A SECURE AGGREGATED MESSAGE AUTHENTICATION SCHEME FOR VEHICULAR AD HOC NETWORKS

Huei-Ru Tseng
Information and Communications Research Laboratories
Industrial Technology Research Institute
Chutung, Hsinchu, 310140, Taiwan
hueiru@itri.org.tw

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

Emery Jou
Networks and Multimedia Institute
Institute for Information Industry
Tainan, 70955, Taiwan
emeryjou@iii.org.tw

Abstract

Vehicular ad hoc networks (VANETs) are an emerging area of interest for the security community. Due to the scale of the network, the speed of the vehicles, their geographic positions, and the very sporadic connectivity between them, security issues of VANETs are very challenging, especially on how to ensure the authenticity of emergency messages efficiently. In this paper, we propose 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 ensure the conditional privacy preservation and traceability of vehicles.

Keywords: Vehicular ad hoc networks, Authentication, Petri nets, Conditional privacy preservation, Traceability

INTRODUCTION

Vehicular ad hoc networks (VANETs) can be divided into inter-vehicle communications (IVC) and roadside-to-vehicle communications (RVC) that require roadside unit (RSU) equipment. The main goal of VANETs is to achieve safety and comfort for passengers. In VANETs, each vehicle equipped with an on-board unit (OBU) can receive and relay messages through the wireless network without predefined or centralized infrastructure. Vehicle-collision warning, road sign alarms, and in-place traffic view will give the driver essential tools to decide the best path along the way.

Due to the scale of the network, the speed of the vehicles, their geographic positions, and the very sporadic connectivity between them, security issues of VANETs are very challenging. To tackle the security problems, Raya and Hubaux (1) proposed the first solution in a systematic and quantified way for VANETs in 2005. Thereafter, various security mechanisms (2; 3; 4; 5; 6; 7; 8) have been proposed to improve security, efficiency, and functionality in VANETs.

To ensure the authenticity of emergency messages efficiently is also an important security issue for VANETs. In 2008, Zhu et al. (8) proposed an aggregated emergency message authentication (AEMA) scheme to validate an emergency event. The scheme makes use of aggregation and batch verification techniques to reduce the computation overhead. Zhu et al.'s scheme (8) is based on certificate-based public key cryptography. Therefore, aggregation and batch verification in Zhu et al.'s scheme (8) have two parts, certificates and signatures.

In order to simplify the certificate management as in traditional public key infrastructure (PKI), Shamir (9) proposed identity-based public key cryptography (ID-PKC) in 1984. In ID-PKC, an entity's public key is derived directly from certain aspects of its identity. Private keys are generated for entities by a trusted third party called a private key generator (PKG). Therefore, the entity's private key fully depends on its public known identity and the master secret owned by the PKG. Obviously, ID-PKC suffers from the key escrow problem, i.e., the dishonest PKG can forge the signature of any entity; meanwhile, the entity can deny the signature actually signed by itself.

To overcome the key escrow problem of ID-PKC, Al-Riyami and Paterson (10) proposed a new paradigm called certificateless public key cryptography (CL-PKC). In CL-PKC, a trusted third party called a key generation center (KGC) helps the entity to compute a partial private key from the entity's identity and the KGC's master key. The entity then combines the partial private key with a secret value to generate its actual private key. Thus, the entity's private key is not available to the KGC. The entity's public key is also computed from the KGC's public parameters together with the entity's secret value. The CL-PKC scheme overcomes the key escrow problem in ID-PKC and does not require the use of certificates to guarantee the authenticity of public keys.

In this paper, we propose a secure aggregated message authentication (SAMA) scheme in certificateless public key settings to validate emergency messages in VANETs. The proposed SAMA scheme enhances Zhang and Zhang's scheme (11) to reduce the computation overhead. In the SAMA scheme, the entity makes use of its partial private key generated by the KGC and the private key chosen by itself to generate the signatures on the emergency messages. Due to the characteristics of CL-PKC, the SAMA scheme only needs signature aggregation and batch verification. Compared to Zhu et al.'s scheme (8), the SAMA scheme achieves more efficient authentication on emergency messages.

Privacy preservation is another important security requirement for VANETs, where the source privacy of the emergency message is envisioned to emerge as a critical security issue since privacy-sensitive information, such as the driver's name, position, and driving route, could be jeopardized (4). Therefore, how to preserve the privacy of vehicles is regarded as a fundamental security requirement in VANET communications. However, a malicious driver may abuse the privacy protection by damaging the regular driving environment, such as escaping from the investigation when he involved in a dispute event of emergency messages. Therefore, the privacy preservation in VANETs should be conditional, i.e., senders are anonymous to receivers while traceable by the KGC, namely conditional privacy preservation (4). With traceability, once a dispute occurs to the emergency message, the KGC can reveal the identities of the vehicles.

Moreover, Petri nets (12) 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 scheme. Our analysis shows that the proposed scheme can successfully defend forgery attacks and ensure the conditional privacy preservation and traceability of the vehicles.

The rest of this paper is organized as follows: In Section II, we state the concept of bilinear pairings and introduce the mathematical problems used in this paper. Next, the proposed SAMA scheme is presented in Section III. Then, we shall present the security analysis of our SAMA scheme and provide a performance comparison with other aggregated signature schemes in Section IV. Finally, we will conclude our paper in Section V.

PRELIMINARIES

In this section, we first briefly state the concepts of bilinear pairings and introduce the mathematical problems needed for our proof of security. The notations with their meanings throughout this paper are listed in Table 1.

Bilinear Pairings

Let $\mathbb{G}_1$ be a cyclic additive group of 160-bit prime order q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order. A map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is called a bilinear map if it satisfies the following properties:

1. Bilinearity: $e(Q, W + Z) = e(Q, W)e(Q, Z)$ and $e(Q + W, Z) = e(Q, Z)e(W, Z)$, for all $Q, W, Z \in \mathbb{G}_1$.
2. Non-degeneracy: There exists $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for $P, Q \in \mathbb{G}_1$.

Mathematical Problems

Now we specify the mathematical difficult problems used in this paper as follows.

Definition 1. Discrete Logarithm Problem (DLP). Given a prime p, a generator g of $\mathbb{Z}_p^*$, and an element $\beta \in \mathbb{Z}_p^*$, the DLP is to find the integer α, $0 \leq \alpha \leq p-2$, such that $g^\alpha \equiv \beta \pmod{p}$.

Definition 2. Elliptic Curve Discrete Logarithm Problem (ECDLP). Given a group $\mathbb{G}_1$ of prime order q, two elements P and Q, the ECDLP is to find an integer $l \in \mathbb{Z}_q^*$, such that $Q = lP$ whenever such an integer exists.

Table 1: Notations.

Symbol	Definition
KGC	A key generation center
$\mathcal{V}_j$	The j-th vehicle
ID_j	A real-identity of the vehicle $\mathcal{V}_j$
PID_j	A pseudo-identity of the vehicle $\mathcal{V}_j$
$\mathbb{G}_1$	A cyclic additive group
$\mathbb{G}_2$	A cyclic multiplicative group
q	The order of the groups $\mathbb{G}_1$ and $\mathbb{G}_2$
e	$e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
s	A master key of the KGC
P_{pub}	A public key of the KGC
(x_j, D_j)	A private key of the vehicle $\mathcal{V}_j$
PK_j	A public key of the vehicle $\mathcal{V}_j$
$\mathcal{E}_i$	The emergency event i
SER_j^i	The secure emergency report generated by the vehicle $\mathcal{V}_j$ for the emergency event $\mathcal{E}_i$
$Type_i$	The type of the emergency event $\mathcal{E}_i$
Loc_i	The location where the emergency event $\mathcal{E}_i$ takes place
$Time_j^i$	The time when the vehicle $\mathcal{V}_j$ makes the report on the emergency event $\mathcal{E}_i$
Sig_j^i	The signature generated by the vehicle $\mathcal{V}_j$ on the emergency event $\mathcal{E}_i$
$Enc(\cdot)$	A secure symmetric encryption algorithm (13)
$Dec(\cdot)$	A secure symmetric decryption algorithm (13)
$H_1(\cdot)$	A hash function such as $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_2(\cdot)$	A hash function such as $H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_3(\cdot)$	A hash function such as $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
$\|\|$	Message concatenation operation

THE PROPOSED SCHEME

In this section, the SAMA scheme is presented. The scheme is divided into four phases: system setup, registration, signature generation, and aggregated authentication.

System Model

Assume the inter-vehicle communication (IVC) in VANETs without any presence of fixed infrastructure such as access points (APs), road side units (RSU), and satellite communication for assisting in data propagation. The medium used for communication among vehicles is based on 5.9 GHz Dedicated Short Range Communications (DSRC) protocol identified as IEEE 802.11p (14). We assume that there is a KGC which is in charge of generating a vehicle's partial private key. The full private key is finally generated by the vehicle that makes use of the partial private key obtained from the KGC and the secret information chosen by itself. The system model is illustrated in Figure 1.

Security Requirements

The inter-vehicle communication in VANETs is subject to the security requirements: message authentication, conditional privacy preservation, and traceability.

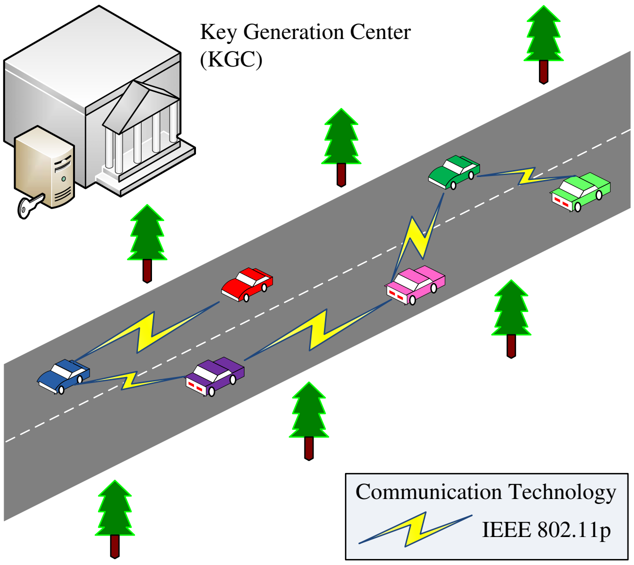

Figure 1: The system model of the SAMA scheme.

- **Message authentication** Similar to wireless sensor networks (15; 16), the major threat that can target specifically VANET aggregation schemes is that of false information dissemination, where attacker's goal is to make the vehicles to accept false emergency reports. Therefore, emergency messages from vehicles have to be authenticated to confirm that they are indeed sent unaltered.

- **Conditional privacy preservation** Privacy preservation is regarded as a fundamental security requirement in VANET communications since overhearing privacy-sensitive information could happen frequently. However, privacy protection may be abused by malicious drivers. Therefore, conditional privacy preservation should be provided in VANETs, i.e., senders are anonymous to receivers while traceable by the KGC, such that the identities can be uniquely revealed by the KGC under exceptional cases.

- **Traceability** The KGC should have the ability to retrieve a vehicle's real-identity from its pseudo-identity once a dispute occurs to the emergency message.

System Setup

Prior to the network deployment, the KGC sets up the system parameters as follows:

1. Let $\mathbb{G}_1$ be a cyclic additive group generated by P with a prime order q, and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map.

2. The KGC first chooses a random number $s \in \mathbb{Z}_q^*$ as its master key and sets $P_{pub} = sP$ as its public key.

3. The KGC defines hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$, and $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, and a secure symmetric encryption algorithm $Enc(\cdot)$ (13).

4. The KGC publishes the system parameters $(\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_1(\cdot), H_2(\cdot), H_3(\cdot), Enc(\cdot))$.

Additionally, the format of a security emergency report (SER) (8) is also defined by the KGC. For an emergency event $\mathcal{E}_i$, the vehicle V_j generates a SER_j^i as follows:

$$SER_j^i = (Type_i, Loc_i, PID_j, Time_j^i, Sig_j^i, PK_j) \tag{1}$$

Note that for a specific emergency event $\mathcal{E}_i$, it is assumed that the relevant SERs will share the same $Type_i$ and Loc_i. For the detailed definition of each component of a SER, please refer to Table 1.

Registration

Prior to join the VANET, each vehicle has to register to the KGC. Suppose a new vehicle $\mathcal{V}_j$ with the identity ID_j wants to register with a KGC for IVC services. The details are presented as follows.

1. $\mathcal{V}_j$ sends ID_j to the KGC through an existing secure channel.
2. Upon receiving ID_j, the KGC first checks its validity. If ID_j is valid, the KGC uses the master key s to encrypt the real-identity ID_j into a pseudo-identity PID_j as follows.
$$PID_j = Enc_s(ID_j) \tag{2}$$
3. The KGC generates the partial private key D_j as follows.
$$D_j = sQ_j \tag{3}$$
where $Q_j = H_1(PID_j)$.
4. The KGC sends the pseudo-identity PID_j and the partial private key D_j back to $\mathcal{V}_j$ over a secure channel.
5. After receiving PID_j and D_j, V_j chooses a random number $x_j \in \mathbb{Z}_q^*$, sets its full private key as (x_j, D_j), and computes its public key PK_j as follows.
$$PK_j = x_jP \tag{4}$$

Signature Generation

When an emergency event $\mathcal{E}_i$ is sensed by the vehicle j and the observation is $(Type_i, Loc_i, Time_j^i)$, $\mathcal{V}_j$ generates a SER as follows.

1. $\mathcal{V}_j$ computes a pair (W_i, S_j) as follows.
$$W_i = H_2(Type_i \| Loc_i) \tag{5}$$
$$S_j = H_3(Type_i \| Loc_i \| Time_j^i \| PID_j \| PK_j) \tag{6}$$
where W_i is the hash value of the event statement and S_j is the hash value of the event statement binding the vehicle $\mathcal{V}_j$'s pseudo-identity and public key.
2. With the private key (x_j, D_j), $\mathcal{V}_j$ generates the signature Sig_j^i on (W_i, S_j) as follows.
$$Sig_j^i = D_jS_j + x_jW_i \tag{7}$$

Thus, $(Type_i, Loc_i, PID_j, Time_j^i, Sig_j^i, PK_j)$ constitutes a SER claim. After that, $\mathcal{V}_j$ broadcasts SER_j^i to its neighbors.

Given $SER_j^i = (Type_i, Loc_i, PID_j, Time_j^i, Sig_j^i, PK_j)$, a single SER verification can be performed by a verifier as follows.

1. The verifier first computes a triple (Q_j, W_i, S_j) as follows.

$$Q_j = H_1(PID_j) \tag{8}$$

$$W_i = H_2(Type_i \| Loc_i) \tag{9}$$

$$S_j = H_3(Type_i \| Loc_i \| Time_j^i \| PID_j \| PK_j) \tag{10}$$

2. After that, the verifier checks the validity of the signature as follows.

$$e(Sig_j^i, P) \overset{?}{=} e(Q_j S_j, P_{pub}) e(W_i, PK_j) \tag{11}$$

If equation (11) holds, the signature is accepted. The correctness of equation (11) can be checked as follows:

$$\begin{aligned} e(Sig_j^i, P) &= e(D_j S_j + x_j W_i, P) \\ &= e(D_j S_j, P) e(x_j W_i, P) \\ &= e(s Q_j S_j, P) e(W_i, x_j P) \\ &= e(Q_j S_j, sP) e(W_i, x_j P) \\ &= e(Q_j S_j, P_{pub}) e(W_i, PK_j) \end{aligned} \tag{12}$$

Aggregated Authentication

Aggregated authentication consists of two parts, signature aggregation and batch verification. The detailed procedures are presented as below.

- **Signature aggregation** For a specific emergency event $\mathcal{E}_i$, any vehicle can act as an aggregate signature generator, namely aggregator, who can aggregate a collection of individual signatures that have the same event statement, $Type_i$ and Loc_i. Given n SERs, where $SER_j^i = (Type_i, Loc_i, PID_j, Time_j^i, Sig_j^i, PK_j)$ by $\mathcal{V}_j (1 \leq j \leq n)$, the aggregator can obtain SER_{agg} as follows.

$$\begin{aligned} SER_{agg} = \; & (Type_i, Loc_i, PID_1, PID_2, \ldots, PID_n, \\ & Time_1^i, Time_2^i, \ldots, Time_n^i, \\ & Sig_1^i, Sig_2^i, \ldots, Sig_n^i, \\ & PK_1, PK_2, \ldots, PK_n) \end{aligned} \tag{13}$$

Then the aggregator computes Sig_{agg} as follows.

$$\begin{aligned} Sig_{agg} &= \sum_{j=1}^{n} Sig_j^i \\ &= \sum_{j=1}^{n} (D_j S_j + x_j W_i) \end{aligned} \tag{14}$$

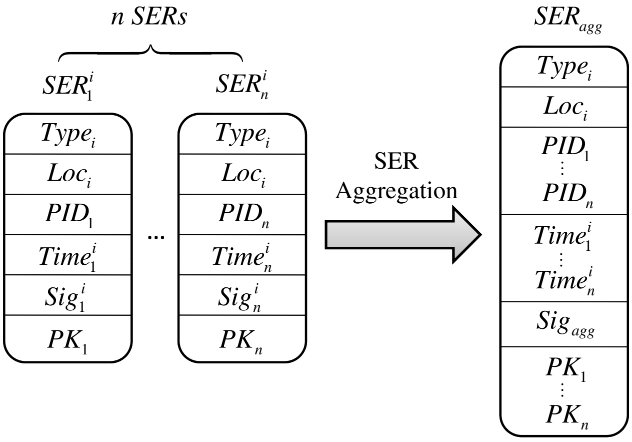

Figure 2: SER aggregation.

Now the aggregator obtains SER_{agg} as follows.

$$\begin{aligned} SER_{agg} \quad = \quad & (Type_i, Loc_i, PID_1, PID_2, \ldots, PID_n, \\ & Time_1^i, Time_2^i, \ldots, Time_n^i, \\ & Sig_{agg}, PK_1, PK_2, \ldots, PK_n) \end{aligned} \tag{15}$$

The aggregation procedure is illustrated in Figure 2.

- **Batch verification** Given the aggregate signature Sig_{agg} and the message set SER_{agg}, the aggregator computes a triple (Q_j, W_i, S_j) for $1 \leq j \leq n$ as follows.

$$Q_j = H_1(PID_j) \tag{16}$$

$$W_i = H_2(Type_i \| Loc_i) \tag{17}$$

$$S_j = H_3(Type_i \| Loc_i \| Time_j^i \| PID_j \| PK_j) \tag{18}$$

After that, the aggregator checks the validity of the aggregate signature as follows.

$$e(Sig_{agg}, P) \stackrel{?}{=} e(\sum_{j=1}^{n} Q_j S_j, P_{pub}) e(W_i, \sum_{j=1}^{n} PK_j) \tag{19}$$

If equation (19) holds, the aggregate signature is accepted. The correctness of equation (19) can be checked as follows:

$$\begin{aligned} e(Sig_{agg}, P) \quad &= \quad e(\sum_{j=1}^{n}(D_j S_j + x_j W_i), P) \\ &= \quad e(\sum_{j=1}^{n} sQ_j S_j, P) e(\sum_{j=1}^{n} x_j W_i, P) \\ &= \quad e(\sum_{j=1}^{n} Q_j S_j, sP) e(W_i, \sum_{j=1}^{n} x_j P) \\ &= \quad e(\sum_{j=1}^{n} Q_j S_j, P_{pub}) e(W_i, \sum_{j=1}^{n} PK_j) \end{aligned} \tag{20}$$

Table 2: Formal definition of a Petri net.

A Petri net is a 5-tuple, (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).

ANALYSIS OF THE SAMA SCHEME

In this section, we show that the SAMA scheme can resist forgery attacks and ensure the conditional privacy preservation and traceability of vehicles. In addition, we provide a performance comparison with other aggregate signature schemes for VANETs.

Security Analysis

We shall use Petri nets (12) to model and analyze the proposed scheme. Next, security properties of our scheme will be specified.

Petri Net Model

We used a Petri net to model the SER generation of the SAMA scheme. The formal definition of a Petri net (17) is listed in Table 2. 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. The directed 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 is illustrated in Figure 3. The definitions of the places and transitions used in this model are listed in Table 3 and Table 4, respectively. We use the HPSim Petri net tool (18) to model our proposed scheme.

Security Properties

We now analyze the security properties of our scheme. The security of the proposed scheme is based on the difficulty of ECDLP, which is believed infeasible to solve in polynomial time. We will show that our scheme can resist forgery attacks and ensure the conditional privacy preservation and traceability of vehicles.

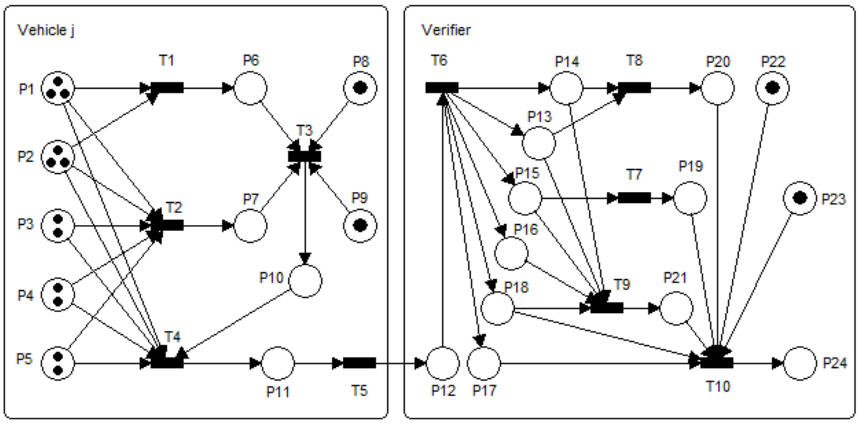

Figure 3: A Petri net model of the SER generation of the SAMA scheme.

Table 3: Definitions of places.

Place	Definition	Place	Definition
P_1	$Type_i$	P_{13}	$Type_i$
P_2	Loc_i	P_{14}	Loc_i
P_3	PID_j	P_{15}	PID_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}	Success verification message

Theorem 1. *The proposed scheme can resist a forgery attack.*

Proof. If an adversary $\mathcal{A}$ wants to forge the vehicle $\mathcal{V}_j$ to produce a valid signature on the emergency event $\mathcal{E}_i$; according to the SER generation phase, $\mathcal{A}$ first computes a pair (W_i^*, S_j^*) as follows.

$$W_i^* = H_2(Type_i^* \| Loc_i^*) \tag{21}$$

$$S_j^* = H_3(Type_i^* \| Loc_i^* \| Time_j^{i*} \| PID_j \| PK_j) \tag{22}$$

After that, $\mathcal{A}$ generates the signature Sig_j^{i*}, where

$$Sig_j^{i*} = D_j S_j^* + x_j W_i^* \tag{23}$$

However, $\mathcal{A}$ cannot compute a valid signature unless $\mathcal{A}$ can obtain D_j and also derive x_j from PK_j. Based on the difficulty of ECDLP, it is computationally infeasible to compute x_j from PK_j. As shown in Figure 3, computing Sig_j^i is defined in transition T_3, which has four input places, P_6, P_7, P_8, and P_9. Place P_8 is the value of D_j and place P_9 is the value of x_j. Because having no idea about D_j and x_j, $\mathcal{A}$ cannot compute a valid signature and hence cannot launch a forgery attack. □

Table 4: Definitions of transitions.

Trans.	**Definition**	**Trans.**	**Definition**
T_1	Compute W_i	T_6	Split SER_j^i
T_2	Compute S_j	T_7	Compute Q_j
T_3	Compute Sig_j^i	T_8	Compute W_i
T_4	Constitute SER_j^i	T_9	Compute S_j
T_5	Transmit SER_j^i	T_{10}	Check $e(Sig_j^i, P) \overset{?}{=} e(Q_jS_j, P_{pub})e(W_i, PK_j)$

Theorem 2. *The proposed scheme can ensure the conditional privacy preservation of vehicles.*
Proof. In the SAMA scheme, we propose to use pseudo-identities to preserve the identity privacy of witness vehicles. Since the vehicle $\mathcal{V}_j$ uses the pseudo-identity PID_j during its communication with other vehicles, the real-identity ID_j is protected. As shown in Figure 3, constituting SER_j^i and broadcasting SER_j^i to the verifier are defined in transition T_4 and T_5, respectively. Transition T_4 has six input places, P_1, P_2, P_3, P_4, P_5, and P_{10}. Place P_3 is the value of PID_j. However, only the KGC has the ability to trace the real-identity from the pseudo-identity PID_j. Hence, the conditional privacy preservation can be satisfied in the proposed scheme. □

Theorem 3. *The proposed scheme can provide the traceability of vehicles.*
Proof. Given the pseudo-identity PID_j, only the KGC, with the master key s, can trace the real-identity as follows.

$$\begin{aligned} Dec_s(PID_j) &= Dec_s(Enc_s(ID_j)) \\ &= ID_j \end{aligned} \tag{24}$$

Therefore, once a dispute occurs to the emergency message, the KGC has the ability to reveal the real-identity of the vehicle from the disputed message, in which the traceability can be achieved. □

Performance Evaluation

We use the computation and communication overhead as the metric to evaluate the performance of the proposed SAMA scheme. The evaluation parameters are defined in Table 5. The performance comparison between Zhu et al.'s scheme (8) and the SAMA scheme is presented in Table 6. According to the implementation results in (19), which observes processing time (in milliseconds) for an MNT curve of embedding degree $k = 6$ and 160-bit q, running on an Intel Pentium IV 3.0 GHz machine, T_P is 4.5 ms and T_M is 0.6 ms. Therefore, elliptic curve point multiplication operations are much cheaper in comparison to pairing operations.

From Table 6, Zhu et al.'s scheme (8) requires five pairings for verifying n distinct signatures and certificates; however, in the SAMA scheme, it requires only three pairings for verifying n distinct signatures without certificates. Therefore, our proposed scheme achieves better time efficiency than Zhu et al.'s scheme (8).

Table 5: Evaluation parameters.

Symbol	Definition
T_H	Time for performing a one-way hash function
T_E	Time for performing an exponentiation operation
T_P	Time for performing a bilinear pairing operation
T_M	Time for performing an elliptic curve point multiplication operation
T_A	Time for performing an elliptic curve point addition operation
T_{ENC}	Time for performing a symmetric encryption operation

Table 6: Performance comparison of aggregate signature schemes for VANETs.

	Zhu et al.'s scheme (8)	SAMA scheme
Registration	$1T_H + 2T_E$	$1T_H + 2T_M + 1T_{ENC}$
Sig. generation	$3T_H + 2T_E + 2T_M$	$2T_H + 2T_M + 1T_A$
Sig. verification	$4T_H + 1T_E + 5T_P$	$3T_H + 3T_P + 1T_M$
Sig. aggregation	$2(n-1)T_M$	$(n-1)T_A$
Batch verification	$(n+3)T_H + nT_E + 5T_P + 4(n-1)T_M$	$(2n+1)T_H + 3T_P + nT_M + 2(n-1)T_A$

Table 7: Broadcasting message format from a vehicle to its neighbors.

Component	$Type_i$	Loc_i	PID_j	$Time_j^i$	Sig_j^i	PK_j
Size (Bytes)	8	8	8	8	40	40

The communication overhead is in terms of the following aspect: the overhead incurred by broadcasting a SER from a vehicle to other vehicles within its transmission range. In our analysis, we assume the size of the element in $\mathbb{G}_1$ is 160-bit. The approximated length of the SER is shown in Table 7. $Type_i, Loc_i, PID_j$, and $Time_j^i$ each costs 8 bytes. The fifth part is the 40-byte signature on the emergency event and the last part is the public key of the vehicle, which also costs 40-byte. Thus, the communication overhead incurred by broadcasting a SER from a vehicle to its neighbors is 112 bytes.

CONCLUSIONS

In this paper, we propose a secure aggregated message authentication (SAMA) scheme based on bilinear pairings for VANETs. The SAMA scheme makes use of aggregation and batch verification techniques for emergency message verification to reduce the computation overhead. Compared to Zhu et al.'s scheme (8), the SAMA scheme achieves more efficient authentication on emergency messages. Moreover, we used Petri nets in the security analysis of the proposed scheme. Our analysis shows that the proposed scheme can successfully defend forgery attacks and ensure the conditional privacy preservation and traceability of vehicles.

ACKNOWLEDGEMENTS

This work was supported by the National Science Council, Taiwan, Republic of China, under grant NSC 97-2221-E-009-048-MY3, NSC 97-2221- E-009-049-MY3, and NSC 96-2628-E-009-014-MY3.

REFERENCES

(1) 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.

(2) 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.

(3) M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, 2007, pp. 39–68.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) A. Shamir, "Identity based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology*, 1984, pp. 47–53.

(10) S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of the ASIACRYPT*, 2003, pp. 452–473.

(11) L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Computer Communications*, vol. 32, no. 6, Apr. 2009, pp. 1079–1085.

(12) C. A. Petri, *Kommunikation mit automaten.* PhD thesis, University of Bonn, 1962.

(13) D. R. Stinson, *Cryptography: Theory and practice.* Boca Raton, FL, Chapman & Hall/CRC, 2006.

(14) "IEEE 802.11p, Amendment 6: Wireless access in vehicular environments (WAVE)," 2010.

(15) L. Hu and D. Evans, “Secure aggregation for wireless networks,” in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT 2003)*, Jan. 2003, pp. 384–391.

(16) Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: A secure hop-by-hop data aggregation protocol for sensor networks,” *ACM Transactions on Information and System Security*, vol. 11, no. 4, Jul. 2008.

(17) T. Murata, “Petri nets: Properties, analysis and applications,” *Proceedings of the IEEE*, vol. 77, no. 4, Apr. 1989, pp. 541–580.

(18) “HPSim 1.1 Petri nets simulation tool, copyright© 1999-2002 Henryk Anschuetz.”

(19) M. Scott, “Efficient implementation of crytographic pairings,” [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf.