附件一

行政院國家科學委員會補助專題研究計畫 □成果報告 ■期中進度報告

異質網路環境之行動搜尋關鍵技術-子計畫一:

車用隨意網路存取控制與連結機制之研究(1/3)

計畫類別：□ 個別型計畫　　■ 整合型計畫
計畫編號：97-2221-E-009-049-MY3
執行期間：　97 年 08 月 01 日至 100 年 07 月 31 日

計畫主持人：簡榮宏 教授
共同主持人：
計畫參與人員： 鄭安凱、黃文彬、黃志賢、曾宇田、陶嘉瑋

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、
列管計畫及下列情形者外，得立即公開查詢
■涉及專利或其他智慧財產權，□一年■二年後可公開查詢

執行單位：國立交通大學資訊工程學系(所)

中　華　民　國　98　年　5　月　31　日

中文摘要：

本子計畫為期三年，主要研究目標在於發展VANET 網路之存取控制協定(Media Access Control, MAC)及連結機制(Connectivity Support)。

根據統計，每年超過數千萬的交通事故是因為車輛撞擊所引起的。而導致車輛撞擊的因素因有許多，而駕駛者的行為(driver behavior) 是最重要的因素。在行車過程當中，駕駛者若無法對緊急發生的事故即時作出煞車反應，則經常會造成一連串的車輛撞擊 (chain car collision)。 VANET 網路的建構可大幅改善這樣的問題。當緊急事故發生時，前方車輛可將些事故的訊息，直接透過無線媒介的傳遞給後方的車輛，以避免中間車因為視線上阻隔的所帶來的延遲。此訊息可再藉由車輛上無線裝置的轉送(message relaying)，快速的傳遞給更後面的車輛，因此可以免除掉駕使者本身所需反應時間，此系統稱作聯合碰撞避免(cooperative collision avoidance, 簡稱 CCA)。然而，當過多的訊息於無線媒介中傳送時，則會有嚴重干擾的關題(interference)，進而導致較大的傳輸延遲 (delivery delay)，這將直接威脅到駕駛人的安全。另一方面，由於車載隨意網路之網路範圍、車輛行進速度、車輛之相關地理位置，及其車輛之間連接的分散性，使得車用隨意網路通訊的安全問題隨之而生，特別是在車用隨意網路中，當行進車輛間有突發的緊急事件發生時，要如何快速以及有效地驗證此一緊急事件，是個值得探討的議題。

有鑑於此，本子計畫第一年的研究目地有二: (1) 針對 CCA 系統提出一個有效的訊息廣播機制(broadcast mechanism)。此機制主要是透過功率控制 (power control) 來減少實體層中(physical layer) 訊息互相干擾的問題，而功率的調整則是根據車輛之間所需的安全距離(safe distance) 來加以設計。(2) 提出一個安全的聚集訊息驗證機制(secure aggregated message authentication scheme，簡稱 SAMA)。此機制是基於免憑證公開金鑰密碼系統(certificateless public key cryptography，簡稱 CL-PKC)，用以驗證車用隨意網路之突發緊急事件。經由效能的評估，此機制可有效地降低聚集訊息驗證所需之計算量。並驗證此一方法可有效地抵禦偽造攻擊(forgery attacks)，同時提供車輛之隱私保護(privacy protection)。

關鍵詞： 車用隨意無線網路、聯合車輛碰撞避免、功率控制、安全訊息驗證

英文摘要：

The goal of subproject 1 is to provide the medium access control mechanism and connectivity support for vehicle ad-hoc networks.

In each year, over million of traffic accidents occur due to automobile crashes. While different factor contribute to vehicle crashes, driver behavior is considered to be the leading cause. The inability of drivers to react in time to emergency situation often creates a potential fro chain collision. These events can be potentially avoided by the cooperative collision avoidance system under vehicle ad-hoc network. However, as long as many emergency messages are transmitted on the air, the interference problem will become very serious, leading to a longer delivery delay. On the other hand, security issues of VANETs are very challenging, especially on how to ensure the authenticity of emergency messages efficiently.

In the first year, we have proposed an efficient broadcast mechanism for the CCA system using power control technique. The main idea for power control is based on the safe distance between vehicles. Simulation results show that our protocol can efficiently reduce the delivery delay and confine the broadcast area. For the security issue, we have proposed a secure aggregated message authentication (SAMA) scheme in certificateless public key settings to validate emergency messages for VANETs. We make use of aggregation and batch verification techniques for emergency message verification to reduce the computation overhead. Moreover, the SAMA scheme is modelled and analyzed with Petri nets. Our analysis shows that the SAMA scheme can successfully defend forgery attacks and preserve the privacy of vehicles.

Keywords: Vehicle Ad-Hoc Network, Cooperative Collision Avoidance, Power Control, Secure Message Authentication.

一、 前言

隨著無線通訊網路技術的進步，加上電子元件價格漸漸下降以及行車安全問題越來越受重視，各國政府紛紛投入智慧型運輸系統(Intelligent Transport Systems, ITS)的研究[1-7]。ITS 為應用先進的電子、通信、資訊與感測等技術，以整合人、路、車的管理策略，其主要的目地為提供即時(real-time)的資訊，並增進運輸系統的安全、效率及舒適性，同時也減少交通對環境的衝擊。

車用隨意網路(Vehicle Ad-hoc Network, VANET)，為當前了為實現 ITS 所發展出重要網路架構[8]。在個架構下，每一個搭載無線通訊設備的車輛，都可以透過路旁的路側系統(Road Side Unit, RSU) 連線到 Server 端索取所需的資訊。而當車輛距離基地台太遠超出傳訊範圍時，也可透過其它的車輛幫忙轉送。換句話說，每一個車輛都可視為是一部行動無線路由器(mobile wireless router)。因此，這樣的架構可大幅提升網路建置彈性，只要有車輛的地方，即可是 VANET 的涵蓋範圍。

針對車輛安全部分，根據統計，每年超過數千萬的交通事故是因為車輛撞擊所引起的[9]。而導致車輛撞擊的因素因有許多，諸如車輛機械問題、天候狀況、行車時段等。其中，駕駛者的行為(driver behavior) 是最重要的因素。在行車過程當中，駕駛者若無法對緊急發生的事故（如落石、緊急煞車、車輛打滑) 即時作出煞車反應，則經常會造成一連串的車輛撞擊 (chain car collision)，也就是俗稱的連環車禍。

細究其原因，當一連串的車輛於道路上行駛時，每輛車都必需對前方可能發生的事故，作出即時的反應。然而，受限於視線上的阻隔，駕駛者通常必需視前方車輛的後車燈 (tall brake light) 閃爍與否，來能決自己是否也要作出煞車的反應。也就說，後方駕駛者可能在前方事故發生後一段時間才能作出反應。此時，若是有車輛沒有與前方車輛保持足夠的距離，則有可能發生追撞的事件。另一方面，在察覺到前方事故之後，駕駛人本身也需要一段額外的時間 (driver reaction time) 來對此訊息作出煞車的回應，這段反應時間通常介於 0.75 至 1.5 秒之間[10]。也就是說，在車速 70mph 下，車輛還必需滑行 75 至 150 英尺後，駕駛者才會開始踩下煞車。因此，如何減少事故發生以至煞車回應所需的這段時間，成為避免車輛事故的關鍵議題。

VANET 網路的建構可大幅改善這樣的問題。當緊急事故發生時，前方車輛可將些事故的訊息，直接透過無線媒介的傳遞給後方的車輛，以避免中間車因為視線上阻隔的所帶來的延遲。此訊息可再藉由車輛上無線裝置的轉送(message relaying)，快速的傳遞給更後面的車輛，因此可以免除掉駕使者本身所需反應時間。這樣的系統稱作聯合碰撞避免(cooperative collision avoidance, 簡稱 CCA) [10-14]。然而，當過多的訊息於無線媒介中傳送時，則會有嚴重干擾的關題(interference)，進而導致較大的傳輸延遲 (delivery delay)，這將直接威脅到駕駛人的安全。

因此，本計畫的主要目的之一，為針對 CCA 系統提出一個有效的訊息廣播機制(broadcast mechanism)。此機制主要是透過功率控制 (power control) 來減少實體層中(physical layer) 訊息互相干擾的問題，而功率的調整則是根據車輛之間所需的安全距離(safe distance) 來加以設計。考慮到 VANET 網路高度的變動性與有限的頻寬，我們所設計的機制完全不需要任何拓撲的資訊與週期性資料的交換。

另一方面，由於車載隨意網路之網路範圍、車輛行進速度、車輛之相關地理位置，及其車輛之間連接的分散性，使得車用隨意網路通訊的安全問題隨之而生，特別是在車用隨意網路中，當行進車輛間有突發的緊急事件發生時，要如何快速以及有效地驗證此一緊急事件，是個值得探討的議題。

有鑑於此，本子計畫的另一個目的，為提出一個安全的聚集訊息驗證機制(secure aggregated message authentication scheme，簡稱 SAMA)。此機制是基於免憑證公開金鑰密碼系統(certificateless public key cryptography，簡稱 CL-PKC)，用以驗證車用隨意網路之突發緊急事件。經由效能的評估，此機制可有效地降低聚集訊息驗證所需之計算量。此外，我們利用 Petri nets 分析提出之機制，並驗證此一方法可有效地抵禦偽造攻擊(forgery attacks)，同時提供車輛之隱私保護(privacy protection)。

二、 研究目的

本計畫為總計畫「異質網路環境之行動搜尋關鍵技術」之第一子計畫，主要的目的為提供車用隨意網路之存取控制與連結機制。為了達成這個目標，在第一年的研究中，我們針對此網路中重要的安全應用(safety applications)，進行兩項主要的研究 (1)車用隨意網路安全訊息廣播機制; (2) 車用隨意網路安全訊息驗證機制。以下分別述之:

1. 車用隨意網路安全訊息廣播機制

當車輛超出傳輸範圍時，安全訊息可透過車輛之間的無線裝制來進行轉送，因此必需有適當的轉送機制。然而，傳統的隨意行動網路(Mobile Ad Hoc Network, MANET) routing，確不完全適用於 VANET 的安全應用下，主要原因要二: (1) 傳統的 MANET routing 封包中，必需指定明確的目地端，但是在 VANET 中的安全訊息經常是沒有固定的對向; (2) MANET routing 在真正傳送資料封包前，需要一個 route discovery 的階段來建立適當的路徑，而這個階段需要額外的時間與頻寬，對於低延遲需求要高的安全應用是不允許的。

因此，安全訊息的傳送必需以廣播導向(broadcast oriented)的方式來設計。然而透過無線媒介進行廣播，經常會造成嚴重的干擾，甚至導致廣播風暴的現像(broadcast storming)，所以在設計上必需利用額外的資訊來降低這樣的問題。常用的方法是透過車輛上的衛星定位裝置(global positioning system, GPS) 所取得的地理資訊來限制轉送的區域。如文獻[10][12]，在每一個安全訊息中夾帶傳送車輛的位置資訊，收端可依據和送端的距離決定傳送的優先順序，以避免同時轉送所帶來的干擾。而文獻[11][12]則是用送端相對收端的方向，來決定是否要進行傳送。文獻[14]更進一步利用地理資訊，估算出可能的威脅程度，使處在較高危險區域的車輛優先轉送。

雖然現有的方法已利用地理資訊來減少過多轉送帶來的干擾，但是由於傳送功率是固定的，因此每一次傳送所造成的干擾範圍仍是無法降低。有鑑於此，在提出的方法中，我們利用功率控制的方式來真正降低干擾範圍。在此同時，我們利用地理資訊所估算的安全距離限止最低的功率，以確保所有潛在受到威脅的車輛都能收到安全訊息。此外，考慮到 VANET 網路高度的變動性與有限的頻寬，我們所提備的機制完全不需要任何拓撲的資訊與週期性資料的交換。

2. 車用隨意網路安全訊息驗證機制

在安全訊息驗證方面，Raya 與 Hubaux [15]針對車用隨意網路的安全問題，於 2005 年提出系統性解決方法。隨後，許多用以增進安全、效率，與功能性之相關研究因應而生[16-27]。在 2008 年，Zhu [27]等人針對行車突發緊急事件的驗證程序，提出一個聚集訊息驗證機制。此機制植基於憑證公開金鑰密碼系統(certificate public key cryptography)，故此機制之聚集驗證包括憑證驗證與簽章驗證兩部份。

為了有效地簡化傳統公開金鑰密碼系統所需之憑證管理，Shamir [28]於 1984 年提出以身份為基礎之公開金鑰密碼系統(ID-based public key cryptography，簡稱 ID-PKC)。此密碼系統中，使用者的公鑰是由使用者的身份識別碼(identity)推導產生。此系統存在一公正第三者(trusted third party，簡稱 TTP)，亦即私鑰產生者(private key generator，簡稱 PKG)，用以協助使用者產生其私鑰。故 ID-PKC 可能會衍生金鑰托管(key escrow)的問題。

Al-Riyami 與 Paterson [29]為解決 ID-PKC 的金鑰托管問題，提出免憑證公開金鑰密碼系統(certificateless public key cryptography，簡稱 CL-PKC)的概念，在 CL-PKC 中，存在一公正第三者，亦即金鑰產生中心(key generation center，簡稱 KGC)，協助使用者產生部份使

用者私鑰。使用者隨後自行產生一秘密資訊，再與部份使用者私鑰結合，產生完整者的使用者私鑰。因此，KGC 無法得知使用者的完整私鑰，即能有效解決 ID-PKC 之金鑰托管問題，亦同時能降低憑證的使用率。

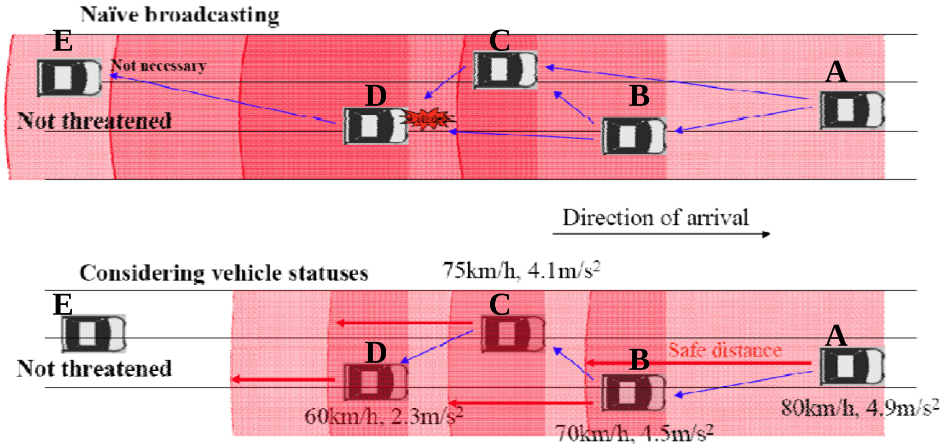
因此，我們提出一個安全的聚集訊息驗證機制，用以驗證車用隨意網路之突發緊急事件。此機制乃植基於 CL-PKC，並採用改進之 Zhang 與 Zhang 所提出的免憑證聚集簽證機制[30]，因此驗證聚集訊息只需要驗證聚集簽章的部份。經由效能的評估，此機制可有效地降低驗證所需之計算量。此外，我們利用 Petri nets [31]分析所提出之機制，並驗證此一方法可有效地抵禦偽造攻擊，同時提供車輛之隱私保護。

三、 研究方法

以下針對本子計畫第一年的研究成果，分成兩部分進行說明。

1. 車用隨意網路安全訊息廣播機制

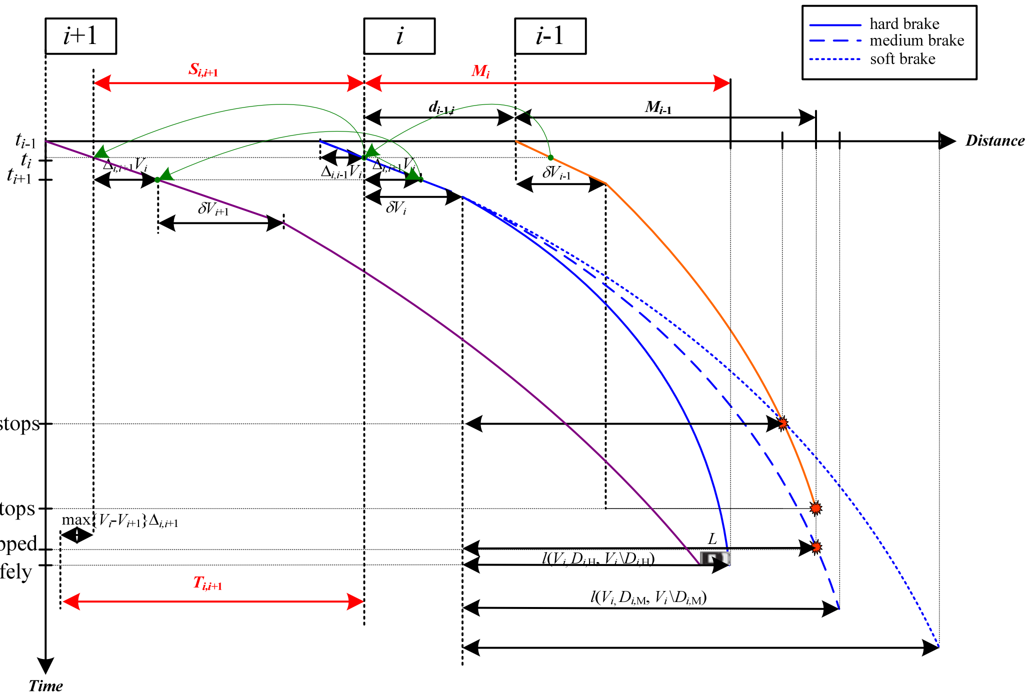
此廣播機制的主要概念，是利用功率控制(power control)的方式，來達到減少實體層干擾(physical interference)，以及限制廣播區域(broadcasting area)的效果。而傳送功率的調整是根據車輛與車輛之間的安全距離 (safe distance)。如圖一所示，在沒有功率控制的情況下(上圖)，每台車輛都必需以最大的功率進行傳輸，因此中間兩台車輛 (車輛 B C)將會收到前方車輛(車輛 A)所廣播的安全訊息，而這兩台車輛又必需將此訊息轉送給後方車輛，使得至後方車輛(車輛 D)同時收來相同的訊息，而導致干擾的發生。相較之下，我們的方法只將訊息傳送給少於安全距離內的車輛，較不會有多台車輛同時進行送或收的問題，因此可減少干擾的發生。這同時也能避免不受威脅的車輛收到此訊息的情況，如下圖，最左邊的車輛(車輛 E)已和前面的車陣保持足夠的距離，因此在我們的機制下將不會收到冗餘的訊息。



圖一、訊息廣播使用功率控與未使用功率控制之比較

接下來，我們利用下面的例子介紹安全距離在 VANET 網路下該如何估算。在圖二中，有三輛車(i+1, i, i-1)由左至右的行駛，車輛 i-1 是第一個察覺事故的車輛，而車輛 i 必需將此訊息轉將給車輛 i-1，我們將估算車輛 i-1 與車輛 i 之間的安全距離。當車輛 i-1 的駕駛者察覺事故後，需要一段反應時間 δ(driver reaction time)才會踩下煞車，因此在車速為 $V_{\text{i-1}}$ 的情況下，車輛 i-1 會滑行$\delta V_{\text{i-1}}$ 的距離後才開始減速，直到滑行了 $\delta V_i + \frac{V_i^2}{2D_i}$ 距離後才會真正的停止下來。另一方面，由於訊息傳送本身也會有延遲時間$\Delta_{\text{i,i-1}}$，因此在車速為 V_i 的情況下，車輛 i 的駕使人會在滑行了$\Delta_{\text{i,i-1}}V_i$ 距離後才發覺此訊息，相同的這位駕使者也會在滑行了$\delta V_{\text{i-1}}$ 的距離後才開始減速。此時，依據車輛的行速度 V_i、煞車力道 D_i，以及車輛間的距離 $d_{i\text{-}1,i}$，車輛 i 與車輛 i-1 之間會有三種可的情況: (1) 車輛 i 與車輛 i-1 都安全的停下，沒有發生任何碰撞; (2)車輛 i 撞擊到已停止下來的車輛 i-1; (3) 車輛 i 撞擊到行徑間的車輛 i-1。這三種情況將導使得車輛 i 在完全停止下來之前，產生不同的滑行距離 M_i，詳細的計算公式如下所示:

$$M_i = \min\left\{\begin{array}{c} \delta V_i + \dfrac{V_i^2}{2D_i} \\ d_{i-1,i} + M_{i-1} - L, \\ \chi_{i-1,i} \end{array}\right\}.$$



圖二、車用隨意網路滑行距離、安全距離、及傳輸半徑之估算

接著，根據此滑行距離 M_i，以及後方車輛的煞車力道 D_{i+1}，行車速度 V_{i+1}，和所需求的息訊傳遞時間，我們能估算出在車輛移動下的所需保持的安全距離 $S_{i,i+1}$，

$$S_{i,i+1} = (\Delta_{i,i+1} + \delta)V_{i+1} + l(V_{i+1}, D_{i+1}, V_{i+1} / D_{i+1}) + L - M_i \,.$$

最後，根據此安全距離 $S_{i,i+1}$，以及收到訊息前的車距變動，我們能算出對車輛 i+1 所需要的最小傳輸半徑 $T_{i,i+1}$，

$$T_{i,i+1} = S_{i,i+1} + \Delta_{i,i+1} \max\{V_i - V_{i+1}, 0\} \,.$$

Fig. 2: Safe distance and Broadcast Range

然而後方車輛的資訊（如 V_{i+1}、D_{i+1}）經常是無法事先取得的，因些在實作上可以改下列的估算公式

- $\hat{S}_i = (\tau + \delta)V_{\max} + l(V_{\max}, D_r, V_{\max} / D_r) + L - M_i$;

- $\hat{T}_i = \hat{S}_i + \tau \max\{V_i - V_{\min}, 0\}$;

其中 $V_{\max}$ 及 $V_{\min}$ 分別是最大與最小可能的速度（如高速公路的行車上下限制）。

2. 車用隨意網路安全訊息驗證機制

本機制運作於車用隨意網路之車輛的車間通訊，並假設是在無固定路邊設備的協助下進行資料的傳遞。本機制存在一 KGC，用以建置系統初始參數的設定與協助車輛產生部份私鑰。此機制主要分為四個階段：系統設置、註冊、安全緊急報告(security emergency report，簡稱 SER)產生、SER 聚集驗證。

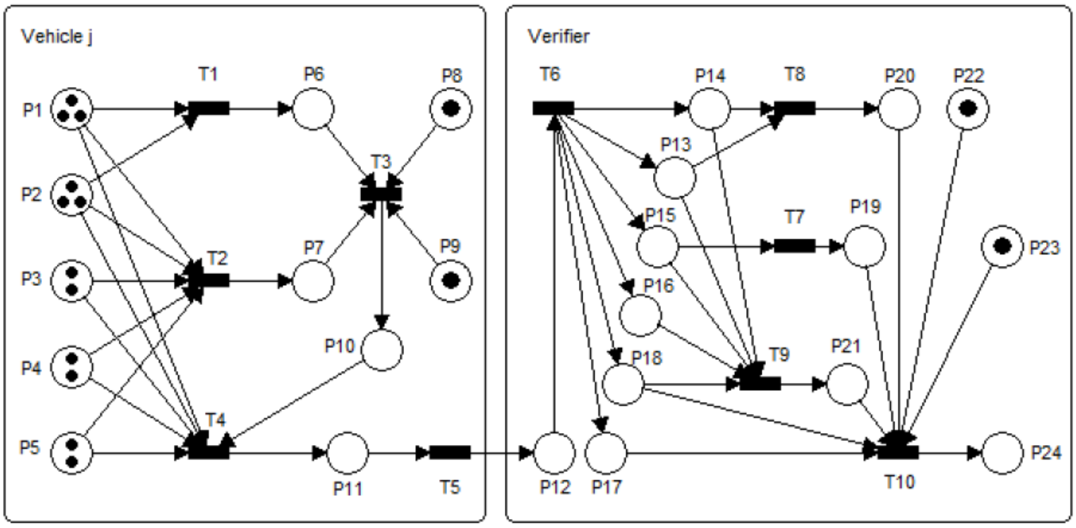
- 系統設置階段：KGC 產生與公開系統參數，以及定義 SER 格式。
- 註冊階段：車輛透過向 KGC 註冊，以取得部份私鑰，隨後自行選取一秘密資訊，與其部份私鑰結合，以產生完整的車輛私鑰，同時車輛亦自行計算其相對應之公鑰。
- SER 產生階段：車輛 j 針對緊急事件 i 所產生之 SER，如表一所示。

表一、SER 格式

類型 ($Type_i$)	地點 (Loc_i)	車輛識別碼 (ID_j)	時間 ($Time_j^i$)	簽章 (Sig_j^i)	車輛公鑰 (PK_j)

- SER 聚集驗證階段：任何車輛皆可針對所收到緊急事件 i 之 SER 進行批次驗證。

我們使用 Petri nets [31]分析所提出機制之資訊流，並可藉此驗證此機制可抵禦偽造攻擊，同時提供車輛之隱私保護，詳細說明可於附錄查詢。本機制之 Petri net 模型如圖三所示，其中的 place 與 transition 定義分別如表二與表三所示。



圖三、SAMA 機制之 Petri net 模型

表二、相關 Places 之定義

Place	定義	Place	定義
P_1	$Type_i$	P_{13}	$Type_i$
P_2	Loc_i	P_{14}	Loc_i
P_3	ID_j	P_{15}	ID_j
P_4	$Time_j^i$	P_{16}	$Time_j^i$
P_5	PK_j	P_{17}	Sig_j^i
P_6	W_i	P_{18}	PK_j
P_7	S_j	P_{19}	Q_j
P_8	D_j	P_{20}	W_i
P_9	x_j	P_{21}	S_j
P_{10}	Sig_j^i	P_{22}	P
P_{11}	SER_j^i	P_{23}	P_{pub}
P_{12}	SER_j^i	P_{24}	驗證成功資訊

表三、相關 Transitions 之定義

Transition	定義	Transition	定義
T_1	計算 W_i	T_6	分解 SER_j^i
T_2	計算 S_j	T_7	計算 Q_j
T_3	計算 Sig_j^i	T_8	計算 W_i
T_4	建構 SER_j^i	T_9	計算 S_j
T_5	傳送 SER_j^i	T_{10}	驗證 $e(Sig_j^i, P) \overset{?}{=} e(Q_j S_j, P_{pub}) e(W_i, PK_j)$

在效能評估方面，如表四所示，我們利用計算量作為效能評估的指標。如表五所示，當驗證 n 個 SERs 時，Zhu 等人所提之機制[27]需要 5 次群數對(bilinear pairings)的計算，以驗證聚集簽章與憑證；由於本機制採用免憑證公開金鑰密碼系統，故僅需要 3 次群數對的計算來驗證聚集簽章，故本機制可有效地降低聚集訊息驗證之計算量。

表四、效能評估參數定義

符號	**定義**
T_H	執行一次單向雜湊函數所需之時間
T_E	執行一次指數運算所需之時間
T_P	執行一次群數對運算所需之時間
T_M	執行一次橢圓曲線點乘積運算所需之時間
T_A	執行一次橢圓曲線點加法運算所需之時間

表五、聚集訊息驗證機制效能比較表

階段 方法	Zhu 等人提出之機制[13]	我們所提出之 SAMA 機制
註冊階段	$1T_H + 2T_E$	$1T_H + 2T_M$
SER 產生階段	$3T_H + 2T_E + 2T_M$	$2T_H + 2T_M + 1T_A$
單一 SER 驗證	$4T_H + 1T_E + 5T_P$	$3T_H + 3T_P + 1T_M$
SER 聚集	$2(n\text{-}1)T_M$	$(n\text{-}1)T_A$
SER 批次驗證	$(n+3)T_H + nT_E + 5T_P + 4(n\text{-}1)T_M$	$(2n+1)T_H + 3T_P + nT_M + 2(n\text{-}1)T_A$

四、 本子計畫第二年研究目標

在達成第一年的目標後，車用隨意網路已具備期本傳輸及驗證安全訊息的能力，接著我要朝第二年的目標——高速載具集化及功率指定之研發——來努力，進一步提升大規模車用隨意網路的傳輸能力。

叢集化是指在一擁有眾多節點的網路裡，根據網路管理者預先決定好，每個cluster所涵蓋範圍的大小、裡面所包含的成員數、或是節點間最大所能容忍的hop數來選出cluster。每個cluster 裡必須至少有一個管理者(cluster-head)來負責管理其cluster裡的每個成員。此行為稱為intra-cluster communication。Cluster-head除了管理自己cluster裡的成員，每個cluster-head之間也必須隨時保持聯繫，彼此交換訊息。此即為inter-cluster communication。叢集化的目的是為了將網路劃分成許多小型網路，使其成為階層式的架構。使用cluster 的方式來管理網路，除了可以大量減少flooding 的封包數量，更可以簡化原本非常複雜的網路拓撲問題。在MANET 網路上使用cluster 的觀念來管理網路已經有相當多學者研究。而要將其應用到VANET 網路上，由於VANET 網路的特性，每台車輛均受到行進方向以及行車速度上的限制，故必須做進一步的修改。

而關於功率指定部分，在VANET 網路裡，通訊設備可經由車輛的動力得到電力，因此一般在無線網裡能源有效的問題顯得較為次要。然而，過高的傳輸半行仍然會對網路的效能帶來負面的影響，因此這部分所提到的研究，主要集中在如何有效地分配VANET 上車輛通訊所需的功率。在VANET 網路裡，網路密度是多變的，在密度低的情況下，若是通訊所使用的功率太低，則會造成部分車輛被孤立，而無法與其它車輛的通訊，反之若在密度高的情況下，卻使用高的發射功率，將會造成多餘的功率浪費，還會使得訊息碰撞的機率增加。因此，如何配合網路密度來調整車輛的傳輸功率，使得在低密度之情況下能使用較高功率、較遠的傳輸半徑，在高密度時，轉換成較小功率，便是這部分的重點。

我們將利用第一年在安全訊息傳送的成果與經驗，來達成這兩個目標。

五、 計畫結果

本年度的計畫成果包括 1 篇已發表的會議論文(ICC 2009)，以及 2 篇完成的議論文，這兩篇論文將分別投稿至 PIMRC 2009 以及 ICPADS 2009，並培育了 4 位碩士和 1 位博士。

六、 參考文獻

[1]. Vehicle Safety Communications Consortium, http://www-nrd.nhtsa.dot.gov.

[2]. Dedicated Short Range Communications Project, http://www.leearmstrong.comIDSRC.

[3]. The Pre VENT Project, http://www.prevent-ip.org.

[4]. Car2Car Communication Consortium, http://www.car-to-car.org.

[5]. Internet ITS Consortium, http://www.internetits.org.

[6]. The NOW: Network on Wheels Project, http://twww.network-on-wheels.de.

[7]. ITS Taiwan, http://www.its-taiwan.org.tw.

[8]. National Center for Statistics and Analysis, "Traffic Safety Facts 2003", Report DOT HS 809 767 Nat'l. Highway Traffic Safety Admin., U.S. Dot, Washington, DC, 2004.

[9]. ASTM E22213-03, "Standard specification for telecommunication and information exchange between roadside and vehicle ytem – 5GHz band dedicated short range communications (DSRC) MAC and PHY specifications," *ATM International*, July, 2003.

[10]. X. Yang, J. Liu, F. Zhao, N.H. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning", In Proc. of 1st Annual International Conference on Mobile and Ubiquitous Systems, pp. 114-123, 2004.

[11]. [BT06] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety", *IEEE Communications Magazine*, Vol. 44, No. 1, pp. 535-547, 2006.

[12]. [WT-7] N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, and V. Saderar, "Broadcast storm mitigation techniques in vehicular ad hoc networks", *IEEE Wireless Communications*, Vol. 14, no. 6, pp. 84-94, 2007.

[13]. [BT06] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety", *IEEE Communications Magazine*, Vol. 44, No. 1, pp. 535-547, 2006.

[14]. [YB08] F. Yu, and S. Biwas, "Impacts of radio access protocols on cooperative vehicle collision avoidance in urban traffic intersections", *Journal of Communications*, 2008.

[15] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," In *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN 2005)*, Nov. 2005.

[16] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation in VANETs," In *Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks (VANETs*

2006), Sep. 2006, pp. 67-75.

[17] J. Nikodem and M. Nikodem, “Secure and scalable communication in vehicle ad hoc networks,” In *Proceedings of the International Conference on Computer Aided System Theory (EUROCAST 2007)*, Feb. 2007, pp. 1167-1174.

[18] M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, 2007, pp. 39-68.

[19] C. Zhang, R. Lu, P. H. Ho, and A. Chen, “A location privacy preserving authentication scheme in vehicular networks,” In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2008)*, Mar. 2008, pp. 2543-2548.

[20] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, “Security in vehicular ad hoc networks,” *IEEE Communications Magazine*, vol. 46, no. 4, Apr. 2008, pp. 88-95.

[21] C. Langley, R. Lucas, and H. Fu, “Key management in vehicular ad-hoc networks,” In *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT 2008)*, May 2008, pp. 223-226.

[22] N. W. Wang, Y. M. Huang, and W. M. Chen, “A novel secure communication scheme in vehicular ad hoc networks,” *Computer Communications*, vol. 31, no. 12, Jul. 2008, pp. 2827-2837.

[23] C. T. Li, M. S. Hwang, and Y. P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,” *Computer Communications*, vol. 31, no. 12, Jul. 2008, pp. 2803-2814.

[24] C. I. Fan, R. H. Hsu, and C. H. Tseng, “Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks,” In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, Sep. 2008.

[25] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening privacy protection in VANETs,” In *Proceedings of the IEEE International Conference on Wireless and Mobile Computing (WIMOB 2008)*, Oct. 2008, pp. 508-513.

[26] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, Nov. 2008, pp. 3357-3368.

[27] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, “AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks,” In *Proceedings of the IEEE International Conference on Communications (ICC 2008)*, May 2008, pp. 1436-1440.

[28] A. Shamir, “Identity based cryptosystems and signature schemes,” In *Proceedings of the Advances in Cryptology (Crypto 1984)*, 1984, pp. 47-53.

[29] S. Al-Riyami and K. Paterson, “Certificateless public key cryptography,” In *Proceedings of the ASIACRYPT*, 2003, pp. 452-473.

[30] L. Zhang and F. Zhang, “A new certificateless aggregate signature scheme,” *Computer Communications*, vol. 32, no. 6, Apr. 2009, pp. 1079-1085.

[31] C. A. Petri, “Kommunikation mit Automaten,” Ph. D. Thesis, University of Bonn, 1962.

七、附錄

IEEE International Conference on Communications (*ICC* 2009), 2009 June

A Chaotic Maps-based Key Agreement Protocol that Preserves User Anonymity

Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan 30010
{hueiru, rhjan, wuuyang}@cs.nctu.edu.tw

***Abstract*—A key agreement protocol is a protocol whereby two or more communicating parties can agree on a key or exchange information over an open communication network in such a way that both of them agree on the established session keys for use in subsequent communications. Recently, several key agreement protocols based on chaotic maps are proposed. These protocols require a verification table to verify the legitimacy of a user. Since this approach clearly incurs the risk of tampering and the cost of managing the table and suffers from the stolen-verifier attack, we propose a novel key agreement protocol based on chaotic maps to enhance the security. The proposed protocol not only achieves mutual authentication without verification tables, but also allows users to anonymously interact with the server. Moreover, security of the proposed protocol is modelled and analyzed with Petri nets. Our analysis shows that the proposed protocol can successfully defend replay attacks, forgery attacks, and stolen-verifier attacks.**

***Index Terms*—Key agreement protocol, Chaotic maps, Stolen-verifier attacks, Anonymity, Petri nets.**

I. Introduction

A key agreement protocol is a protocol whereby two or more communicating parties can agree on a key or exchange information over an open communication network in such a way that both of them agree on the established session keys for use in subsequent communications. In 1976, Diffie and Hellman invented the first key agreement protocol [1], in which two parties jointly exponentiate a generator with random numbers, in such a way that an eavesdropper has no way of guessing the key. However, their protocol does not provide authentication of the communicating parties, and is thus vulnerable to the man-in-the-middle attacks. Since then, a variety of secure key agreement protocols have been developed to prevent man-in-the-middle and related attacks.

Since the 1990s, chaotic systems [2-7] have been used to design secure communication protocols. Two main approaches to the use of chaotic systems in designing communication protocols are analog and discrete digital. The former is based on chaos synchronization using chaotic circuits, and the latter is designed for generating chaotic ciphers.

In 2003, Kocarev and Tasev [8] proposed a public-key encryption algorithm based on Chebyshev chaotic maps [9] as its semi-group properties meet the cryptographic requirements. However, Bergamo et al. [10] proved that Kocarev and Tasev's protocol [8] is insecure since an adversary can efficiently recover the plaintext from a given ciphertext. Later, in order to address Bergamo et al.'s attack [10], Xiao et al. proposed a novel key agreement protocol [11]. Recently, Han [12] pointed out that Xiao et al.'s protocol [11] is still insecure against their new attacks that can hinder the user and the server from establishing a session key even though the adversary cannot obtain any private information from the communicating parties. In 2008, Yoon and Yoo [13] proposed a new key agreement protocol based on chaotic maps that can resist Han et al.'s developed attacks [12] and off-line password guessing attacks, and can reduce the numbers of communication rounds.

However, these protocols [11, 13] still have several security weaknesses. In these protocols, the server needs a verification table. The verification table could be tampered or stolen and there is the cost of managing the table. In addition, users would wish to obtain services anonymously.

Taking the security threats and privacy issues into consideration, we propose a chaotic maps-based key agreement protocol that not only fixes these weaknesses, but also aims to preserve user anonymity. The crucial merits of the proposed protocol include: (1) it achieves mutual authentication between a server and a user; (2) it allows users to anonymously interact with the server to agree on session keys; (3) a server and a user can generate sessions keys for protecting the subsequent communications. Moreover, Petri nets [14] may be used to infer what an attacker could know if he happens to know certain items in the security protocol. We used Petri nets in the security analysis of the proposed protocol. Our analysis shows that the proposed protocol can successfully defend replay attacks, forgery attacks, and stolen-verifier attacks.

The rest of this paper is organized as follows: In Section 2, we state the definitions of Chebyshev chaotic map and introduce the hash function based on chaotic maps. Next, our proposed protocol is presented in Section 3. Then, we shall analyze our proposed protocol, show that our protocol can resist several attacks, and provide a comparative study with

This work was supported by the National Science Council, Taiwan, Republic of China, under grant NSC 97-2221-E-009-048-MY3 and NSC 97-2221-E-009-049-MY3.

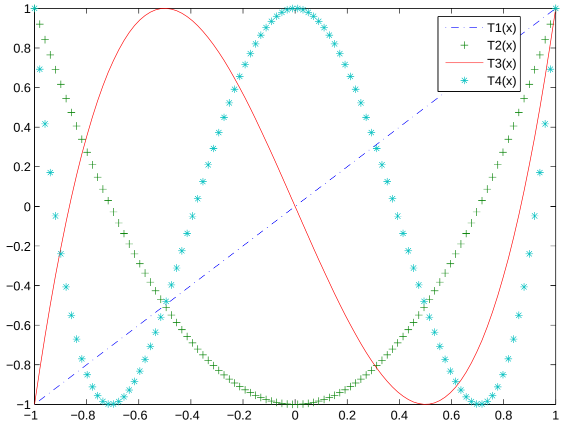


Fig. 1. Chebyshev polynomials

other key agreement protocols in Section 4. Finally, we will conclude our paper in Section 5.

II. Preliminaries

In this section, we define Chebyshev chaotic maps and introduce the hash functions based on chaotic maps.

A. Chebyshev Chaotic Maps

Chebyshev polynomial [9] and its properties [8, 11, 13] are described as follows.

Definition 1. *The Chebyshev polynomial $T_n(x)$ is a polynomial in x of degree n, defined by the following relation:*

$$T_n(x) = \cos n\theta, \text{ where } x = \cos\theta \ (-1 \le x \le 1) \qquad (1)$$

With Definition 1, the recurrence relation of $T_n(x)$ is defined as:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \text{for any } n \ge 2, \qquad (2)$$

together with the initial conditions $T_0(x) = 1, T_1(x) = x$.

Some examples of Chebyshev polynomials are shown as follows: (see Figure 1)

$$\begin{aligned} T_2(x) &= 2x^2 - 1 & (3)\\ T_3(x) &= 4x^3 - 3x & (4)\\ T_4(x) &= 8x^4 - 8x^2 + 1 & (5)\end{aligned}$$

Chebyshev polynomials have two important properties [8, 11, 13]: the semi-group property and the chaotic property.

- The semi-group property:

$$\begin{aligned} T_r(T_s(x)) &= \cos(r\cos^{-1}(\cos(s\cos^{-1}(x))))\\ &= \cos(rs\cos^{-1}(x))\\ &= T_{sr}(x)\\ &= T_s(T_r(x)) \qquad (6)\end{aligned}$$

- The chaotic property: If the degree $n > 1$, Chebyshev polynomial map: $T_n : [-1, 1] \to [-1, 1]$ of degree n is a chaotic map with its invariant density $f^*(x) = \frac{1}{\pi\sqrt{1-x^2}}$ for Lyapunov exponent $\lambda = \ln n > 0$.

B. Hash Functions based on Chaotic Maps

The hash function used in the previous key agreement protocols [11, 13] is based on the following chaotic one-way hash function [15]. A one-dimension piecewise linear chaotic system is defined as:

$$X(t+1) = F(X(t), P) \qquad (7)$$

where $F(u, P) =$

$$\begin{cases} u/P & \text{if } 0 \le u < P,\\ (u-P)/(0.5-P) & \text{if } P \le u < 0.5,\\ (1-u-P)/(0.5-P) & \text{if } 0.5 \le u < 1-P,\\ (1-u)/P & \text{if } 1-P \le u \le 1,\end{cases}$$

where $X \in [0, 1]$ and $P \in (0, 0.5)$. X_i is the chaining variable, where $0 \le i \le 3N$. X_0 is an initial value of the chaining variable and is chosen from $(0, 1)$.

Given a pending message M, H_0 is a constant which is chosen from $(0, 1)$. The 3-unit iterations—1st to N-th, $(N+1)$-th to $2N$-th, $(2N+1)$-th to $3N$-th—ensure that each bit of the final hash value will be related to all bits of the message. The following is a brief referring to how to generate the hash value:

- The pending message M is translated to the corresponding ASCII numbers, then by means of linear transform, these ASCII numbers are mapped into an array C whose length N is the number of characters in the message and whose elements are numbers in $[0, 1]$.
- The iteration process is as follows:
  1) 1st: $P_1 = (C_1 + H_0)/4 \in [0, 0.5), X_1 = F(X_0, P_1) \in [0, 1]$;
  2) 2nd to N-th: $P_i = (C_i + X_{i-1})/4 \in [0, 0.5), X_i = F(X_{i-1}, P_i) \in [0, 1]$;
  3) $(N+1)$-th: $P_{N+1} = (C_N + X_N)/4 \in [0, 0.5), X_{N+1} = F(X_N, P_{N+1}) \in [0, 1]$;
  4) $(N+2)$-th to $2N$-th: $P_i = (C_{2N-i+1} + X_{i-1})/4 \in [0, 0.5), X_i = F(X_{i-1}, P_i) \in [0, 1]$;
  5) $(2N+1)$-th: $P_{2N+1} = (C_1 + H_0)/4 \in [0, 0.5), X_{2N+1} = F(X_{2N}, P_{2N+1}) \in [0, 1]$;
  6) $(2N+2)$-th to $3N$-th: $P_i = (C_{i-2N} + X_{i-1})/4 \in [0, 0.5), X_i = F(X_{i-1}, P_i) \in [0, 1]$.
- Next, X_N, X_{2N}, X_{3N} are transformed to the corresponding binary format, and 40, 40, 48 bits after the decimal point are extracted, respectively, and are juxtaposed from left to right to form a 128-bit hash value.

For more details, the reader is referred to [15].

III. Proposed Key Agreement Protocol

In this section, we propose a chaotic maps-based key agreement protocol. The proposed protocol does not require a verification table while achieving both mutual authentication and session key agreement between a server and a user. We list the notations used in this paper in Table I.

Different from the previous key agreement protocols [11, 13] where the server and user i share the hash value $h_{PW} =$

TABLE I
NOTATIONS

Symbol	Definition
U_i	User i
ID_i	User i's identity
PW_i	User i's password
K_s	The server's private key
sn	The session number
$H(\cdot)$	A one-way hash function based on chaotic maps
$E(\cdot)$	A symmetric key encryption algorithm
$D(\cdot)$	A symmetric key decryption algorithm
SK_i	The session key constructed by the server and user i
$\oplus$	The exclusive-or (XOR) operation

$H(ID_i, PW_i)$, the server does not require any verification table in the proposed protocol. Before performing the key agreement protocol, the server first publishes system parameters including Chebyshev polynomials, $E(\cdot)$, $D(\cdot)$, and $H(\cdot)$. Suppose a new user U_i with the identity ID_i wants to communicate with a server for establishing session keys. U_i randomly chooses his password PW_i and sends the pair $(ID_i, H(PW_i))$ to the server in person or through an existing secure channel. Upon receiving the message, the server juxtaposes ID_i and $H(PW_i)$ from left to right as the pending message, and uses the one-way hash function $H(\cdot)$ to compute $H(ID_i, H(PW_i))$. Then the server computes Reg_i as follows:

$$Reg_i = H(ID_i, H(PW_i)) \oplus H(K_s) \tag{8}$$

where K_s is the server's private key.

After that, the server transmits Reg_i back to U_i over a secure channel. Note that U_i has to keep Reg_i secret.

The details of the proposed key agreement protocol are presented as follows.

1) $U_i \rightarrow Server : \{sn, R_i, C_1\}$
   U_i first chooses three random numbers r_i, r, and v, where $r_i \in [-1, 1]$ is the seed x of the Chebyshev polynomial of degree r and v is a nonce. Next, U_i computes the pair (R_i, K_i) as follows.

$$R_i = Reg_i \oplus H(v) \tag{9}$$

$$K_i = H(ID_i, H(PW_i)) \oplus H(v) \tag{10}$$

   Then U_i encrypts ID_i, r_i, and $T_r(x)$ with K_i:

$$C_1 = E_{K_i}(ID_i, r_i, T_r(x)) \tag{11}$$

   Finally, U_i transmits sn, R_i, and C_1 to the server, where sn is the session number.

2) $Server \rightarrow U_i : \{sn, ID_s, C_2, AU_s\}$
   Upon receiving the message, the server computes $K_i = R_i \oplus H(K_s)$, and extracts ID_i, r_i, and $T_r(x)$ from C_1 with K_i. The server first checks the validity of ID_i, and then chooses two random numbers s and r_t, where s is the degree of the Chebyshev polynomial and r_t is a nonce. Next, the server computes the pair (C_2, SK_i) as follows.

$$C_2 = E_{K_i}(ID_s, r_t, T_s(x)) \tag{12}$$

$$SK_i = T_s(T_r(x)) = T_{rs}(x) \tag{13}$$

   Finally, the server computes the authentication value AU_s and sends sn, ID_s, C_2, and AU_s back to U_i.

$$AU_s = H(ID_i, r_i, r_t, SK_i) \tag{14}$$

3) $U_i \rightarrow Server : \{sn, AU_i\}$
   After receiving the message, U_i extracts ID_s, r_t, and $T_s(x)$ from C_2 with K_i. Next, U_i computes the pair (SK_i, AU_s') as follows.

$$SK_i = T_r(T_s(x)) = T_{rs}(x) \tag{15}$$

$$AU_s' = H(ID_i, r_i, r_t, SK_i) \tag{16}$$

   Then U_i checks whether AU_s and AU_s' are equal. If so, the identity of the server is authenticated. Next, U_i computes AU_i as follows.

$$AU_i = H(ID_s, r_i, r_t, SK_i) \tag{17}$$

   Finally, U_i sends sn and AU_i back to the server.

4) After receiving sn and AU_i, the server computes AU_i' as follows.

$$AU_i' = H(ID_s, r_i, r_t, SK_i) \tag{18}$$

   Then the server checks whether AU_i and AU_i' are equal. If so, the identity of U_i is authenticated.

After mutual authentication and key agreement between U_i and the server, SK_i is used as a shared session key.

IV. Analysis of Our Scheme

In this section, we show that our protocol can resist several notorious attacks. In addition, we provide a comparative study with other key agreement protocols.

A. Security Analysis

We first use Petri nets [14] to model and analyze the proposed protocol. Next, security properties of our protocol will be specified.

1) Petri Net Model: We used a Petri net to model our security protocol. The formal definition of a Petri net [16] is listed in Table II. Petri nets are composed from graphical symbols designating places (shown as circles), transitions (shown as rectangles), and directed arcs (shown as arrows). The places denote (atomic and composite) data items. The transitions denote decryption or decomposition operations. Arcs run between places and transitions.

When a transition fires, a composite data item is decomposed or decrypted, resulting in one or more simpler data items. Since we assume an open network environment, all data items in the transmitted messages are assumed to be public, and are known to the attacker. There will be tokens in the places representing the data items in the transmitted messages initially. From this initial marking, we can infer what an attacker can know eventually. Furthermore, we can also experiment what an attacker can know if he knows additional data items from other sources. The Petri net model

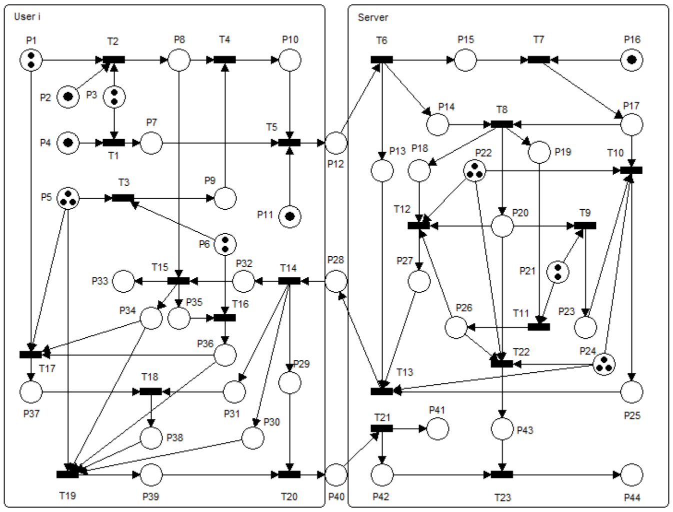


Fig. 2. A Petri net model of the proposed key agreement protocol

TABLE II
FORMAL DEFINITION OF A PETRI NET

A Petri net is a 5-tuple, $PN = (P, T, F, W, M_0)$ where:
$P = \{P_1, P_2, \cdots, P_m\}$ is a finite set of places,
$T = \{T_1, T_2, \cdots, T_n\}$ is a finite set of transitions,
$F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs (flow relation),
$W : F \rightarrow \{1, 2, 3, \cdots\}$ is a weight function,
$M_0 : P \rightarrow \{0, 1, 2, 3, \cdots\}$ is the initial marking,
$P \cap T = \emptyset$ and $P \cup T \neq \emptyset$.
A Petri net structure $N = (P, T, F, W)$ without any specific initial marking is denoted by N.
A Petri net with the given initial marking is denoted by (N, M_0).

is illustrated in Figure 2. The definitions of the places and transitions used in this model are listed in Table III and Table IV, respectively. The model is simulated with the HPSim Petri net simulation tool [17].

2) Security Properties: The security of the proposed protocol is based on the difficulty of the discrete logarithm problem (DLP) and the Diffie-Hellman problem (DHP), which are believed to be unsolvable in polynomial time. We first specify the mathematical difficult problems [13] used in this paper.

Definition 2. *The discrete logarithm problem (DLP) is defined as follows: given an element α, find the integer r such that $T_r(x) = \alpha$.*

Definition 3. *The Diffie-Hellman problem (DHP) is defined as follows: given $T_r(x)$ and $T_s(x)$, find $T_{rs}(x)$.*

Now we show that our protocol can resist replay attacks, forgery attacks, and stolen-verifier attacks, and also analyze the following security properties: mutual authentication, user anonymity, and known-key security.

Theorem 1. *The proposed protocol can resist a replay attack.*

Proof. Assume an adversary A eavesdrops the messages $\{sn, R_i, C_1\}$ and $\{sn, AU_i\}$ sent by U_i and replays them to log in to the system in a later session. Upon receiving the replay message, the server computes $K_i = R_i \oplus H(K_s)$, and extracts ID_i, r_i, and $T_r(x)$ from C_1 with K_i. The server first checks the validity of ID_i, and then chooses two random numbers s^* and r_t^*. Next, the server computes the pair (C_2^*, SK_i^*) as follows.

$$C_2^* = E_{K_i}(ID_s, r_t^*, T_{s^*}(x)) \qquad (19)$$

$$SK_i^* = T_{s^*}(T_r(x)) = T_{rs^*}(x) \qquad (20)$$

Finally, the server computes the authentication value AU_s^* and sends sn, ID_s, C_2^*, and AU_s^* back to A.

$$AU_s^* = H(ID_i, r_i, r_t^*, SK_i^*) \qquad (21)$$

After receiving the message, A has to transmit $\{sn, AU_i^*\}$ back to the server. However, A cannot just replay the message AU_i directly since the random number r_t and the session key SK_i embedded in AU_i are different from r_t^* and SK_i^* in this

TABLE III
DEFINITIONS OF PLACES

Place	Definition	Place	Definition
P_1	ID_i	P_{23}	$T_s(x)$
P_2	$H(PW_i)$	P_{24}	ID_s
P_3	$H(v)$	P_{25}	C_2
P_4	Reg_i	P_{26}	SK_i
P_5	r_i	P_{27}	AU_s
P_6	r	P_{28}	$Packet\{sn, ID_s, C_2, AU_s\}$
P_7	R_i	P_{29}	sn
P_8	K_i	P_{30}	ID_s
P_9	$T_r(x)$	P_{31}	AU_s
P_{10}	C_1	P_{32}	C_2
P_{11}	sn	P_{33}	ID_s
P_{12}	$Pakcet\{sn, R_i, C_1\}$	P_{34}	r_t
P_{13}	sn	P_{35}	$T_s(x)$
P_{14}	C_1	P_{36}	SK_i
P_{15}	R_i	P_{37}	AU_s'
P_{16}	$H(K_s)$	P_{38}	Success verification message
P_{17}	K_i	P_{39}	AU_i
P_{18}	ID_i	P_{40}	$Packet\{sn, AU_i\}$
P_{19}	$T_r(x)$	P_{41}	sn
P_{20}	r_i	P_{42}	AU_i
P_{21}	s	P_{43}	AU_i'
P_{22}	rt	P_{44}	Success verification message

TABLE IV
DEFINITIONS OF TRANSITIONS

Trans.	Definition	Trans.	Definition
T_1	Perform XOR operation to compute R_i	T_{13}	Transmit $\{sn, ID_s, C_2, AU_s\}$
T_2	Compute K_i	T_{14}	Split the packet
T_3	Compute $T_r(x)$	T_{15}	Decrypt C_2 with K_i
T_4	Encrypt $\{ID_i, r_i, T_r(x)\}$ with K_i	T_{16}	Compute SK_i
T_5	Transmit $\{sn, R_i, C_1\}$	T_{17}	Compute AU_s'
T_6	Split the packet	T_{18}	Check $AU_s \overset{?}{=} AU_s'$
T_7	Perform XOR operation to compute K_i	T_{19}	Compute AU_i
T_8	Decrypt C_1 with K_i	T_{20}	Transmit $\{sn, AU_i\}$
T_9	Compute $T_s(x)$	T_{21}	Split the packet
T_{10}	Encrypt $\{ID_s, r_t, T_s(x)\}$ with K_i	T_{22}	Compute AU_i'
T_{11}	Compute SK_i	T_{23}	Check $AU_i \overset{?}{=} AU_i'$
T_{12}	Compute AU_s		

session. As shown in Figure 2, computing AU_i is defined in transition T_{19}, which has five input places, P_5, P_{30}, P_{34}, P_{36}, and P_{38}. Place P_{34} is the value of r_t and place P_{36} is the value of SK_i. Because having no idea about r_t^* and SK_i^*, the adversary cannot launch a replay attack. □

Theorem 2. *The proposed protocol can resist a forgery attack.*

Proof. If an adversary A wants to impersonate U_i, A has to create a valid authentication value AU_i^*. Assume A eavesdrops the message $\{sn, R_i, C_1\}$ sent by U_i and uses it to log in to the system in a later session. Upon receiving the message, the server computes $K_i = R_i \oplus H(K_s)$, and extracts ID_i, r_i, and $T_r(x)$ from C_1 with K_i. The server first checks the validity of ID_i, and then chooses two random numbers s^* and r_t^*. Next, the server computes the pair (C_2^*, SK_i^*) as follows.

$$C_2^* = E_{K_i}(ID_s, r_t^*, T_{s^*}(x)) \tag{22}$$

$$SK_i^* = T_{s^*}(T_r(x)) = T_{rs^*}(x) \tag{23}$$

Finally, the server computes the authentication value AU_s^* and sends sn, ID_s, C_2^*, and AU_s^* back to A.

$$AU_s^* = H(ID_i, r_i, r_t^*, SK_i^*) \tag{24}$$

However, A cannot compute a correct authentication value $AU_i^* = H(ID_s, r_i, r_t^*, SK_i^*)$ unless A can obtain K_i to get ID_i, r_i, and $T_r(x)$ by decrypting C_1 and get ID_s, r_t^*, and $T_{s^*}(x)$ by decrypting C_2^*, and also derive r from $T_r(x)$ to compute SK_i^*. Based on the difficulty of DLP, it is computationally infeasible to compute r from $T_r(x)$. As shown in Figure 2, computing SK_i^* is defined in transition T_{16}, which has two input places, P_6 and P_{35}. Place P_6 is the value of r. Because having no idea about K_i and SK_i^*, the adversary cannot compute a valid authentication value and hence cannot launch a forgery attack. □

Theorem 3. *The proposed protocol can resist a stolen-verifier attack.*

Proof. The stolen-verifier attack means that an adversary who steals the password-verifier from the server can use it directly to masquerade as a legitimate user in an authentication run. Different from the previous key agreement protocols [11, 13] where the server and user i shared the hash value $h_{PW} = H(ID_i, PW_i)$, the server does not require any verification table in the proposed protocol. Since the proposed protocol does not require a verification table, the proposed protocol can prevent the stolen-verifier attack. □

Theorem 4. *The proposed protocol can provide mutual authentication.*

Proof. The security of the session key is based on the difficulty of DLP and DHP, which are believed to be unsolvable in polynomial time. Using equation (6), the session key between the server and U_i is established as follows:

$$SK_i = T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x)) \tag{25}$$

As shown in Figure 2, computing a session key SK_i is defined in transition T_{16} and transition T_{11}. Therefore, U_i and the server can use the session key SK_i in subsequent communications. □

TABLE V
COMPARISON OF SECURITY PROPERTIES

	Xiao et al.'s protocol [11]	**Yoon & Yoo's protocol [13]**	**Proposed protocol**
Replay attacks	Insecure	Secure	Secure
Forgery attacks	Insecure	Secure	Secure
Stolen-verifier attacks	Insecure	Insecure	Secure
Mutual authentication	Not provide	Provide	Provide
User anonymity	Not provide	Not provide	Provide
Known-key security	Provide	Provide	Provide

Theorem 5. *The proposed protocol can provide user anonymity.*

Proof. If an adversary A eavesdrops the messages, he cannot extract the user's identity from the ciphertext $C_1 = E_{K_i}(ID_i, r_i, T_r(x))$ since it is encrypted with K_i, which is unknown to the adversary. In addition, due to the use of the nonce, the messages submitted to the server are different in each session. As shown in Figure 2, decrypting C_1 is defined in transition T_8, which has two input places, P_{14} and P_{17}. Place P_{17} is the value of K_i, which is only known to the user and the server. Hence, it is difficult for the adversary to discover a user's identity. Clearly, the proposed protocol can provide user anonymity. □

Theorem 6. *The proposed protocol can provide known-key security.*

Proof. Known-key security means that the compromise of a session key will not lead to further compromise of other secret keys or session keys. Even if a session key SK_i is revealed to an adversary, he still cannot derive other session keys since they are generated from the random numbers r and s. Hence, the proposed protocol can achieve known-key security. □

We summarized the security properties of key agreement protocols in Table V.

B. *Efficiency Analysis*

In this section, we examine the performance of our proposed protocol. The evaluation parameters are defined in Table VI. The performance comparison among the proposed protocol, Xiao et al.'s protocol [11], and Yoon & Yoo's protocol [13] is presented in Table VII. We use the computational overhead as the metric to evaluate the performance of key agreement protocols. We can see from Table VII that the computations among these protocols are very similar. The only difference is that the proposed protocol takes few more XOR operations and hash operations for each user and the server, due to fixing the security weaknesses in Xiao et al.'s protocol [11] and Yoon and Yoo's protocol [13] and preserving user anonymity.

V. CONCLUSIONS

We propose a chaotic maps-based key agreement protocol that not only fixes the weaknesses of the existing chaotic maps-based key agreement protocols [11, 13], but also aims to preserve user anonymity. The crucial merits of the proposed

TABLE VI
EVALUATION PARAMETERS

Symbol	**Definition**
T_X	Time for performing an XOR operation
T_H	Time for performing a one-way hash function based on chaotic maps
T_E	Time for performing a symmetric encryption operation
T_D	Time for performing a symmetric decryption operation
T_{CM}	Time for performing a Chebyshev chaotic map operation

TABLE VII
PERFORMANCE COMPARISON OF CHAOTIC MAPS-BASED KEY AGREEMENT PROTOCOLS

	Xiao et al.'s protocol [11]	**Yoon & Yoo's protocol [13]**	**Proposed protocol**
Per user	$1T_H + 1T_E + 1T_D + 2T_{CM}$	$2T_H + 1T_E + 1T_D + 2T_{CM}$	$2T_X + 5T_H + 1T_E + 1T_D + 2T_{CM}$
The server	$1T_H + 1T_E + 1T_D + 2T_{CM}$	$2T_H + 1T_E + 1T_D + 2T_{CM}$	$1T_X + 3T_H + 1T_E + 1T_D + 2T_{CM}$

protocol include: (1) it achieves mutual authentication between a server and a user; (2) it allows users to anonymously interact with the server to agree on session keys; (3) a server and a user can generate sessions keys. Moreover, we used Petri nets in the security analysis of the proposed protocol. Our analysis shows that the proposed protocol can successfully defend replay attacks, forgery attacks, and stolen-verifier attacks.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, Nov. 1976, pp. 644-654.

[2] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, Dec. 2001, pp. 1498-1509.

[3] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, 2001, pp. 6-21.

[4] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, Feb. 1990, pp. 821-824.

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, Jun. 1998, pp. 1259-1284.

[6] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Physical Review A*, vol. 44, no. 4, Aug. 1991, pp. 2374-2383.

[7] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, Jun. 2002, pp. 238-242.

[8] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," In *Proceedings of the International Symposium on Circuits and Systems (ISCAS '03)*, vol. 3, May 2003, pp. III-28-III-31.

[9] J. C. Mason and D. C. Handscomb, *Chebyshev polynomials*, Chapman & Hall/CRC, Boca Raton, Florida, 2003.

[10] P. Bergamo, P. D'Arco, A. Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Transactions on Circuits and Systems-I*, vol. 52, no. 7, Jul. 2005, pp. 1382-1393.

[11] D. Xiao, X. Liao, and S. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177, no. 4, Feb. 2007, pp. 1136-1142.

[12] S. Han, "Security of a key agreement protocol based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 38, no. 3, Nov. 2008, pp. 764-768.

[13] E. J. Yoon and K. Y. Yoo, "A new key agreement protocol based on chaotic maps," In *Proceedings of The Second KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA '08)*, Mar. 2008, pp. 897-906.

[14] C. A. Petri, "Kommunikation mit Automaten," Ph. D. Thesis, University of Bonn, 1962.

[15] D. Xiao, X. Liao, and S. Deng, "One-way hash function construction based on chaotic map with changeable-parameter," *Chaos, Solitons & Fractals*, vol. 24, no. 1, Apr. 2005, pp. 65-71.

[16] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, Apr. 1989, pp. 541-580.

[17] HPSim 1.1 Petri nets simulation tool, copyright© 1999-2002 Henryk Anschuetz.