An Efficient and Secure Authentication Scheme for Vehicle Sensor Networks

Jiani Zhang[1], Debiao He[1], Neeraj Kumar[2], Kim-Kwang Raymond Choo[3]

[1] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, China
[2] Department of Computer Science and Engineering, Thapar University, India
[3] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, USA
{zhangjiani, hedebiao}@163.com, nehra04@yahoo.co.in, raymond.choo@fulbrightmail.org

Abstract

Vehicle sensor networks (VSNs) have applications in intelligent transportation system and smart cities, as they enable vehicles to exchange information for improving traffic security and efficiency. However, VSNs are also subject to a broad range of attacks, including those typically associated with wireless networks. While a large number of authentication schemes have been proposed in the literature, most of these schemes failed to achieve the claimed security attributes. For example, Zhou et al. (2017) proposed a trust-extended authentication scheme for VSNs. However, their scheme cannot provide user anonymity or security against several known attacks as claimed. Thus, we construct a new authentication scheme based on Elliptic Curve Cryptography (ECC), and demonstrate our scheme is secure in the random oracle model. We also show that our scheme can satisfy a number of security requirements. Finally, findings from the performance evaluation suggest that our scheme is more practical for VSNs deployment.

Keywords: Vehicle Sensor Networks, Vehicle-to-vehicle, Provable security, ECC-based authentication

1 Introduction

In recent years, techniques such as vehicle sensor networks (VSNs) [1-4], cloud computing [5-7] have developed rapidly. Especially, vehicle sensor networks (VSNs), have gained traction among researchers and those involved in intelligent transportation system and smart city planning and development. This is not surprising, since VSNs can facilitate interactions between vehicles (e.g. exchange of information such as location, speed, and road conditions); thus, contributing to better management of traffic congestion and driver/road safety.

A typical VSNs can consist of two communication models [8], namely: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) – see Figure 1. In such an infrastructure, each vehicle is equipped with an On-Board-Unit (OBU), which includes an event data recorder (EDR) and a tamper-proof device (TPD). Here, EDR is used for recording critical data (e.g. preloaded parameters and secret keys), and TPD is designed to prevent attackers from obtaining secret information in OBU. A dedicated short range communication (DSRC) protocol is used for communication among vehicles.

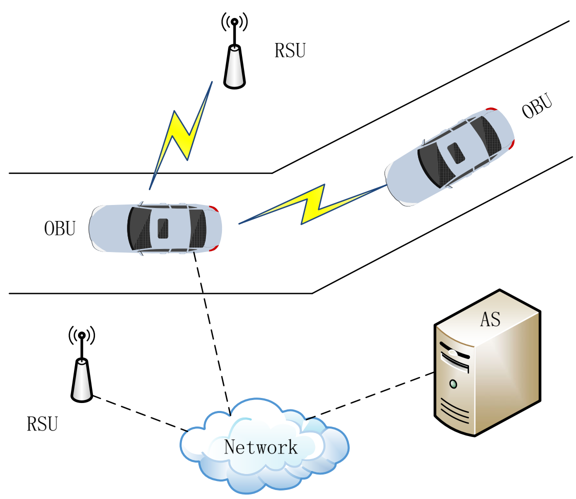

Figure 1. Example structure of VSNs

Specifically, all vehicles will periodically broadcast two kinds of messages, namely: traffic conditions (including degree of crowding, and weather conditions) and vehicles status (including speed, distance, and location). Vehicles nearby can execute analysis on these messages and adjust speed or routes, with the aims of avoiding traffic accidents and/or minimizing traffic congestion. Besides, Road Side Units (RSUs) can send relevant messages to traffic control center. The latter will then formulate traffic-related management responses/strategies based on the

*Corresponding Author: Debiao He; E-mail: hedebiao@163.com
DOI: 10.3966/160792642019032002029

information received. Additionally, authentication server (AS) can be utilized to remotely authenticate vehicles and RSUs.

Although the use of VSNs greatly enhance traffic security and efficiency in intelligent transportation system, it is subject to various attacks [9-10] due to the inherent properties in VSNs (e.g. wireless channel instability and insecurity, and dynamic topological structure). Besides, all vehicles need to reveal their identity and location when communicating with others in the wireless network [11-12]. Therefore, authentication schemes with anonymity [13-16] are necessary to address the above security and privacy concerns [17]. Additionally, low computation cost should be part of the design requirement, particularly for deployment in fast-moving scenarios.

A large number of authentication schemes have been proposed for vehicle communication in VSNs, although the design of secure schemes has been shown to be challenging. One such recent scheme is that of Zhou et al [18]. Specifically, the authors proposed a trusted-extend authentication scheme. However, the scheme cannot provide user anonymity and with stand common attacks i.e. impersonate attack, modification attack, replay attack, and man-in-the-middle attack. Therefore, we propose a new authentication scheme based on [18] to facilitate secure vehicle communication within VSNs.

1.1 Our Contributions

In this paper, we design an efficient and secure authentication scheme for VSNs based on [18]. The main contributions of our scheme are listed as follows.

- We present our authentication scheme and execute rigorous analysis in the random oracle model. Additionally, informal secrecy proof proves that our scheme could resist various attacks and meet security requirements for VSNs.
- We execute the performance evaluation in terms of security attributes and computation overhead. The results show that our scheme is feasible for VSNs deployment.

1.2 Organization

The remainder of this paper is organized as follows. In Sections 2 and 3, we will discuss related literature and relevant background materials. In Sections 4 and 5, we present our proposed scheme and validate its security, respectively. Performance evaluation, in terms of security attributes and computation cost, is presented in Section 6. The paper concludes in Section 7.

2 Related Work

As previously discussed, designing authentication schemes for secure vehicle communication in VSNs is not a new research area. For example, as early as 2007, Raya et al. [19] proposed an authentication scheme in which vehicles employed new keys in every authentication phase to provide unlinkability of messages. However, the limitations associated with this scheme are significant storage and management overheads. Lu et al. [20] proposed a conditional privacy preservation authentication (CPPA) scheme using anonymous certificates, where each vehicle is issued a short-term anonymous certificate when it passes a RSU. Thus, such a scheme has low efficiency due to frequent interaction between vehicles and RSUs. To overcome the weakness in [20], Freudiger proposed an improved CPPA scheme. However, in this latter scheme, vehicles have to store a large number of anonymous certificates. Thus, this incurs significant storage costs on the vehicles. Later, Sivagurunathan et al. [21] introduced a distributed trust based authentication scheme for a cluster environment, based on threshold cryptography. In a separate work, Porambage et al. [22] proposed an authentication scheme for sensor networks using certificates. However, the scheme cannot ensure the unlinkability of messages. Other schemes based on bilinear pairing that had been proposed in the literature, such as those reported in [23-25], suffered from a number of limitations and weaknesses (e.g. significant computational costs and security vulnerabilities).

In 2014, Chuang et al. [26] proposed a trust-extended authentication scheme. However, their scheme cannot resist impersonation attack, since the real identity of a user could be obtained. Moreover, there exist message linkability. Kumari et al. [27] proposed a scheme, designed to be resilient to internal attacks. Later, Zhou et al. [18] proposed an improved authentication scheme based on [27], but their scheme fails to provide user anonymity, and is subject to impersonation attack, modification attack etc. Thus, this partially motivates the research in designing a provably secure scheme for VSNs.

3 Preliminaries

3.1 Elliptic Curve

We define $y^2 \equiv x^3 + ax + b \bmod p$ a non-singular elliptic curve over F_P, where p is a prime, $F_p = \{0,1,\cdots p-1\}$, $a,b \in F_p$ and $4a^3 + 27b^2 \bmod p \neq 0$.

Definition1 (Elliptic Curve Point Addition). Suppose that $Q_1 = (x_1, y_1)$, $Q_2 = (x_2, y_2)$, $Q_1, Q_2 \in G$, where G is a cyclic group generated by a point P, then we have: $Q_3 = (x_3, y_3) = Q_1 + Q_2$, where:

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p \quad \textbf{(1)}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p \quad \textbf{(2)}$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & Q_1 \neq Q_2 \\ \frac{3x_1^2 + a}{2y_1} \bmod p & Q_1 = Q_2 \end{cases} \quad \textbf{(3)}$$

Definition2 (Elliptic Curve Point Multiplication). Suppose that $Q \in G$, where G is a cyclic group generated by a point P, then we have,

$$5Q = Q + Q + Q + Q + Q \quad \textbf{(4)}$$

Definition3 (Elliptic Curve Diffie-Hellman (ECDH) Assumption). Suppose that $Q = a \cdot P,\ Q, P \in G,$ where G is a cyclic group generated by a point P, then ECDH assumption is that it is computationally infeasible to compute a.

Definition4 (Elliptic Curve Computational Diffie-Hellman (ECCDH) Assumption). Suppose that $Q_1, Q_2 \in G$, $Q_1 = a \cdot P$, $Q_2 = b \cdot P$, where G is a cyclic group generated by a point P, then ECCDH assumption is that it is computationally infeasible to compute $Q_3 = abP$.

3.2 Security and Privacy Requirements

Based on the above reviews, the security and privacy requirements in VSNs are as follows:

- Message authentication: Vehicles and RSUs can verify the validity of received messages and identify the modification.
- Identity anonymity: Attackers cannot obtain the real identity of vehicles by intercepting messages over public channel.
- Message unlinkability: Attackers cannot distinguish whether two messages are sent by the same vehicle.
- Session key agreement: Vehicles will produce a session key to establish a secure session. The session key is used for protecting transmitted messages over public channel.
- Forward secrecy: The leakage of private key of one or more vehicles will not affect security of the previous session key.
- Resistance to attacks: The authentication scheme should resist various attacks (e.g. impersonation attack, modification attack, replay attack, man-in-the-middle attack etc.).

4 The Proposed Scheme

In our proposed scheme, there exist three types of vehicles. The detailed description are as follows and notions are listed in Table 1.

- Law Executors (LE): a kind of permanently-trusted vehicle. It obtains key set and parameters and can authenticate mistrusted vehicles. It is the only one type of vehicles equipped with TPD.

Table 1. Notations

Notation	Definition
p	a large prime
P	a generator of G
G	a cyclic group generated by a point P
Z_p^*	the set consisting of all primes in $\{0,1,\cdots,p-1\}$
r	a randomly selected number from Z_p^*
x	private key of AS a random number selected by AS
P_{pubi}	public key of U_i
x_i	private key of U_i
psk	a secure key set produced by AS
ID_i	identity of U_i
PW_i	password of U_i
AID_i	alias of U_i
$h()$	secure hash function
$E()/D()$	symmetric key encryption or decryption operation
$\oplus$	XOR operation
$\|\|$	combination of strings
sk	session key
MSG_{KU}	key update messages

- Mistrusted Vehicle (MV): a kind of mistrusted vehicle.
- Trusted Vehicle (TV): a kind of trusted vehicle. A MV transforms to be a TV after getting psk in the authentication phase.

4.1 Setup Phase

In this phase, AS performs initiation procedures and produces several system parameters and private key.

(1) AS chooses a cyclic group G generated by a point P, a prime number p.

(2) AS randomly chooses a number $x \in Z_p^*$ as its secret key.

(3) AS produces a key set $\{psk_i, i = 1, 2, \cdots, n\}$ by the rule as follows: $psk_n = h(nonce)$, $psk_{n-1} = h(h(nonce))$, ..., $psk_1 = h^n(nonce)$. Each psk is valid in specific time. It turns to be invalid when the lifetime expires and should be revoked.

4.2 Registration Phase

4.2.1 LE Registration Phase

In this phase, LE sends a registration request to AS. AS returns a secure key set $\{psk_i, i = 1, 2, \cdots, n\}$ and $\{G, P, p\}$ to LE. Upon receiving the parameters, LE stores them into secure hardware and finishes the registration phase.

4.2.2 Vehicle Registration Phase

In this phase, vehicles obtains private key and public key. As shown in Figure 2, the steps below are executed between them.

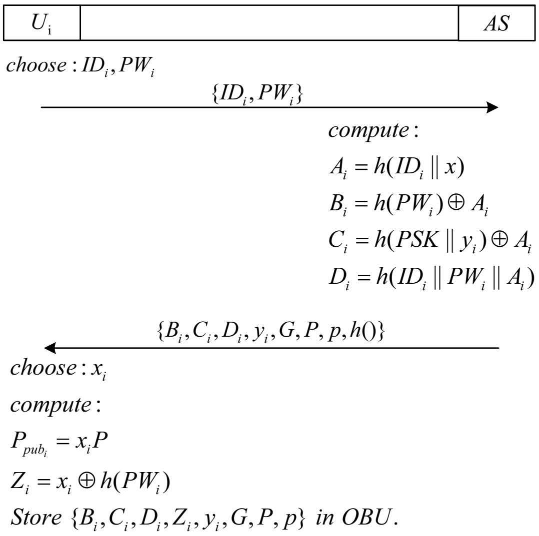

Figure 2. Vehicle registration phase

(1) U_i firstly selects his/he ID_i, PW_i and submits $\{ID_i, PW_i\}$ to AS via trustworthy channel.

(2) AS randomly chooses a number y_i and computes: $A_i = h(ID_i \| x)$, $B_i = h(PW_i) \oplus A_i$, $C_i = h(psk \| y_i) \oplus A_i$, and $D_i = h(ID_i \| PW_i \| A_i)$. Then, AS sends $\{B_i, C_i, D_i, y_i, G, P, p, h()\}$ to U_i.

(3) OBU_i stores $\{B_i, C_i, D_i, y_i, G, P, p, h()\}$ into secure hardware. Then, OBU_i randomly chooses a number x_i as private key, and computes $P_{pubi} = x_i \cdot P$ as public key. Finally, OBU_i computes $Z_i = x_i \oplus h(PW_i)$ and stores $\{Z_i\}$ into secure hardware.

4.3 Mutual Authentication Phase

In this phase, a MV obtains psk and transforms to be a TV. As shown in Figure 3, the steps below are executed between them.

(1) U_i inputs his/her ID_i and PW_i. OBU_i computers $A_i = h(PW_i) \oplus B_i$ and checks whether $D_i = h(ID_i \| PW_i \| A_i)$ holds. If not, the process will be terminated; otherwise, OBU_i randomly chooses a number r_i and computes: $AID_i = E_{h(r_i)}(ID_i)$, $M_1 = E_{h(A_i)}(r_i)$, $M_2 = h(r_i \| AID_i \| C_i \| y_i)$. Finally, OBU_i sends $\{AID_i, M_1, M_2, C_i, y_i\}$ to LE_j.

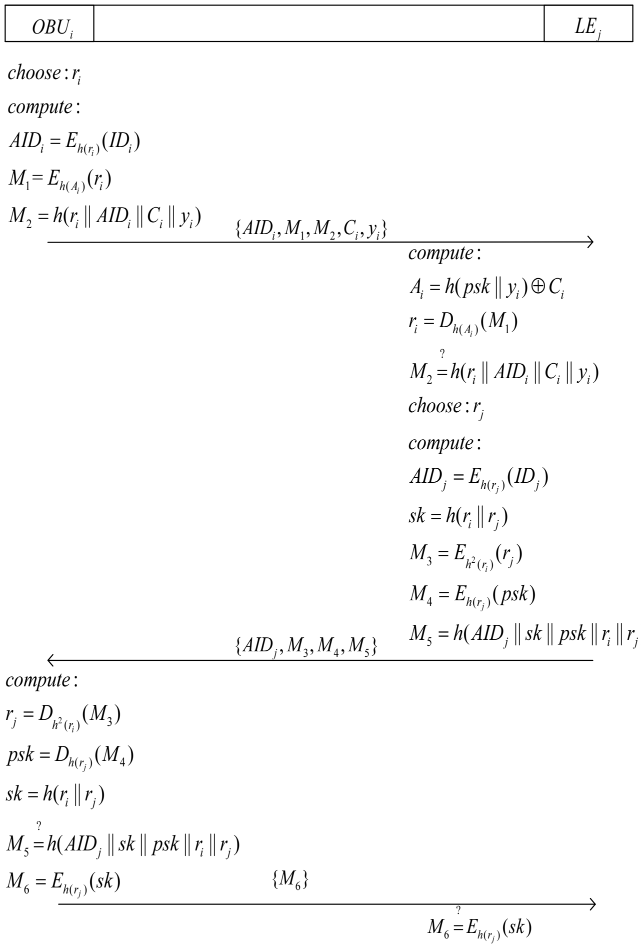

Figure 3. Mutual authentication phase

(2) After receiving $\{AID_i, M_1, M_2, C_i, y_i\}$, LE_j calculates: $A_i = h(psk \| y_i) \oplus C_i$, $r_i = D_{h(A_i)}(M_1)$ and checks whether $M_2 = h(r_i \| AID_i \| C_i \| y_i)$ holds. If not, the process will be terminated; otherwise, LE_j randomly chooses a number r_j and calculates: $AID_j = E_{h(r_j)}(ID_j)$, $sk = h(r_i \| r_j)$, $M_3 = E_{h^2(r_i)}(r_j)$, $M_4 = E_{h(r_j)}(psk)$, and $M_5 = h(AID_j \| sk \| psk \| r_i \| r_j)$. Finally, LE_j sends $\{AID_j, M_3, M_4, M_5\}$ to OBU_i.

(3) After receiving $\{AID_j, M_3, M_4, M_5\}$, OBU_i computes: $r_j = D_{h^2(r_i)}(M_3))$, $psk = D_{h(r_j)}(M_4)$, $sk = h(r_i \| r_j)$ and checks whether $M_5 = h(AID_j \| sk \| psk \| r_i \| r_j)$ holds. If not, the process will be terminated; otherwise, OBU_i computes $M_6 = E_{h(r_j)}(sk)$, $E_i = h(PW_i) \oplus psk$. OBU_i stores E_i in hardware and sends $\{M_6\}$ to LE_j.

(4) After receiving $\{M_6\}$, LE_j checks whether $M_6 = E_{h(r_j)}(sk)$ holds. If not, the process will be terminated; otherwise, OBU_i finishes the authentication phase.

4.4 Trusted-extended Authentication Phase

In this phase, a TV transformed from a MV can act as LE and authenticate other MVs. The procedures are the same as in the mutual authentication phase.

4.5 Secure Communication Phase

In this phase, two TVs authenticate each other and establish a secure session. As shown in Figure 4, the steps below are executed between them.

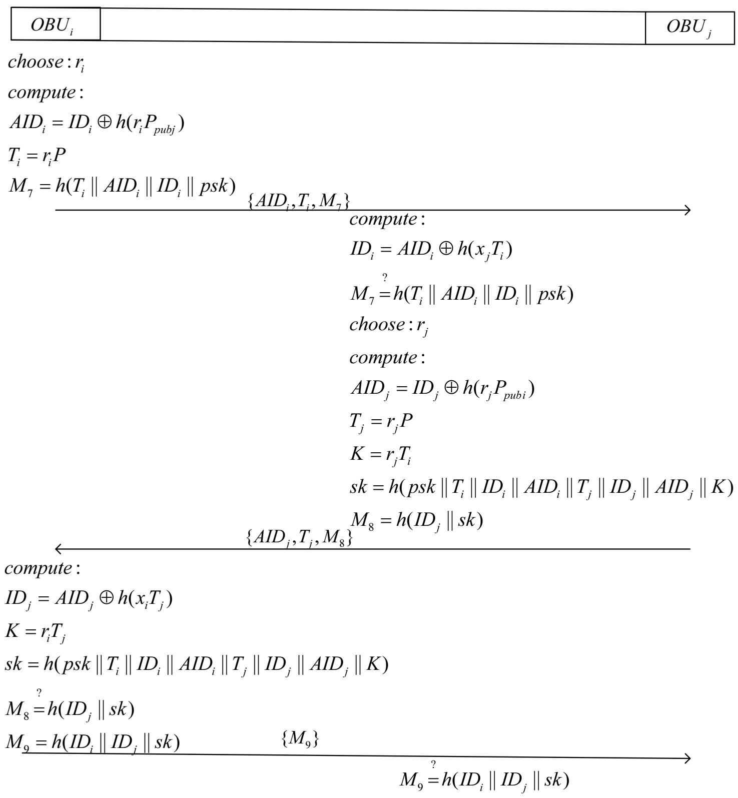

Figure 4. Secure communication phase

(1) OBU_i computes: $psk = E_i \oplus h(PW_i)$, $x_i = Z_i \oplus h(PW_i)$. Then, OBU_i randomly chooses a number r_i and calculates: $AID_i = ID_i \oplus h(r_i \cdot P_{pubj})$, $T_i = r_i \cdot P$, $M_7 = h(T_i \| AID_i || ID_i \| psk)$. Finally, OBU_i sends $\{AID_i, T_i, M_7\}$ to OBU_j.

(2) After receiving $\{AID_i, T_i, M_7\}$, OBU_j computes $ID_i = AID_i \oplus h(x_j \cdot T_i)$, and checks whether $M_7 = h(T_i \| AID_i || ID_i \| psk)$ holds. If not, the process will be terminated; otherwise, OBU_j randomly chooses a number r_j and calculates: $AID_j = ID_j \oplus h(r_j \cdot P_{pubi})$, $T_j = r_j \cdot P$, $K = r_j \cdot T_i$, $sk = h(psk \| T_i \| ID_i \| AID_i \| T_j \| ID_j \| AID_j \| K)$, $M_8 = h(ID_j || sk)$. Then, OBU_j sends $\{AID_j, T_j, M_8\}$ to OBU_i.

(3) After receiving $\{AID_j, T_j, M_8\}$ from OBU_j, OBU_i computes: $ID_j = AID_j \oplus h(x_i \cdot T_j)$, $K = r_i \cdot T_j$, $sk = h(psk \| T_i \| ID_i \| AID_i \| T_j \| ID_j \| AID_j \| K)$. OBU_i then checks whether $M_8 = h(ID_j || sk)$ holds. If not, the process will be terminated; otherwise, OBU_i computes: $M_9 = h(ID_i \| ID_j || sk)$ and sends $\{M_9\}$ to OBU_j.

(4) After receiving $\{M_9\}$, OBU_j checks whether $M_9 = h(ID_i \| ID_j || sk)$ holds. If not, the process will be terminated; otherwise, a secure session has been established with session key: $sk = h(psk \| T_i \| ID_i \| AID_i \| T_j \| ID_j \| AID_j \| K)$.

4.6 Key Update Phase

In this phase, a TV performs key update procedures when the lifetime of psk is approaching expiration; otherwise, we revoke invalid psk. The detailed steps are as follows.

(1) OBU_i randomly chooses a number r_i and computes: $M_1 = psk_{old} \oplus r_i$, $M_2 = psk_{old} \oplus MSG_{KU}$, $M_3 = h(r_i \| MSG_{KU})$. Then, OBU_i sends $\{M_1, M_2, M_3\}$ to LE_j.

(2) After receiving $\{M_1, M_2, M_3\}$, LE_j computes r_i, MSG_{KU} and checks whether $M_3 = h(r_i \| MSG_{KU})$ holds. If not, the process will be terminated; Otherwise,

LE_j randomly chooses a number r_j and computes: $M_4 = r_j \oplus h(r_i)$, $M_5 = psk_{new} \oplus r_j$, $M_6 = h(r_j \| psk_{new})$, $sk = h(r_i \| r_j \| psk_{new})$. Finally, LE_j sends $\{M_4, M_5, M_6\}$ to OBU_i.

(3) After receiving $\{M_4, M_5, M_6\}$, OBU_i calculates: $r_j = M_4 \oplus h(r_i)$, $psk_{new} = M_5 \oplus r_j$ and checks whether $M_6 = h(r_j \| psk_{new})$, $psk_{old} = h(psk_{new})$ holds. If not, the process will be terminated; otherwise, OBU_i renews psk and computes $sk = h(r_i \| r_j \| psk_{new})$. Finally, OBU_i sends $sk \oplus h(r_j)$ to LE_j.

(4) After receiving $sk \oplus h(r_j)$, LE_j computes $h(r_j)$ and verifies the correctness of $h(r_j)$. If true, key update phase has been finished.

5 Security Analysis

5.1 Security Model

In this section, we propose a security model and the security of our scheme is defined by a game played between an adversary A and a challenger C. We denote l the lth instance of U_i. A can execute queries to C and C makes replies as follows.

- $h_i(M_i)$: A executes a query to C with message M_i C generates a random number $r_i \in Z_p^*$ and returns it to A. C records (M_i, r) in the list L_{h_i}.
- $Extract(ID_i)$: A executes a query to C with ID_i. C returns the private key of U_i and stores it in the list L_k.
- $Send(\Pi_{U_i}^l; M_i)$: A executes a query to C with message M_i. C runs the scheme and returns the result to A.
- $Reveal(\Pi_{U_i}^l)$: A executes a query to C. C returns the session key established in $\Pi_{U_i}^l$ to A.
- $Corrupt(ID_i)$: A executes a query to C with ID_i. C returns the private key of U_i to A.
- $Test(\Pi_{U_i}^l)$: C selects a nonce $b \in \{0,1\}$. If $b = 1$, C returns the session key established in $\Pi_{U_i}^l$ to A; Otherwise, C returns a random number of the same length.

We consider A violates the authenticated key agreement (AKA) if he/she can guess b correctly. Suppose that $b^{''}$ corresponds to the session key, the advantage that A violates AKA is defined as :

$$Adv^{AKA}(A) = 2pr[b = b'] - 1 \quad \textbf{(5)}$$

Definition 1 (AKA-secure). We define a scheme is AKA-secure if $Adv^{AKA}(A)$ is negligible for any polynomial adversary A.

We consider A violates the mutual authentication (MA) if he/she can forge legal requests and reply messages. Suppose that E_1 and E_2 be the events that A generates legal request and reply messages respectively, the advantage that A violates MA is defined as:

$$Adv^{MA}(A) = pr[E_1] + pr[E_2] \quad \textbf{(6)}$$

Definition 2 (MA-secure). We define a scheme is MA-secure if $Adv^{MA}(A)$ is negligible for any polynomial adversary A.

5.2 Security Theorems

Theorem 1. In the mutual authentication phase, we assume $|h|$ be the range of hash functions, $|D|$ be the space of passwords. Let A be an adversary against semantic security of the scheme within a time bound t. Then, the advantage of A to violate the mutual authentication phase can be defined as:

$$Adv_{\Pi,D}^{A} \le \frac{q_h^2}{|h|} + \frac{2q_s}{|D|} \quad \textbf{(7)}$$

where q_s is the number of Send query, q_e is the number of Execute query, and q_h is the number of hash query.

Proof. We execute a series of games $G_i (0 \le i \le 4)$ to stimulate the attacks from A. For each G_i, we define $Succi$ be the event that A successfully guesses b in the Test query.

Game 0 In this game, all the instances of OBU_i and LE_j are simulated. According to the definition of event $Succi$ aforementioned, we get:

$$Adv_{\Pi,D}^{A} = 2pr[Succ0] - 1 \quad \textbf{(8)}$$

Game 1 This game is identical to **Game0** except that hash query is simulated by maintaining a hash list $List_h$. Upon receiving a hash query with value x, $List_h$ is searched. If record (x, r) exists, r is returned; Otherwise, it returns a random number r and adds (x, r) in $List_h$. All oracles are simulated in this game, and we consider the game is perfectly indistinguishable from a real execution. Hence,

$$pr[Succ1] = pr[Succ0] \quad \textbf{(9)}$$

Game 2 This game is identical to **Game1** except that the game will be terminated if any collision occurs. Since $\{AID_i, M_1, M_2, C_i, y_i\}$ and $\{AID_j, M_3, M_4, M_5\}$ are transmitted over public channel, according to birthday paradox, the probability of collision in hash oracle is at most $\frac{q_h^2}{2|h|}$. Hence,

$$\left|pr[Succ1]\text{-}pr[Succ2]\right| \le \frac{q_h^2}{2|h|} \quad \textbf{(10)}$$

Game 3 The game is identical to **Game 2** except that the game will be terminated if A can obtain session key without asking oracle h. Hence,

$$\left|pr[Succ2]\text{-}pr[Succ3]\right| \le \frac{q_s}{|D|} \quad \textbf{(11)}$$

Game 4 This game is identical to **Game 3** except that A executes hash queries with the messages $\{AID_i, M_1, M_2, C_i, y_i, AID_j, M_3, M_4, M_5\}$. Since the possibility of correctly guessing b is $\frac{1}{2}$. Thus,

$$pr[Succ3] = \frac{1}{2} \quad \textbf{(12)}$$

According to games above, we obtain:

$$Adv_{\Pi,D}^{A} \le \frac{q_h^2}{|h|} + \frac{2q_s}{|D|} \quad \textbf{(13)}$$

Theorem 2. In the secure communication phase, we assume G be a group with a prime order p, $|D|$ be the space of passwords, and $|h|$ be the range of hash functions. Suppose that A be an adversary against semantic security of the scheme within a time bound t. Then, the advantage of A to violate the secure communication phase can be defined as:

$$Adv_{\Pi,D}^{A} \le \frac{2(q_h+q_e)}{p} + \frac{q_h^2}{|h|} + \frac{(q_s+q_e)^2}{p} + \frac{2q_s}{|D|} + 2q_h Adv_G^{ECCDH}(q_s+q_e) \quad \textbf{(14)}$$

Proof. Similarly, We execute a series of games $G_i(0 \le i \le 6)$ to stimulate the attacks from A. For each G_i, we define $Succi$ be the event that A successfully guesses b in the Test query.

Game 0. In this game, all the instances of OBU_i and OBU_j are simulated as a real execution. According to the definition of event $Succi$ aforementioned, we get:

$$Adv_{\Pi,D}^{A} = 2pr[Succ0] - 1 \quad \textbf{(15)}$$

Game 1 All oracles executed in **Game 0** are simulated in this game. We consider the game is perfectly indistinguishable from a real execution. Hence,

$$pr[Succ1] = pr[Succ0] \quad \textbf{(16)}$$

Game 2 This game is identical to **Game 1** except that we stop executing guessing attacks on the identity of OBU_i. Hence,

$$\left|pr[Succ1]\text{-}pr[Succ2]\right| \le \frac{q_h+q_e}{p} \quad \textbf{(17)}$$

Game 3 This game is identical to **Game 2** except that all executions are terminated if any collision occurs. Since transmitted messages include $\{AID_i, T_i, M_6\}$, $\{AID_j, T_j, M_7\}$, $\{M_8\}$, the probability of collision in hash oracle is at most $\frac{q_h^2}{2|h|}$. Additionally, the possibility of collision in the communicated messages is at most $\frac{(q_s+q_e)^2}{2p}$. Hence,

$$\left|pr[Succ2]\text{-}pr[Succ3]\right| \le \frac{q_h^2}{2|h|} + \frac{(q_s+q_e)^2}{2p} \quad \textbf{(18)}$$

Game 4 This game is identical to **Game 3** except that we stop executing Corrupt query to OBU. The parameters $\{B_i, C_i, D_i, y_i, Z_i, E_i\}$ stored in OBU could be obtained by A via executing Corrupt query. However, it will not expose the session key for the security of ID_i, PW_i, x. Hence,

$$\left|pr[Succ3]\text{-}pr[Succ4]\right| \le \frac{q_s}{|D|} \quad \textbf{(19)}$$

Game 5 This game is identical to **Game 4** except that we execute private oracles to compute sk. A issues a hash query on $psk \| T_i \| ID_i \| AID_i \| T_j \| ID_j \| AID_j \| k$. Hence,

$$\left|pr[Succ4]\text{-}pr[Succ5]\right| = \frac{1}{2} \quad \textbf{(20)}$$

Game 6 We assume that the instance (A, B) based on ECCDH assumption is simulated in this game. We randomly choose $a, b, c, d \in Z_p^*$, and let $T_i = aA$, $T_j = bA$, $P_{pubi} = cB$, $P_{pubj} = dB$. Here, We denote $\gamma = ECCDH(T_i, P_{pubj}) + ECCDH(T_j, P_{pubi})$. Then, we have,

$$ECCDH(T_i, P_{pubj}) = adECCDH(A, B) \quad \textbf{(21)}$$

$$ECCDH(T_j, P_{pubi}) = bcECCDH(A, B) \quad \textbf{(22)}$$

$$\gamma = (ad + bc)ECCDH(A, B) \quad \textbf{(23)}$$

Hence,

$$pr[Succ6] \le q_h Adv_G^{ECCDH}(q_s+q_e) \quad \textbf{(24)}$$

According to games above, we get:

$$Adv_{\Pi,D}^{A} \le \frac{2(q_h+q_e)}{p}+\frac{q_h^2}{h}+\frac{(q_s+q_e)^2}{p} + \frac{2q_s}{|D|}+2q_h Adv_G^{ECCDH}(q_s+q_e) \quad \textbf{(25)}$$

5.3 Other Discussions

In this section, we provide other analysis on our scheme. Let MAP denote the mutual authentication phase and SCP denote the secure communication phase. The result show that our proposed scheme can provide various security attributes as follows.

- **Message authentication:** In MAP, LE_j authenticates OBU_i by checking whether $M_2 = h(r_i||AID_i \| C_i \| y_i)$ holds. Similarly, OBU_i authenticates LE_j by checking whether $M_5 = h(AID_j \| sk \| r_j \| psk)$ holds in SCP.
- **Identity anonymity:** In MAP, Alias rather than real identity of U_i is transmitted over public channel ($AID_i = E_{h(r_i)}(ID_i)$). Attackers cannot obtain ID_i for the difficulty of computing r_i. Similarly, to obtain ID_i from AID_i in SCP is to solve ECCDH assumption.
- **Message unlinkability:** In MAP, the random number is distinct in different session, attackers cannot distinguish whether two messages are from the same OBU.
- **Session key agreement:** In SCP, sk is $sk = h(psk \| T_i \| ID_i \| AID_i \| T_j \| ID_j \| AID_j \| K)$. sk cannot be forged for ECCDH assumption.
- **Forward secrecy:** In SCP, attackers cannot compute T_i, T_j, AID_i, AID_j, sk despite the compromise of x_i, x_j for ECCDH assumption.
- **Resistance to impersonation attack:** In MAP, LE_j authenticates the identity of OBU_i by checking whether $M_2 = h(r_i||AID_i \| C_i \| y_i)$ holds. Attackers could not generate valid authentication message for the secrecy of r_i.
- **Resistance to modification attack:** In SCP, attackers cannot obtain AID_i, T_i, any modified communication messages will not pass the authentication.
- **Resistance to replay attack:** In SCP, the messages $\{AID_i, T_i, M_7\}$, $\{AID_j, T_j, M_8\}$ are transmitted between OBU_i and OBU_j. Attackers cannot prove identity to OBU_j by replaying them in the next session as r_i, r_j are distinct.
- **Resistance to man-in-the-middle attack:** In SCP, a malicious OBU_i cannot calculate sk for ECCDH assumption despite the obtainment of psk.

6 Performance Evaluation

In this section, we compare the performance of our scheme with Zhou et al.'s scheme [18] in terms of security attributes, computation cost etc.

6.1 Security Attributes Analysis

In our proposed scheme, the key parameters e.g. ID_i, PW_i, r_i and sk) are secure from attackers. ID_i, PW_i, r_i and sk cannot be derived by intercepting communicated messages from public channel. AS shown in Table 2, our proposed scheme can provide more security attributes than [18].

Table 2. Security attributes analysis

Security attributes	C1	C2	C3	C4	C5	C6	C7	C8	C9
Zhou's scheme [18]	Y	Y	Y	Y	Y	Y	N	N	Y
Our scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y

C1: Message authentication
C2: Identity anonymity
C3: Message unlinkability
C4: Session key agreement
C5: Forward secrecy
C6: Resistance to impersonation attack
C7: Resistance to modification attack
C8: Resistance to replay attack
C9: Resistance to man-in-the-middle attack

6.2 Computation Cost Analysis

In this section, we compare computation cost of our scheme with [18]. The notations and execution time [10] of operations are listed in Table 3.

Table 3. Notation and Execution time (ms)

Notation	Definition	Time (ms)
T_{pa}	the execution time of a point addition operation	0.0018
T_{sm}	the execution time of a scalar multiplication operation.	0.442
T_e	the execution time of a symmetric key encryption or decryption operation.	0.0087
T_h	the execution time of a hash function operation.	0.0001

To analyze the computation cost, we implement our scheme using MIRACL, which is a widely used cryptographic library and provides execution time of many cryptographic operations. The hardware platform include Windows 7 operating system, an Intel I7-4770 processor, 3.40 GHz clock frequency.

In Zhou et al's scheme [18], the vehicles need to execute fourteen hash function operations ($14T_h$) in

MAP. Besides, the vehicles need to execute twelve hash function operations, fourteen scalar multiplication operations and six point addition operations ($12T_h + 14T_{sm} + 6T_{pa}$) in SCP. Therefore, the total computation cost of [18] is $26T_h + 14T_{sm} + 6T_{pa} \approx 6.2014ms$.

For our scheme, the vehicles need to execute eleven hash function operations, eight symmetric key encryption or decryption operations ($12T_h + 8T_e$) in MAP. Besides, the vehicles need to execute twelve hash function operations, eight scalar multiplication operations ($11T_h + 8T_{sm}$) in SCP. Therefore, the total computation cost of our scheme is $23T_h + 8T_{sm} + 8T_e \approx 3.6079ms$.

As shown in Table 4 and Figure 5, our proposed scheme has lower computation cost compared with Zhou et al.'s scheme [18]. Thus, our scheme is more practical for deployment in VSNs.

Table 4. Comparison of computation cost

	MAP	SCP	Total computation cost (ms)
Zhou et al.' scheme [18]	$14T_h \approx 0.0014ms$	$12T_h + 14T_{sm} + 6T_{pa} \approx 6.2000ms$	$26T_h + 14T_{sm} + 6T_{pa} \approx 6.2014ms$
Our proposed scheme	$12T_h + 8T_e \approx 0.0708ms$	$11T_h + 8T_{sm} \approx 3.5371ms$	$23T_h + 8T_{sm} + 8T_e \approx 3.6079s$

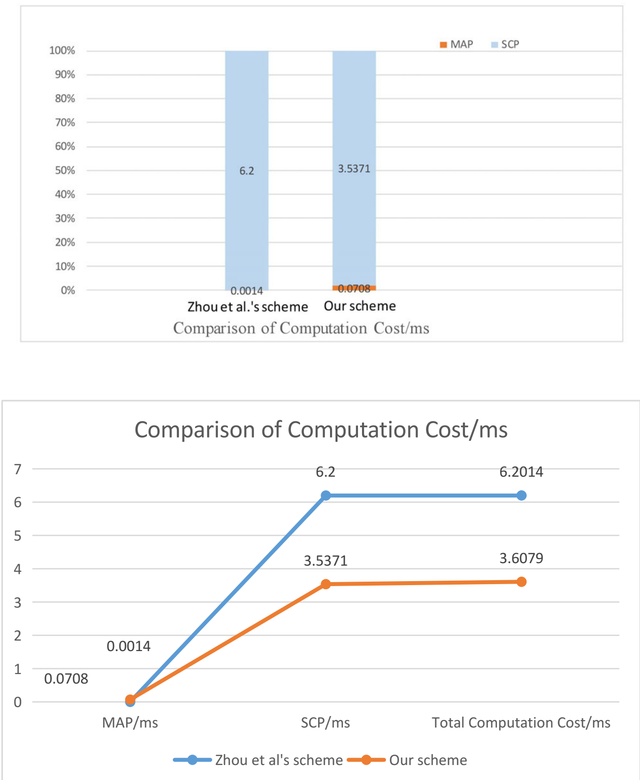

Figure 5. Comparison of computation cost

7 Conclusion

In this paper, we propose an improved authentication scheme based on Zhou et al.' s scheme [18] for vehicle communication in VSNs. The security of our scheme is formally demonstrated in the random oracle model, as well as presented using a security analysis. We also demonstrated that our scheme has better performance, in terms of security attributes and computation costs, compared with [18]. We are to design more efficient three-factor or multi-factor anonymous authentication schemes for VSNs in the future.

Acknowledgements

The work was supported by the National Natural Science Foundation of China (NOs. 61572379, 61572370, 61772377), and the Natural Science Foundation of Hubei Province of China (No. 2017CFA007). We thank the anonymous reviewers for the valuable comments and suggestions which helped us improve the content, organization, and presentation of this paper.

References

[1] J. Yao, X. Yan, C. Qian, H. Li, Wireless Network Localization Algorithm Based on Tikhonov Regularization for Anisotropic Networks, *Journal of Internet Technology*, Vol. 19, No. 3, pp. 927-938, May, 2018.

[2] Shivashankar, G. Varaprasad, S. H. Narayanagowda, Implementing a New Power Aware Routing Algorithm Based on Existing Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, *IET Networks*, Vol. 3, No. 2, pp. 137-142, June, 2014.

[3] A. Husain, B. Kumar, A. Doegar, Performance Evaluation of Routing Protocols in Vehicular Ad Hoc Networks, International *Journal of Ad Hoc and Ubiquitous Computing*, Vol. 6, No. 1-2, pp. 38-45, August, 2011.

[4] A. Prakash, S. Tripathi, R. Verma, N. Tyagi, R. Tripathi, K. Naik, Vehicle Assisted Cross-layer Handover Scheme in NEMO-based VANETs (VANEMO), *International Journal of Internet Protocol Technology*, Vol. 6, No. 1-2, pp. 83-95, June, 2011.

[5] X. Chen, J. Li, J. Weng, J. Ma, W. Lou, Verifiable Computation over Large Database with Incremental Updates, *IEEE Transactions on Computers*, Vol. 65, No. 10, pp. 3184-3195, October, 2016.

[6] X. Chen, J. Li, X. Huang, J. Ma, W. Lou, New Publicly Verifiable Databases with Efficient Updates, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 5, pp. 546-556, September, 2015.

[7] X. Chen, J. Li, J. Ma, Q. Tang, W. Lou, New Algorithms for Secure Outsourcing of Modular Exponentiations, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25,

No. 9, pp. 2386-2396, September, 2014.

[8] D. He, S. Zeadally, N. Kumar, J. H. Lee, Anonymous Authentication for Wireless Body Area Networks with Provable Security, *IEEE Systems Journal*, Vol. 11, No. 4, pp. 2590-2601, December, 2017.

[9] M. Bayat, M. Barmshoory, M. Rahimi, M. R. Aref, A Secure Authentication Scheme for Vanets with Batch Verification, *Wireless Networks*, Vol. 21, No. 5, pp. 1733-1743, July, 2015.

[10] D. He, S. Zeadally, B. Xu, X. Huang, An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme for Vehicular Ad Hoc Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 12, pp. 2681-2691, December, 2015.

[11] J. T. Isaac, S. Zeadally, J. S. Cámara, Security Attacks and Solutions for Vehicular Ad Hoc Networks, *IET Communications*, Vol. 4, No. 7, pp. 894-903, April, 2010.

[12] J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A Lightweight Multi-layer Authentication Protocol for Wireless Body Area Networks, *Future Generation Computer Systems*, Vol. 78, pp. 956-963, January, 2018.

[13] D. He, N. Kumar, M. K. Khan, L. Wang, J. Shen, Efficient Privacy-aware Authentication Scheme for Mobile Cloud Computing Services, *IEEE Systems Journal*, Vol. 12, No. 2, pp. 1621-1631, June, 2018.

[14] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, Y. Xiang, Block Design-based Key Agreement for Group Data Sharing in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, 2017. DOI: 10.1109/TDSC.2017.2725953.

[15] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, Anonymous and Traceable Group Data Sharing in Cloud Computing, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 4, pp. 912-925, April, 2018.

[16] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, K. Kim, Identity-based Chameleon Hashing and Signatures without Key Exposure, *Information Sciences*, Vol. 265, pp. 198-210, May, 2014.

[17] J. Shen, J. Shen, X. Chen, X. Huang, W. Susilo, An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 10, pp. 2402-2415, May, 2017.

[18] Y. Zhou, X. Zhao, Y. Jiang, F. Shang, S. Deng, X. Wang, An Enhanced Privacy-preserving Authentication Scheme for Vehicle Sensor Networks, *Sensors*, Vol. 17, No. 12, pp. 2854, December, 2017.

[19] M. Raya, J. Hubaux, Securing Vehicular Ad Hoc Networks, *Journal of Computer Security*, Vol. 15, No. 1, pp. 39-68, January, 2007.

[20] R. Lu, X. Lin, H. Zhu, P. Ho, X. Shen, ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, *27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, Phoenix, AZ, 2008, pp. 1229-1237.

[21] S. Sivagurunathan, V. Mohan, P. Subathra, Distributed Trust Based Authentication Scheme in a Clustered Environment Using Threshold Cryptography for Vehicular Ad Hoc Network, *International Journal of Business Data Communications and Networking*, Vol. 6, No. 2, pp. 1-18, 2010.

[22] P. Porambage, C. Schmitt, P. Kumar, A. V. Gurtov, M. Ylianttila, Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications, *IEEE Wireless Communications and Networking Conference*, Istanbul, Turkey, 2014, pp. 2728-2733.

[23] J. Li, Y. Zhang, X. Chen, Y. Xiang, Secure Attribute Based Data Sharing for Resource-limited Users in Cloud Computing, *Computers & Security*, Vol. 72, pp. 1-12, January, 2018.

[24] J. Li, J. Li, X. Chen, C. Jia, W. Lou, Identitybased Encryption with Outsourced Revocation in Cloud Computing, *IEEE Transactions on Computers*, Vol. 64, No. 2, pp. 425-437, February, 2015.

[25] M. Zheng, H. Zhou, J. Chen, An Efficient Protocol for Two-party Explicit Authenticated Key Agreement, *Concurrency and Computation: Practice and Experience*, Vol. 27, No. 12, pp. 2954-2963, August, 2015.

[26] M. Chuang, J. F. Lee, TEAM: Trust Extended Authentication Mechanism for Vehicular Ad Hoc Networks, *IEEE Systems Journal*, Vol. 8, No. 3, pp. 749-758, September, 2014.

[27] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, V. Odelu, An Enhanced and Secure Trustextended Authentication Mechanism for Vehicular Adhoc Networks, *Security and Communication Networks*, Vol. 9, No. 17, pp. 4255-4271, November, 2016.

Biographies

Jiani Zhang received her B.S. degree in information security from Hubei University. She is currently pursuing a M.S. degree of Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University. Her main research interests include cryptography and information security.

Debiao He received his Ph.D. degree in applied mathematics from Wuhan University. He is currently a professor of Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security.

Neeraj Kumar received his Ph.D. in CSE from Shri Mata Vaishno Devi University. He is now an Associate Professor in the Department of Computer Science and Engineering, Thapar University, India. His research focuses on mobile computing, routing and security issues in mobile ad hoc, sensor and mesh networks.

Kim-Kwang Raymond Choo received his Ph.D. in Information Security in 2006 from Queensland University of Technology. He currently holds the Cloud Technology Endowed Professorship at the University of Texas. He was named the Cybersecurity Educator of the Year - APAC in 2016.