Appl. Math. Inf. Sci. 6 No. 2S pp. 463S-469S (2012)

Applied Mathematics & Information Sciences
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

Cryptanalysis of A PAACP: A Portable Privacy-Preserving Authentication and Access Control Protocol in Vehicular Ad Hoc Networks

Wei-Chen Wu[1,2] and Yi-Ming Chen[1]

[1] Department of Information Management, National Central University, Taoyuan County 32001,Taiwan, R.O.C.
[2] Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County 32544,Taiwan, R.O.C.
Corresponding author: Email: wwu@hsc.edu.tw

Received July 15, 2011; Revised Aug. 15, 2011; Accepted Sep. 2, 2011
Published online: 1 January 2012

Abstract: Vehicular ad hoc networks (VANETs) are emerging to improve road safety and traffic management. Privacy and security are very important in VANETs. Existing authentication protocols to secure VANETs raise challenges such as certificate distribution and reduction of the strong reliance on tamper-proof devices. Recently, Yeh et al. proposed a portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks (PAACP). However, PAACP in the authorization phase is breakable and cannot keep privacy in VANETs. In this paper, we present a cryptanalysis of an attachable blind signature and show that the PAACP's Authorized Credential (AC) is not secure and private even the AC secretly stored in a tamper-proof device. Our analysis showed that in PAACP, an eavesdropper can construct the AC from an intercepted blind document. As a result, PAACP in the authorization phase is breakable, and as any outsider can know who has which access privileges to access which service, the user's privacy in VANETs is jeopardized.

Keywords: VANET, Cryptanalysis, Authentication, Access Control.

1 Introduction

Vehicular ad hoc networks have recently been proposed as an effective tool for improving both road safety and the comfort experienced while driving. The immediate impacts include alleviating the vehicle-traffic congestion and improving operations management in support of public safety goals, such as collision avoidance. Equipping vehicles with various kinds of on-board sensors and instrumenting the vehicle-to-vehicle communication capability will allow large-scale sensing, decision, and control actions in support of these objectives. The allocation of 75 MHz in the 5.9 GHz band licensed for Dedicated Short Range Communication (DSRC) [1] by the U.S. National Intelligent Transportation Systems Architecture [2], which supports seven separate channels, may also enable the future delivery of rich multimedia contents to vehicles at short-to-medium range via either vehicle-to-vehicle or vehicle-to-roadside links in Vehicle Ad Hoc Networks (VANETs).

As VANETs are a special case of mobile ad hoc networks (MANETs) that aim to enhance the safety and the efficiency of road traffic it, there are a number of distinguishing features and limitations that are related to the very nature of wireless communications in VANETs and the rapid movement of the vehicles that are involved in those communications. Compared with wired or other wireless networks, VANETs are very dynamic, and their communications are volatile. In such networks, nodes are vehicles that are equipped with communication devices known as on-board units (OBUs), and depending on the applications, OBUs are used to establish communications with other vehicles or roadside units (RSUs) such as traffic lights or traffic signs.

In the recent years, several researches on VANETs have been investigated by academic or industries. The CAR 2 CAR Communication Consortium [3] is leading the efforts to create a European industry standard for vehicle-to-vehicle communication systems predicated upon wireless local area network components in Europe. In the U.S., the Intelligent Transportation Systems Committee, which is sponsored by the IEEE Vehicular Technology Society, has defined the standard for wireless access in vehicular environments [4]. Recently, some works addressed the security issues. As an instance of MANET, VANETs may suffer any malicious user's behaviors, such as bogus information and replay attacks on the disseminated messages. Among various security threats, privacy preservation in VANETs is one of the new challenges to protect users' private information, for example, Chen and Wei [5-6] proposed a safe distance based location privacy scheme, called SafeAnon. By simulating vehicular mobility in a cropped Manhattan map, they evaluated the performance of SafeAnon scheme under various conditions to show that their proposed scheme can simultaneously achieve location privacy as well as traffic safety. However, as Chen and Wei focused on the issues of vehicles' location privacy, little discussions were put on the initial authentication phase of communications among vehicles.

In 2005, Raya *et al*. [7] first proposed a solution to mention both security and privacy issues for safety-related applications, such as emergency warnings, lane changing assistance, intersection coordination, traffic-sign violation warnings, and road-condition warnings [8]. To shorten the processing delay, in Raya and Hubaux's communication scheme, safety messages will not contain any sensitive information. In 2008, Wang, *et al*. [9] reviewed Raya and Hubaux's communication scheme and argued that though Raya and Hubaux paid much attention to safety-related applications, non-safety-related applications, such as maps offering [10-11], advertisements, and entertainment information [12], were neglected. To address this issue, Wang *et al* proposed a secure communication scheme which can support the non-safety-related applications in VANETs. Unfortunately, their scheme did not address the scalability issue. In 2008, Li *et al*.[13] proposed a secure and efficient communication scheme with privacy preservation, called SECSPP, for non-safety applications in VANETs. SECSPP discussed the security issue among service providers, roadside units and vehicles. In SECSPP, a vehicle needs to acquire a blind signature for privacy preservation before the vehicle accesses the desired services from its neighboring RSU. A service provider (SP) is responsible for signing and verifying the validity of signatures, and also involves in session key establishment between the RSUs and requesting vehicles. Recently, Yeh *et al.* proposed a portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks (named PAACP in brevity) [14]. However, PAACP in the authorization phase is breakable and cannot keep privacy in VANETs.

In this paper, we present a cryptanalysis of an attachable blind signature and show the PAACP's Authorized Credential (AC) is not secure and private even the AC secretly stored in a tamper-proof device. Our analysis showed that in PAACP, an eavesdropper can construct the AC from an intercepted blind document. As a result, PAACP in the authorization phase is breakable, and as any outsider can know who has which access privileges to access which service, the user's privacy in VANETs is jeopardized.

The remainder of this paper is organized as follows. Section 2 briefs the related work and schemes. A cryptanalysis of an attachable blind signature and evidence that the PAACP's AC is not secure are presented in Section 3. Finally, we conclude this paper and indicate some future research directions in Section 4.

2 Related Work

In 2011, Yeh *et al*. proposed a novel portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks [14], named PAACP, for non-safety applications in VANETs. In addition to the essential support of authentication, key establishment, and privacy preservation, PAACP is developed to provide sophisticated differentiated service access control, which will facilitate the deployment of a variety of non-safety applications. Besides, the portability feature of PAACP can eliminate the backend communications with service providers. To get rid of the communication with service providers, they proposed a novel portable access control method to store a portable service right list (*SRL*) into each vehicle, instead of keeping the *SRL*s in the service providers. In order to assure the validity and privacy of an *SRL*, Yeh *et al.* proposed a novel attachable blind signature [14]. Based on the attachable blind

signature, vehicles (OBUs) cannot tamper the SRL. Therefore, PAACP can prevent privilege elevation attacks [15]. As for privacy protection of users, the SP cannot trace the current location of the requesting vehicle, due to the attachable blind signature and the no need of any verification by SP. In addition, PAACP is more efficient than conventional access control schemes since RSUs can verify the correctness of an SRL without backend communications with SPs. As a result, PAACP is desirable for large scale VANETs. To the best of our knowledge, PAACP is the first study supporting sophisticated service access control without the scalability problem in VANETs. First, we introduce the traditional blind signature in section 2.1 and in section 2.2 review the attachable blind signature in and then study the authorization phase of the PPACP scheme in section 2.3.

2.1 Blind Signature

A traditional blind signature is similar to a digital signature except that it allows a person to get another person to sign a message without revealing the content of a message. It could be implemented by different cryptosystems, such as RSA and ElGamal. In 1983, Chaum's scheme uses RSA-based blind signatures [16]. First, we briefly introduce the conventional RSA-based blind signature. Generate the product of two (large) primes p and q, and a pair of public and private keys, e and d, such that ed=1(mod $\phi(N)$). The pair N, e is made public in an authenticated way and d is kept secret. A user U_A blinds a message m with a random blind factor r and computes the blind document.

$$BD = r^e m (\text{mod } N)$$

The blind document is then sent to the signer. Once receiving BD, the signer signs BD by his/her private key d as

$$BD' = BD^d = rm^d (\text{mod } N)$$

Then the signer sends BD' back to U_A. Upon receiving BD', U_A unblinds BD' by the blind factor r to obtain the signer's signature

$$BD'' = m^d = \frac{BD'}{r}$$

Finally, U_A confirms the integrity of BD'' by checking

$$(BD'')^e = m$$

The signer does nothing but signs the blind document BD sent from the user in a traditional blind signature. Such a traditional blind signature is not designed for access control in origin. In terms of access control, the service provider (SP) plays the role of the signer and also confirms whether the requested access privileges for a user are legal. Since the blind document containing the requested access privileges is blinded by a random number r, it is infeasible for the SP to check whether the requested access privileges are legal. To ensure the genuineness of the requested access privileges, Yeh *et al.* propose an attachable blind signature in section 2.2.

2.2 Attachable Blind Signature

In order to assure the validity and privacy of an *SRL*, Yeh *et al.* proposed a novel attachable blind signature [14]. Attachable blind signatures also could be implemented by different cryptosystems, such as RSA and ElGamal [17]. The RSA-based attachable blind signature will be introduced and key pair (e, d) is public/private key respectively and let "$X \rightarrow Y$: Z" denotes a sender X sending a message Z to a receiver Y.

- $U_A \rightarrow$ Signer: BD_1, BD_2

A user U_A blinds a message m with a random number a, two blind factors r_1, r_2 and then computes the two blind documents as below:

$$BD_1 = (r_1)^e m^a (\text{mod } N) \quad (2.1)$$
$$BD_2 = (r_2)^e m^{(1-a)} (\text{mod } N) \quad (2.2)$$

,where e is the public key of the signer. The blind document BD_1 and BD_2 are then sent to the signer.

- Signer $\rightarrow U_A$: BD_1', BD_2'

Once the signer receives BD_1 and BD_2, he/she attaches a message m' into BD_2 as

$$BD_2^{\#} = (r_2)^e m^{(1-a)} m' (\text{mod } N)$$

and computes BD_1' and BD_2' by his/her private key d are sent back to a user U_A

$$BD_1' = (BD_1)^d = (r_1^e m^a)^d = r_1 (m^a)^d (\text{mod } N) \quad (2.3)$$
$$BD_2' = (BD_2^{\#})^d = (r_2^e m^{(1-a)} m')^d = r_2 (m^{(1-a)} m')^d (\text{mod } N) \quad (2.4)$$

- U_A obtain the blind signature BD''

Upon receiving BD_1' and BD_2', a user U_A first decrypt blinds BD_1' and BD_2' by the blind factor r_1, r_2 respectively to obtain the BD_1^u and BD_2^u as

$$BD_1^u = \frac{BD_1'}{r_1} = \frac{r_1(m^a)^d}{r_1} = (m^a)^d \pmod N$$
$$BD_2^u = \frac{BD_2'}{r_2} = \frac{r_2(m^{(1-a)}m')^d}{r_2} = (m^{(1-a)}m')^d = (m^{(1-a)d})(m')^d \pmod N$$

and generates the signer's blind signature by

$$BD'' = BD_1^u \, BD_2^u = m^d (m')^d \pmod N$$

Finally, a user U_A confirms the integrity of BD'' by checking $(BD'')^e=(m^d(m')^d)^e = mm'$ whenever needed. Note that Yeh *et al*. proposed an attachable blind signature scheme that attaches a message m' into the signature and still keeps the privacy of user's message m. To withstand a privileges elevation attack, PAACP takes advantage of m' to ensure the validity of m. However, attachable blind signature is breakable and cannot keep privacy. In the section 3, we will present a cryptanalysis of an attachable blind signature and show m' cannot keep privacy.

2.3 The Authorization Phase of The PPACP Scheme

First, let "||" denote the conventional string concatenation operator and "$X \rightarrow Y$: Z" also denote a sender X sending a message Z to a receiver Y. In the authorization phase, a vehicle V_i creates a service right list $SRL_i^{V_i}=\{SVID_1||AR_1||SVID_2||AR_2||\ldots||SVID_k||AR_k\}$, where $SVID_k$ denotes the index of the kth service, and AR_k represents the granted access privileges of $SVID_k$. The $SRL_i^{V_i}$ is set in the authorized credential $AC_i^{V_i}=\{SID_t||T_{expired}||SRL_i^{V_i}\}$, where SID_t is the identification of the tth service provider and $T_{expired}$ is the expired time of $SRL_i^{V_i}$ in SID_t and then blinds $AC_i^{V_i}$ into blind documents $BD1_i$, $BD2_i$. To obtain the corresponding portable authorized credential for later use, V_i sends the blind documents with its signature σ_i to the service provider S_t. After checking the validity of σ_i, S_t generates similarly the service right list $SRL_i^{S_t}$, stores $SRL_i^{S_t}$ in $AC_i^{S_t}=\{SID_t||T_{expired}||SRL_i^{S_t}\}$ and attaches $AC_i^{S_t}$ into blind documents $BD1_i$, $BD2_i$ based on the attachable blind signature. Then, S_t delivers the blind documents back to V_i. Finally, V_i will obtain the portable authorized credential AC_i^*, where AC_i^* consists of both $AC_i^{V_i}$ and $AC_i^{S_t}$. AC_i^* is stored in V_i's tamper-proof device. The details are described below:

- $V_i \rightarrow S_t$: VID_i, σ_i, $BD1_i$, $BD2_i$

V_i chooses blind factors RN_1, RN_2 and a random number a, first, and then computes blind documents $BD1_i$, $BD2_i$ with PK_{S_t}, where PK_{S_t} is a public key of S_t. Finally, V_i sends its identity VID_i, signature $\sigma_i=\{BD1_i, BD2_i\}^{SKV_i}$,where SK_{V_i} is a private key of V_i and the blinded documents $BD1_i$, $BD2_i$ to S_t.

$$BD1_i = (RN_1)^{PK_{S_t}} (AC_i^{V_i})^a \pmod N \quad (2.5)$$
$$BD2_i = (RN_2)^{PK_{S_t}} (AC_i^{V_i})^{(1-a)} \pmod N \quad (2.6)$$

- $S_t \rightarrow V_i$: $BD1_i'$, $BD2_i'$

Once S_t receives a message $\{VID_i, \sigma_i, BD1_i, BD2_i\}$ from V_i, S_t checks whether the σ_i is valid by V_i's public key PK_{V_i}. If the answer is yes, V_i is successfully authenticated; otherwise, this session is dropped. Then S_t generates the authorized credential $AC_i^{S_t}$ according to the selling contract for V_i and attaches it into $BD2_i^{\#}$ as

$$BD2_i^{\#} = BD2_i \, AC_i^{S_t} = (RN_2)^{PK_{S_t}} (AC_i^{V_i})^{(1-a)} (AC_i^{S_t}) \pmod N$$

Then, S_t computes $BD1_i'$ and $BD2_i'$ are sent back to V_i.

$$BD1_i' = BD1_i^{SK_{S_t}} = ((RN_1)^{PK_{S_t}} (AC_i^{V_i})^a)^{SK_{S_t}} = (RN_1)(AC_i^{V_i})^{aSK_{S_t}} \quad (2.7)$$
$$BD2_i' = (BD2_i^{\#})^{SK_{S_t}} = ((RN_2)^{PK_{S_t}} (AC_i^{V_i})^{(1-a)} (AC_i^{S_t}))^{SK_{S_t}} = (RN_2)((AC_i^{V_i})^{(1-a)} (AC_i^{S_t}))^{SK_{S_t}} \quad (2.8)$$

- V_i obtains portable authorized credential AC_i^*

After obtaining $BD1_i'$, $BD2_i'$ from S_t, V_i decrypt blinds them as follows:

$$BD1_i^u = \frac{BD1_i'}{RN_1} = (AC_i^{V_i})^{aSK_{S_t}}$$
$$BD2_i^u = \frac{BD2_i'}{RN_2} = ((AC_i^{V_i})^{(1-a)} (AC_i^{S_t}))^{SK_{S_t}}$$

In order to get the portable authorized credential $AC_i^*= (AC_i^{V_i}AC_i^{S_t})^{SKS_t}$, V_i computes

$$BD1_i^{\,u}\, BD2_i^{\,u}$$
$$= (AC_i^{V_i})^{aSK_{S_t}} ((AC_i^{V_i})^{(1-a)} (AC_i^{S_t}))^{SK_{S_t}}$$
$$= (AC_i^{V_i} AC_i^{S_t})^{SK_{S_t}}$$

V_i can confirm the integrity of AC_i^* by checking that $(AC_i^*)^{PKS_t}$ is equal to $AC_i^{V_i} AC_i^{S_t}$ whenever needed. If it holds, V_i keeps AC_i^* for the subsequent service requests; otherwise, V_i will stop this phase. In this regard, Yeh et al. proposed V_i could protect AC_i^* in secret by a tamper-proof device after obtaining AC_i^*. Note that if both V_i and S_t are legal, $AC_i^{V_i}$ and $AC_i^{S_t}$ should be the same. For this reason, the square root of $(AC_i^*)^{PKS_t}$ is equal to $AC_i^{V_i}$ or $AC_i^{S_t}$.

$$\sqrt{(AC_i^*)^{PK_{S_t}}} = AC_i^{V_i} = AC_i^{S_t} \qquad (2.9)$$

3 CRYPTANALYSIS

In this section, we present a cryptanalysis of an attachable blind signature and show the PAACP's *AC* is not secure even if *AC* stores in secret by a tamper-proof device. An eavesdropper is able to construct *AC* from an intercepted blind document. Consequently, PAACP in the authorization phase is breakable and cannot keep privacy in VANETs. Any outsiders can know who has which access privileges to access which service.

3.1 The Weakness of The Attachable Blind Signature

We present a cryptanalysis of an attachable blind signature and show *m'* cannot keep privacy.

Cryptanalysis 1. To acquire a message *m*', an intruder can eavesdrop BD_1, BD_2 in the ($U_A \rightarrow$ Signer) channel and also eavesdrop BD_1', BD_2' in the (Signer$\rightarrow U_A$) channel. After stealing BD_1, BD_2, BD_1' and BD_2', the intruder can use public key *e* of the signer to compute as the following equation:

$$\frac{(BD_1' \cdot BD_2')^e}{(BD_1 \cdot BD_2)} = m'$$

< *Proof of Cryptanalysis* 1>

According to eq. (2.1) and (2.2), the values of $(BD_1 BD_2)$ will be computed as:

$$(BD_1 \cdot BD_2)$$
$$= ((r_1)^e m^a)((r_2)^e m^{(1-a)}) (\text{mod } N)$$
$$= (r_1 \cdot r_2)^e m (\text{mod } N)$$

According to eq. (2.3), (2.4) and use public key *e* of the signer, the values of $(BD_1'BD_2')^e$ will be computed as:

$$(BD_1' \cdot BD_2')^e$$
$$= (r_1 (m^a)^d)^e (r_2 (m^{(1-a)} m')^d)^e (\text{mod } N)$$
$$= (r_1^e (m^a))(r_2^e (m^{(1-a)} m')) (\text{mod } N)$$
$$= (r_1^e r_2^e)(m^a m^{(1-a)} m') (\text{mod } N)$$
$$= (r_1 \cdot r_2)^e (mm') (\text{mod } N)$$

Finally, an intruder can acquire message *m*' as following

$$\frac{(BD_1' \cdot BD_2')^e}{(BD_1 \cdot BD_2)}$$
$$= \frac{(r_1 \cdot r_2)^e (mm') (\text{mod } N)}{(r_1 \cdot r_2)^e m (\text{mod } N)}$$
$$= m'$$

3.2 An Attack on PPACP Scheme

Cryptanalysis 2. Similarly, To acquire authorized credential $AC_i^{V_i}$ and $AC_i^{S_t}$, an intruder can eavesdrop $BD1_i$, $BD2_i$ in the ($V_i \rightarrow S_t$) channel and also eavesdrop $BD1_i'$, $BD2_i'$ in the ($S_t \rightarrow V_i$) channel. After stealing $BD1_i$, $BD2_i$, $BD1_i'$ and $BD2_i'$, the intruder can use public key PK_{S_t} of the S_t to compute as the following equation:

$$\frac{(BD1_i' \cdot BD2_i')^{PK_{S_t}}}{(BD1_i \cdot BD2_i)} = AC_i^{S_t}$$

< *Proof of Cryptanalysis* 2>

According to eq. (2.5) and (2.6), the values of $(BD1_i BD2_i)$ will be computed as:

$$(BD1_i \cdot BD2_i)$$
$$= ((RN_1)^{PK_{S_t}} (AC_i^{V_i})^a)\ ((RN_2)^{PK_{S_t}} (AC_i^{V_i})^{(1-a)}) (\text{mod } N)$$
$$= ((RN_1 RN_2)^{PK_{S_t}} AC_i^{V_i} (\text{mod } N)$$

According to eq. (2.7), (2.8) and use public key PK_{S_t} of the S_t, the values of $(BD1_i'BD2_i')^{PKS_t}$ will be computed as:

$$(BD1_i' \cdot BD2_i')^{PK_{S_t}}$$
$$= ((RN_1)(AC_i^{V_i})^{aSK_{S_t}})^{PK_{S_t}} ((RN_2)((AC_i^{V_i})^{(1-a)} (AC_i^{S_i}))^{SK_{S_t}})^{PK_{S_t}} (\text{mod } N)$$
$$= ((RN_1)^{PK_{S_t}} (AC_i^{V_i})^a ((RN_2)^{PK_{S_t}} ((AC_i^{V_i})^{(1-a)} (AC_i^{S_i}))) (\text{mod } N)$$
$$= (RN_1^{PK_{S_t}} RN_2^{PK_{S_t}})((AC_i^{V_i})^a ((AC_i^{V_i})^{(1-a)} (AC_i^{S_i}))) (\text{mod } N)$$
$$= (RN_1 RN_2)^{PK_{S_t}} (AC_i^{V_i})(AC_i^{S_i}) (\text{mod } N)$$

Then, an intruder can acquire authorized credential $AC_i^{S_t}$ and then also acquire $AC_i^{V_i}$ as following

$$\frac{(BD1_i' \cdot BD2_i')^{PK_{S_t}}}{(BD1_i \cdot BD2_i)} = \frac{(RN_1 RN_2)^{PK_{S_t}} (AC_i^{V_i})(AC_i^{S_i})(\text{mod } N)}{(RN_1 RN_2)^{PK_{S_t}} (AC_i^{V_i})(\text{mod } N)} = AC_i^{S_i}$$

Finally, according to eq. (2.9), $AC_i^{S_t}$ is equal to $AC_i^{V_i}$. Yeh et al. claimed that an attachable blind signature can keep privacy, no one could comprehend the access privileges in $AC_i^{V_i}$ and no one can realize who is accessing those services. On the basis of our cryptanalysis, $AC_i^{S_t}=\{_{SIDt}||T_{expired}||SRL_i^{S_t}\}$ and $AC_i^{V_i}=\{SID_t||T_{expired}||SRL_i^{V_i}\}$ could be comprehended by outsiders and then decode $SRL_i^{S_t}$ and $SRL_i^{V_i}$ respectively. On a previous description, the service right list is as $SRL_i^{V_i} = \{SVID_1||AR_1||SVID_2||AR_2||\ldots||SVID_k||AR_k\}$. Hence, anyone can know who has which access privileges to access which service even if AC_i^* stores in secret by a tamper-proof device.

4 Conclusions and Future Research

In this paper, we present a cryptanalysis of an attachable blind signature and show the PAACP's Authorized Credential (AC) is not secure and private even the AC secretly stored in a tamper-proof device. Our analysis showed that in PAACP, an eavesdropper can construct the AC from an intercepted blind document. As a result, PAACP in the authorization phase is breakable, and as any outsider can know who has which access privileges to access which service, the user's privacy in VANETs is jeopardized.

In the future, we intend to not only address the security issue appearing in PAACP but also the communication overhead issue which is raised when cryptographic operations are needed in secure communications. Instead of adopting blind-signature approach, we plan to develop a low overhead scheme based on one-way hash function to address these two issues. Expectably, our new scheme will achieve more functionality and satisfy security features in VANETs.

Acknowledgements

This work was partially supported by the National Science Council of Taiwan, R.O.C. under Grant No. 100-2218-E-008-006 and the Software Research Center of National Central University. The authors thank the anonymous reviewers for their valuable comments.

References

[1] Dedicated Short Range Communications (DRSC) Home. [Online]. Available: http://www.leearmstrong.com/Dsrc/DSRCHomeset.htm

[2] National ITS Architecture. [Online]. Available: http://www.iteris.com/itsarch/index.htm

[3] Car 2 Car Communication Consortium. [Online]. Available: http://www.car-to-car.org/

[4] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments, IEEE Std. 1609.2-2006. (2006).

[5] Y. Chen and Y. Wei, SafeAnon: a safe location privacy scheme for vehicular networks, *Telecommunication Systems*, (2010), 1-16.

[6] Y. Wei and Y. Chen, Safe Distance Based Location Privacy in Vehicular Networks, *IEEE 71th Vehicular Technology Conference*, (2010), 1-5.

[7] M. Raya, J. Hubaux, The security of vehicular ad hoc networks, *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*. (2005).

[8] L. Wischhof, A. Ebner, H. Rohling, Information dissemination in self-organizing intervehicle networks, *IEEE Transactions on Intelligent Transportation Systems*. Vol.6, No.1, (2005), 90-101.

[9] N. Wang, Y. Huang, W. Chen, A novel secure communication scheme in vehicular ad hoc networks, *Computer Communications*. Vol.31, No.12, (2008), 2827-2837.

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

[11] J. Isaac, J. Camara, S. Zeadally, J. Marquez, A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks, *Computer Communications*. Vol.31, No.10, (2008), 2478-2484.

[12] C. Zhang, X. Lin, R. Lu, P. Ho, X. Shen, An efficient message authentication scheme for vehicular communications, *IEEE Transactions on Vehicular Technology*, Vol.57, No.6, (2008), 3357-3368.

[13] C. Li, M. Hwang, Y. 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, (2008), 2803-2814.

[14] L. Yeh, Y. Chen, J. Huang, Paacp: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks, *Computer Communications*. Vol.34, No.3, (2011), 447-456.

[15] Y. Chen, L. Yeh, An efficient authentication and access control scheme using smart cards, *The Proceedings of International Conference on Parallel and Distributed Systems*, (2005).
[16] D. Chaum. Blind signatures for untraceable payments. *In Advances in Cryptology-CRYPTO82*, (1983), 199-203.
[17] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*. Vol.31, No.4, (1985), 469-472.

Wei-Chen Wu was born in Taipei, Taiwan, Republic of China. He received the B. S. degree in Information Management from Ming Chuan University, Taipei, Taiwan, in 1986, the M. S. degree in Information Management from Shih Hsin University, Taipei, Taiwan, in 2004, respectively. He will receive the Ph. D. degree in Information Management from National Central University in 2012. From 2004 to now, he is also the Director of the Computer Center at Hsin Sheng College of Medical Care and Management. His current research interests include information & security, cryptography and computer communications.

Yi-Ming Chen is a professor of the Department of Information Management, National Central University, Taiwan. He received the Ph.D. from the Department of Electrical Engineering from National Cheng Kung University, Taiwan, in 1990. He has been a visiting scholar in the Department of Electrical Engineering and Computer Science of the University of Illinois at Chicago, from 1998 to 1999. His current research interests focus on the area of network security, secure programming and distributed systems.