在車載網路上有效之金鑰分配實現遠距離與安全之推播訊息傳遞

吳威震[1]　陳奕明[2]
[1]新生醫護管理專科學校電子計算機中心
[1,2]中央大學資訊管理學系
[1]wwu@hsc.edu.tw
[2]cym@cc.ncu.edu.tw

摘要

由於車載網路(VANET)是藉由無線通訊技術進行資料傳輸，如何能在 VANET 上提供快速與安全的推播訊息服務，是一個很重大的挑戰與需要解決的問題，尤其是當有交通壅塞與事故發生時，訊息該如何有效與正確的傳遞，是本論文的研究重點，即使距離事故發生幾十公里遠的車輛，將可透過車載通訊設備得知目前事故發生狀況與道路路況，並提供駕駛人相關建議與行駛路徑，以改善交通流量，提供更好的交通品質。在本研究中將以密碼學中金鑰分配的方式來實現遠距離之推播訊息服務，且滿足車輛的隱私性與相關的資訊安全需求，本研究將利用雙線性配對函數來解決安全與效率的問題。在效能上，預期減少 25%以上的訊息傳遞次數，當車輛經過愈多的路側單元，幾乎可以減少一半以上的訊息傳遞次數。在安全上，金鑰是被有效的保護，且只有被授權的車輛才能被驗證獲取相關的推播訊息服務，並滿足前推安全、後推安全與避免重送攻擊與女巫攻擊等威脅。

關鍵詞：車載網路；推播訊息；金鑰分配；密碼學；資訊安全。

1. 前言

隨著無線網路通訊的進步，許多 VANET 的相關議題與應用被提出後[1, 3-5, 7-10]，Raya 等人將 VANET 簡單區分為安全相關應用(Safety-related applications)與其他應用 [5]，而 Bai 等人[1]則將 VANET 區分成三種等級，這三種等級最下層主要為商業應用、中間層主要以提供駕駛人方便為目的的應用、最上層為安全上的應用。無論是在車載上提供非安全相關訊息傳遞(Unsafety-Related Message)，例如提供單純的娛樂資訊，或與安全相關訊息傳遞(Safety-Related Message)，例如即時交通資訊等，這些在 VANET 所交換的資訊更顯為重要，若無做適當的保護措施，輕則只有財產損失，重則將影響生命安全。如何讓安全相關訊息(Safety-Related Message)在車輛與事故處理單位中有效地被傳遞是一個重要的議題。此外在網路安全的議題上有關 VANET 的應用中，時常成為攻擊者鎖定的目標，藉由無線通訊技術，攻擊者很容易在無線電波涵蓋的範圍內進行封包監聽、資料竄改、阻斷服務攻擊或其他攻擊等等，對攻擊目標造成嚴重的影響，網路的安全及一些包含乘客身份相關的隱私資訊會受到威脅，且這些推播訊息是必須被驗證過的，以避免推播訊息被惡意竄改，造成有心人士利用此推播訊息獲取相關的道路或交通資源。

基於處理車輛節點增加、並免過多的 V2V 通訊與 VANET 網路延展性的變化，本論文將提出一種新的金鑰分配方式來解決 VANET 節點的快速變化，以實現遠距離與安全之推播訊息傳遞。在此架構的推播訊息服務中無論是 V2V 通訊過程，或車輛與 RSU 在通訊過程中，相鄰的 RSU 會彼此作金鑰交換與同步，此時可採離線方式來達到金鑰交換，讓車輛在高速行進過程中，減少與 RSU 的訊息溝通次數，並能快速通過取得相關的會議金鑰，這裡所指的離線方式是針對車輛無須直接連線至 RSU，只須 RSU 之間彼此交換資訊。本架構的推播訊息方式是先透過與鄰近 RSU 推播訊息傳遞，讓鄰近 RSU 能獲取附近地區的交通狀況，透過此方式將能達成遠距離推播訊息傳遞，最後每個 RSU 透過本地推播訊息傳遞，將所收到的推播訊息傳給所屬廣播範圍內的車輛。而在隱私處理方式，將處理身分識別的匿名化，VANET 各節點中將無法得知對方的實際身分，也包含 RSU 的身分識別匿名化，以避免透過惡意之 RSU 獲取相關交換資訊。因此基於資訊安全與效能的考量下，本論文將透過雙線性配對函數達到車載網路之有效匿名與金鑰交換協定。因此本研究目的是在 VANET 上針對安全相關訊息(Safety-Related Message)提供一套安全又有效的推播訊息傳遞，以實現幾時在幾十公里遠的車輛也能快速獲取遠距離的交通狀況且這些推播訊息是必須被驗證過的，以避免推播訊息被惡意竄改，造成有心人士利用此推播訊息獲取相關的道路或交通資源。

2. 推播訊息傳遞

本研究所提之推播訊息傳遞架構中將以雙線性配對函數來解決安全上與效能上的問題，並分為八個階段。首先當所有 R_j 與 V_i 完成(2.2)註冊階段後，將各別得到對應的臨時匿名識別碼 R_{IDj} 與 V_{IDi}。接著進入(2.3)廣播驗證階段，R_j 廣播訊息 m_j，V_i 驗證合法性並根據所經過的 RSU 接收所有的 m_j。接著進入(2.4)會議金鑰協定，R_j 與 V_i 共同產生會議金鑰 K_j。最後進入(2.5)RSU 彼此金鑰交換與同步。此時由 RSU 之間彼此交換金鑰，由於這個

動作可選擇任何時段來處理為 RSU 之間的交換，這將不影響整個車載網路的通訊成本。爾後當 V_i 進入另一區的 RSU 廣播範圍透過(2.6) 鄰近金鑰請求即可獲取該區的會議金鑰，無須再一次透過(2.3)廣播驗證與(2.4)會議金鑰協定來可獲取。

本架構的推播訊息方式是先透過(2.8)鄰近RSU 推播訊息傳遞，讓鄰近 RSU 能獲取附近地區的交通狀況，透過此方式將能達成遠距離推播訊息傳遞，最後每個 RSU 透過本地推播訊息傳遞，將所收到的推播訊息傳給所屬廣播範圍內的 V_i，透過以上方式將能實現遠距離與安全之推播訊息傳遞。

表 1 符號說明

符號表示	說明
CP	服務提供者
RSU	路側單元
MS_j	第 j 個 RSU 所推播的訊息
R_j	第 j 個 RSU
RID_i	R_j 之身分識別碼
R_{IDj}	R_j 之匿名識別碼
$C=E_K(m)$	使用 K 對明文 m 對稱式加密成密文 C
$m=D_K(C)$	使用 K 對密文 C 對稱式解密成明文 m
V_i	第 i 台車輛
VID_i	V_i 之身分識別碼
V_{IDi}	V_i 之匿名識別碼
A→B：C	A 傳遞訊息 C 至 B
H_1, H_2, H_3, H_4	單向雜湊函數

2.1 系統設定階段

G_1 為一序大質數 q 的加法群，G_2 則為一序同為大質數 q 的乘法群，而 $e:G_1\times G_1\rightarrow G_2$ 為雙線性映射函數，其生成數為 P，並使 4 個雜湊函數 H_1, H_2, H_3 與 H_4，本架構中之各角色將分別產生私密金鑰與對應之公開金鑰。

- CP：自行隨機產生一個亂數 $s \in Z^*_q$，且計算 $P_{pub}=sP$，除了保持 s 為私密外，其餘$\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$皆為公開值。
- R_j：隨機產生一個亂數 $x_j \in Z^*_q$，且計算 $P_{xj}=x_jP$，x_j 為 R_j 之私密金鑰，P_{xj} 為對應之公開金鑰。
- V_i：隨機產生一個亂數 $y_i \in Z^*_q$，且計算 $P_{yi}=y_iP$，y_i 為 V_i 之私密金鑰，P_{yi} 為對應之公開金鑰。

2.2 註冊階段

註冊階段將分為 V_i 對 CP 註冊與 R_j 對 CP 註冊兩種，CP 經過一段時間收到與許多 R_j 與 V_i 的註冊後，詳細說明如下。

2.2.1 V_i 向 CP 註冊

- $V_i \rightarrow$ CP：VID_i, y_iP
  V_i 用自己的私密金鑰 y_i 計算出 y_iP，並將自己的身分識別碼 VID_i 與 y_iP 送至 CP 註冊。
- CP $\rightarrow V_i$：V_{IDi}, T_i
  CP 收到 VID_i 與 y_iP 後，先檢驗 $P_{yi}?= y_iP$，若相等，則同意 V_i 註冊，並配發一個臨時匿名識別碼 $V_{IDi}=H_1(VID_i, P_{yi}, sP, T_i)$，$T_i$ 為時間戳記，CP 並將 V_i 註冊的相關資訊加入其資料庫中$\{VID_i, y_iP, V_{IDi}, T_i\}$。

2.2.2 R_j 向 CP 註冊

- $R_j \rightarrow$CP：RID_j, x_jP, M_j
  R_j 用自己的私密金鑰 x_j 計算出 x_jP 與 $M_j=H_1(RID_j, x_j)$，並將自己的身分識別碼 RID_j, x_jP 與 M_j 送至 CP 註冊。
- CP $\rightarrow R_j$：R_{IDj}
  CP 收到 RID_j, x_jP 與 M_j 後，先檢驗 $P_{xj}?= x_jP$，若相等，則同意 R_j 註冊，並配發一個臨時匿名識別碼 $R_{IDj}=H_1(RID_j, P_{xj}, s)$，TA 並將 R_j 註冊的相關資訊加入其資料庫中$\{RID_j, x_jP, R_{IDj}, M_j\}$。

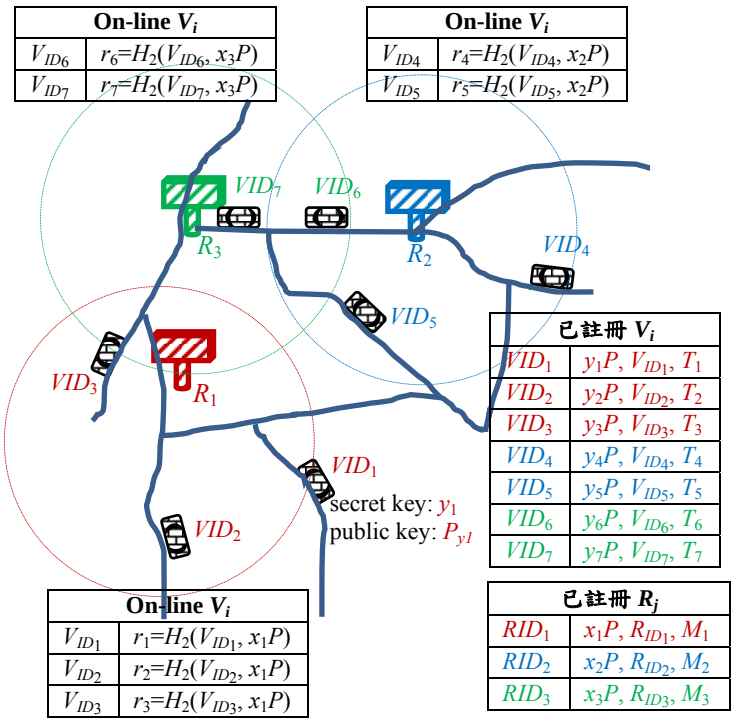

圖 1 廣播階段

2.3 廣播驗證階段

此階段是當某一 V_i 進入 R_j 的廣播通訊範圍後，由 V_i 採匿名的方式對 R_j 提出請求，R_j 也將採匿名的方式廣播給所有的 V_i，詳細說明如下：

- $V_i \rightarrow R_j$：V_{IDi}
  V_i 對通訊範圍內的 R_j 提出請求，並送出其匿名

的 V_{IDi}。

- $R_j \rightarrow V_i$：$R_{IDj}, e_j, P_{xj}, Q, m_j$
  任一通訊範圍內的 R_j 收到 V_{IDi} 後，計算 $r_i = H_2(V_{IDi}, x_jP)$與 $e_j = r_i \oplus R_{IDj}$，並建置即時資料庫，儲存 V_{IDi} 與 r_i，透過即時資料庫可了解目前有哪些 V_i 是在 R_j 通訊範圍內。為了對 R_j 通訊範圍內所有的 V_i 廣播，R_j 從即時資料庫將所有 V_{IDi} 的 r_i 取出，計算出 $Q=\Pi r_i$，並產生一個 Nonce 值 N，最後用 r_i 當作對稱式加密金鑰將 Q 與 N 加密成 $m_j=E_{ri}(Q, N)$，如圖 1 所示，最後將其匿名的 R_{IDj} 與 e_j, P_{xj}, Q, m_j 廣播給所有的 V_i。
- V_i 驗證廣播訊息正確性
  V_i 收到 $R_{IDj}, e_j, P_{xj}, Q, m_j$ 後，使用其真實身分 VID_i、私密金鑰 y_i、公開值 P, P_{pub} 與時間戳記 T_i 驗證 $e(y_iP_{xj}, (e_j \oplus H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj}))P)?=e(P_{yi}, P_{xj})^{R_{IDj}}$.

2.4 會議金鑰協定

會議金將使用 Diffie & Hellman[2]的方式來產生，V_i 與 R_j 雙方藉由金鑰協定階段分別取得 Z_j 與 W_i 值，並分別使用自己的 Q 值與 N 來各自產生會議金鑰 $Z_j{}^Q$ 與 $W_i{}^N$，此時 $K_j=\alpha^{QN}$。

- $V_i \rightarrow R_j$：N', W_i
  當任何一個 V_i 收到 m_j 後，V_i 使用其真實身分 VID_i、私密金鑰 y_i、公開值 P、P_{pub} 與時間戳記 T_i 計算 $r_i'=H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj})$，並用其當作對稱式解密金鑰解開 $D_{ri'}(m_j)$，並驗證解開後的 Q 是否相等，最後計算 $W_i=\alpha^Q$，並將解開的 N'與 W_i 傳回給 R_j。
- $R_j \rightarrow V_i$：Z_j
  R_j 收到 N'與 W_i 後，驗證 $N'=N$ 是否相等，若相等則計算 $Z_j=\alpha^N$ 並將 Z_j 廣播回傳給 V_i，此時 R_j 與 V_i 可自行產生會議金鑰 $K_j=Z_j^Q=W_i^N=\alpha^{QN}$。

下一次會議金鑰的產生由 R_j 決定，可能根據舊的 V_{old} 離開而產生新的 Q'為$(\Pi r_i)/r_{old}$，或新的 V_{new} 進入而產生 Q'則為$(\Pi r_i) \cdot r_{new}$ 或會議期效過期等因素，將考慮重新產生新的會議金鑰 K_j。

2.5 RSU 彼此金鑰交換與同步

RSU 金鑰交換的目的為當任一車輛 V_i 由 R_j 進入另個 R_k 時，無須透過會議金鑰協定，直接能透過一個⊕運算快速取得 R_k 的會議金鑰 K_k，主要方式是 RSU 採用離線運算的方式彼此交換資訊，假設 R_1 與 R_2 為本次要做金鑰交換的兩個 RSU，每個 RSU 皆有自己的協議資料庫(Agreement Database)紀錄與那些 RSU 達成金鑰共享協議，由於採用離線運算，故所有傳遞的通道，皆屬封閉式安全的通道， RSU 之間金鑰交換，並說明如下：

- CP $\rightarrow R_1$：M_2
  CP 根據之前 R_2 註冊時的相關資料，將 M_2 傳送至 R_1。
- CP $\rightarrow R_2$：M_1
  CP 根據之前 R_1 註冊時的相關資料，將 M_1 傳送至 R_2。
- $R_1 \rightarrow R_2$：$R_{ID1}, C_{1,2}, t_1$
  R_1 計算 $C_{1,2}= H_3(M_2, t_1)$，t_1 為的時間戳記，最後將 $R_{ID1}, C_{1,2}$ 與 t_1 傳送至 R_2。
- $R_2 \rightarrow R_1$：$R_{ID2}, C_{2,1}, t_2, C_{1,2} \oplus K_2$
  R_2 收到 $R_{ID1}, C_{1,2}, t_1$ 後，使用自己的識別碼 RID_2 與私密金鑰 x_2 檢查 $C_{1,2}?= H_3(H_1(RID_2, x_2), t_1)$，若正確則計算 $C_{2,1}= H_3(M_1, t_2)$，t_2 為時間戳記，最後將 $R_{ID2}, C_{2,1}, t_2$ 與 $C_{1,2} \oplus K_2$ 傳送至 R_1，這裡的 K_2 為 R_2 與其範圍內 V_i 所協議的會議金鑰。
- $R_1 \rightarrow R_2$：$C_{2,1} \oplus K_1$
  R_1 收到 $R_{ID2}, C_{2,1}, t_2$ 與 $C_{1,2} \oplus K_2$ 後，R_1 使用自己的識別碼 RID_1 與私密金鑰 x_1 檢查 $C_{2,1}?= H_3(H_1(RID_1, x_1), t_2)$，若正確則能計算 R_2 的會議金鑰 $K_2=C_{1,2} \oplus K_2 \oplus H_3(M_2, t_1)$，並將 R_{ID2} 與 K_2 加入 R_1 自己的協議資料庫，最後將與 $C_{2,1} \oplus K_1$ 傳送至 R_2，R_2 收到後，也能正確則能計算 R_2 的會議金鑰 $K_1=C_{2,1} \oplus K_1 \oplus H_3(M_1, t_2)$ ，並將 R_{ID1} 與 K_1 加入 R_2 自己的協議資料庫，這裡的 K_1 為 R_1 與其範圍內 V_i 所協議的會議金鑰。

2.6 鄰近金鑰請求

此階段為 V_i 於不同 RSU 之間快速獲取金鑰方式，假設 $V_{i,Rj}$ 為一個 V_i 且是在 R_j 通訊範圍內並經過 R_k 時 $V_{i,Rj}$ 欲獲取 K_k。

- $V_{i,Rj} \rightarrow R_k$：P_{xj}
  當 $V_{i,Rj}$ 進入 R_k 通訊範圍內時，$V_{i,Rj}$ 傳送 P_{xj} 給 R_k 告知想獲取 K_k。
- $R_k \rightarrow V_{i,Rj}$：$K_j \oplus K_k$
  R_k 收到 P_{xj} 後，使用 P_{xj} 向 CP 提出匿名識別碼請求，CP 將告知其為 R_{IDj}，R_k 將從協議資料庫中判斷是否與 R_j 有協議金鑰共享，若有，則傳送 $K_j \oplus K_k$ 至 $V_{i,Rj}$。最後 $V_{i,Rj}$ 收到 $K_j \oplus K_k$ 後，使用自己的會議金鑰 K_j 作互斥或運算，將能得到 K_k 值。

當 $V_{6,R3}$ 為一個 VID_6 且皆在自己 R_3 與鄰近 R_2 通訊範圍內，當 VID_6 想獲取鄰近 R_2 的 K_2 時將採以下步驟：

- $V_{6,R3} \rightarrow R_2$：P_{x3}
  當 $V_{6,R3}$ 進入 R_2 通訊範圍內時，$V_{6,R3}$ 傳送 P_{x3} 給 R_2 告知想獲取 K_2。
- $R_2 \rightarrow V_{6,R3}$：$K_3 \oplus K_2$
  R_2 收到 P_{x3} 後，使用 P_{x3} 向 CP 提出匿名識別碼請求，CP 將告知其為 R_{ID3}，R_2 將從協議資料庫中判斷是否與 R_3 有協議金鑰共享，若有，則傳送 $K_3 \oplus K_2$ 至 $V_{6,R3}$。最後 $V_{6,R3}$ 收到 $K_3 \oplus K_2$ 後，使用自己的會議金鑰 K_3 作互斥或運算，將能得到 K_2 值。

2.7 匿名識別碼請求

任何已註冊之 R_j 皆可使用另一 R_k 之 P_{xk} 向 CP 提出匿名識別碼請求，例如當 $V_{i,Rj}$ 於不同 RSU(R_k) 之間想快速獲取金鑰時，R_k 會向 CP 提出匿名識別

碼請求，如(3.6)鄰近金鑰請求中所描述。

- R_k→ CP : RID_k, x_kP, P_{xj}
  R_k 送出自己的真實識別碼 RID_k，與 x_k 自己的私密金鑰所計算的 x_kP，並透過 R_j 的 P_{xj} 向 CP 提出匿名識別碼請求。
- CP→ R_k: R_{IDj}
  CP 檢查 P_{xk} ?=x_kP，若正確，並計算 R_{IDj}=$H_1(RID_j, P_{xj}, s)$給 R_k。

2.8 鄰近 RSU 推播訊息傳遞

此過程為 RSU(R_j) 傳遞 Safety-Related Message(MS_j)至其他 RSU(R_k)，R_k 將告知所屬範圍內的 V_i 即時改變之行駛路徑與對策，假設 MS_j 的訊息結構為 MS_j=Traffic Jam & Accident ||Suggestion。

- R_j → R_k：R_{IDj}, $C_{j,k}$, t_j, MS_j
  R_j 計算 $C_{j,k}$= $H_3(M_k, t_j)$，t_j 為的時間戳記，並將其匿名識別碼 R_{IDj} 與 $C_{j,k}$, t_j, MS_j 傳遞至 R_k。
- R_k 檢查 $C_{j,k}$? = $H_3(H_1(RID_k, x_k), t_j)$，若相等，則 MS_j 是正確的訊息，R_k 將告知所屬範圍內的 V_i 即時改變之行駛路徑與對策。此時 R_k 也將執行聯集運算 MS_k=MS_k∪MS_j 傳給其他 RSU，這裡的聯集運算是分別對 Traffic Jam & Accident 與 Suggestion 分別作聯集。

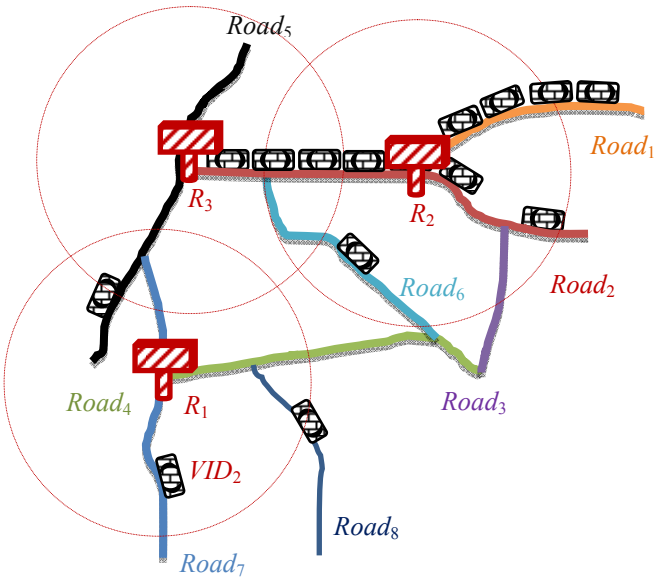

圖 2 RSU 訊息傳遞

從圖 2 範例中顯示出 MS_2 為 $Road_1Road_2||Road_3Road_6$ 此推播訊息將表示 $Road_1$ 與 $Road_2$ 目前處於壅塞現象，建議行駛路徑為 $Road_3$ 與 $Road_6$，而 MS_3 為 $Road_2||Road_5Road_6$ 此推播訊息將表示 $Road_2$ 目前處於壅塞現象，建議行駛路徑為 $Road_5$ 與 $Road_6$，MS_1 為 $empty||Road_4Road_5Road_7Road_8$ 此推播訊息將表示無壅塞現象，建議行駛路徑為 $Road_4$、$Road_5$、$Road_7$ 與 $Road_8$。

- R_2→ R_3：R_{ID2}, $C_{2,3}$, t_2, MS_2
  R_2 計算 $C_{2,3}$= $H_3(M_3, t_2)$，t_2 為的時間戳記，並將 R_{ID2} 與 $C_{2,3}$, t_2, MS_2=$Road_1Road_2||Road_3Road_6$ 傳遞至 R_3。
- R_3→ R_1：R_{ID3}, $C_{3,1}$, t_3, MS_3
  R_3 檢查 $C_{2,3}$? = $H_3(H_1(RID_3, x_3), t_2)$，若正確，持續將 MS_3 傳遞下去至 R_1，此時 MS_3 為 MS_2∪MS_3 的聯集，如下所示。

$$\begin{array}{ll} MS_3 = & Road_2 \,||\, Road_5Road_6 \\ \cup \quad MS_2 = & \underline{Road_1Road_2 \,||\, Road_3Road_6} \\ MS_3 = & Road_1Road_2 \,||\, Road_3Road_5Road_6 \end{array}$$

R_3 計算 $C_{3,1}$= $H_3(M_1, t_3)$，t_3 為的時間戳記，並將 R_{ID3} 與 $C_{3,1}$, t_3, MS_3=$Road_1Road_2||Road_3Road_5Road_6$ 傳遞至 R_1。R_1 檢查 $C_{3,1}$? = $H_3(H_1(RID_1, x_1), t_3)$，若正確，$MS_3$ 是正確的訊息。

2.9 新的 V_i 加入

在推播訊息服務中 V_{new} 為新的成員，且進入 R_j 通訊範圍內，同樣會向 R_j 告知 V_{IDi} 進入，類似廣播階段，但唯一差別在於 R_j 在傳遞{R_{IDj}, e_j, P_{xj}, Q_{new}, m_j}時，不會廣播給所通訊範圍內的 V_i，而只有將其傳給 V_{new}，主要是避免過於頻繁的 V_{new} 加入時，重複多次的{R_{IDj}, e_j, P_{xj}, Q_{new}, m_j}廣播，此時的 Q=Πr_i • r_{new}，r_{new} 為 V_{new} 所產生的值，此時也將考慮重新產生新的會議金鑰 K_j。

- V_{new}→ R_j：N', W_i
  當 V_{new} 收到{R_{IDj}, e_j, P_{xj}, Q_{new}, m_j}後，V_{new} 使用其真實身分 VID_i、私密金鑰 y_i、公開值 P、P_{pub} 與時間戳記 T_i 計算 r_i=$H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj})$，並用其當作對稱式解密金鑰解開 $D_{ri}(m_j)$，並驗證解開後的 Q_{new} 是否等於 Q • r_{new}，若相等則計算 W_i=α^{Qnew} 並將解開的 N'與 W_i 傳回給 R_j。
- R_j→V_{new}：Z_j
  R_j 收到 N'與 W_i 後，驗證 N'=N 是否相等，若相等則計算 Z_j=α^N 並將 Z_j 廣播回傳給 V_{new}，此時 R_j 與 V_{new} 可自行產生會議金鑰 K_j=Z_j^{Qnew} =W_i^N=α^{QnewN}。

2.10 舊的 V_i 離開

在推播訊息服務中 V_{old} 為舊的成員，且離開 R_j 通訊範圍內，此時不即時更新會議金鑰 K_j，而是在一個時間周期內更新會議金鑰值時，重新計算 Q_{update}=(Π r_i)/r_{old}，r_{old} 為 V_{old} 所產生的值。

- R_j→ V_i：m_j'
  R_j 計算 m_j'=$E_{ri}(Q_{update}, N+1)$廣播傳給 V_i。
- V_i→ R_j：N+1, W_i
  當任何一個 V_i 收到 m_j'後，V_i 使用其真實身分 VID_i、私密金鑰 y_i、公開值 P、P_{pub} 與時間戳記 T_i 計算 r_i'=$H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj})$，並用其當作對稱式解密金鑰解開 $D_{ri'}(m_j')$，並驗證解開後的 Q_{update} 是否相等，最後計算 W_i=$\alpha^{Qupdated}$，並將解開的 N+1 與 W_i 傳回給 R_j。。

- $R_j \rightarrow V_i : Z_j$
  R_j 收到 N+1 與 W_i 後，驗證 *Nonce* 是否為 N+1，若是，則計算 $Z_j=\alpha^{N+1}$ 並將 Z_j 廣播回傳給 V_i，此時 R_j 與 V_i 可自行產生會議金鑰 $K_j= Z_j^{Qupdated}=W_i^{N+1}=\alpha^{Qupdated\,(N+1)}$。

2.11 車載之間訊息傳遞方式

在推播訊息服務中假設 V_i 與 V_j 分別在不同的 R_j 與 R_k 時，當 V_i 與 V_j 需互相傳遞訊息時，會採取如下步驟:

- $V_{i,Rj} \rightarrow V_{j,Rk}: R_{IDj}, E_{Kj}(MS_j, T_{sm}), T_j$
  $V_{i,Rj}$ 將使用當下的會議金鑰 K_j 將時間戳記 T_j 與 MS_j 做對稱式加密，並將所在之匿名 R_{IDj}, $E_{Kj}(MS_j, T_{sm})$, T_j 傳遞至 $V_{j,Rk}$。

$V_{j,Rk}$ 收到後根據所在之匿名 R_{IDj} 執行 3.6 鄰近金鑰請求步驟：V_j 於不同 RSU 之間彼此金鑰獲取方式，解開訊息 D_{Kj} (E_{Kj} $E_{Kj}(MS_j, T_{sm})$)後，檢查時間戳記 T_j，若在合理時間內，表示此 MS_j 訊息是正確的。

3. 安全與效能分析

本論文預期能在 VANET 上提供安全與有效的多媒體資訊分享服務與推播訊息服務，因此對於研究成果將以減少訊息傳遞次數、時間效能上與安全上進行分析。

3.1 減少訊息傳遞次數

本論文所提的推播訊息服務，將透過(2.5)RSU 彼此金鑰交換與同步來減少會議金鑰協議中的訊息傳遞次數。在傳統的車載網路金鑰交換協定時，至少雙方需先經過認證階段，再經過金鑰交換階段，但當驗證的雙方成員時常在改變時，此時所需花費的時間成本將相對的提高，例如在車載網路中當某台車輛(V_i)經過一路側單元(R_j)時，假設雙方要彼此產生一把會議金鑰時，除非彼此事前就相互信任，否則就必須先經過認證階段，在處理一般認證階段時需 2 個往返次數的傳遞，首先由受驗證端發出驗證請求，並由驗證端來驗證是否為合法之受驗證端，若要達到相互認證的程度，則勢必大於 2 個往返次數，若認證通過後，真正要交換金鑰時，也至少需 2 個往返次數才能彼此收到對方的訊息，才能彼此獲得相同的會議金鑰。

總的來說，每台車輛經過一 RSU 時，至少需處理 4 個往返次數的處理時間才能達到驗證與取得金鑰，因此在車載網路中，當每台車輛 V_i 經過一 R_j 後，下一分鐘又經過另一 RSU R_{j+1}，最後在此車輛行駛的期間中經歷過 m 個 R_m，當 m 很大時，這必定造成極大的處理時間。

表 2 訊息往返次數比較計算時間分析

RSU	傳統方式	本論文架構	改善率
m 個	4m	2+2m	4m-(2+2m)/(4m) =(m-1)/2m
2 個	8	6	(8-6)/8=25%
3 個	12	8	33%
50 個	200	102	49%

本論文所提之金鑰分配方式在(2.5)RSU 彼此金鑰交換與同步與(2.6)鄰近金鑰請求中將可減少訊息傳遞次數，表 2 是比較當車輛經過不同數量的 RSU 時，所需花的訊息往返次數，當車輛經過 2 個 RSU 時，從傳統方式來看，需花費 8 個往返次數，本論文架構只需花費 6 個往返次數，其改善率可達 25%，也可說在此論文的 VANET 環境下至少可達減少 25%的訊息往返次數；當車輛經過 3 個 RSU 時，從傳統方式來看，需花費 12 個往返次數，本論文架構只需花費 8 個往返次數，此時的改善率可達 33%；當車輛經過 50 個 RSU 時，從傳統方式來看，需花費 200 個往返次數，本論文架構只需花費 102 個往返次數，這時地的改善率幾乎可達到一半的效率；依此類推，當車輛經過 m 個 RSU 時，從傳統方式需花費 4m 個往返次數，本論文架構只需花費 2+2m 個往返次數，由此推論，車輛經過 RSU 愈多，本論文架構將更有效率。

3.2 時間效能分析

表 3 預期時間成本 (RSU 數 j=10)

步驟	運算成本	花費時間
系統設定階段	不討論	不影響
註冊階段	不討論	不影響
廣播驗證階段	$2T_H+T_X+T_E$ ≈ 60 T_S+2T_H	0.523 秒
會議金鑰協定	$T_S+2T_E+2T_H$ ≈ 121 T_S+2T_H	1.0537 秒
RSU 彼此金鑰交換與同步	不討論	不影響
鄰近金鑰請求	T_X	≈ 0
匿名識別碼請求	不討論	不影響
鄰近 RSU 推播訊息傳遞	jT_S ≈ 10 T_S	0.087 秒
本地推播訊息傳遞	T_S	0.0087 秒
T_S:執行一個對稱式加解密運算所需花費的時間 T_A:執行一個非對稱式加解密運算所需花費的時間 T_E:執行一個指數運算所需花費的時間 T_H:執行一個雜奏函數運算所需花費的時間 T_X:執行一個互次或運算所需花費的時間		

本論文對於計算時間的複雜度的計算將以對稱式加解密為基礎來分析，已知執行一個對稱式加解密需花費 0.0087 秒時間與執行一個雜奏函數運算需花費 0.0005 秒時間，故所有計算方式的時間複雜度都將轉換成對稱式加解密的時間複雜度，根據[6]說明，執行一個對稱式加解密系統至少快 100 倍的非對稱式加解密系統，也就是說執行 DES 加解密系統至少快 100 倍的 RSA 或 PKI 加解密系統，執行一個指數運算所需的時間幾乎等於執行

60 次對稱式加解密運算，此外互次或的運算時間非常快，故本論文將忽略此種計算的時間複雜度，如表 3 說明當 RSU 數為 10 台時所花費之時間成本。

3.3 安全性分析

本章節將針對在推播訊息服務在安全上進行分析，以確保前推安全、後推安全、金鑰保護上、驗證、授權、避免重送攻擊與女巫攻擊。

- 前推安全(Forward secrecy)：此安全上的保證是指任何一台車輛在未進入 R_j 的通訊範圍內前，將不可以獲取相關的推播訊息服務。在推播訊息服務中任何未進入 R_j 的 V_d 將無法獲得來自 R_j 所傳遞的$\{R_{IDj}, e_j, P_{xj}, Q_{new}, m_j\}$，也無法解開 $D_{ri}(m_j)$與計算出 $W_i=\alpha^{Qnew}$。因此將 V_d 將不可能自行產生會議金鑰 $K_j=\alpha^{QnewN}$。
- 後推安全(Backward secrecy)：此安全上的保證是指任何一台車輛在離開 R_j 的通訊範圍內後，將不可以再獲取相關的推播訊息服務。在推播訊息服務中任何一台車輛在離開R_j的 V_d將無法再獲得會議金鑰 K_j，因為此時將重新計算 $Q'=(\Pi r_i)/r_{old}$。
- 金鑰保護(Key Protection)：此安全上的保證是保證金鑰是安全的，不會被竊取。在推播訊息服務中使用 $Q=\Pi r_i$ 來了解當下在 R_j 下的 V_i 有哪些成員，並用 r_i 當作對稱式加密金鑰將 Q 與 N 加密成 $m_j=E_{ri}(Q, N)$，且會議金將使用 Diffie & Hellman[2]的方式來產生，只有合法已註冊的 V_i 才能得到 r_i，並解開 $E_{ri}(Q, N)$，最後才能計算出會議金鑰 $K_j=Z_j^Q=W_i^N=\alpha^{QN}$。
- 驗證(Authentication)：此安全上的保證是所有的個體 V_i 與 R_j 獲取任何服務皆需要被驗證過。在推播訊息服務中是採用雙線性配對函數來完成驗證動作，不但 V_i 對 CP 需註冊與 R_j 對 CP 也需註冊，以確保 R_j 的合法性。
- 授權(Authorization)：此安全上的保證是所有的個體 V_i 與 R_j 皆需要被授權。在推播訊息服務中任何未經授權 V_i 將無法驗證以下等式。

$$
\begin{aligned}
&e(y_iP_{xj}, (e_j \oplus H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj}))P)\\
&=e(y_i x_jP, (e_j \oplus H_2(H_1(VID_i, y_iP, P_{pub}, T_i), P_{xj}))P)\\
&=e(y_i x_jP, (e_j \oplus H_2(V_{IDi}, P_{xj}))P)\\
&=e(y_i x_jP, (e_j \oplus r_i)P)\\
&=e(y_i x_jP, R_{IDj}P)\\
&=e(y_i P, R_{IDj} x_jP)\\
&=e(P_{yi}, P_{xj})^{R_{IDj}}
\end{aligned}
$$

- 重送攻擊(Replay attack)：此安全上的保證任何之惡意竊聽者無法在網路上取得之相同資訊後，重新傳送後並獲得驗證通過。在推播訊息服務中在廣播驗證階段使用一個 Nonce 值，並驗證其合法性，只有接收者驗證來自發送者的 Nonce 值重未被使用過的才是合法發送者。
- 女巫攻擊(Sybil attack)：是一種攻擊者透過大量匿名實體增加不成比例的巨大影響，來破壞其網路的信任系統。在推播訊息服務中在匿名處理在註冊時皆已完成，所有 V_i 與 R_j 皆須匿名，V_i 匿名帳號為 $V_{IDi}=H_1(VID_i, P_{yi}, sP, T_i)$，$R_j$ 匿名帳號為 $R_{IDj}=H_1(RID_j, P_{xj}, s)$。

4. 結論與未來研究重點

本論文透過有效的金鑰分配方式實現遠距離與安全之推播訊息傳遞，主要解決問題有:(1)即使距離事故發生幾十公里遠的車輛，將可快速得知遠距離事故發生狀況與道路路況，並提供駕駛人相關建議與行駛路徑，以改善交通流量，提供更好的交通品質；(2)提供快速與安全的推播訊息服務，避免推播訊息被惡意竄改，造成有心人士利用此推播訊息獲取相關的道路或交通資源，只有被授權的車輛才能被驗證獲取相關的推播訊息服務；(3)滿足車輛的隱私性與相關的資訊安全需求並滿足前推安全、後推安全與避免重送攻擊與女巫攻擊等威脅；(4)在效能上，預期減少 25%以上的訊息傳遞次數，當車輛經過愈多的路側單元，幾乎可以減少一半以上的訊息傳遞次數。未來研究重點將放在實際模擬的環境上，並比較其他傳統傳遞訊息的方式的，藉以證明此研究的安全性與效能。

參考文獻

[1] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in *Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006, pp. 1-25.

[2] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on,* vol. 22, pp. 644-654, 1976.

[3] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS," *NEC network laboratories,* 2006.

[4] J. T. Isaac, J. S. Camara, S. Zeadally, and J. T. Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," *Computer Communications,* vol. 31, pp. 2478-2484, 2008.

[5] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security,* vol. 15, pp. 39-68, 2007.

[6] B. Schneier and P. Sutherland, *Applied cryptography: protocols, algorithms, and source code in C*: John Wiley & Sons, Inc., 1995.

[7] N. W. Wang, Y. M. Huang, and W. M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer Communications,* vol. 31, pp. 2827-2837, 2008.

[8] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," *Intelligent Transportation Systems, IEEE Transactions on,* vol. 6, pp. 90-101, 2005.

[9] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *ITS Telecommunications Proceedings, 2006 6th International Conference on*, 2006, pp. 761-766.

[10] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *Vehicular Technology, IEEE Transactions on,* vol. 57, pp. 3357-3368, 2008.