ATCS: A Novel Anonymous and Traceable Communication Scheme for Vehicular Ad Hoc Networks

Wei Hu, Kaiping Xue, Peilin Hong, and Chuchu Wu

(Corresponding author: Kaiping Xue)

The Information Network Lab of EEIS Department,
University of Science and Technology of China (USTC), Hefei, China (Email: kpxue@ustc.edu.cn)

(Received Oct. 4, 2009; revised and accepted Jan. 15 & Apr. 24, 2010)

Abstract

Generally vehicles in VANETs should periodically broadcast safety messages. Since safety messages contain traffic related information and are sensitive to location privacy, it is essential to ensure anonymity, authenticity and traceability in broadcast. These conflicting requirements make it difficult to design a secure communication scheme for VANETs. In this paper, we propose a signature scheme which provides anonymous, authenticated and traceable communication based on the efficient combination of (t, n)-threshold signature and Weil Pairing. ATCS scheme aims to provide the authenticity of signed broadcasting messages to prevent internal attacks. And meanwhile the proposed scheme can also keep characteristics of anonymity and traceability. According to the performance evaluation compared with two related schemes, from the perspective of security enhancements, the additional cost of our proposal is acceptable.

Keywords: Anonymous and traceable communication, (t, n)-threshold signature, vehicular ad-hoc networks, weil pairing

1 Introduction

In VANETs, vehicles can communicate with infrastructure and other vehicles. The former is called Vehicle-to-Infrastructure (V2I) communication and the latter is called Vehicle-to-Vehicle (V2V) communication. In V2V communication, vehicles periodically broadcast safety messages. Safety messages contain traffic information and geographic information and thus can be used by other vehicles to avoid traffic jams and traffic accidents.

Since malicious attackers may acquire originators' privacy (identity, driving pattern and location) from safety messages, V2V communication should provide anonymity in broadcast. However, traditional signature s chemes, like [3, 8, 13], cannot be used to trace anonymous attackers. To satisfy conflicting requirements of security and privacy, some novel signature schemes were proposed to provide anonymous and traceable communication. In [5], Laurendeau *et al.* introduced the SAB protocol using PKI infrastructure. Since SAB protocol employs certificates to authenticate vehicles, it is costly and inefficient. In [7], Li *et al.* introduced a light-weighted communication scheme called SECSPP scheme. This scheme ensures anonymous communication for authorized vehicles and thus could preserve identity privacy. However, since SECSPP scheme requires anonymous interaction between communication parties to authenticate each other, it is only impractical in unicasting, but not impractical in broadcasting. Kim *et al.* in [4] and Lu *et al.* in [9] respectively introduced anonymous signature schemes that are based on Weil Pairing. Although these two signature schemes could be used to trace anonymous originators, they cannot distinguish fake messages generated by internal attackers with legitimate identification. In such case, internal attackers will not be traced and punished until fake messages are received by target vehicles and reported to the third agent.

To prevent internal attacks, V2V communication should provide authenticity in broadcast. In [2], Daza *et al.* proposed an endorsing scheme to provide group authentication in communication. The endorsing scheme could prevent internal attack using (t, n)-threshold signature. Nevertheless, even if endorsing scheme could make it harder to launch internal attack, collusion attack is still possible. In that case, since signature schemes in [2] cannot provide traceability, collusion attackers cannot be traced and punished.

According to the above discussion, it is necessary to design a new communication scheme for VANETs. This scheme should provide anonymity, traceability and authenticity in broadcast. To meet these conflicting requirements, in this paper we propose a novel anonymous and traceable communication scheme (named ATCS) based on the combination of (t, n)-threshold signature and Weil

Pairing. Based on the (t, n)-threshold signature used in the endorsing scheme [2], ATCS scheme aims to provide the authenticity of signed broadcasting messages in AnonySign scheme [4] to prevent internal attacks. And meanwhile the proposed scheme can also keep characteristics of anonymity and traceability in [4]. According to the performance evaluation compared with Endorsing Signature [2] and Anonymous Signature [4], the additional cost of our proposal is acceptable.

The rest of the paper is organized as follows: Section 2 introduces two related signature schemes. Then based on the two related scheme in Section 2, Section 3 introduces our proposed ATCS scheme in details. Section 4 gives the performance evaluation and security analysis. Conclusion is provided in Section 5.

2 Two Related Signature Schemes

Before introducing ATCS, for clarity, we introduce two related signature schemes in this section. The first is an anonymous signature scheme which makes use of Weil Pairing [4], the second one is an endorsing signature scheme which is on the base of group-based (t, n)-threshold signature [2]. Our scheme is the effective combination of these two schemes.

2.1 Anonymous Signature Scheme Using Weil Pairing

In this section, we introduce the anonymous signature scheme AnonySign in [4]. Basic procedure contains four phases: Setup phase, Extract phase, AnonySign phase and AnonyVerify phase. To trace attackers, TA should implement the fifth phase: Trace phase.

- **Setup Phase.** In this phase, TA generates system parameters. The system parameters are listed as follows:
  - Admissible Bilinear Map: $\hat{e}$;
  - Random selected prime number: $q, t \in Z_q^*$;
  - Cyclic groups of order q: G_1 and G_2;
  - Generator of G_1: p;
  - Cryptographic hash functions: H_1: $(0,1)^* \rightarrow G_1$ and $H_2 : (0,1)^* \rightarrow Z_q^*$.

  TA sets t as its private master key and sets $\{\hat{e}, G_1, G_2, q, p, H_1, H_2\}$ as its public information.

- **Extract Phase.** In this phase, TA generates user parameters for each requesting vehicle. Take the $vehicle_i$ for example, the parameters are listed as follows.
  - Public identity of $vehicle_i$: ID_i;
  - Private key of $vehicle_i$: $D_i = t^{-1}H_1(ID_i)$ and $S_i = tH_(ID_i)$.

- **AnonySign Phase.** In this phase, $vehicle_i$ signs safety message m. Firstly, $vehicle_i$ randomly selects $r \in Z_q^*$ and $k \in Z_q^*$. Then, $vehicle_i$ computes $x_i = D_i$, $Y_i = rD_i$, $Z_i = krD_i$, $h = H_2\{m \| X_i \| Y_i \| Z_i\}$, $V_i = k(r+h)S_i + rS_i$ and sets $\omega_i = \{X_i, Y_i, Z_i, V_i\}$ as the signature of m.

- **AnonyVerify Phase.** In this phase, $vehicle_j$ checks whether safety message m is trustworthy by verifying the signature ω_i. To verify $\omega_i m vehicle_j$, checks if $\hat{e}(D_j, V_u) = \hat{e}(S_j, Z_i + hX_i, Y_i)$ hold. If it holds, m is considered as trustworthy. Else reports TA of attack. To trace attackers, TA should implement the Trace phase:

- **Trace Phase.** In this phase, TA traces originators of fake messages. Upon receiving fake message m, its signature $\omega_i = \{X_i, Y_i, Z_i, V_i\}$ and a set of identities of possible attackers: $\{ID_S\}$, TA follows the following steps. Firstly, TA randomly selects $vehicle_k$ whose user parameters are known to TA and computes $TA = \hat{e}(tX_k, tY_k)$. Then, for each $ID_j \in \{ID_S\}$, TA computes $Q_j = H_1(ID_j)$ and checks if $\hat{e}(tZ_i, Q_j) = T$ holds. Once the equation holds, $vehicle_j$ is considered as the originator of fake message m.

According to the introduction, AnonySign makes any originator traceable and thus could provide traceability in broadcast. However, AnonySign could not distinguish fake messages originated by internal attackers with legitimate identification. Therefore, AnonySign could not prevent internal attack beforehand. To prevent internal attack beforehand, signature scheme needs to provide authenticity in broadcast.

2.2 Endorsing Scheme Using Group-based (t, n)-Threshold Signature

In this section, we introduce the (t,n)-threshold signature based endorsing signature scheme in [2]. Basic procedure of the endorsing scheme in [2] contains five phases: Setup phase, Announcement generation phase, Announcement endorsement phase, Announcement composition phase and Announcement verification phase.

- **Setup Phase.** In this phase, TA generates system parameters and user parameters. Assume that there are n vehicles in the VANET. Firstly, TA randomly generates secret polynomial $f(x) = \sum_{i=1}^{t-1} a_i x^i + SK$ with degree $t-1$, where SK is TA's secret key, and respectively PK is TA's public key. Then, TA divides n vehicles into r groups so that there are $\lfloor n/r \rfloor$ vehicles in each group (for suitable rounding, the number of vehicles in some groups may be a little more than that). Parameters are listed as follows:
  - Randomly selected public information of $group_i$: α_i;

  - Secret key share of $group_i$: $SK_i = f(\alpha_i)$, respectively PK_i is the public key for $group_i$.

- **Announcement Generation Phase.** In this phase, assume that $Vehicle_i$ intends to broadcast safety message m. Firstly, $vehicle_i$ generates the hash of m: $H_i(m)$. Then, $vehicle_i$ computes $\omega(m) = H_i(m)^{SK_i}$ and broadcasts $\{m, \omega_i(m)\}$.

- **Announcement Endorsement Phase.** In this phase, vehicles endorse m by generating their individual signature of m. Assume that $vehicle_j$ receives $\{m, \omega_i(m)\}$. Firstly, $vehicle_j$ checks whether m conveys real information. If $vehicle_j$ considers m as trustworthy, it would compute $\omega_j(m) = H_i(m)^{SKl}$ and broadcasts $\{\omega_i(m), \omega_j(m)\}$ to return it to $vehicle_j$.

- **Signature Composition Phase.** In this phase, after receiving enough individual signatures of message m from other vehicles, $vehicle_i$ generates integrated signature of m. With a set A of at least t individual signature $\{\omega_i(m)\}$, which are generated by different secret key share respectively, the trustworthy signature can be composed as follows.

  We first express Lagrange coefficients as $\lambda_i = \Pi_{i\neq j}\langle\frac{-\alpha_j}{\alpha_i-\alpha_j}\rangle$ for each $i \in A$. Then we can compute a standard signature as:

$$\omega(m) \quad = \quad \Pi_{i\in A}\omega_i(m)^{\lambda_i} = H(m)\Sigma_{i\in A}^{\lambda_i SK_i} = H(m)^{SK} \tag{1}$$

  After generating the trustworthy signature of m, $vehicle_i$ broadcasts $\{m, \omega(m)\}$.

- **Announcement Verification Phase.** Any legitimate user that receives $\{m, \omega(m)\}$. could check whether $\omega(m)$ is correct using public key PK.

According to the above discussion, the endorsing scheme [2] makes it hard to sign fake messages and thus could provide authenticity in broadcast. Therefore, we can combine endorsing signature scheme with AnonySign scheme to enhance the security of V2V broadcasting, which can provide both anonymity, traceability, and also authenticity to prevent internal attacks beforehand.

3 Our Proposed ATCS Scheme

Based on previous discussion, both AnonySign scheme [4] and Endorsing Scheme [2] are vulnerable. For instance, Anonymous Signature [4] can not distinguish fake messages and thus is vulnerable to internal attack. Meanwhile, Anonymous Signature [4] can not prevent collusion attack. To solve these security problems and provide a more secure communication, we propose a novel anonymous and traceable communication scheme (ATCS scheme) based on the efficient combination of both the AnonySign scheme in [4] and the endorsing scheme in [2]. Based on the endorsing scheme [2], ATCS aims to improve the authenticity of the AnonySign scheme [4] to prevent internal attacks, which can also keep characteristics of anonymity and traceability in [4].

3.1 Pre-deployment Process

Before deploying a VANET, TA needs to setup anonymous signature parameters and assign them to new vehicles.

- **System Parameters Setup.** Once on, TA generates system parameters for anonymous signature. The system parameters are listed as follow:

  - Admissible Bilinear Map: $\hat{e}$;
  - Random selected prime number: $q, t \in Z_q^*$;
  - Cyclic groups of order q: G_1 and G_2;
  - Generator of G_1: p;
  - Cryptographic hash functions: $H_1 : (0,1)^* \rightarrow G_1$ and $H_2 : (0,1)^* \rightarrow Z_q^*$.

  TA sets t as its private master key and sets $\{\hat{e}, G_1, G_2, q, p, H_1, H_2\}$ as its public information.

- **Handling New Vehicles.** Before a new vehicle leaves the factory or joins in the VANET, TA generates and assigns it user parameters securely. The user parameters are listed as follows.

  - Public identity of $vehicle_i$: ID_i;
  - Private key of $vehicle_i$: $D_i = t^{-1}H_1(ID_i)$ and $S_i = tH_i(ID_i)$.

The user parameters may be replaced periodicity through V2I communication.

3.2 Threshold Signature Parameters Setup and Extract Process

Assume that RSU_i is in charge of vehicular communication over $Segment_i$. Since traffic volume of $Segment_i$ varies from time to time, RSU_i should periodicity carry out this process to reset and extract threshold signature parameters.

According to [2], the extended group-based private protocol takes an adaptive scheme to select threshold signature parameters, which could be realized without TA. However, it is quite possible that vehicles would have to experience several failure attempts before achieving proper parameters. Therefore, the compound version of such protocol would be much too costly in selecting proper parameters. Here, we propose a novel parameter setup scheme that involves TA to setup parameters, which requires no attempts.

History information is helpful in predicting traffic volume. For example, we can always expect high traffic volume in downtown. Moreover, traffic volume in the same region may not vary too much during one or two minutes.

Therefore, we assume that using history information, traffic volume can be predicted. Assume that according to prediction, there are n vehicles entering $Segment_i$ during the time interval $\Delta t = t_2 - t_1$. With the prediction, RSU_i follows following steps to setup parameters.

Firstly, RSU_i randomly generates secret polynomial $f(x) = \Sigma_{i=1}^{t-1} a_i x^i + SK$ with degree $t-1$. Then, RSU_i divides n vehicles into r groups so that there are $\lfloor n/r \rfloor$ vehicles in each group (exact algorithm should be designed according to road condition). Signature parameters are listed as follows.

- Randomly selected public information of $group_i$: α_i;
- Secret key share of $group_i$: $SK_i = f(\alpha_i)$;
- Secret key of RSU_i: SK;
- Public key of RSU_i: PK.

For vehicles that enter $Segment_i$ during the time interval Δt, RSU_i assigns them predetermined signature parameters. Firstly, upon receiving $vehicle_i$'s apply, RSU_i assigns $vehicle_i$ to $group_i$. Then, RSU_i sends $\{E_{Ki}(a_i, PK), SK_i\}$ to $vehicle_i(E()$ can be ID-based encryption function just like D. Boneh *et al.* proposed in [1] and K_i is RSU_i's secret key). After receiving such message, $vehicle_i$ gets threshold signature parameter triple $\{\alpha_i, PK, SK_i\}$.

3.3 Signature Generation and Verify Process

The main process contains two phases: Individual signature generation and verification phase, integrated signature generation and verification phase. To trace attackers, TA should implement the third phase: Trace phase.

- **Individual Signature Generation and Verification Phase.** Assume that $Vehicle_i$ intends to broadcast safety message m. In this phase, $Vehicle_i$ broadcasts m so that it can be authenticated by nearby vehicles.

  - **Broadcast Safety Message**
    Firstly, $vehicle_i$ generates the hash of safety message m: $H_i(m)$. Then, $vehicle_i$ computes $\omega_i(m) = H_i(m)^{SKi}$ and broadcasts $\{m, \omega_i(m)\}$.
  - **Generate Individual Signature**
    Assume that $vehicle_i$ receives the message m. If $\{m, \omega_i(m)\}$ believes that safety message m conveys real information, $vehicle_i$ shall authenticate m by generating its own individual signature of m. Firstly, $vehicle_j$ generates the hash of safety message m: $H_j(m)$. Then, $vehicle_j$ computes $\omega_j(m) = H_j(m)^{SK_i}$ and sets $m^* = \{\alpha_j, \omega_j\}$ as the authentication message.
  - **Verify Individual Signature**
    Upon receiving $\{m^*, \varepsilon_j\}$, $vehicle_i$ verifies m^* by checking whether m^* is generated by legitimate user. With signature $\varepsilon_j = \{X_j, Y_j, Z_j, V_j\}$, $vehicle_i$ checks if $\hat{e}(D_i, V_j) = \hat{e}(S_i, Z_j + hX_j, Y_j)$ holds. If it holds, m^* should be generated by legitimate user and is considered as valid. Else $vehicle_i$ reports TA of attack.

- **Integrated Signature Generation and Verification Phase:**
  In this phase, $vehicle_i$ generates and verifies the integrated signature of safety message m.

  - **Generate and Verify Integrated Signature**
    According to Equation 1, $vehicle_i$ should collect at least t different authentication message $\{\alpha_i, \omega_j\}$, which were generated by different secret key share respectively, to compose the trustworthy signature $\omega = H(M)^{SK}$.

    Assume that $vehicle_i$ has already received enough authentication messages from nearby vehicles. Firstly, $vehicle_i$ composes the integrated signature $\omega = H(M)^{SK}$. using Equation (1). Then, $vehicle_i$ checks whether ω is the correct signature using public threshold signature parameter PK. If ω is considered as false, $vehicle_i$ shall report TA of attack.
  - **Generate Anonymous Signature**
    To prevent possible collusion attack, $vehicle_i$ generates anonymous signature of (m, ω). Firstly, $vehicle_i$ chooses randomly $r \in Z_q^*$ and $k \in Z_q^*$. Then, $vehicle_i$ computes $X_i = kD_i, Y_i = rD_i, Z_i = krD_i, h = H_2\{m\|\omega|\ X_i\|Y_i\|Z_i\}$, $V_i = k(r+h)S_i + rS_i$ and sets $\varepsilon_i = \{X_i, Y_i, Z_i, V_i\}$ as the signature of $\{m, \omega\}$. After that, $vehicle_i$ broadcasts $\{m, \omega, \varepsilon_i\}$.

    As we can see in this section, with anonymous signature ε_i, any originator of fake messages could be traced. Moreover, since any vehicle can't generate the integrated signature ω of m without authentication from other vehicles, it is hard to launch internal attack.

    To trace originators of fake messages, TA should implement the Trace phase:

    * **Trace Phase.** Upon receiving fake message m, its signature $\omega_i = \{X_i, Y_i, Z_i, V_i\}$ and a set of identities of possible attackers: $\{ID_S\}$, TA follows the following steps. Firstly, TA randomly selects $vehicle_k$ whose user parameters are known to TA and computes $T = \hat{e}(tX_k, tY_k)$. Then, for each $ID_j \in \{ID_S\}$, TA computes $Q_j = H_1(ID_j)$ and checks if $(tZ_i \hat{,} Q_j)$ holds. Once the equation holds, $vehicle_j$ is considered as the originator of fake message m.

Table 1: Assumption

Message	Size
$\{m, H(m)^{SK_j}\}$	F+H
$\{m, \sigma = \{m, X, Y, Z, V\}\}$	F+L

4 Performance Evaluation and Security Analysis

In this section, we discuss the performance and security of ATCS scheme and compare with schemes in [2] and [4] respectively.

4.1 Performance Evaluation

Assume that RSU_j is in charge of vehicular communication in its coverage area (named $Segment_j$). To analyze the performance of ATCS scheme, we calculate the total size of messages that a vehicle needs to broadcast in $Segment_j$.

At first, for simplicity, let F be the size of a safety message, L be the size of an anonymous signature, and H be the size of a hash value. We give an example of our assumption in Table 1.

Then, we assume that in $Segment_j$, $vehicle_i$ needs to broadcast m safety messages and n authentication messages. Table 2 shows the calculation result.

After that, for simplicity, we assume that each vehicle has k within-range neighbors and each one needs to broadcast m safety messages in $Segment_j$. Thus $vehicle_i$ is expected to receive $m \times k$ application for authentication from its k within-range neighbors. So, for simplicity, we assume that $n \approx km$.

Furthermore, to improve the efficiency, ATCS should adopt short threshold signature. However, short threshold signature would make communication vulnerable. To meet the conflicting requirements of security and efficiency, we assume that threshold signature should provide at least the same level of security as anonymous signature does. According to [6], 1024-bit traditional discrete logarithm (TDL) system and 160-bit elliptic curve cryptosystem offer approximate the same level of security. Thus, to offer the same level of security, the signature size of Anonymous Signature [4] should be 640 bit and the signature size of Endorsing Scheme [2] would be 1024 bit. For simplicity, we assume that $H \approx 2L$.

Based on previous discussion, we show the approximate result in Table 3.

According to [12], the WAVE could enable V2V communications over distance of less than 1000m. Since in general, most cars would move in the speed from 50 km/h to 140km/h, they won't stay in $Segment_j$ for too long. In other words, a car won't broadcast too many safety messages and thus m can't be too large. Therefore, we can conclude that although the cost of ATCS is much greater than the cost of Anonymous Signature [4], it's only 10% to 25% more than the cost of Endorsing Signature [2].

Therefore, compared with Endorsing Signature [2], ATCS performs worse in terms of communication cost. However, ATCS scheme is designed to solve some security problems, just as the next section discusses, rather than improving performance. The additional cost, about 10% to 25%, can be considered as acceptable.

4.2 Security Analysis

In this section, we analyze the security of ATCS by comparing it with Anonymous Signature [4] and Endorsing Signature [2].

1) **Some Possible Attacks**
In this section, we discuss some possible attacks. These attacks could break Anonymous Signature [4] or Endorsing Signature [2]. However, none of them could successfully break ATCS.

- **Anonymous Signature [4].**
  - **Internal Attack**
    Members with legitimate identity could sign messages. Since any message with legitimate signature is considered as trustworthy, internal attackers with legitimate identity could sign fake messages and thus make them trustworthy. In other words, internal attackers could broadcast fake messages to cause traffic jams and even traffic accidents. Although any originator is traceable, internal attack could not be prevented beforehand.
- **Endorsing Signature [2].**
  - **Collusion Attack**
    Collusion attack is always possible. Although endorsing scheme makes it hard to generate legal signature for fake messages, a number of attackers above a certain threshold could still sign fake messages. In such case, Endorsing Signature[2] could not trace and punish attackers.
  - **Fake Authentication Messages**
    Upon receiving apply for authentication: $\{m, \omega_i(m)\}$, attackers could broadcast fake authentication messages so as to prevent any within-range vehicles from generating trustworthy threshold signature. In such case, attackers cannot be traced and punished.
- **ATCS Scheme.**
  - **Internal Attack**
    To generate trustworthy signature, users have to broadcast messages to get them authenticated by other vehicles. In such case, fake messages would not be authenticated

Table 2: The calculation result

	ATCS	Anonymous Signature[4]	Endorsing Scheme[2]
Safety message with individual signature	F+H		F+H
Authentication messages	Approximate 2H+L		Approximate 2H
Safety message with integrated signature	F+H+L	F+L	F+H
Total	2mF+(2m+2n)H+(m+n)L	mF+mL	2mF+(2m+2n)H

Table 3: Approximate result

	ATCS	Anonymous Signature[4]	Endorsing Scheme[2]
Size	2mF+4mL(k+1)+m(k+1)L	mF+mL	2mF+4mL(k+1)

and thus most internal attack could be prevented beforehand.

– **Collusion Attack**
Since TA could trace any originator. Even if ATCS could not prevent collusion attack beforehand, attackers could be traced and punished.

– **Fake Authentication Messages**
Since any authentication message is signed by anonymous signature, attackers are traceable and thus could prevent such attack.

2) **Overall Discussions**
Raya and Aubaux [11] described a security architecture of VANETs, Parno and Perrig [10] proposed possible threat in VANETs. Based on these works, before the overall discussion, we present some security requirements for V2V communications in Table 4.

- **Anonymous Signature.** As we can see in Section 2.1, Anonymous Signature [4] is an Identity-Based Signature scheme. Such signature scheme can provide anonymity and traceability in broadcast using Weil Pairing. Applying this scheme, receivers can verify whether messages are from legal members without any knowledge of originators. Moreover, any originators could be traced by TA. Thus anonymous signature [4] could meet the requirement of message integrity, entity authentication, non-repudiation, anonymity, unlinkability and traceability. However, such scheme could not help prevent internal attack.

- **Endorsing Signature.** As we can see in Section 2.2, Endorsing Signature [2] makes use of group-based (t, n)-threshold signature scheme to provide anonymity and authenticity in broadcast. Applying this signature scheme, fake messages may not get authenticated and thus would not be signed. Moreover, group-based signature could preserve originators' identity. Thus Endorsing Signature [2] could meet the requirement of message integrity, entity authentication, anonymity, unlinkability and Group Authentication. However, collusion attack is always possible. Once collusion attack occurs, originator of fake messages would be untraceable. Furthermore, Endorsing Signature [2] could not distinguish fake authentication messages.

- **ATCS Scheme.** As the description in Section 3, ATCS scheme makes use of the combination of both Weil Pairing and (t, n)-threshold signature to provide anonymity, traceability and authentication in broadcast. Applying this signature scheme, fake messages can not get authenticated and thus would not be signed. Moreover, group-based signature could preserve originators' identity. Furthermore, any originator is traceable. Thus, ATCS could meet the requirement of Message integrity, entity authentication, non-repudiation, anonymity, traceability and group authentication.

  Based on previous discussion, we present the result in Table 5.

According to the above discussion, both AnonySign scheme [4] and Endorsing scheme [2] are vulnerable to some possible attacks and thus can't meet all the secure requirements for V2V communication. In comparison, ATCS scheme could prevent these possible attacks and thus could meet all the secure requirements for communication. Therefore, we conclude that ATCS is more secure.

5 Conclusion and Future Works

In this paper, we propose a novel signature scheme. This signature provides anonymity, traceability and authentication in broadcast. Our proposed ATCS scheme, makes

Table 4: Security requirements

Requirements	**Detail description**
Message Integrity	Any receiver could verify whether the safety message was altered during the transmission. In other words, nobody can forge the signature.
Entity Authentication	A receiver can verify whether the sender is a legal member.
Non-Repudiation	The real originator cannot deny that he/she generated the message.
Anonymity	Secure communication would not reveal any identity information of sender and receiver.
Unlinkability	Different interactions of the same user cannot be related.
Traceability	With TA, any originator of safety messages can be traced.
Group Authentication	Before broadcasted, a message should be verified by a group of users and get authenticated.

Table 5: Security requirements

	AnonySign scheme[4]	Endorsing scheme[2]	ATCS scheme[2]
Message Integrity	Yes	Yes	Yes
Entity Authentication	Yes	Yes	Yes
Non-Repudiation	Yes	No	Yes
Anonymity	Yes	Yes	Yes
Unlinkability	Yes	Yes	Yes
Traceability	Yes	No	Yes
Group Authentication	No	Yes	Yes

use of effective combination of Weil Pairing and group-based (t, n)-threshold signature. Based on the endorsing scheme [2], ATCS scheme aims to provide the authenticity of the AnonySign scheme [4] to prevent internal attacks, which can also keep characteristics of anonymity and traceability in [4]. According to the performance evaluation compared with Endorsing Signature [2], the additional cost of our proposal is acceptable.

In the future works, we will implementation scheme in the demo test bed and we will focus on communication cost, computing cost and storage cost cased by the scheme.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No.60903216, No.60772033 and National High-Tech Key Program of China under Grant No.2009AA012000.

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *The 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 213-229, 2001.

[2] V. Daza and J. D. Ferrer, "Trustworthy privacy-preserving car-generated announcements in vehicular Ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876-1886, 2009.

[3] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," *The 11th Annual International Cryptology Conference on Advances in Cryptology*, pp. 457-469, 1991.

[4] B. H. Kim, K. Y. Choi, J. H. Lee, and D. H. Lee, "Anonymous and traceable communication using tamper-proof device for vehicular Ad Hoc networks," *The 2007 International Conference on Convergence Information Technology*, pp. 681-686, 2007.

[5] C. Laurendeau and M. Barbeau, "Secure anonymous broadcasting in vehicular," *The 32nd IEEE Conference on Local Computer Networks*, pp. 661-668, 2007.

[6] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology*, vol. 14, no. 4, pp. 255-293, 2001.

[7] 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, pp. 2803-2814, 2008.

[8] R. Lu and Z. Chao, "A directed signature scheme based on RSA assumption," *International Journal of Network Security*, vol. 2, no. 3, pp. 182-186, 2006.

[9] R. X. Lu, X. D. Lin, H. J. Zhu, P. H. Ho, and X. M. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1454-1466, 2009.

[10] B. Parno and A. Perrig, "Challenges in securing vehicular networks," *The Workshop on Hot Topics in Networks (HotNets-IV)*, pp. 1-6, 2005.

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

[12] IEEE Standard, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages*, IEEE Std 1609.2, pp. 1-105, 2006.

[13] J. Zhang and W. Zou, "On the security of Huang-Chang multi-signature schemes," *International Journal of Network Security*, vol. 5, no. 1, pp. 62-65, 2007.

Wei Hu ireceived his B. S. degree of Information Security from University of Science and Technology of China (USTC) in July, 2010. He will be a doctoral student in Lehigh University. His research interests include Network security and Cryptography.

Kaiping Xue received the Ph.D. degree of Communication and Information Systems from University of Science and Technology of China (USTC) in 2007. Now he works as an Lecturer at Department of Infosec and EEIS of USTC. His research interests include Distributed Network and Network security.

Peilin Hong is a Professor in the Department of Electronic Engineering and Information Science, University of Science and Technology of China (USTC). Her research interests include next generation Internet, policy control, IP QoS and information security. She has published 2 books and over 100 academic papers in journals and conference proceedings.

Chuchu Wu received her B. S. degree of Communication and Information Systems from University of Science and Technology of China (USTC) in July, 2010. She will be a doctoral student in University of California, Los Angele(UCLA). Her research interests include Network Information Theory, Multimedia Communication and Network Security.