車載網路保護隱私技術

黃仁俊　　黃晨晏　　蕭宇凱
淡江大學資訊工程系　　淡江大學資訊工程系　　淡江大學資訊工程系
junhwang@ms35.hinet.net　　gogoexb@yahoo.com.tw　　shiaukae@gmail.com

摘要：車載網路(VNET)是基於無線傳輸技術進步所推衍發展的網路，其為以車輛及基地台構成的特殊型態行動無線網路，主要可將其應用在確保行車安全，並改善交通狀況等方面，但因通訊都是透過無線傳輸，使得惡意第三者可以輕易的取得或竄改網路中傳輸的資訊，因此產生了保護車輛隱私與確保資料完整性的相關安全議題。為了保護使用者的隱私，目前雖有一些相關研究提出保護車輛的隱私的技術，但都沒辦法提供完善的車輛隱私保護方案，因此本篇論文提出基於 Weil Pairing 的車載網路隱私保護技術以保護駕駛者的隱私，並在不同的通訊模式中提供適當的安全需求。

關鍵字：車載網路、隱私、網路安全

第一節 緒論

近幾年來，由於車輛的普遍以及無線網路技術的發展，針對運輸系統的通訊能力的關注也逐漸增加，在交通工具極為普遍的同時，交通事故也逐漸頻繁，交通事故往往帶來大量嚴重的生命或財產上的損失。為此以行動隨意網路為基礎的智慧型運輸系統(Intelligent Transport Systems, ITS)[1]車載網路逐漸受到重視，希望能夠提供安全且有效率的交通管理系統，來降低這些交通意外的發生，同時也能夠增加交通上的運輸效率與方便性。

車載網路是由兩種角色[14,16]所構築而成的網路，分別為：

1. 路邊基地台(Road-side Base Station)：簡稱基地台，為佈建在道路兩邊的基礎設施，彼此之間以實體線路相連結，可以提供車輛各項服務，例如，路況查詢或搜尋特定的地點等，並主動廣播警告訊息通知其範圍內的所有車輛，例如，出現土石崩塌或車禍。另外，基地台會與其它網路連線提供網際網路(Internet)服務，並由後端授權伺服器負責控制車輛使用者存取網路服務。
2. 車輛(Vehicle)：車載網路的車輛使用者，具備車載網路所需的裝置。

在考慮隱私權的情況之下，我們認為車載網路中的通訊情形應該分為下列三種通訊模式：

1. 車輛與基地台通訊模式：車輛連結車載網路的基本模式，在此模式中必須考慮車輛與基地台的相互鑑別之基本安全需求後，車輛與基地台可以交換資訊。
2. 車輛廣播模式：車輛發送警告訊息給其通訊範圍內的所有車輛以及基地台。
3. 基地台廣播模式：基地台傳送訊息給通訊範圍內所有車輛。

車載網路的通訊是透過無線傳輸，因此攻擊者可以很輕易的取得網路中的資訊進行偷窺、竄改或偽冒。安全議題是車載網路一個基本且重要的議題，陸陸續續有許多相關的研究做這方面的討論[3,5,8,11]，其中車輛使用者的隱私保護尤為重要[8,11]，因為車載網路無線傳輸過程，車輛的隱私很容易受到破壞，目前也有許多相關研究討論此議題[3,4, 7, 9, 15, 16, 18, 19, 20]。假名(pseudonym)的使用是最常使用的方法之一，藉此車輛在車載網路中通訊得以隱藏車輛的真實身份。但僅使用假名並沒有辦法完成保護車輛行蹤隱私，特定假名的車輛移動路徑，在單純假名的保護下仍存在被攻擊者掌握的可能，進一步遂行其犯罪行為。Li 等人[10]提出擺動與互換(Swing and Swap)的方法，讓車輛之間交換彼此的假名；Gerlach 等人[4]也曾提出混淆背景(Mix-contexts)的方式，讓車輛偵測四周想換假名的車輛的數目達一定數量後，一起更新假名； Xi 等人[17]則提出讓車輛在通訊時將自己的假名與鄰近其它車輛的假名混合後使用的方法。這些學者方法的核心概念，都是透過讓車輛變更所用的假名，來混淆攻擊者對個別車輛行蹤的追蹤。

假名與相關技術保護了車輛的隱私，但卻也引發了其他的安全威脅[12]，因假名同樣隱藏攻擊者的身分，惡意車輛在隱藏自己的身份情況下在車載網路進行不當的行為，例如廣播假的警告訊息以謀取自己的私利。此外，在考慮隱私保護之同時我們也必須考慮車輛可以即時驗證訊息以確定資訊真實性且必要時特定人士有還原惡

意車輛身份之能力。Choi 等人[3]提出利用長短不同時效的假名，讓基地台擁有短時間內可追蹤特定車輛的能力。但其方法在車輛與車輛之間的通訊，接收訊息的車輛必須再與基地台通訊才能驗證收到的訊息，這對一些分秒必爭的安全警告訊息來說，會造成延遲。Kim 等人[7]提出基於『訊息驗證碼鏈』(Message Authentication Code Chain, MAC-chain)的方法，允許授權伺服器透過車輛的身份與基地台來追蹤車輛的行蹤。但其用車輛的真實身份來追查其行蹤，再判斷是否與事件有關的做法，有如大海撈針，效能不盡理想；而且其方法在基地台共謀將得以掌握某個個別車輛的行蹤；Lu 等人[9]則考慮車輛在登入時，基地台儲存關於車輛的資訊，必要時基地台可以透過這些資訊還原車輛的真實身份。但若基地台共謀，將破壞車輛行蹤隱私的能力。Zhang 等人[19]採用『k-匿名』(k-anonymity)與 Zhang 等人[20] 透過防竄改裝置(Tamper-proof device, TPD)追蹤訊息廣播者真實身份的方法，但此二方法車輛都需等待基地台再廣播相關訊息方可確認廣播訊息內容，使車輛廣播形同基地台廣播其效能與即時性有改善空間。Kamat 等人[6]考慮以身份識別為基礎的簽章加密法，可信任的機構可以從中取得車輛的真實身份。但其方法經由數個基地台共謀的情況，即可以破壞車輛行蹤隱私。

車載網路的車輛在不同基地台移動是一定要考慮的情境，然車輛由一個基地台的通訊範圍移動到另一個基地台服務範圍時，為了確保安全，新的基地台與車輛必須相互鑑別後，基地台再繼續提供網路服務；為維持網路服務品質這種換手鑑別時程不可太久，而在保護隱私的情況下讓車輛與基地台進行鑑別比不保護隱私的情況更為複雜[18]，且車輛的移動速度迅速，確保快速的讓新的基地台完成鑑別是很重要的；此外，車輛在換手鑑別時的資訊，可能提供基地台共謀以得知車輛的行蹤，進而破壞車輛隱私的保護。Zhang 等人[18]利用了盲簽章(blind signature)的特性，車輛在換手前進行預先鑑別(Pre-authentication)的動作，車輛可以快速的在不同的基地台之間進行換手的動作，同時又保護到車輛的隱私。但其方法只考慮到車輛與基地台通訊的模式，而沒有考慮廣播通訊模式如何進行，而這種模式是快速傳遞訊息的方法，但若兼具驗證訊息考量時往往可能破壞行蹤隱私。

綜整車載網路面臨的各項安全威脅[6,7,9,14,18]，我們整理表一條列車載網路不同的通訊模式應該分別滿足的安全需求。本論文針對車載網路的安全性提出了一基於 Weil pairing 的較完整解決方案，其提供表一的各項安全功能，尤其著重在隱私的保護，其根據不同的

表一、車載網路安全需求

模式 / 功能與安全性	車輛與基地台	基地台廣播	車輛廣播
鑑別	YES	YES	YES
換手鑑別	YES	NO	NO
私密性	YES	NO	NO
匿名	YES	NO	YES
匿蹤	YES	NO	YES
完整性	YES	YES	YES
不可否認性	NO	YES	YES
責任	NO	NO	YES
前推安全 (Forward secrecy)	YES	NO	NO

通訊模式，提出一個安全且能保護車輛身份與行蹤的隱私，並提供有效率的換手鑑別機制，且能阻止惡意的車輛利用身份及行蹤隱私保護遂行攻擊。同時也考慮當車載網路而引起的交通糾紛或財產甚至性命上的損失時，能夠讓現實世界中的法律部門，例如，警局或法院等，有能力還原與糾紛或事件相關的車輛的身份進行究責。

後續章節中，第二節介紹我們的方法；第三節則是針對我們方法與現有的方法做功能的比較與安全性分析，並在第四節做結論。

第二節 車載網路保護隱私技術

我們的方法中參與的角色分別是授權伺服器(Authorization sever)：是可信任的第三者，負責管理車輛資格，並扮演車載網路危安事件發生後，還原車輛真實身份的角色；基地台(Base Station)：部署在道路兩旁的基礎設施；車輛(Vehicle)：車載網路的使用者。論文方法建立在橢圓曲線 Weil pairing 的基礎上[2]。在 Weil pairing 中，G_1 為循環加法群，G_2 為循環乘法群，G_1, G_2 具同樣的序列(order) q，Weil pairing 為 e: $G_1 \times G_1 \rightarrow G_2$ 需符合下列幾項特性[2,21]

(1). 雙線性(Bilinear)：對所有 Q, $R \in G_1$ 與 a,

$b \in Z_q^*$，則 $e(a \cdot R, b \cdot Q) = e(R, Q)^{ab}$。

(2). 不可退化(Non-degenerate)：一定存在 $Q, R \in G_1$，使得 $e(Q, R) \neq 1_{G_2}$，也就是沒有對映到 G_2 上的單位元素。

(3). 可計算性(Computable)：對於任何的 $Q, R \in G_1$，一定會存在一個有效率的演算法來計算 $e(Q, R)$。

後續 2.1 節說明在車載網路建置時程序及車輛向授權伺服器註冊的過程。2.2 至 2.4 節分別介紹我們三種通訊模式的運作模式。關於方法中所用的參數符號，請參閱表二。

2.1. 預先部署

授權伺服器 AS 公佈公開值 G 與 $C_{AS}(= MK_{AS} \cdot G)$；並提供基地台：身份碼 RI_i、密鑰 SK_{RI_i} $(=MK_{AS} \cdot H_0(RI_i))$、私鑰 PR_{RI_i} $(\in Z_q^*)$與相對應的公鑰 PU_{RI_i} $(= PR_{RI_i} \cdot SK_{RI_i})$。

車輛在第一次使用網路前必須先透過安全通道以身份 V 向給授權伺服器 AS 註冊。授權伺服器 AS 鑑別車輛的身份後，紀錄並提供車輛假名 $P_1=E(MK_{AS}, V||N)$、密鑰 $SK_V = MK_{AS} \cdot H_0(P_1)$ 與預先共享密鑰 K_{AS-V}，其中的 N 與預先共享密鑰都是隨機亂數。

2.2. 車輛與基地台通訊模式

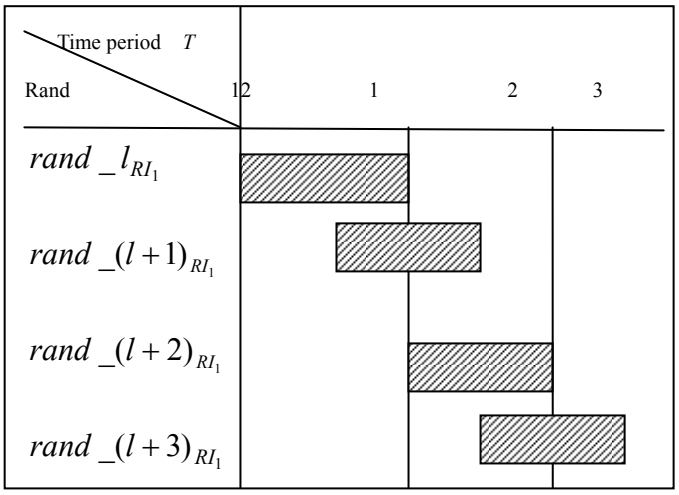
車輛欲取得網路服務需採車輛與基地台通訊模式。此模式需考慮兩種型態，其一為車輛欲使用網路服務進行登入鑑別程序，基地台與車輛進行相互鑑別；另一型態為車輛在連線網路的狀態下因為移動而從現在的基地台換到其他基地台時，需考慮讓車輛快速換手鑑別以確保安全並保持網路連線，本論文方法善用已經被提供服務的基地鑑別過的的資訊，讓新的基地台對車輛進行快速換手鑑別，縮短鑑別延遲以維持使用者的網路連線確保網路服務品質。

表二、符號表

符號	說　　明
AS	授權伺服器。
RI_i	基地台 i 的身份碼。
V	車輛的身份碼。
MK_{AS}	授權伺服器 AS 的密鑰(secret key)。
PR_i/PU_i	基地台 RI_i 或車輛 V 的私鑰與公鑰，$i \in RI_i, V$。
SK_i	基地台 RI_i 或車輛 V 的密鑰(secret key)，$i \in RI_i, V$。
K_{AS-V}	授權伺服器 AS 與車輛 V 的預先共享密鑰(pre-shared key)。
$E(K, X)$	使用金鑰 K 對明文 X 做對稱式加密。
w_{V-RI_u}	車輛 V 與基地台 RI_i 通訊時用的會議金鑰(session key)。
e()	雙線性配對的對映(map)。
H()	單向雜湊函數(one way hash function)。
$H_0()$	雜湊函數(hash function)$\{0,1\}^* \rightarrow G_1$。
$H_1()$	雜湊函數$\{0, 1\}^* \rightarrow Z_q^*$。
$H_2()$	雜湊函數 $G_2 \rightarrow \{0, 1\}^n$，$n$ 的值需與對稱式加解密的金鑰的位元長度相當，以符合安全需求。
$F(U)$	$F(U)$表 G_1 上的點 U 的 x 座標與 y 座標串接在一起。
$\oplus$	循環加法群 G_1 群中的運算子。
$a \cdot R$	表對 G_1 中運算元 R 連加 a 次。
$\otimes$	循環乘法群 G_2 群中的運算子。
C_{AS}	授權伺服器 AS 公佈的公開參數。
$rand\_l_{RI_i}$	基地台 RI_i 的第 l 個隨機亂數。
G	G_1 上的點為公開值。
T	時段。
ts_i	基地台 RI_i 或車輛 V 的時戳

本論文方法假設基地台在每隔 $T/2$ 的時間，產生隨機亂數 $rand\_l_{RI_i}$，其生命週期 T。圖一為一例說明假設 T 為一小時，基地台於 12：00 開始產生 $rand\_l_{RI_i}$ 後，到 13:30 亂數產生的情形。圖一的例子清楚可以發現每一基地台除了起始的 T/2 時段只擁有一隨機亂數外，其他時段 l 都存在兩個隨機亂數與其對應，一個是該時段產生的 $rand\_l_{RI_i}$，另一為上一時段產生的 $rand\_(l-1)_{RI_i}$。基地台每次產生一隨機亂數 $rand\_l_{RI_i}$ 後計算對應的 S_{RI_i} $(= rand_l_{RI_i} \cdot G)$並以安全通道傳送$(T_{RI_i}, S_{RI_i}, RI_i)$給相鄰的其他基地台，我們以$(T^*, RI^*, S^*)$表示某基地台持有周邊所

有相鄰基地台的時段 T^*所對應的 S^*與身份碼 RI^*的集合。



圖一、隨機亂數的產生與生命週期

2.2.1. 登入鑑別

車輛啟動網路連線時，將以下列步驟與離車輛通訊範圍內最近的基地台，RI_1，進行連線登入。圖二說明車輛 V 登入基地台 RI_1 的流程示意圖。

步驟 1. 車輛 V 選隨機亂數 N 並計算 w_{V-RI_1} = e($H_0(RI_1)$, SK_V)，傳送訊息 $\{P_1||RI_1||E(H_2(w_{V-RI_1}), N||H(N))\}$給基地台 RI_1。

步驟 2. 基地台 RI_1 以下列子步驟鑑別車輛並回傳適當訊息：

步驟 2.1. 計算 w'_{V-RI_1} =e(SK_{RI_1},$H_0(P_1)$)，並解密驗證收到的訊息以鑑別身份。

步驟 2.2. 回傳訊息$\{RI_1||P_1||E(H_2(w'_{V-RI_1}), (T^*, RI^*, S^*)||H(N||F(S^*)))\}$給車輛 V。

步驟 3. 車輛 V 以 w_{V-RI_1} 解密及驗證$\{RI_1||P_1||E(H_2(w'_{V-RI_1}),(T^*,RI^*,S^*)||H(N||F(S^*)))\}$鑑別基地台後，儲存$(T^*, RI^*, S^*)$供後續的換手鑑別使用，並以 w_{V-RI_1} 為與基地台 RI_1 的會議金鑰。

步驟 4. 車輛 V 選擇新的隨機亂數 N'，傳送$\{P_1||RI_1||E(K_{AS\text{-}V}, N'||H(N'))\}$給基地台 RI_1。

步驟 5. 基地台 RI_1 將$\{P_1||E(K_{AS\text{-}V},N'||H(N'))\}$轉送給授權伺服器 AS。

步驟 6. 授權伺服器 AS 以下列子步驟驗證訊息，並產生車輛 V 新假名與對應密鑰：

步驟 6.1. 取得 P_1 相對應的預先共享密鑰 $K_{AS\text{-}V}$。並解密及驗證$\{E(K_{AS\text{-}V}, N'||H(N'))\}$。

步驟 6.2.產生 V 的新假名 P_2= $E(MK_{AS}, V||N')$ 及相對應的密鑰 SK'_V= MK_{AS} • $H_0(P_2)$，更新資料庫中的$(V、P_1、K_{AS\text{-}V})$為$(V、P_2、K_{AS\text{-}V})$。

步驟 6.3. 回傳訊息$\{P_1||E(K_{AS\text{-}V}, P_2||SK'_V||H(N'||P_2||F(SK'_V)))\}$給基地台 RI_1。

步驟 7. 基地台 RI_1 傳送訊息$\{RI_1||P_1||E(K_{AS\text{-}V}, P_2||SK'_V||H(N'||P_2||F(SK'_V)))\}$給車輛 V。

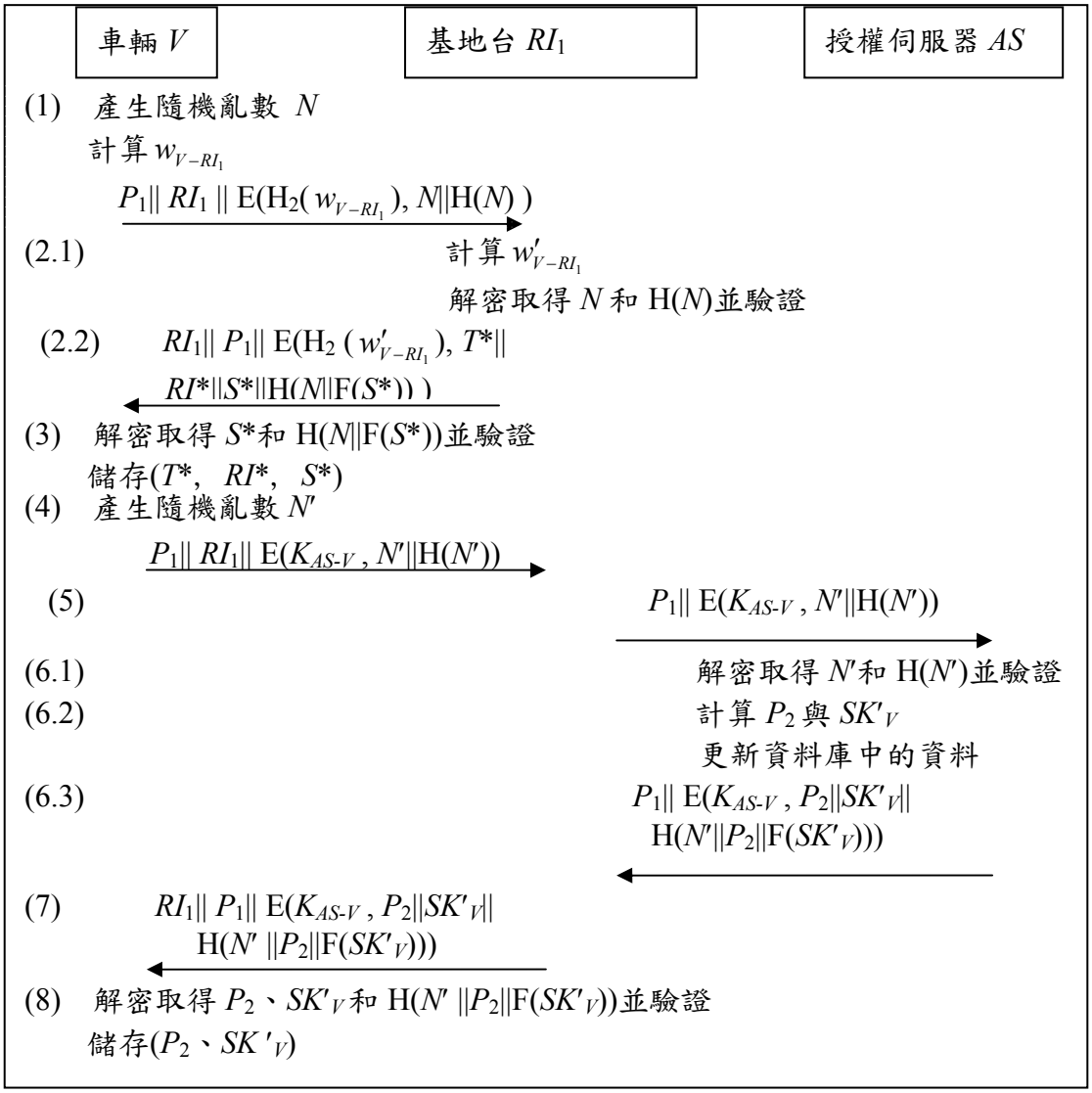
步驟 8. 車輛 V 以預先共享密鑰 $K_{AS\text{-}V}$ 解密及驗證$\{RI_1||P_1||E(K_{AS\text{-}V},P_2||SK'_V||H(N'||P_2||F(SK'_V)))\}$後，儲存$(P_2, SK'_V)$做為下一次的登入或車輛廣播通訊模式中的新假名與對應密鑰。

2.2.2. 換手鑑別

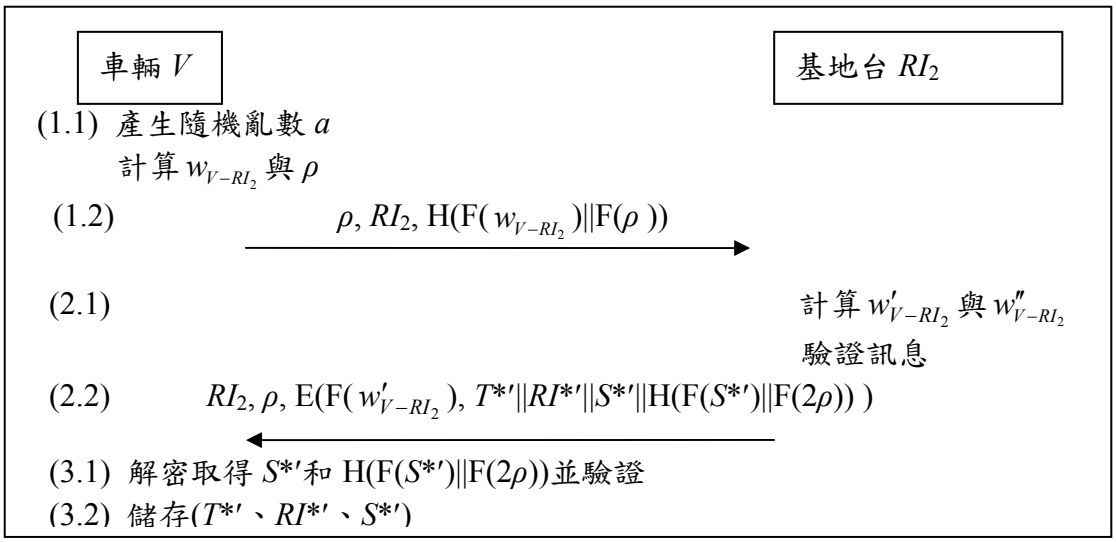
車輛在連線網路的狀態下因具移動性可能從一個基地台(RI_1)的通訊範圍內移動到另一個基地台(RI_2)的通訊範圍內，為保持網路通訊與安全必須進行換手鑑別程序，使車輛與新基地台相互鑑別後繼續網路通訊，此換手鑑別必需簡短且快速，以確保車輛與基地台的連線不會中斷並影響品質。我們的方法善用登入鑑別或前一次換手鑑別所取得的資訊(T^*, RI^*, S^*)減少鑑別延遲，車輛 V 將執行下列步驟完成快速換手鑑別，其中(T^*, RI^*, S^*)僅包含行進道路上前後之基地台資訊，並非如一般無線網路中通訊範圍內所有的基地台數量可能很多，因此雖然我們的方法基地台需定期提供相鄰基地台(T^*, RI^*, S^*)，但因數量有限其通訊量應在可接受的範圍內，圖三為其示意圖。

步驟 1. 車輛 V 選出隨機亂數值 a 計算 w_{V-RI_2}=a • S_{RI_2} 與 ρ=a • G 並傳送訊息$\{\rho||RI_2||H(F(w_{V-RI_2})||F(\rho))\}$給基地台 RI_2，ρ 為一個臨時性的假名。

步驟 2. 基地台 RI_2 執行下列子步驟鑑別車輛，並提供相關供下一次鑑別的資訊：



圖二、登入鑑別流程示意圖



圖三、車輛換手鑑別示意圖

步驟 2.1. 計算 w'_{V-RI_2} (=($rand\_l_{RI_2}$)・ρ) 與 w''_{V-RI_2} (=($rand\_(l-1)_{RI_2}$)・ρ)，並驗證 $\{\rho||RI_2||H(F(w_{V-RI_2})||F(\rho))\}$ 中的雜湊值與何者相符合；若都不符合鑑別失敗，不提供網路連線。

步驟 2.2.假設步驟 2.1 中 w'_{V-RI_2} 符合，計算並回傳訊息 $\{RI_2||\rho||E(F(w'_{V-RI_2}),(T^{*\prime},RI^{*\prime},S^{*\prime})||H(F(S^{*\prime})||F(2\rho)))\}$ 給車輛 V。

步驟 3. 車輛 V 以 w_{V-RI_2} 解密並驗證 $\{RI_2||\rho||E(F(w'_{V-RI_2}),T^{*\prime}||RI^{*\prime}||S^{*\prime}||H(F(S^{*\prime})||F(2\rho)))\}$ 後，儲存$(T^{*\prime}, RI^{*\prime}, S^{*\prime})$，提供後續換手鑑別之用。$w_{V-RI_2}$ 為本次網路連線與基地台 RI_2 的會議金鑰。

2.3. 車輛廣播模式

車輛在已經以登入網路持續連接網路下，其裝置偵測到的一些即時路況時，例如：車禍、道路積水等，將以車輛廣播模式通知其它的車輛與基地台，通訊範圍內的車輛數目可能很多，我們的方法主張避免以個別傳送訊息方式傳遞廣播訊息減輕通訊的成本負擔與整體網路效能的下降外，我們的方法提供車輛雖然以假名廣播，但任一接收者在無法知曉其確切身份之條件下，仍然可以判斷訊息來自不知名的合法使用者，唯獨授權伺服器 AS 在發現有人刻意散播假訊息時，有能力追溯該車輛真實身份。

若車輛以假名 P_1 透過基地台 RI_i 登入網路後，未進行換手鑑別前即需廣播，則其僅以假名 $\beta=P_1$ 以下列步驟 1 與 2 進行廣播訊息 M；若車輛登入網路後已換手到目前基地台 RI_i，而以臨時假名 ρ 進行網路連線且已持有授權伺服器 AS 合法登錄但未用的新假名為 P_2，則除了以假名 $\beta=P_2$ 完成步驟 1 與 2 廣播外，廣播後假名 P_2 已曝光，故需以當時臨時假名 ρ 執行步驟 3 至步驟 7，透過基地台 RI_i 以假名 P_2 自授權伺服器 AS 再取得另一新假名 P_3 做為其未來離開基地台 RI_i 範圍後運作的假名，藉此方能確實達到除了授權伺服器 AS 以外的任意第三者無法掌握某一特定匿名車輛的行蹤。假設車輛 V 持密鑰 SK'_V，圖四是車輛 V 進行車輛廣播過程的示意圖。

步驟 1. 車輛 V 以下列子步驟完成廣播訊息 M：

步驟 1.1. 隨機產生私鑰 PR_V 與隨機亂數 r_1，$PR_V, r_1 \in Z_q^*$，計算 $L'=r_1+H_1(M||ts_V)\times PR_V \bmod q$、$\sigma'=r_1 \cdot H_0(\beta)$ 與 $PU_V=PR_V \cdot SK'_V$；其中(L', σ')為訊息 M 的簽章，PU_V 是車輛為此廣播所選擇之私鑰 PR_V 所對應的公鑰。

步驟 1.2.廣播訊息$\{\beta||M||L'||\sigma'||PU_V||ts_V\}$。

步驟 2. 車輛 V 周邊的車輛或基地台 RI_i 檢查訊息中時戳 ts_V，並以授權伺服器 AS 的公開值 C_{AS} 計算並判斷 $e(L' \cdot H_0(\beta), C_{AS})$與 $e(\sigma', C_{AS}) \otimes e(PU_V, H_1(M, ts_V) \cdot G)$是否相等以驗證廣播訊息 M 並確定來自假名 β 的合法第三者。

步驟 3. 車輛 V 選出一個新的隨機亂數 N''，傳送 $\{\rho, RI_i, E(F(w_{V-RI_i}), P_2||E(K_{AS-V}, N''||H(N''))\}$ 給基地台 RI_i。

步驟 4. 基地台 RI_i 以 w'_{V-RI_i} 解密並轉送 $\{P_2||E(K_{AS-V}, N''||H(N''))\}$給授權伺服器 AS。

步驟 5. 授權伺服器 AS 以下列子步驟鑑別並產生車輛新假名 P_3。

步驟 5.1. 以 P_2 相對應的預先共享密鑰 K_{AS-V} 進行解密及驗證。

步驟 5.2. 產生 $P_3=E(MK_{AS}, V||N'')$及相對應的密鑰 $SK''_V=MK_{AS} \cdot H_0(P_3)$。並以$(V、P_3、K_{AS-V})$取代資料庫中的$(V、P_2、K_{AS-V})$。

步驟 5.3. 傳送訊息 $\{P_2||E(K_{AS-V}, P_3||SK''_V||H(N''||P_3||F(SK''_V)))\}$給基地台 RI_i。

步驟 6. 基地台 RI_i 轉送訊息 $\{RI_i||\rho||E(K_{AS-V}, P_3||SK''_V||H(N''||P_3||F(SK''_V)))\}$給車輛。

步驟 7. 車輛 V 以預先共享密鑰 K_{AS-V} 解密與驗證訊息，並儲存(P_3, SK''_V)以供下一次的登入鑑別或車輛廣播時的假名與對應密鑰。

2.4. 基地台廣播模式

基地台傳訊息給其通訊範圍內所有的車輛時，通訊範圍內的車輛數目可能很多，所以採基地台廣播模式，將訊息一次傳送給其通訊範圍內的所有車輛避免耗費大量計算與通訊成本。詳細的基地台廣播步驟描述如下：

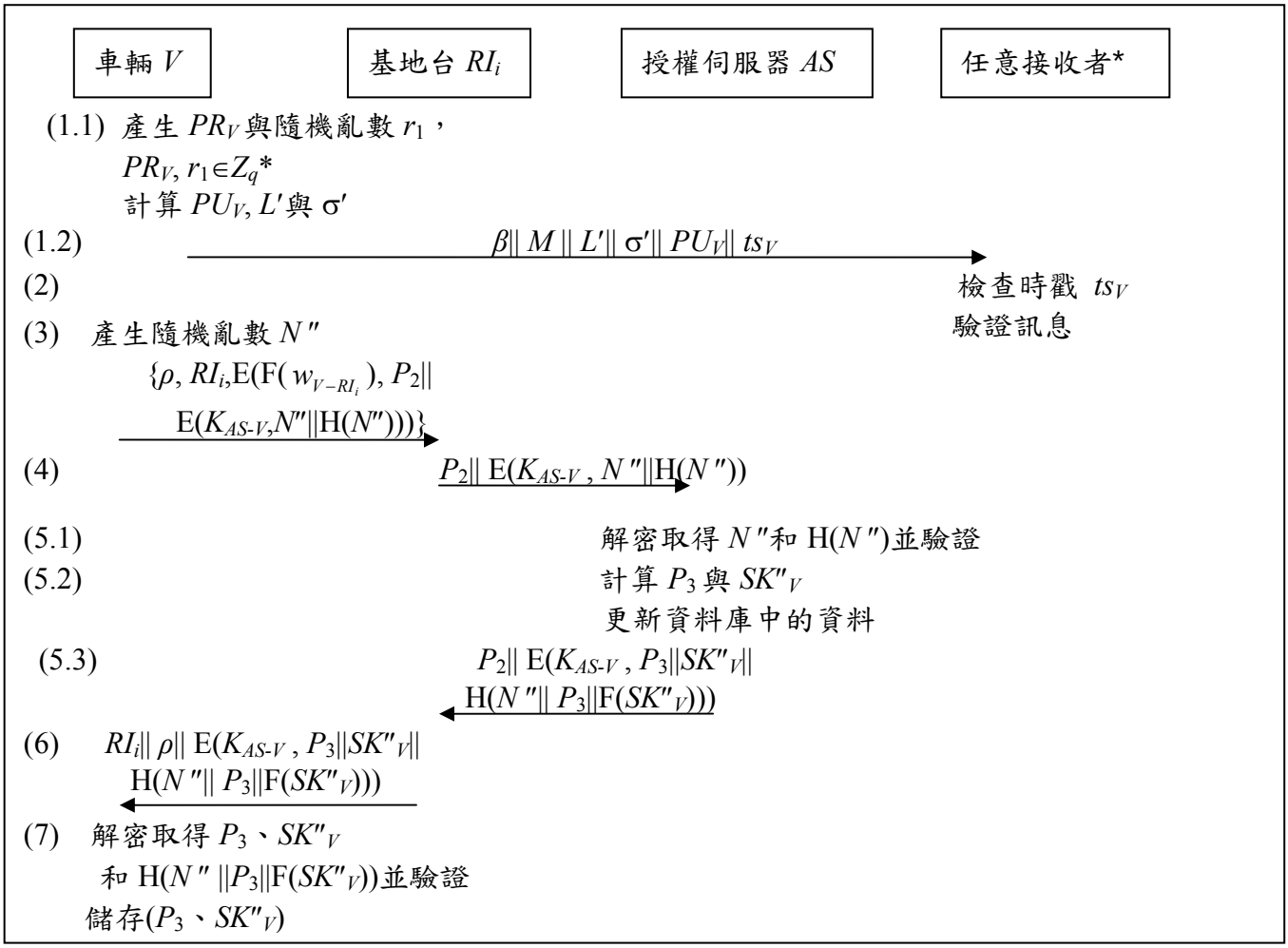
步驟 1. 基地台以下列步驟廣播訊息 M。

步驟 1.1. 選擇隨機亂數 r，$r \in Z_q^*$，並計算

$L=r+\mathrm{H}_1(M||ts_{RI_i})\times PR_{RI_i} \bmod q$ 與 $\sigma=r\cdot\mathrm{H}_0(RI_i)$，$(L, \sigma)$是訊息 M 的簽章。

步驟 1.2.廣播訊息$\{RI_i||M||L||\sigma||PU_{RI_i}||ts_{RI_i}\}$。

步驟 2. 位於基地台 RI_i 通訊範圍內的車輛檢查訊息內的時戳ts_{RI_i}並以授權伺服器 AS 的公開值 C_{AS} 判斷 $e(L\cdot\mathrm{H}_0(RI_i), C_{AS})$與$e(\sigma,C_{AS})\otimes e(PU_{RI_i},\mathrm{H}_1(M||ts_{RI_i})\cdot G)$是否相等進行廣播訊息 M 的驗證並確定來自基地台。



圖四、車輛廣播流程示意圖

第三節安全性分析與比較

本節比較我們的方法與其他學者的方法[6,9,18]，3.1 節做整體安全功能比較；3.2 節說明我們的方法如何達到安全功能；最後 3.3 節就計算效能進行比較。

3.1. 安全功能比較

我們的方法同時考慮表三中車輛與基地台、車輛廣播與基地台廣播等三種的通訊模式及相關功能與安全性； Kamat 等人[6]和 Lu 等人[9]的方法只考慮車輛與基地台通訊模式與車輛廣播模式兩種；Zhang 等人的方法則只考慮到車輛與基地台通訊模式。

表三、通訊模式的比較

模式(Model)	我們的方法	Kamat et al. [6]	Lu et al. [9]	Zhang et al. [18]
車輛與基地台	YES	YES	YES	YES
車輛廣播	YES	YES	YES	NO
基地台廣播	YES	NO	NO	NO

在車輛與基地台通訊模式中，我們的方法提供表四條列的所有安全功能，但是 Kamat 等人和 Lu 等人的方法沒有考慮換手鑑別情形也無法達到匿蹤的要求。

在車輛廣播模式，我們的方法、Kamat 等人

和 Lu 等人所提出的方法均提供鑑別、匿名、匿蹤、完整性與責任等安全功能。而 Zhang 等人的方法並沒有考慮到車輛廣播模式。

此外，我們的方法也進一步考慮基地台廣播訊息提供鑑別、完整性與不可否認性的安全功能，其他三者則未對基地台廣播訊息進行討論。

表四、車輛與基地台通訊模式安全功能比較表

功能 (Capability)	我們的方法	Kamat et al.[6]	Lu et al.[9]	Zhang et al.[18]
雙向鑑別	YES	YES	YES	YES
換手鑑別	YES	N/A	N/A	YES
私密性	YES	YES	YES	YES
匿名	YES	YES	YES	YES
匿蹤	YES	N/A	N/A	YES
前推安全	YES	YES	YES	YES

3.2. 安全分析

本節依不同通訊模式逐一介紹我們的方法如何達到不同的模式中所要求的安全需求。我們方法以 Weil pairing 為基礎其安全性，主要建立在橢圓曲線離散對數難題與橢圓曲線 Diffie-Hellman 難題等二難題上，後續子節將據此討論分析。

定義一. 橢圓曲線離散對數難題(Elliptic Curve Discrete Logarithm Problem, ECDLP)：給予 Q 與 R 是兩個在序列(order)為 q 的橢圓曲線上的點，找出 a，滿足 $Q = a \cdot R$， $a \in Z_q^*$。

定義二. 橢圓曲線 Diffie-Hellman 難題(Elliptic Curve Diffie-Hellman Problem, ECDHP)：假設 G 是序列(order)為 q 的橢圓曲線上的基點(base point)，且 $Q = c \cdot G$ 和 $R = d \cdot \mathrm{G}$，且 $c, d \in Z_q^*$。則給予 Q 與 R，找出點 $U = (c \times d) \cdot G$。

3.2.1. 鑑別

三種通訊模式皆應達到鑑別[6,7,14,18]，目的使車輛被基地台、授權伺服器或其它車輛鑑別身份的合法性以確保網路基本安全功能，在車輛與基地台通訊模式為連接網路的基礎我們進一步考慮雙向鑑別。3.2.1.1 節與 3.2.1.2 節等兩子節分別就車輛與基地台通訊模式中兩種鑑別方式分析說明如何達到雙向鑑別目標，3.2.1.3 節分析兩種廣播模式鑑別功能。

3.2.1.1. 登入鑑別

登入鑑別中，基地台 RI_1 與假名為 P_1 的車輛 V 在步驟 1 至步驟 3 進行雙向鑑別。基地台 RI_1 解密並驗證訊息$\{P_1 \| RI_1 \| \mathrm{E}(\mathrm{H}_2(w_{V-RI_1}), N \| \mathrm{H}(N))\}$正確後，因只有擁有授權伺服器 AS 所給予的假名與相對應的密鑰 SK_V 的車輛 V，才能藉由$\mathrm{e}(\mathrm{H}_0(RI_1), SK_V)$的式子計算會議金鑰 w_{V-RI_1} 產生此訊息，故得以確認車輛 V。相對於車輛 V 而言，解密並驗證$\{RI_1 \| P_1 \| \mathrm{E}(\mathrm{H}_2(w'_{V-RI_1}), (T^*, RI^*, S^*) \| \mathrm{H}(N \| \mathrm{F}(S^*)))\}$正確後，因只有基地台 RI_1 才能以其密鑰計算出會議金鑰 w'_{V-RI_1} $(=\mathrm{e}(SK_{RI_1}, \mathrm{H}_0(P_1)))$並產生此訊息而鑑別基地台的身份。

如果攻擊者在這個階段中想要偽裝成車輛 V 或基地台 RI_1，因為無法取得車輛 V 或基地台 RI_1 的密鑰 SK_V 或 SK_{RI_1}，進而導出正確的 w_{V-RI_1} 或 w'_{V-RI_1} 來產生合作訊息供對方驗證。即使攻擊者 X 為一合法車輛註冊後取得了自己的密鑰 SK_X $(= MK_{AS} \cdot \mathrm{H}_0(P_X))$及假名為 P_X，因 ECDLP 難題，所以攻擊者 X 無法算出授權伺服器 AS 的密鑰 MK_{AS}，因此攻擊者無法隨意產生一個假名 P_Y 及相對應的密鑰 SK_Y $(= MK_{AS} \cdot \mathrm{H}_0(P_Y))$。故攻擊者無法偽冒成別人或自己任意產生假名以及相對應的密鑰。

在登入鑑別步驟 4 至步驟 8 為車輛透過基地台與授權伺服器 AS 交換訊息提供車輛一新假名與對應密鑰供下次鑑別或廣播使用，為確保安全，步驟中包含授權伺服器 AS 與車輛 V 雙向鑑別，因為只有正確的雙方才持有正確的預先共享密鑰(pre-shared key) $K_{AS\text{-}V}$ 並用它對訊息進行加密與驗證，進而確信對方身份。

3.2.1.2. 換手鑑別

車載網路中，車輛移動造成其在不同基地台間換手應是不可以忽略的一環，車輛 V 由基地台 RI_1 移動到基地台 RI_2 服務範圍，基地台 RI_2 與車輛須快速且彼此鑑別以維持網路服務品質之餘兼顧安全性。我們的方法中，基地台 RI_2 由車輛是否擁有由自己所產生並已秘密傳送給鄰近基地台的 S_{RI_2} 值，以確定該車輛其為在鄰近基地台鑑別過的不知名合法車輛。我們的方法中車輛經基地台鑑別過後，該基地台即加密鄰近基地台當時的 S_{RI_2} 值給車輛，故當基地台 RI_2 收到訊息並

用所持有的兩個隨機亂數分別算出 w'_{V-RI_2} 與 w''_{V-RI_2}，若車輛訊息與其一比對相符合，則確信車輛有 S_{RI_2} 值，因為只有擁有 S_{RI_2} 的車輛才能產生與 w'_{V-RI_2} 或 w''_{V-RI_2} 其中之一相符合的 w_{V-RI_2} ($=a \cdot S_{RI_2}$)並以其產生可以通過檢驗的訊息，所以基地台 RI_2 可以相信這個車輛有在它鄰近的基地台鑑別過的車輛。

就車輛 V 而言，用於換手鑑別用的 S_{RI_2} 是由已經相互鑑別過的前一個合法基地台加密傳送給它，所以車輛 V 相信 S_{RI_2} 的正確性。只有正確基地台 RI_2 才能以 S_{RI_2} 中的 $rand\_l_{RI_2}$ 產生正確的雜湊值傳送相關訊息供車輛比對，車輛 V 收到並解密基地台訊息比較結果相符後可以相信基地台 RI_2 的身份。

如果攻擊者在這個階段想要破壞換手鑑別，偽冒成受過鑑別的車輛 V，其必須取得基地台 RI_2 的 S_{RI_2}，但該值是由地台 RI_2 的鄰近基地台鑑別某一車輛合法後才加密提供且其必須同時具假名所對應的密鑰才能通過鑑別，攻擊者無法得逞。若攻擊者為一受過鑑別之車輛並想偽冒成基地台 RI_2，因為 ECDLP 難題，攻擊者就算得到 $S_{RI_2}=(rand\_l_{RI_2}) \cdot G$ 也無法算出其中的隨機亂數 $rand\_l_{RI_2}$，所以攻擊者無法偽冒成基地台 RI_2 欺騙車輛。

3.2.1.3. 基地台廣播與車輛廣播

車輛收到由基地台或其他車輛廣播的訊息時，車輛須驗證訊息是否來自合法的發送者。無論是車輛廣播或基地台廣播，只有合法的車輛或基地台有能力產生訊息 M 的簽章(L, σ)，使得其他接收者以授權伺服器 AS 的公開值 C_{AS} 計算並比較 $e(L \cdot H_0(RI_i), C_{AS})$ 與 $e(\sigma, C_{AS}) \otimes e(PU_{RI_i}, H_1(M \| ts_{RI_i}) \cdot G)$兩值相等，以相信訊息 M 來自合法的發送者。攻擊者嘗試偽造訊息簽章過程將面臨解 ECDLP 難題而不可行。

3.2.2. 私密性(Confidentiality)

車輛與基地台通訊模式中必須考慮到訊息的私密性[6,7]，私密性為確保通訊中的訊息除了正在通訊的車輛與基地台之外，沒有任意第三者可以得知訊息的內容。在我們的方法中，車輛會在登入和換手鑑別後，利用自己及基地台的秘密值來產生會議金鑰，此會議金鑰可保護登入以及之後通訊的訊息，攻擊者欲得知通訊內容，就必須要取得通訊的會議金鑰，但此舉攻擊者將面臨解 ECDLP 與 ECDHP 等難題。

3.2.3. 匿名(Anonymity)與位置隱私

匿名是保護車輛身份的隱私，關於車輛身份的任何資訊，不會因為車輛所傳送的訊息而被推導出來[6,7,9,18]。在我們的方法中，車輛以可以被鑑別為以合法的假名進行網路連線，且假名是以授權伺服器 AS 的密鑰加密車輛身份與隨機亂數產生，因此攻擊者無法自可被鑑別為合法的假名分析出車輛真實身分，當車輛確實達到匿名後車輛的位置隱私[14,15,18]也達到了。

3.2.4. 匿蹤(Untraceability)

匿蹤為攻擊者不能夠利用車輛進行的任何通訊，來追蹤特定車輛的行蹤，包括不能追蹤任一假名車輛的行蹤，即使是基地台共謀，也不能夠憑藉車輛與這些不同的基地台之間的通訊，得以追蹤特定的車輛[6,7,9,18]。與位置隱私不同的地方，在於匿蹤進一步不容許追蹤任一假名車輛的行蹤。我們的方法在車輛與基地台通訊模式與車輛廣播模式下都具備匿蹤功能。

車輛以合法假名登入網路後，每更換一個基地台就自行更換一個假名，且這假名間無相關性，因此攻擊者無法分析通訊的假名來追蹤特定車輛行蹤。縱使有數個基地台共謀，基地台在換手鑑別過程只能判斷車輛為已被合法鑑別並來自鄰近的基地台，但車輛已自行變換假名且其與前一假名無相關性，因此基地台無法與相鄰基地台的先前車輛的假名做任何連結，以掌握某特定車輛的行蹤，除非網路中只有一部車輛。

在車輛廣播訊息時，廣播的訊息只能判斷為來自合法假名的車輛，車輛不但在不同基地台會以不同假名廣播，使用的驗證用的公鑰 PU_V 也是搭配每次隨機產生的對應私鑰而不同，因此攻擊者無法利用任何訊息來追蹤特定車輛。假如數個基地台共謀，尤其換手基地台雖然可能掌握 P_2 與 ρ 之間的關係，但車輛離開基地台後將改以另一換手臨時假名或新假名 P_3 進行各種活動，因此基地台無法得知某一特定車輛的行蹤。

3.2.5. 完整性(Integrity)

三種模式中皆應達到完整性[6,7,9,14]。完整性目的確保廣播的訊息不會在傳送的過程中受

到任意第三者的變造、破壞甚至是偽造訊息。我們的方法中，在車輛與基地台模式中，所有的訊息經過雜湊後並加密的保護，所以如果攻擊者嘗試竄改訊息，使用者在解密後的驗證會發現不吻合，進而得之訊息被竄改，在基地台廣播模式與車輛廣播模式中，基地台或車輛在廣播訊息前都會用臨時私鑰對訊息進行簽章，並提供可被驗證的對應公鑰以利驗證簽章。而我們提供的簽章方法建立在 ECDLP 基礎上，攻擊者擬破壞完整性將面臨解 ECDLP 難題。

3.2.6. 不可否認性(Non-repudiation)

在基地台廣播模式與車輛廣播模式中必須達到不可否認性[6,14]。不可否認性杜防傳送者否認曾經廣播該訊息，憑藉的根據是簽章只有該傳送者有能力產生，因此不可否認。在我們的方法中簽章由私鑰產生，但伴隨簽章會送出對應的公鑰，而接收者以授權伺服器 *AS* 的公開值搭配該公鑰與傳送者身份(有可能是車輛假名或基地台)來驗簽章，在我們的方法中只有合法假名的車輛或基地台擁有關鍵的密鑰才有能力產生簽章用的私鑰所對應公鑰，使得簽章驗證成功，因此傳送者將無法否認其產生該簽章。

3.2.7. 責任(Responsibility)

在車輛廣播模式中達到責任的安全需求，是為了要追究廣播假訊息者的法律責任。尤其為了保護車輛隱私我們的方法提供匿名廣播的功能，當發現有假訊息傳播時必須能同時找出訊息傳送者的真實身份並使其無法否認有傳送過此訊息，進而追究其責任。有關不可否認性，3.2.6 節已分析我們的方法所運用之技術可以使該持假名車輛不可否認傳播該訊息，進一步我們說明授權伺服器 *AS* 有能力透過訊息中的資訊，還原該假名車輛真實身份。在我們的方法中車輛 V 的假名是由授權伺服器 *AS* 用它的密鑰 MK_{AS} 加密車輛的真實身份 V 與一個隨機亂數來產生。因此授權伺服器 *AS* 只需用密鑰 MK_{AS} 對訊息中的假名解密即可取得每一假名所對應的車輛真實身份。

3.2.8. 前推安全

前推安全是指即使攻擊者取得了某次通訊用的會議金鑰與相關資訊，其仍然無法推導出以前通訊曾經使用過的會議金鑰 [13]。在我們的方法中，車輛與基地台通訊模式在鑑別完成後，雙方會產生相同的會議金鑰供運作後續雙方交換資料過程所需的安全功能；在我們方法中登入鑑別會議金鑰：w_{V-RI_1} = e($H_0(RI_1)$, SK_V)= e(SK_{RI_1}, $H_0(P_1)$)，換手鑑別會議金鑰：w_{V-RI_2} =$a \cdot S_{RI_2}$ =($rand\_l_{RI_2}$)$\cdot\rho$，此會議金鑰與假名和當時的基地台有關，又車輛每更換基地台一定換一新假名且假名間毫無關聯，又從會議金鑰逆推其產生之參數將面臨 ECDHP 難題，因此攻擊者取得了車輛 V 在某次與基地台的會議金鑰，仍無法導出先前車輛曾經使用過的會議金鑰，所以可以達到前推安全。

3.3. 計算效能比較

為清楚呈現我們的方法與其他三個方法[6, 9, 18]的計算量比較，定義表五的符號表示各種不同運算元的計算成本符號，藉以清楚說明各方法計算成本比較。

表五、計算量符號定義

符號	表示的計算量
T_{Hash}	雜湊(hash)運算。
$T_{Parring}$	Weil pairing 運算。
T_{Add}	在 G_1 上的加法運算。
T_{Mul}	在 G_1 上的純量與點的乘法運算。
T_{Sym}	對稱式加解密(Symmetric encryption/ decryption)的運算。
T_{Asym}	非對稱式加解密(Asymmetric encryption/decryption)的運算。

3.3.1. 車輛與基地台通訊模式

表六說明每個方法在車輛與基地台通訊模式中登入與換手鑑別計算成本，Kamat 等人的方法在登入階段需要進行非對稱式加解密，因為非對稱式加解密的計算時間比對稱式加解密的耗時許多，因此其方法明顯比我們與其他二個方法僅使用對稱式加密法情形耗費較多計算成本。Lu 等人的方法雖然在進行對稱式加解密加解密的次數比我們的方法少，但其使用 Weil Pairing 的運算相對比我們多許多，而我們的方法在登入鑑別會有較多的運算成本是為換手鑑別做準備，而 Lu 等人的方法並沒有考慮換手鑑別功能，但在車載網路中車輛的移動不應是可以忽略的一環。Zhang 等人所提出的方法雖然提供車輛換手鑑別的功能，但不管是在登入鑑別或換手鑑別，我們方法所需的計算量都相對較少。綜合而論，

在車輛與基地台通訊模式下，我們方法的計算效能皆優於其它三者。

表六、車輛與基地台通訊模式計算量的比較

	登入鑑別的計算量	換手鑑別的計算量
我們的方法	$9T_{Sym}+2T_{Parring}+1T_{Mul}+9T_{Hash}$	$2T_{Sym}+4T_{Mul}+2T_{Hash}$
Kamat et al.[6]	$4T_{Asym}+3T_{Sym}+4T_{Parring}+5T_{Mul}+2T_{Add}+6T_{Hash}$	N/A
Lu et al.[9]	$4T_{Sym}+9T_{Parring}+22T_{Mul}+10T_{Add}+6T_{Hash}$	N/A
Zhang et al.[18]	$10T_{Sym}+2T_{Parring}+6T_{Mul}+3T_{Add}+1T_{Hash}$	$4T_{Sym}+2T_{Parring}+7T_{Mul}+1T_{Add}+3T_{Hash}$

3.3.2. 車輛廣播模式

車輛廣播模式主要用於車輛發送緊急訊息告知周邊車輛及基地台，其後訊息的通知將交給基地台，我們分兩個部份說明車輛廣播的計算成本，第一部份是從車輛開始廣播訊息到接收到此訊息的其它車輛或基地台做完訊息的驗證，所需的整體計算量的比較。第二部份則是當惡意車輛廣播錯誤的訊息，相關的部門單位找出廣播錯誤訊息車輛的真實身份所需的計算量。表七為我們的方法與其他兩者計算量的比較。Kamat 等人的方法在廣播訊息中需要進行對稱式加解密，我們的方法不需要進行任何的加解密。Lu 等人的方法雖然同樣不需要進行加解密，但在整體計算量上我們很明顯的比它們少。在事件發生後，追蹤車輛身份所需的計算量比較，我們的方法與 Kamat 等人的方法等人的方法只需要進行一次對稱式加解密，Lu 等人的方法則多出一次 G_1 上的加法與兩次 G_1 上的純量與點的乘法，且基地台會需要額外的儲存成本儲存以下的資訊(RID_i, T_i, Y, R_2, σ_1)。所以我們的方法在車輛廣播中，不管是廣播時所需的計算量，或是為了追蹤廣播假訊息的車輛真實身份上的計算量，以及基地台是否需要為此而有額外的儲存成本這點，都優於其它三者。

第四節 結論

車載網路(VNET)環境下，保護車輛真實身份、位置與行蹤的隱私，是隱私性中非常重要的議題。我們考慮到全面性的通訊模式，提出以 Weil pairing 為基礎的隱私保護技術，讓基地台要提供車輛服務時，可以在不需得知車輛真實身份的情況下，與車輛完成互相鑑別。同時我們的方法也可以提供通訊中的私密性、完整性與不可否認性。甚至在車輛廣播模式中，面對一些廣播假訊息的惡意車輛時，我們方法中的授權伺服器有能力透過訊息來還原這些惡意車輛的真實身份，並提供給相關的法律單位，去追究該惡意車輛所應負起的法律相關責任。因此，本論文的方法可以在保護使用者隱私性的同時，也達到基本的通訊安全需求與車載網路環境下特殊的責任需求。此外，我們的方法不只是提供完整的功能與安全性，所需的計算量與較其它方法少。所以，我們的方法更適合做為車載網路安全保護機制。

表七、車輛廣播模式計算量的比較

	廣播計算量	追蹤的計算量	基地台需要的額外儲存空間
我們的方法	$3T_{Parring}+4T_{Mul}+4T_{Hash}$	$1T_{Sym}$	0
Kamat et al.[6]	$2T_{Sym}+4T_{Parring}+5T_{Mul}+2T_{Add}+6T_{Hash}$	$1T_{Sym}$	0
Lu et al.[9]	$3T_{Parring}+12T_{Mul}+5T_{Add}+3T_{Hash}$	$1T_{Sym}+2T_{Mul}+1T_{Add}$	RID_i, T_i, Y, R_2, σ_1

誌謝

本研究部份成果為國科會補助的專題計畫所支持，計畫編號：NSC 98-2221-E-032 -019

參考文獻

[1] O. Andrisano, R. Verdone, M. Nakagawa, "Intelligent Transportation Systems: The Role of Third-Generation Mobile Radio Networks", *IEEE Communications Magazine*, Volume 38, Issue 9, pp.144-151, 2000

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003

[3] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks", *in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pp. 79 – 87, 2005

[4] M. Gerlach and F. Güttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real", *in Proceedings of IEEE 65th Vehicular Technology Conference*, pp. 2521-2525, 2007.

[5] J.-P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004.

[6] P. Kamat, A. Baliga, W. Trappe, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks", *Security and Communication Networks*. Volume 1, Issue 3, pp. 233 – 244, 2008

[7] S. H. Kim, B. H. Kim, Y. K. Kim, and D. H. Lee, "Auditable and Privacy-Preserving Authentication in Vehicular Networks", *in Proceedings of The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pp. 19-24, 2008

[8] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "Sevecom - secure vehicle communication", *in Proceedings of IST Mobile Summit*, 2006.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen,"ECPP：Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", *in Proceedings of the 27th Conference on Computer Communications*, pp. 1229 – 1237, 2008

[10] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy", *in Proceedings of the 5th ACM workshop on Privacy in electronic society*, pp. 19 - 28, 2006

[11] T. Leinmüller, E. Schoch and C. Maihöfer, "Security requirements and solution concepts in vehicular ad hoc networks", *in Proceedings of the Fourth Annual Conference on Wireless on Demand Network Systems and Services*, pp. 84-91, 2007.

[12] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", *in Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, 2005. [Online].Available:http://www.ece.cmu.edu/~bparno/

[13] M. D. Raimondo, R. Gennaro, "New approaches for deniable authentication", *in Proceedings of the 12th ACM conference on Computer and communications security* , pp.112-121, 2005

[14] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks", *In Proceeding of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN)*, pp.11-21, 2005

[15] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA：Robust Location Privacy Scheme for VANET", *IEEE Selected Areas in Communications*, Volume 25, pp. 1569-1589, 2007

[16] Y. Toor, P. Muhlethaler, A. Laouiti, "Vehicle Ad Hoc networks: applications and related technical issues", *IEEE Communications Surveys & Tutorials*, Volume 10, Issue 3, pp.74-88, 2008

[17] Y. Xi, W. Shi and L. Schwiebert, "Mobile anonymity of dynamic groups in vehicular networks", *Security and Communication Networks*, Volume 1, Issue 3, pp. 219 – 231, 2008

[18] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A Location Privacy Preserving Authentication Scheme in Vehicular Networks", *in Proceedings of Wireless Communications and Networking Conference*, pp. 2543-2548, 2008.

[19] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE：An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks", *in Proceedings of IEEE International Conference on Communications*, pp. 1451-1457, 2008

[20] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks", *in Proceedings of the 27th Conference on Computer Communications*, pp. 246-250, 2008