}$，以 AP 的祕密金鑰 K_{AP} 與 D_{AP} 作互斥運算(xor)，將 $K_{C\text{-}AP}$ 雜湊，接著使用 AS 公開金鑰 KU_{AS} 將 $ID_C||ID_{AP}||K_{AP} \oplus D_{AP}||R_{AP}||h(K_{C\text{-}AP})$ 加密，將值傳送給 AS。

步驟三. AS→AP : $Sid\|D_{AP}\|$

$M_1 = h(Sid\|ID_C\|ID_{AP}\|D_C\|D_{AP}\|h(K_{C\text{-}AP})\|R_C)$

$M_2 = h(Sid||ID_C||ID_{AP}||D_C||D_{AP}||R_{AP})$

AS 收到資料後，得到 Sid、ID_C、ID_{AP}、D_C、D_{AP}，並用私鑰解密，得到 R_C、R_{AP} 及 $h(K_{C\text{-}AP})$，再將 $sid||ID_C||ID_{AP}||D_C||D_{AP}||h(K_{C\text{-}AP})||R_C$ 和 $sid||ID_C||ID_{AP}||D_C||D_{AP}||R_{AP}$ 分別雜湊後形成 M_1 及 M_2 連同 D_{AP} 傳給 AP。

步驟四. AP→C： $Sid\|D_{AP}\|M_1$

AP 收到 M_1 及 M_2 後，以 R_{AP} 驗證 M_2 的正確性，再將 $Sid\|D_{AP}\|M_1$ 傳給 C。

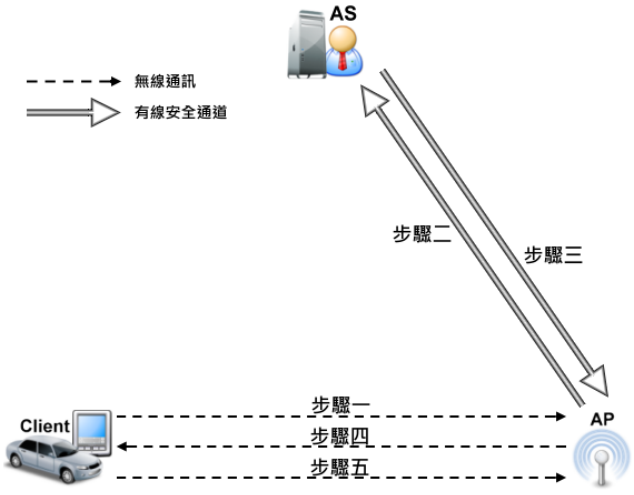

圖 2. 車輛與 AP 認證協定

步驟五.C→AP： $Sid||M_3$

C 收到資料後，首先計算出 $K_{C\text{-}AP} = h(Sid||ID_C||ID_{AP}||g^{N_C*N_{AP}})$，再以 R_C 驗證 M_1，計算 $M_3 = h(sid\|ID_C\|ID_{AP}\|D_C\|D_{AP}\|h(K_{C\text{-}AP}))$，將 M_3 傳給 AP。

AP 收到 M_3 並驗證 M_3；若驗證成功，則接受 C 與 AP 間的會議金鑰 $K_{C\text{-}AP}$。

4.2 C 在 AP 間的換手協定

由於 C 在行進時會一直在相臨的 AP 間不斷換手(Handoff)，因而我們需要設計一高效率且安全的換手機制。考量若每次認證若都需連回原 AS 做認證將產生額外延遲（delay），因而我們提出藉由相臨 AP 互助方式來提升認證效率。藉由下列情境說明我們的方法。假設 C 由 AP1 移動至 AP2，此時 C、AP1、AP2 三者間執行下列協定。

步驟一：C →AP2： $Sid\|ID_C\|ID_{AP2}\|D_C = g^{N_C}||ID_{AP1}||h(ID_C||ID_{AP2}||D_C||K_{C\text{-}AP1})$

C 偵測到要進入 AP2 的範圍時送出訊息 $Sid||ID_C||ID_{AP2}||D_C = g^{N_C}||ID_{AP1}||h(ID_C||ID_{AP2}||D_C||K_{C\text{-}AP1})$ 給 AP2，其中 D_C 為新產生的 Diffie-Hellman 暫時金鑰，而 $K_{C\text{-}AP1}$ 為 C 與前一 AP1 間的會議金鑰。

步驟二：AP2 ⇒AP1： $Sid\|ID_C\|ID_{AP2}\|D_C\|ID_{AP1}||h(ID_C||ID_{AP2}||D_C||K_{C\text{-}AP1})\|D_{AP2} = g^{N_{AP2}}$

AP2 透過它與 AP1 間的安全通道將 C 在步驟一的資料加上其暫時 Diffie-Hellman 金鑰 $D_{AP2} = g^{N_{AP2}}$ 傳送給 AP1。

步驟三：AP1 ⇒ AP2： $h(ID_C\|ID_{AP2}\|D_C\|D_{AP2}||K_{C\text{-}AP1})$

AP1 首先以 $K_{C\text{-}AP1}$ 驗證 $h(ID_C||ID_{AP2}||D_C||K_{C\text{-}AP1})$ 資料的正確性；若正確，則代替 AP2 產生可驗證 $D_{AP2} = g^{N_{AP2}}$ 的驗證訊息 $h(ID_C\|ID_{AP2}\|D_C\|\ D_{AP2}||K_{C\text{-}AP1})$，並回傳。

步驟四：AP2 ⇒ C： $Sid||D_{AP2} = g^{N_{AP2}}||h(ID_C||ID_{AP2}||D_C||D_{AP2}||K_{C\text{-}AP1})$

C 以 $K_{C\text{-}AP1}$ 驗證 $D_{AP2} = g^{N_{AP2}}$ 及

$h(ID_C \| ID_{AP2} \| D_C \| D_{AP2} \| K_{C\text{-}AP1})$的一致性；若正確，C 及 AP2 則共享新會議金鑰 $K_{C\text{-}AP2} = h(Sid \| ID_C \| ID_{AP2} \| g^{N_C * N_{AP2}})$。

4.3 使用者(U)與 VSS 間的認證-以指紋為基礎

由於行車間若要求使用者輸入密碼認證可能會有行車安全顧慮，本論文提出在行車間以使用者指紋認證可改善此缺點。此指紋認證 3PEKE 協定改良自簡等人之可證明式 3PEKE 協定[6]；有別於以往的 3PEKE 雙方都是共享秘密金鑰或密碼；此機制中使用者與 AS 間以指紋特徵值 $Fingerprint_{minutiae_U}$ 來辨識身份及收費；而車載服務伺服器(VSS)與 AS 間共享一把秘密金鑰 K_{VSS}。此協定執行時機為當 C 與 AP 已建立安全通道後且使用者想存取 VSS 保護服務時；因此底下描述時將不強調 U 須透過 C 與 AP 間的安全管道傳輸資料的基本條件，而直接描述 U、AS、與 VSS 間高階的協定描述。圖 3 是我們所提出的 U 與 VSS 透過 AS 認證並產生金鑰的過程：

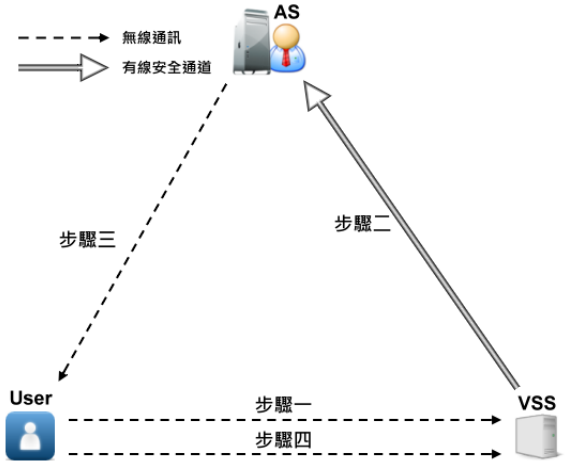

圖 3. 指紋基礎之 3PEKE 認證協定

步驟一. U→VSS：

$Sid \| ID_U \| ID_{VS} \| D_U = g^{N_U} \| E_{KU_{AS}}(ID_U \| ID_{VSS} \| Fingerprint_{minutiae_U} \oplus ext(D_U) \| R_U)$

由 U 發出服務要求後，隨機產生亂數 N_U，計算出 $D_U = g^{N_U}$，以 U 的指紋影像特徵值 $Fingerprint_{minutiae_U}$ 與 $ext(D_U)$ 作互斥運算(xor)，其中 $ext(D_U)$ 代表的意思是通常 $Fingerprint_{minutiae_U}$ 的長度遠大於 D_U 的長度，因此將兩者做 XOR 前需將 D_U 做必要的擴充；任合安全的擴充都可以被使用，例如：利用單向雜湊 $h()$ 擴充 $ext(D_U) \equiv D_U \| h(D_U) \| h(h(D_U)) \| \ldots$ 至必要長度。接著使用 AS 公開金鑰 KU_{AS} 將 $ID_U \| ID_{VSS} \| Fingerprint_{minutiae_U} \oplus ext(D_U) \| R_U$ 加密，並串接 $Sid \| ID_U \| ID_{VSS} \| D_U = g^{N_U}$ 後，將值傳送給 VSS。

步驟二. VSS→AS：

$Sid \| ID_U \| ID_{VSS} \| D_U = g^{N_U} \| D_{VSS} = g^{N_{VSS}} \| E_{KU_{AS}}(ID_U \| ID_{VSS} \| Fingerprint_{minutiae_U} \oplus ext(D_U) \| R_U) \| E_{KU_{AS}}(ID_U \| ID_{VSS} \| K_{VSS} \oplus D_{VSS} \| R_{VSS} \| h(K_{U\text{-}VSS}))$

VSS 在收到 U 所提出的服務要求後，隨機產生亂數 (N_{VSS}，R_{VSS})，使用雜湊函數 $h(Sid \| ID_U \| ID_{VSS} \| g^{N_U * N_{VSS}})$計算出 U 與 VSS 間的會議金鑰 $K_{U\text{-}VSS}$，計算 $D_{VSS} = g^{N_{VSS}}$，再以 VSS 的秘密金鑰 K_{VSS} 與 D_{VSS} 作互斥運算(xor)，將 $K_{U\text{-}VSS}$ 雜湊，接著使用 AS 公開金鑰 KU_{AS} 將 $ID_U \| ID_{VSS} \| K_{VSS} \oplus D_{VSS} \| R_{VSS} \| h(K_{U\text{-}VSS})$ 加密，將此資料及上一步驟 U 所產生的 $E_{KU_{AS}}(ID_U \| ID_{VSS} \| Fingerprint_{minutiae_U} \oplus D_U \| R_U)$ 傳送給 AS。

步驟三. AS→U：$Sid \| D_{VSS} \| M_1 \| M_2$

AS 收到資料後，得到 Sid、ID_U、ID_{VSS}、D_U、D_{VSS}，並用私鑰解密，得到 R_U、R_{VSS}、$h(K_{U\text{-}VSS})$ 及 $fingerprint_{minutiae}$，AS 將此指紋特徵值與註冊時的指紋特徵值比對，驗證身分後，再計算 $M_1 = h(Sid \| ID_U \| ID_{VSS} \| D_U \| D_{VSS} \| h(K_{U\text{-}VSS}) \| R_U)$ 及 $M_2 = h(Sid \| ID_U \| ID_{VSS} \| D_U \| D_{VSS} \| R_{VSS})$，再將 $D_{VSS} \| M_1 \| M_2$ 傳給 U。

步驟四. U→VSS：$M_2 \| M_3$

C 收到資料後，計算出 $K_{U\text{-}VSS} = h(Sid \| ID_U \| ID_{VSS} \| g^{N_U * N_{VSS}})$，再驗證所收到 M_1 的合法性。若成功再計算 $M_3 = h(Sid \| ID_U \| ID_{VSS} \| D_U \| D_{VSS} \| h(K_{U\text{-}VSS}))$

，連同上一步驟所收到的M_2一併傳給 VSS。

VSS 收到M_2、M_3後，驗證M_2以確認 D_U 的合法性，再驗證M_3以確認 U 擁有相同的會議金鑰$K_{U\text{-}VSS}$，並提供使用者所選擇的車載服務。

5. 安全性及效率評估

5.1 安全分析

因車載網路中 C 與 AP 間是藉由無線網路通訊以及 U 需經過認證才能存取 VSS，所以我們根據幾項常見的攻擊，進行安全性的評估如下所示：

(1)互相驗證(Mutual authentication)：車載電腦(C)和 AP 必須對彼此的身分進行驗證並產生認證金鑰。在我們的架構中，此部份是修改自簡等人的 3PEKE 協定 [6]，由於該機制已經過正規化證明；我們修改的部份包括：修改機制以共享金鑰取代安全較弱的密碼，因而修改機制擁有更強的安全度，也同時繼承原機制的雙向認證特質。

而 U 與 VSS 間的機制也是修改自簡等人的可證明式 3PEKE 協定 [6]- 將原先的兩對共享密碼分別以 U 的 $Figerprint_{minuitae_U}$ 及 VSS 的金鑰取代；由於 $Figerprint_{minuitae_U}$ 的亂度類似於密碼，而 VSS 的金鑰強度勝過密碼，因而 U 與 VSS 間的機制也可繼承原機制的雙向認證功能。

(2)會議金鑰的安全性(Session key security)：會議金鑰的安全性指的是當協定成功的執行時，只有正確的通訊方可以取得會議金鑰。在我們的協定(C 與 AP 間認證金鑰、U 與 VSS 間認證金鑰)都直接繼承原可證明金鑰機制的安全。

(3)換手協定的安全：本架構假設 AP 間已建立安全通道；而我們的換手機制是藉由舊 AP (AP1)利用舊會議金鑰協助認證 C 的新亂數D_C及 AP2 的新亂數 D_{AP2} 以產生新會議金鑰 $K_{C\text{-}AP2} = h(Sid \| ID_C \| ID_{AP2} \| g^{N_C * N_{AP2}})$；因此若 AP1 是安全的則此新金鑰$K_{C\text{-}AP2}$也是安全。

(4)中間人攻擊(Man-in-middle attack)、重送攻擊(Replay attack)：由於(1)(2)的安全特質，本機制可抵擋中間人攻擊及重送攻擊。

(5)向前安全(Perfect forward secrecy)：向前安全意指攻擊者即使破解此次通訊參與者的永久金鑰也無法利用此資訊去推算過去通訊的會議金鑰及加密內容。在我們的機制中所有的會議金鑰的計算都是以該 session 的亂數計算 Diffie-Hellman key，因此每一金鑰都是獨立且與永久金鑰無關，因而保障了向前安全。

5.2 效率評估

本機制架構簡潔- 由 VANET 管理中心直接管理 AS，而 AS 直接可認證其下的 AP 及 VSS。本架構統一套用改良之高效率可證明式 3PEKE 協定，因而效率高且擴充性好- 可擴充延伸其它服務。

在圖 2 的高階表示圖中會比原機制[6]多出一步驟（原機制需要 4 步）；此乃原機制中假設通訊三方都可直接與任一方通訊；由於 VANET 架構中，AS 要傳資料給 C 一定需要經過 AP，所以圖 2 會出現多一步；但這些表示法都是高階示意圖，不考慮實質上式所需經過的路由器或交換器等網路設備，因此只能當作高階邏輯上所需的步驟；因此本篇的改良機制仍繼承原機制通訊上的高效率。

6. 結論

由於目前車載資訊系統尚未有一套安全標準，且目前已發表的相關研究無法完全滿足 VANET 的全部安全需求；因此，我們提出一整合於 AS 下的統整安全架構搭配改良自可證明式安全的 3PEKE 協定，提供一高整合、高擴充性、高效率的安全協定；此協定以使用者按指紋方式取代行車間輸入密碼的困擾，因而提高行車安全。然而，本機制沒考量車輛匿名性、使用者匿名性及跨領域(如美國 VANET 會跨數州)認證，這些議題將是我們後續研究的主題。

參考文獻

[1] W. Stallings, ***Cryptography and Network Security: Principles and Practice,*** PrenticeHall, 2003.

[2] Hakjae Kim, Ryong Oh, Sungju Lee, Taesup Kim, Sangjoon Lee, Yongwha Chung , Choongho Cho, ***A fingerprint-based user authentication protocol considering both the mobility and security in the telematics environment***, Computer Standards & Interfaces 31 (2009) 1098–1107

[3] A. Jain, R. Bole, S. Panakanti, ***Biometrics: Personal Identification in Networked Society,*** Kluwer Academic Publishers, 1999.

[4] D. Maltoni, ***Handbook of Fingerprint Recognition,*** Springer, 2003.

[5]Y. Chung, A Secure ***Fingerprint Authentication System on an Untrusted Computing Environment***, Proc. TrustBus '05, Lecture Notes in Computer Science, vol. 3592, Springer, 2005, pp. 299–310.

[6] Hung-Yu Chien, Tzong-Chen Wu, ***Highly Efficient Password-Based Three-Party Key Exchange in Random Oracle Model,*** IEEE ISI 2008.

[7] M. Ilyas, S. Ahson, ***Handbook of Wireless Local Area Networks: Applications,*** Technology, Security, and Standards, CRC, 2005.

[8]Ashraf Elgohary, Tarek S. Sobh, M. Zaki, ***Design of an enhancement for SSL/TLS protocols,*** computers &security 25(2006)297–306

[9] I. Cox, M. Miller, J. Bloom, ***Digital Watermarking,*** Morgan Kaufmann Pub, 2002.

[10] IEEE, ***IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation,*** IEEE Standard 802.11f, 2004.

[11] T. Moore, B. Aboba, ***Authenticated Fast Hand-off***, IEEE 802.1-01/553, 2001.