Anonymous Message Authentication Using Modified Random Secret Pre-distribution for VANETs under Sparse RSUs Environment

Chih-Hsueh Lin

Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Taiwan
cslin@nkust.edu.tw

Abstract

In this paper, the chameleon hash function (CHF) and modified random secret pre-distribution (MRSP) will be combined in a secure scheme for authenticating messages in vehicular ad-hoc networks (VANETs). Based on the secrets in the CHF, a trusted authorizer (TA) can issue identities to all RSUs and vehicles. An identity contains one public ID and one private key. The vehicles use the public ID and the private key to ask RSUs for MRSP information. Using the MRSP information, the vehicles can ask other RSUs for new MRSP information in the next time slot, or exchange the information about index set of random secret to build a neighbor set without any negotiation. To generate MRSP information, a pseudo random number generator (PRNG) is maintained by every RSU. A seed value of a PRNG is broadcast by TA in every time slot to generate a common secret pool in every RSU. This paper proposes a fully anonymous message authentication scheme. Based on the results of security analysis and performance evaluation, the proposed scheme outperforms other works.

Keywords: Vehicular Ad-hoc Networks (VANETs), Modified Random Secret Pre-distribution (MRSP), Chameleon Hash Function (CHF), Message authentication, Pairing key

1 Introduction

Owing to the rapid development of intelligent transportation systems (ITS), vehicular ad hoc networks (VANET) have become a hot research topic. A VANET provides an environment in which vehicles can exchange the information about traffic conditions or their own states to help other vehicles to avoid traffic accidents or traffic jams. To maintain privacy, the vehicles must be anonymous to keep their identities and routing paths untraceable, but it must be verified to be legal ones and be recognized when the vehicles make malicious attacking. The exchanging messages must be authenticated that the messages are integrity and are sent by a legal vehicle.

A VANETs generally has a three-tiered structure [17], which includes a trusted authorizer (TA), many road side units (RSUs) that are installed at streetlights or traffic signs, and onboard units (OBUs) in the vehicles. The TA is the central trust tier, which records information about the registration of RSUs and OBUs, and issues them with the identities to present themselves. The TA and RSUs are connected via a wired network. The communication between RSUs and OBUs uses the wireless communication protocol IEEE802.11p, which is a revision of 802.11 with the protocol of wireless access in the vehicular environment (WAVE) added [1]. The RSUs help vehicles authenticate messages or communicate confidentially, but the coverage of each RSU is limited; the cost of installing over a wide area is very high, and so the installation of RSUs must be incremental. Therefore, vehicles must be able to authenticate messages in an environment of sparse RSUs.

In this paper, the chameleon hash function (CHF) [18, 2] is combined with modified random secret pre-distribution (MRSP) [19] to build a message authentication environment for VANETs with sparse RSUs. Based on the CHF, TA keeps two common secrets that will be embedded to all identities as evidence of mutual trust. The TA will issue one identity to each RSU and vehicle. An identity contains one public ID and one private key. The public ID comprises three components - a virtual name, a random key, and a public key- and is used to verify that an entity is legal. The private key is used to claim ownership of the public ID. Without any negotiating process, a CHF pairing key is multiplied by one private key and the other's public key will be used mutual trust and for use as the session key for secure communication between RSUs and vehicles. To help vehicles authenticate messages, every RSU has a pseudo-random number generator (PRNG). One day is divided into M time slots. In every time slot, TA will broadcast a common seed value to all valid RSUs to generate a common secret pool (SP) and a common

[*]Corresponding Author: Chih-Hsueh Lin; E-mail: cslin@nkust.edu.tw

DOI: 10.3966/160792642019122007017

index set (D) for that slot. Any RSU can respond to a request for MRSP information from a legal vehicle. For the MRSP information with the collected announcement of subset of MRSP information from the neighboring vehicles, a vehicle can set up its neighbor set, which includes the information about the neighboring vehicle's virtual name, trust type, and MRSP pairing key. The MRSP pairing key can be derived by the common secret or the common random secret embedded in two vehicles, and will be used to finish message authentication or secure communication without the help of RSU.

The rest of this paper is organized as follows. Section 2 introduces related works and preliminary techniques. Section 3 presents in detail the process of the proposed scheme. Section 4 presents security analysis and performance evaluation of the proposed scheme, and compares in terms of functionality and performance. A brief discussion will be taken in the final section.

2 Related Works and Preliminary Techniques

2.1 Related Works

In 2004, based on the public-key infrastructure (PKI), Hubaux et al. [3] proposed a scheme that a smart vehicle has capabilities to exchange the information included recording, computing, and positioning. It uses the traditional public-key infrastructure. The complexity of computation is too high to finish message authentication under the PKI structure. Moreover, for keeping privacy and the routing path un-traceability, the vehicle must change its certificate frequently; it is a heavy burden for TA.

To overcome the problem of traditional public-key infrastructure, Zhang et al. [4] proposed a scheme, in that scheme, RSU is used to assist message authentication. When a vehicle enters the coverage range of a RSU, the vehicle will establish a secret key after mutual authenticating, and use the secret key to make a short message authentication code (MAC). The RSU will verify the authentication of MAC. However, exposure of the certificate creates the problem that the vehicles will be traceable.

In 2010, Wasef et al. [5] proposed the RSU-aided distributed certificate service (DCS). It provides vehicles with a way that allows them to update their certificates from a RSU effectively. A vehicle can update its certificate from any RSU, even if the vehicle is not in the coverage range of the original RSU. But the performance of DCS depends on the density of the RSUs.

To make privacy, Sun et al. [6] proposed a pseudonymous authentication scheme with privacy preservation (PASS). It is an anonymous authentication scheme and supports DCS. It can decrease the overhead of certificate-updating and reduce the loading of malicious revocation. In PASS, an attacker cannot trace the legitimate vehicles, even when they kidnap the RSU. But it still is a certification based scheme.

Based on the concept of chameleon hash function, Chen et al. [7] make anonymous identity to do anonymous authentication and key-agreement (AAKA). In this scheme, vehicles use a chameleon hash value as its disposable alias. Vehicles can verify the message integrity and make sure the legitimate source. Using two-trapdoor chameleon hash function to implement message authentication in sparse RSU environment was proposed by Kuo in 2015 [21]. Hung et al. [8] proposed a chameleon hash function-based message authentication scheme without RSUs, but they did not solve the problem of malicious revocation. Hung et al. [9] used the bilinear Diffie-Hellman method (BDH) to propose a message authentication scheme in dense RSU environment, which involves certificate request from RSU, but this scheme suffers from malicious revocation.

In WSN, the random key pre-distribution (RKP) [10] is used to get mutual authentication. A random subset of keys in the key pool will be embedded in the sensor nodes before the node deployment. The nodes in WSN can authenticate mutually if they own common secret keys. Due to the plain secret keys in nodes, RKP is vulnerable to compromise attacks [11]. When some nodes are compromised, the attacker can make malicious nodes with the fake subset of secret keys that are collected from the compromised nodes. In [20], modifying RKP to be RSP, the random secrets are embedded in the private keys. Pairing the private key and other's public key, the nodes can get the pairing key and use the pairing key to finish message authentication, if they have the common secret in their private key. In 2015, Yein et al. [12] proposed a random secret pre-distribution (RSP) based message authentication scheme. Depended on the secret embedded in the vehicles, the vehicles can make mutual trust and get pairing key for message authentication. But the proposed scheme can't deny the right of the malicious vehicles. In 2016, Lin et al. [19] added one common secret to RSP to be as MRSP, and set up a secure environment for the sensor layer of Internet of Things (IOT). The concept of MRSP will be involved in the proposed scheme. Within the last two years, other well-known methods of message authentication had been proposed. Two examples are provided below. The identity-based batch verification (IBV) scheme had been proposed to make VANETs more secure and efficient. In Tzeng et al. [15], the proposed IBV scheme provides the provable security in the random oracle model that can satisfy the security and privacy desired by vehicles. In addition, the batch verification of the proposed scheme needs only a small constant number of pairing and point multiplication computations, independent of the number of messages. In 2018, Asaar et al. [16] proposed a new identity-based message authentication scheme using proxy vehicles (ID-MAP). It can satisfy the message authentication requirement, existential unforgeability of underlying signature against adaptively chosen-message and identity attack is proved under elliptic curve discrete logarithm problem in the random oracle model. The ID-MAP not only is more efficient than proxy-based authentication scheme (PBAS).

In section 4, we will compare the functionalities and performances among DCS [5], PASS [6], AAKA [7], BDH [9], RSP [12] and the proposed scheme.

2.2 Preliminary Techniques

2.2.1 Chameleon Hash Function (CHF)

The original concept of chameleon hash function (CHF) was proposed by Chen, Zhang, Susilo and Mu in 2007 [2-4], In this paper, based on the concept of CHF, we redefine the CHF and the parameters as follows

$$\begin{aligned} CH(PID_i) &= CH(VN_i, RK_i, PK_i) \\ &= f(H(VN_i), RK_i)RK_i + PK_i \end{aligned}$$

TA keeps two secrets, x and a, let $Y = xP$ and $CH_{TA} = \alpha Y$ called as chameleon hash function value of TA and published by TA.

TA issues an identity (PID_i, PR_i) to every entity (N_i) that may be RSU or vehicle. PID_i is the public ID and PR_i is the private key of N_i. PID_i included the virtual name (VN_i), random key (RK_i) and public key (RK_i) is used by N_i to present itself. PK_i is equal to RR_iY and PR_i is held by N_i secretly that will be used to claim the ownership of PID_i. PR_i is calculated by TA. When PR_i is assigned as $(a - f(H(VN_i), RK_i)k_ix^{-1}$, the value of $CH(PID_i)$ will be equal to CH_{TA}, that is used to verify the legitimate of PID_i. Random key (RK_i) is equal to k_iP, k_i is a random number for N_i, so there are three secrets (a, x, k_i) in an identity and N+2 secrets in N identities. So the assignment of identity can resist the collusion attacking.

2.2.2 Modified Random Secret Pre-distribution (MRSP)

In [20], random pre-distribution (RSP) is proposed to fix the weakness of plain key in random key pre-distribution (RKP) [11]. In [19], one common secret is embedded into every RSP to be as modified RSP (MRSP). In this paper, we use MRSP to finish mutual trust among the RSU and vehicles. A pseudo random number generator (PRNG) is maintained by every RSU to generate a common secret pool while RSUs receive a common seed value broadcasted by TA in every time slot. Using the common secret pool, the MRSP information issued by any RSUs are similar with the MRSP information issued by other RSU.

2.2.3 Paring Key

For message authentication or secure communication; a session key will be negotiated between the communicating entities. In this paper, we use the concepts of CHF and MRSP, the communicating entities can get pairing key without any negotiating process. HPK_{ai} is the CHF pairing key of R_a and V_i, and MPK_{ij} is the MRSP pairing key of V_i and V_j.

CHF pairing key. R_a publishes its PID_a and holds its PR_a. V_i shows out its PID_i and holds PR_i. R_a calculates HPK_{ai} as $(PR_a \cdot PK_i)^x$, and V_i calculates HPK_{ia} as $(PR_i \cdot PK_a)^x$ independently. Without any negotiating process, HPK_{ai} and HPK_{ia} will be equal to $(PR_aPR_iY)^x$.

MRSP pairing key. In VANET, every vehicle will say hello to its neighbors periodically to claim it is in here. The hello message included anonymous name and the index set of random secret. Based on the hello messages, a vehicle will set up the information about its neighbors. When V_i announces its hello message $\{S_m, AN_i{}^m, D_i{}^m\}$, and receives a hello message $\{S_m, AN_j{}^m, D_j{}^m\}$ sent from V_j. V_i and V_j hold their private name PN_i and PN_j secretly.

V_i checks if any $d_{ix}{}^m \in D_j{}^m - \{d_{i0}{}^m\}$ exits.

If $d_{ix}{}^m$ exists, V_i sets

$$MPK_{ij} = \hat{e}(\frac{H(AN_i{}^m)}{H(PN_i{}^m)})PS_{ix}{}^m, H(AN_j{}^m)P)$$

Otherwise V_i sets

$$MPK_{ij} = \hat{e}(\frac{H(AN_i{}^m)}{H(PN_{i0}{}^m)})PS_{i0}{}^m, H(AN_j{}^m)P)$$

The MPK_{ij} will be equal to $(\hat{e}(H)AN_i{}^m)P, H(AN_j{}^m)P)^y$, y may be the value of common secret $(SP^m(d_{io}{}^m))$ among all vehicles or the value of common random secret $(SP^m(d_{ix}{}^m))$ between V_i and V_j.

3 The Proposed Scheme

In the proposed scheme, TA, RSU and vehicle are the three tiers in VANET structure. TA issues an identity to every RSU and vehicle. TA maintains the valid identity tables for RSUs and vehicles (Table 2, Table 3) and one revoked vehicles table (Table 4). The revoked vehicles table will be broadcasted to all RSU for denying the right of malicious vehicles. Based on the secrets in CHF, TA can issue all of RSUs and vehicles with the identities. An identity contains one public ID and one private key. The public ID will be used to present one entity, and the private key is used to claim the ownership of the public ID. The secrets embedded in public ID will be the evidence for verifying the legal of public ID. The vehicles will use the public ID and private key to ask RSUs for the MRSP information. RSUs will check the validation of vehicles and response the MRSP information request with the MRSP information included new private name, index set of random secrets, set of private secret keys, and signatures.

For message authentication, we apply the concept of MRSP to RSUs and vehicles. For making MRSP, a pseudo random number generator (PRNG) is maintained by every RSU. A seed value of PRNG is broadcasted by TA in every time slot to generate a common secret pool in every RSU. So, the responses of MRSP information request in different RSUs are all the same.

To decrease the overhead of MRSP recording tables in RSUs. The recording table is maintained for only one day in each RSU. One day is splitter into M time slots. At the 1st time slot in every day or the first time the vehicles entering a VANET. The vehicles must make the MRSP information request to ask the nearest RSU for MRSP information using their identities issued by TA. In the following time slots, the vehicles will ask for new MRSP information using their current MRSP information. In the proposed scheme, the vehicles will say hello to their neighbors periodically. The hello message is included the subset of MRSP information. Based on the received hello message, the vehicles can build a set about the information of their neighbors. Based on the information of neighboring vehicles, the vehicles can make message authentication or communication confidentially. For easily understanding, we define the notations 、 definitions and parameters of functions as Table 1.

Table 1. Notations and definitions

TA, R_a, V_i, N_i	TA, R_a and V_i are the trust authorizer (TA). road side unit *a* (R_a) and vehicle *i*(V_i) that are included is this paper. N_i is the entity that may be RSU or vehicle.
RN_i, PN_i, VN_i, AN_i	RN_i, PN_i, VN_i, AN_i and AN_i are the real name, private name, virtual name and anonymous name of entity i used in different situation. RN_i and PN_i will be held secretly. VN_i and AN_i will be published to present the entity.
Z_q, m	Z_q is a finite field that is formed by mod q, where q is a large prime number, $m \in Z_q$.
G, P, Q^x	G is an EC addition group with mod q; P is the generator of G. Q^x is the value of Q on the x axis.
M	M is a character stream or bit stream.
$H(M)$	$H(M)$ is a hash function that maps M to Z_q.
$HMAC(M)_K$	$HMAC(M)_K$ is a hash function that maps M to Z_q with key K.
$\hat{e}(Q, R)$	$\hat{e}(Q, R)$ is a bilinear pairing function that pairs Q and R in G to a value in Z_q. $\hat{e}(Q, R)$ satisfies the functions of pairing. $\hat{e}(Q, R) = \hat{e}(R, Q)$, and $\hat{e}(aQ, bR) = \hat{e}(bQ, aR) = \hat{e}(Q, R)^{ab}$
$Sig(m)_k$	Signature of *m* signed with key *k*.
$SE_k(m)$, $SD_k(m)$	$SE_k(m)$ and $SD_k(m)$ are the symmetric encrypt and decrypt *m* with key *k*.
$ECE_k(m)$, $ECD_k(m)$	$ECE_k(m)$ and $ECD_k(m)$ are the ECC encrypt and decrypt *m* with key *k*.
$f(m, k)$	$f(\cdot)$ is a hash function that maps a *m* in Z_q and a *K* in *G* to a value in Z_q.
$CH(PID_i)$, Y, x, a, k_i, CH_{TA}	$CH(\cdot)$ is a chamelion hash function. $CH(PID_i) = CH(VN_i, RK_i, PK_i) = f(H(VN_i), RK_i)RK_i + PK_i$. $Y = xP$ and $CH_{TA} = aY$, *x* and *a* are the secrets of TA. $RK_i = k_iP$, k_i is a random value for N_i. $PK_i = PR_iY$. If $PR_i = \alpha - f(H(VN_i, RK_i)k_ix^{-1})$, then $CH(PID_i)$ will be equal to CH_{TA} that is the chamelon hash function value published by TA.
PID_i (VN_i, RK_i, PK_i) PR_i	PID_i and PR_i are the two components of N_i's identity. PID_i contains virtual name (VN_i), random key (RK_i) and public key (PK_i) that will be published to present N_i. PR_i is held secretly by N_i used to claim the owenership of PID_i. The value applied (VN_i, RK_i, PK_i) into a chameleon function will be used to verify the legal of PID_i. $CH(PID_i)$ will be equal to CH_{TA} if PID_i is legal.

Table 1. Notations and definitions (continue)

PRNG	*PRNG* is the pseudo random generator maintained by every RSU.
S_m, v_m, SP^m, D^m	S_m is the m^{th} time slot, one day is splidded into M time slots. The v_m is a seed value broadcasted by TA to all valid RSUs to generate a common secret pool (SP^m) and the respective secret index set (D^m) for m^{th} time slot. $D^m = \{d_l{}^m \mid d_l{}^m \in 1 \sim T+1, l = 0 \sim T\}, SP^m = \{SP^m(d_l{}^m \in D^m\}$
$S_m, PN_i{}^m, D_i{}^m,$ $PS_i{}^m, Sig1_i{}^m, Sig2_i{}^m$	The MRSP information of V_i : S_m is the time slot *m*. $PN_i{}^m$ is the private name that is requested by vehicle and is held secretly by V_i . $D_i{}^m$ is the index set of random secret assigned by RSU for V_i . $PS_i{}^m$ is the set of private secret keys assigned by RSU with random secret. $Sig1_i{}^m$ is the signature 1 signed by common secret key (CSK^m). $Sig2_i{}^m$ is the signature 2 signed by the special secret key of V_i ($SSK_i{}^m$) $D_i{}^m = \{d_{ix}{}^m \mid d_{i0}{}^m = d_0{}^m, d_{ix}{}^m \in_R D^m, x = 1 \sim S\}$ $PS_i{}^m = \{PS_{ix}{}^m \mid PS_{ix}{}^m = H(PN_i{}^m)SP^m(d_{ix}{}^m)P, d_{ix}^m \in D_i^m\}$ $Sig1_i{}^m = Sig(H(S_m \parallel VN_a \parallel D_i{}^m))_{CSK^m}, Sig2_i{}^m = Sig(H(S_m \parallel VN_a \parallel PN_i{}^m))_{SSK_i^m}$
$SPK_i^m, SSK_i^m,$ CPK^m, CSK^m	In MRSP, a common secret ($SP^m(d_0^m)$)is embedded into every vehicles (V_i) to be as PS_{io}^m . Every vehicles have PS_{io}^m and its private name PN_i^m . SSK_i^m and SSK_i^m are the special key pair, SPK_i^m is the special public key of V_i that is the 0^{th} private secret key of $V_i(PS_{io}^m)$, SSK_i^m is the repective special secret key that is known by all RSU. $SPK_i^m = H(PN_i^m)SP^m(d_0^m)P = SSK_i^m P = PS_{i0}^m, SSK_i^m = H(PN_i^m)SP^m(d_0^m)$ The information signed by SSK_i^m can be verified by SPK_i^m . CPK^m and CSK^m are the common key pair, common public key (CPK^m) is known by all vehicles and common secret key (CSK^m) is the 0^{th} secret value in SP^m held by all RSUs secretly. $CPK_i^m = SP^m(d_0^m)P = CSK^m P = PS_{i0}^m / H(PN_i^m), SP^m(d_0^m)$ The information signed by CSK^m can be verified by CPK^m .
HPK_{ai}, HPK_{ij}	HPK_{ai} is the CHF pairing key of *RSU* a (R_a) and vehicle *i*(V_i). R_a and V_i have their identites (PID_a, PR_a) and (PID_i, PR_i). The CHF pairing key HPK_{ai} will be $HPK_{ai} = PR_a \cdot PK_i = PR_a \cdot PR_i Y = PR_i \cdot PR_a Y = PR_i \cdot PK_a = HPK_{ia}$ R_a and V_i can get HPK_{ai} and HPK_{ia} without any negotiating process. MPK_{ij} is the MRSP pairing key of V_i and V_j , when $d_{ix}^m \in \{D_i^m \bigcap D_j^m - \{d_{i0}^m\}\}$ exists, $MPK_{ij} = \hat{e}(\frac{H(AN_i^m)}{H(PN_i^m)} PS_{ix}{}^m, H(AN_j{}^m)P)$, otherwise, $MPK_{ij} = \hat{e}(\frac{H(AN_i^m)}{H(PN_i^m)} PS_{i0}{}^m, H(AN_j{}^m)P)$
B_i	The neighbors set of V_i . $B_i = \{B_{ix} \mid B_{ix} = (AN_{ix}, D_x^m, TT_{ix}, MPK_{ix}, PV_{ix}, ET_{ix}), x = 1 \sim N\}$ B_{ix} is the information about the x^{th} neighbor of V_i . $AN_{ix}, TT_{ix}, MPK_{ix}, ET_{ix}$ are the anonymous name, trust type, MRSP pairing key and expire time of x^{th} neighbor, D_x^m is the secret index set of x^{th} neighbor. The trust type (TT_{ix}) may be direct trust ("D"), indirect trust ("I") or un-trust ("U") when V_i and x^{th} neighbor have common random secret, have common direct trust neighbor PV_{ix} or have neither common random secret nor common direct trust neighbor respectively.
$S \to D$: $SID, DID, T_s,$ Sb, MS	The format of a communication, source entity (*S*) sends a message (SID, DID, T_s, Sb, MS) to destination entity (*D*). The message contains source ID (*SID*), destination ID (*DID*), subject of the communication (*Sb*) and message stream (*MS*).

The proposed scheme contains the processes of Initializing and Registering, Common Secret Pool Generating, MRSP Information Requesting and Responding, Neighbor Vehicles Set Building, Message Authenticating, Communicating Confidentially, Revoking of Malicious Entities, and Working under Sparse RSUs Environment. The detail descriptions are as follows.

3.1 Initializing and Registering

TA defines and publishes the information about the public functions and parameters. TA keeps two secret, x and a, set $Y = xP$, $CH_{TA} = aY$ and publishes Y and CH_{TA}. For every entity with its real name (RN_i), TA randomly choices a random value (k_i) to make random key (RK_i) as k_iP, calculates the private key (PR_i) and the public key (RK_i), and then issues an identity included (PID_i and PR_i) to entity *i*. PID_i includes virtual name (VN_i), random key (RK_i) and public key (RK_i). PID_i is used to present entity *i* and PR_i is used to claim the ownership of PID_i. The value of PR_i and (RK_i) are calculated as.

$$PR_i = a - (f(H)VN_i), RK_i)k_i x^{-1}, PK_i = PR_i Y$$

When applying PID_i into $CH(\cdot)$, the value of $CH(PID_i)$ will be equal to CH_{TA}, that will be used to verify the legitimate of PID_i.

TA maintains three tables included valid RSUs table (Table 2), valid vehicles table (Table 3) and revoked vehicles table (Table 4). The formats of three tables are as follows：

Table 2. Valid RSUs

Real Name	Public ID	Private key
RN_a	VN_a, RK_a, PK_a	PR_a
…	…	…

Table 3. Valid vehicles

Real Name	Public ID	Private key
RN_i	VN_i, RK_i, PK_i	PR_i
…	…	…

Table 4. Revoked vehicles

Public ID
VN_j, RK_j, PK_j
…

3.2 Common Secret Pool Generating

A PRNG is maintained in every RSU. In every time slot (S_m), TA will broadcast a seed value to all RSUs that are in valid RSUs table (Table 2) to generate a common secret pool for m^{th} time slot. In m^{th} time slot (S_m), TA sets a seed value (v_m), forms a sharing key (*SK*) function ($F(x)$), encrypts the seed value with sharing key ($SE_{sk}(v_m)$) then broadcasts $\{S_m, F(x), SE_{sk}(v_m)\}$ to all valid RSUs.

CSPG 1:

$TA \rightarrow RSU_s$:

TA, all RSU_s, T_s "Seed Value", $\{S_m, F(x), SE_{sk}(v_m)\}$

In here, $F(x) = SK + \Pi_{all\ PR_a\ in\ table\ 2}(x - PR_a)$.

CSPG 2: When RSU (R_a) receives the broadcasting message, if it is in the valid RSUs table, R_a calculates $SK' = F(PR_a)$ and decrypts $SE_{sk}(v_m)$ using SK' to get v_m. Then R_a generates a secret pool SP^m and the respective index set (D^m) using PRNG with the seed vale (v_m).

3.3 MRSP Information Requesting and Responding

At the 1^{th} time slot (S_1) in every day, or the first time vehicle (V_i) entering the VANET. It must make MRSP information request (MRSP1) using its identity. In the following time slot (S_m), it will make MRSP information request (MRSP2) using its MRSP information request in previous time slot (S_{m-1}).

3.3.1 MRSP Request Using *PID*$_i$ for *m*th Time Slot (MRSP1)

V_i has its $PID_i = (VN_i, RK_i, PK_i)$, holds its PR_i and knows the PID_a of R_a, calculates HPH_{ai} as $(PR_i, PK_a)^x$, selects a private name $PN_i{}^m$, and then sends the MRSP information request to R_a.

MRSP1.1: $V_i \rightarrow R_a$: VN_i, VN_a, T_s, "MRSP1 request", $\{PID_i, HMAC(T_s \| VN_i)_{HPK_{ia}}, SE_{HPK_{ia}}(PN_i{}^m)\}$.

MRSP1.2: When R_a receives the MRSP request.

R_a checks $CH(PID)_i = CH_{TA}$ and verifies $HMAC(T_s \| VN_i)_{HPK_{ia}}$ using HPH_{ai}.

If it is false, R_a rejects the request and ends the process.

Else; R_a decrypts $SE_{HPK_{ia}}(PN_i^m)$ using HPH_{ai} to retrieve the $PN_i{}^m$ makes MRSP information for V_i with $PN_i{}^m$, included $D_i{}^m$ and $PS_i{}^m$, responses the MRSP information, and sets $SSK_i{}^m$ as $H(PN_i^m)$ $SP^m(d_0{}^m)$.

$R_a \rightarrow V_i : VN_a, VN_i, T_s'$, "MRSP1 response", $\{S_m$, $D_i^m, SE_{HPK_{ai}}(PS_i^m), Sig1_i^m, Sig2_i^m\}$.

MRSP 1.3: V_i receives the MRSP1 response sent by R_a.

V_i will decrypt the encrypted message to get its $PS_i^{\ m}$ and set $(S_m, VN_a, D_i^m, Sig1_i^{\ m})$ to present itself in time slot S_m, and choices AN_i^m as its anonymous name in time slot S_m.

3.3.2 MRSP Information Request with the Previous MRSP Information (MRSP 2)

As the response of 3.3.1, V_i uses $(S_m, VN_a, PN_i^{\ m}, Sig2_i^{\ m})$ and AN_i^m to ask RSU_b (R_b) for the new MRSP information of S_{m+1} with new private name ($PN_i^{\ m+1}$).

MRSP 2.1: $V_i \rightarrow R_b : AN_i^{\ m}, VN_a, T_s$, "MRSP2 request", M_i

$$M_i = \{S_m, VN_a, D_i^m, ECE_{CPK^m}(PN_i^{\ m} \,\|\, PN_i^{\ m+1}), \\ Sig2_{Xi}^{\ \ m}, Sig1_{Xi}^{\ \ m}\}$$

MRSP 2.2: R_b receives the MRSP2 request, decrypts $ECE_{CPK^m}(PN_i^{\ m} \,\|\, PN_i^{\ m+1})$ with key CSK^m to get $PN_i^{\ m}$ and new private name $PN_i^{\ m+1}$, using $SPK_i^{\ m}$ and CPK^m to verify $Sig2_i^{\ m}$ and $Sig1_i^{\ m}$

If the verification of signature is false, R_b rejects the request and ends the process.

Else; makes MRSP information for V_i with $PN_i^{\ m+1}$ that includes D_i^{m+1} and $PS_i^{\ m+1}$, and then responses the request as follows.

$R_b \rightarrow V_i : VN_b, AN_i^m, T_s'$, "MRSP2 response", $\{S_{m+1}, D_i^{m+1}$, $SE_{\{SPK_i^{\ m}\}^x}(PS_i^{\ m+1})$, $Sig1_i^{\ m+1}$, $Sig2_i^{\ m+1}\}$. New $PS_i^{\ m+1}$ are encrypted with the special public key of $V_i(SPK_i^{\ m})$.

MRSP 2.3: V_i receives the new MRSP2 information sent by R_b.

It decrypts the encrypted message with $(SPK_i^{\ m})^x$ to get the new $PS_i^{\ m+1}$, sets ($\{S_{m+1}, VN_b, D_i^{m+1}$, $Sig1_i^{\ m+1}$) for hello message and choices ($AN_i^{\ m+1}$) as its new anonymous name.

When RSU (R_a) responses the MRSP information request, it will maintain the MRSP information in MRSP table as Table 5.

In Table 5, the issuer of original information may be TA or RSUs, when the issuer is TA, PID_i is the original information, if the issuer is RSU, the original information is MRSP information of previous time slot. The MRSP information contains time slot (S_m) random secret index set (D_i^m), signature 1 ($Sig1_i^{\ m}$) and the private name ($PN_i^{\ m}$).

Table 5. MRSP table in RSU_a

Original Information		New MRSP Information
Issuer	PID_i or MRSP Information	
TA	$PID_i(VN_i, RK_i, PK_i)$	S_m, D_i^m, $Sig1_i^{\ m}, PN_i^{\ m}$
VN_b	$S_m, D_j^{\ m}$, $Sig1_j^{\ m}, PN_j^{\ m}$	$S_{m+1}, D_j^{\ m+1}$, $Sig1_j^{\ m+1}, PN_j^{\ m+1}$
…	…	…

When RSUs receive the information of revoked vehicles sent by TA, they will maintain the revoking information as Table 6. If the issuer is TA, the information will be kept always, the other information is kept only one day. When RSUs receive a MRSP information request, it has to check the revoked vehicles table before response process.

Table 6. Revoked vehicles table in RSU_a

Issuer	PID_i or MRSP information
TA	$PID_k(VN_k, RK_k, PK_k)$
VN_c	$S_{m-k}, D_k^{\ m-k}, Sig1_k^{\ m-k}, PN_k^{\ m-k}$

3.4 Neighbor Vehicles Set Building

Every vehicle (V_j) will broadcast a hello message to introduce itself periodically. The hello message contains two nearest MRSP information.

NVB1: $R_j \rightarrow all : An_j^{\ m}$, all, T_s, "Hello", { M_{j1}, M_{j2} }

$M_{j1} = \{S_{m-1}, Vn_a, D_j^{\ m-1}, Sig1_j^{\ m-1}\}$ and $M_{j2} = \{S_m$, $Vn_b, D_j^{\ m}, Sig1_j^{\ m}\}$.

The duration of announcing hello message is E minutes.

NVB2: When V_i receives the hello message sent by V_j, V_i selects one of M_{j1} and M_{j2} that is in the nearest time slot, V_i has MRSP information in that time slot. For example it is M_{j2}

V_i checks if the information of V_j is in B_i.

If it is true, sets the respective ET_{ij} as $E+1$ and ends the process.

Else, verifies the $Sig1_j^{\ m}$ with CPK^m

If the verification is false, rejects the hello message and ends process.

Else, sets TT_{ij} = "U", PV_{ij} = "$Null$", $ET_{ij} = E+1$ and MPK_{ij} as

$$MPK_{ij} = e(\frac{H(AN_i^{\ m})}{H(PN_i^{\ m})} PS_{io}^{\ \ m}, H(AN_j^{\ m})P)$$

Check the condition, $\{D_i^{\ m} \bigcap D_j^{\ m}\} - \{D_{i0}^{\ \ m}\} \neq \phi$

If it is true,

sets $d_{ix}^{\ \ m} \in \{D_i^{\ m} \bigcap D_j^{\ m}\} - \{d_{i0}^{\ \ m}\}$,

sets TT_{ij} =“*D*” and MPK_{ij} as

$$MPK_{ij} = e(\frac{H(AN_i^{\ m})}{H(PN_i^{\ m})} PS_{ix}^{\ \ m}, H(AN_j^{\ m})P)$$

Else, checks if any $D_k^{\ m}$ in B_i the TT_{ij} =“*D*” and

$$D_k^{\ m} \bigcap D_j^{\ m} - \{d_{k0}^{\ \ m}\} \neq \phi.$$

If $D_k^{\ m}$ is exist, let PV_{ij} =“ AN_k ” and TT_{ij} =“*I* ”.

Append $\{AN_j, D_j^{\ m}, TT_{ij}, MPK_{ij}, PV_{ij}, ET_{ij}\}$ into B_i .

End process.

Following the building process, the trust type between V_i and V_j may be “*D*” "*D*" , the respective MPK_{ij} is as value of $\hat{e}(H(AN_i^{\ m})P, H(AN_j^{\ m})P)^{SP^m(d_{ix}^{\ \ m})}$, $SP^m(d_{ix}^{\ \ m})$ is value of the common random secret.

Otherwise, the respective MPK_{ij} will be $\hat{e}(H(AN_i^{\ m})P,$ $H(AN_j^{\ m})P)^{SP^m(d_{i0}^{\ \ m})}$, $SP^m(d_{i0}^{\ \ m})$ is the value of common secret.

If the trust type is “*I* ”, the PV_{ij} is the anonymous name of their common direct trust neighbor.

The expired time (*ET*) in B_i will be countered down continuously. When an *ET* is countered to zero, the respective information will be removed, due to the vehicle had moved out the communication range.

3.5 Message Authentication

MA1: Vehicle *i* with its B_i , when V_i broadcasts a message (M_i)to all of its neighbors. V_i forms the verify key (*VK*) shared function $F(x)$ as

$$F(x) = VK + \Pi_{all\ v_j\ in\ B_1}(X - MPK_{ij})$$

then V_i broadcasts the message to all of its neighbors.

$V_i \rightarrow all: AN_i^{\ m}$, All, T_s , “Message”, { M_i , $F(x)$, $HMAC(T_s \,||\, M_i)_{VK}$ }

MA2: When V_j receives the message,

V_j verifies the $HMAC(T_s \,||\, M_i)_{VK}$ with VK' , $VK' =$ $F(MPK_{ji})$

If the verification is true,

If “$\{TT_{ij}\}$” is “*D*”, V_j trusts the message M_i .

Else if “$\{TT_{ij}\}$” is “*I* ”, V_j asks the vehicle PV_{ij} in B_j to make sure the message.

Else, V_j doubts this message.

3.6 Communicating Confidentially

If the trust type (TT_{ij}) between V_i and V_j is “*D*”, they can use the MRSP pairing key (MPK_{ij}) as the session key for secure communication. When the TT_{ij} is “*I* ”, and PV_{ij} is $AN_k^{\ m}$, V_i and V_j can negotiate the session key (SK_{ij}) under the help of V_k .

SK1: V_i assigns a SK_{ij} , encrypts SK_{ij} with MPK_{ij} , passes it to V_k using MPK_{ik} as the authenticating key, and sets $M_{i1} = SE_{MPK_{ij}}(SK_{ij})$.

$V_i \rightarrow V_k : AN_i^{\ m}, AN_k^{\ m}, T_s,$ “Session Key 1”, $\{M_{i1}, HMAC(M_{i1})_{MPK_{ik}}\}$

SK2: When V_k receives the message, it uses MPK_{ki} to verify the message. If the verification is true, V_k passes M_{i1} to V_j using MPK_{kj} as the authenticating key.

$V_k \rightarrow V_j : AN_k^{\ m}, AN_j^{\ m}, T_s',$ “Session Key 2”, $\{M_{i1}, HMAC(M_{i1})_{MPK_{kj}}\}$.

SK3: When V_j receives the message, uses MPK_{jk} to verify the message. If the verification is true, decrypts the message with MPK_{ij} to get the session key MPK_{ij} , then return a response message to V_i .

$V_j \rightarrow V_i : AN_j^{\ m}, AN_i^{\ m}, T_s'',$ “Session Key 3”, $\{HMAC(M_{j1})_{MPK_{ij}}\}$

SK4: V_i verifies the return message with SK_{ij} to make sure that V_j has known the session key.

3.7 Revoking of Malicious Entities

When a RSU is found to make malicious attack, the information of this RSU will be removed from valid RSUs table (Table 2). After that time, this RSU cannot retrieve the new seed value broadcasted by TA anymore. So the right of the malicious RSUs will be denied.

At any time slot (S_m), a vehicle (V_i) may show its PID_i or $(S_m, VN_a, D_i^{\ m}, Sig1_i^{\ m})$ to present itself. For example, at S_m , V_i asked R_a for MRSP information request with PID_i , then got the MRSP information request from R_b , R_c , at S_{m+1} and S_{m+2}, the respective hello message are $(S_m, VN_a, D_i^{\ m}, Sig1_i^{\ m})$, $(S_{m+1}, VN_b,$ $D_i^{\ m+1}, Sig1_i^{\ m+1})$, $(S_{m+2}, VN_c, D_i^{\ m+2}, Sig1_i^{\ m+2})$.

V_i was found to finish malicious attack in $m+2$ time slot. By tracing back the MRSP table in RSU_c , RSU_b and RSU_a , the public ID of V_i will be taken. TA will remove the information of V_i from valid vehicles table, put it into revoked vehicles table, and then broadcast PID_i and $(S_{m+2}, VN_c, PN_i^{m+2})$ to all RSUs. V_i will be denied to make any MRSP information request. Without the MRSP information V_i cannot do any activity in the VANET immediately.

3.8 Working Sparse RSU Environment

In the proposed scheme, a vehicle will ask for MRSP information request in each time slots. It always maintains the MRSP information for two time slots and uses two nearest MRSP information to say hello. For example, V_i keeps the MRSP information $(S_{m-1}, VN_a, D_j^{m-1}, Sig1_i^{m-1})$ and $(S_m, VN_b, D_i^m, Sig1_i^m)$.

V_j has $(S_{m-2}, VN_c, D_j^{m-2}, Sig1_i^{m-2})$ and $(S_{m-1}, VN_d, D_j^{m-1}, Sig1_j^{m-1})$, but does not the information for S_m yet due to some reason.

V_i and V_j broadcast the hello message with two nearest MRSP information, they will use $S_{m-1}{}^{th}$ MRSP information to build the neighbor's information. So in the propose scheme, the longest distance between RSUs is the distance a vehicle running in 2 time slots. If the duration of time slot is one hour, the longest distance between two RSUs will be over hundred kilometers.

4 Security Analysis and Performance Evaluation

In VANET, a vehicle will be anonymous to keep the privacy about its identity and routing path, but it must be verified that it is a legal one, and can be recognized when it did malicious attack. The broadcasting message must be verified that it is integrity and sent by a legal vehicle. A VANET is vulnerable to various malicious attacks included colluding attacks, compromising attacks, masquerading attacks, forging attacks and reply attacks. So, the proposed scheme must be fully anonymous, satisfy all requirements for a VANET, and resist the malicious attacking.

4.1 Security Analysis

In the proposed scheme, a vehicle (V_i) shows out three information to present itself or to ask for the MRSP information.

- The identity issued by TA: (PID_i, PR_i)
- The MRSP information used for announcing hello message: $(S_m, VN_a, D_i^m, Sig1_i^m)$
- The MRSP information used for asking new MRSP information:

$(S_m, VN_a, D_i^m, ECE_{CPK_m}(PN_i^m \| PN_i^{m+1}), Sig2_i^m, Sig1_i^m)$

In here, $PID_i = (VN_i, RK_i, PK_i)$.

$$PR_i = a - f(H(VN_i), RK_i)k_i x^{-1} \quad \textbf{(1)}$$

$$CH(PID_i) = f(H(VN_i), RK_i)RK_i + PK_i \quad \textbf{(2)}$$

$$Sig_i{}^m = Sig(H(S_m \| VN_a \| D_i{}^m))_{CSK}{}^m \quad \textbf{(3)}$$

$$Sig_i{}^m = Sig(H(S_m \| VN_a \| PN_i^m))_{ssk_i}{}^m \quad \textbf{(4)}$$

$$CPK^m = CSK^m P, CSK^m = SP^m(d_0{}^m) \quad \textbf{(5)}$$

$$SPK_i^m = SSK_i^m P, SSK_i^m = H(PN_i{}^m)SP^m(d_0{}^m) \quad \textbf{(6)}$$

4.1.1 Colluding Attacks and Compromising Attacks

V_i has PID_i and PR_i, $CH(PID_i)$ will be equal to CH_{TA}. When PR_i is calculated by formula (1). TA embedded three secrets (a, x, k_i) in PR_i, and $N+2$ secrets ($a, x, k_i, ..., k_n$) in N private keys for N vehicles. So the vehicles cannot make colluding attack to retrieve the secrets (a, x) to masquerade TA.

At m^{th} slots, V_i has $PS_i{}^m$ and $D_i{}^m$,

$$D_i{}^m = \{d_{ix}{}^m \mid d_{i0}{}^m = d_0{}^m, d_{ix}{}^m \in_R D^m, x = 1 \sim S\} \quad \textbf{(7)}$$

$$PS_i{}^m = \{PS_{ix}{}^m \mid PS_{ix}{}^m = H(PN_i{}^m)SP^m(d_{ix}{}^m)P, d_{ix}{}^m \in d_i{}^m\} \quad \textbf{(8)}$$

Based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), it is infeasible to retrieve $SP^m(d_{ix}{}^m)$ from $PS_{ix}{}^m$, so the vehicle cannot retrieve the secrets in secret pool from compromised vehicles.

4.1.2 Masquerading Attacks

An attacker may masquerade to ask for MRSP information or to announce hello message. The attacks may be as follows.

4.1.2.1 Masquerading A Legal Entity to Ask MRSP Information

An attacker knows the condition in formula (2), it can make a fake PID_i' with VN_i', RK_i', PK_i' the value of $CH(PID_i')$ is equal to CH_{TA}. But it cannot make a PR_i' to satisfy $PK_i' = PR_i'Y$ due to the hard problem of ECDLP. So it cannot make a CHF pairing key to pass the verification in the process of MRSP1.

4.1.2.2 Masquerading with Fake MRSP Information to Announce hello Message

A malicious vehicle (V_k) may announce a fake hello message with $S_m', VN_a', D_i^{m\prime}$ or $Sig1_i^{m\prime}$ to avoid the tracking of malicious attack. $Sig1_i^{m'}$ is signed by common secret key (CSK^m) that is the 0^{th} secret in m^{th} time slot ($SP^m(d_0{}^m)$). V_k knows its $PS_{k0}{}^m$ and $PN_k{}^m$ but it is infeasible to retrieve CSK^m to make signature due to the hard problem of ECDLP. Based on the collision resistance of hash function, it is infeasible to make a fake $S_m{}', VN_a{}', D_i^{m'}$ that can pass the verification of signature without the signed key (CSK^m).

4.1.2.3 Masquerading with Fake MRSP Information to Ask New MRSP Information

In the process of MRSP2, ($S_m, VN_a, D_i^m, ECE_{CPK^m}$ $(PN_i^m \| PN_i^{m+1}), Sig2_i^m, Sig1_i^m$) are the MRSP information for asking new MRSP information. PN_i^m and PN_i^{m+1} are the private name of V_i used in S_m and S_{m+1}. Without $PS_{i0}{}^m$ and PN_i^m, an attacker cannot get common public key to make request to pass the verify of $Sig2_i^m$.

4.1.3 Forged Attacks and Replay Attacks

In message authentication, $\{M_i, F(x), HMAC(T_s \| M_i)_{VK}\}$ are the broadcasting message included message (M_i), polynomial function ($F(x)$) that is embedded the verify key of HMAC, and the HMAC of time stamp and M_i. Without the MRSP pairing keys that are set in the process of NVB, an attacker cannot forge a message that can pass the HMCA checking. The time stamp (T_s) in HMAC can resist the replay attack.

4.1.4 Anonymity and Conditional un-Traceability

A vehicle has four names, real name (RN_i), virtual name (VN_i), private name (PN_i) and anonymous name (AN_i). Real name is used for initial registering to get the identity. Virtual name is used to present itself with PID_i for MRSP1, that is exposed only one time in every day. Private name is used to make new MRSP information, it is assigned and kept by V_i. Anonymous name is randomly assigned by V_i at any time. An attacker cannot retrieve the private name or trace the routing path of V_i from anonymous name.

4.1.5 Revoking the Malicious Vehicles

As the description in 4.1, a vehicle (V_i) may used PID_i, ($S_m, VN_a, D_i^m, Sig1_i^m$) or ($S_m, VN_a, D_i^m$, $ECE_{CPK^m}(PN_i^m \| PN_i^{m+1}), Sig2_i^m, Sig1_i^m$) to present itself or to ask for MRSP information. So, when V_i makes malicious attack, it can be traced and revoked as described in 3.7.

4.1.6 Message Authenticating and Communicating Confidentially

As description in 3.5, 3.6 the MRSP pairing key will be calculated in the process of neighbor vehicles set building. Using MRSP pairing key, the vehicle can make message authentication or get the session key for communicating confidentially.

4.2 Performance Evaluating

This section will discuss the possibilities of obtaining MRSP pairing keys and authenticating the sender of messages. The proposed scheme will be compared to DCS [5], PASS [6], AAKA [7], BDH [9], and RSP [12] with respect to functions and performance in message authentication.

4.2.1 Probability of Obtaining MRSP Pairing Keys and Authenticating Sender of Message

As described in Section 3, T is the size of random secret pool in an RSU, S is the number of random secret in a vehicle. Let the number of neighboring vehicles be N. P_{NP} is the probability that two vehicles have no common random secret. P_P is the probability that two vehicles have common random secret and can get a MRSP pairing key generated by the common random secret for message authentication or confidential communication. P_{RP} is the probability that two vehicles have neither common random secret, nor a common direct trusted neighbor, so a broadcast message can be authenticated, but the legate of sender will be doubted.

$$
\begin{aligned}
&P_{NP} = C(T-S,S)/C(T,S)\\
&P_P = 1 - P_{NP}\\
&P_{RP} = P_{NP} \cdot P_{NP}{}^{NP_P} = P_{NP}{}^{(1+P_P N)}\\
&P_T = 1 - P_{NP}
\end{aligned}
$$

When V_i broadcasts a message, V_j has a probability P_T with directly or indirectly authenticated. In P_{NP}, the first term is the probability that V_j cannot be directly authenticated with V_i, and all trusted neighbors of V_j cannot be directly authenticated with V_i also (in the second term). When P_{NP} is smaller than 0.5, the probability that a sender cannot be authenticated is very small, when N is over 10.

4.2.2 Functionality Comparison

The functions of message authentication schemes for VANET are fully anonymous, conditional un-traceability, working under sparse RSUs environment, without certification, or malicious entities revocable. Table 7 compares the six schemes in terms of functionality, and shows that only RSP [12] and the proposed scheme can fulfill the first four functional requirements. The proposed scheme in RSP [12] can only achieve partial malicious attack revocation by recording a light revocation list in TA, the real identities of vehicles are obtained by tracing back from RSUs to the TA. The TA can tell all RSUs to deny registration requests from malicious vehicles, and then the malicious vehicles will be revoked when they want to register again. The proposed scheme maintained a revoked vehicles table in each RSU which sent by TA. The malicious vehicle will be denied to make any MRSP information request by matching revoked vehicles table in RSU, without tracing the tables back from RSUs to TA as RSP [12]. The malicious attack problem is totally solved by maintaining the revoked vehicle tables in each RSU.

Table 7. Comparison of functionality

Scheme Functions	[5] DCS	[6] PASS	[7] AAKA	[9] BDH	[12] RSP	Proposed Scheme
Fully anonymous	partial	yes	partial	partial	yes	yes
Conditional un-traceability	yes	yes	yes	yes	yes	yes
Working under sparse RSUs environment	no	no	yes	no	yes	yes
Without certification	no	no	yes	no	yes	yes
Malicious Entities Revocable	partial	partial	no	no	partial	yes

4.2.3 Performance Evaluating

The construction of a neighbor set and the processes of MRSP information request are performed offline, so the load associated with these processes can be ignored. During message authentication, the message must be signed to show that it had been sent by a legal vehicle and the signature must be verified. The loading of computations in message signing and verifying are measured. The computations may be bilinear pairing (T_p), EC encrypting (T_c), exponential operating (T_e) or HMAC (T_h). The computation times for T_p, T_c, T_e and T_h, measured on a 3 GHZ Pentium 4 PC [13-14] are 4.5 ms, 0.6 ms, 0.54 ms and 0.002 ms, respectively. Table 8 shows the loading of computations and times required by the proposed and other schemes. In the proposed scheme, the generation of F(x) in signing and the calculation of the verify key in verifying are the computations of polynomial function that can be ignored, so the computations involved in signing or verifying in the proposed scheme are HMAC computations only. As shown in Table 8, the proposed scheme and RSP [12] had better functionality and much lower computational complexity than the other four schemes.

Table 8. Comparison of schemes in terms of number of computations and time required

Method Phase	[5] DCS	[6] PASS	[7] AAKA	[9] BDH	[12]RSP	Proposed Scheme
Signing	2Tc	1Tc	2Te	2Tc	T_h	T_h
Verifying	5Tp + 3Tc	3Tp + 4Tc	2Te	Tp + Tc	T_h	T_h
Total Computations	5Tp + 5Tc	3Tp + 5Tc	4Te	Tp + 3Tc	$2T_h$	$2T_h$
Required Time	25.5ms	16.5ms	2.16ms	6.3ms	0.004ms	0.004ms

5 Conclusions

In this paper, we combined the concepts of chameleon hash function (CHF) and modified random secret pre-distribution (MRSP) to build a brand new message authentication scheme for VANET under sparse RSUs that is different from other schemes. Based on the CHF, TA keeps two common secrets that will be embedded to all identities to be as the evidence of mutual trusting. TA will issue one identity to every RSU and vehicle. An identity contains one public ID and one private key. The public ID included virtual name, random key, and public key, is used to present the entity and can be verified to be a legal one. The private key is used to claim the ownership of the public ID. Without any negotiating process, a CHF pairing key multiplied by one private key and other's public key will be used for mutually trusting and to be utilized as the session key of secure communicating between RSUs and vehicles. The proposed scheme especially maintained a revoked vehicles table in each RSU which sent by TA. This idea can lead the malicious vehicle cannot do any activity in the VANET, and overcome the partial malicious attack revocation problem of RSP [12] with minor overhead. The proposed scheme is very simple but can resist against colluding attacks, compromising attacks, masquerading attacks, forging attacks, and replaying attacks, and satisfies all requirements of a secure VANET, such as anonymity, un-traceability, message authentication, secure communication, and malicious entities revocation. The proposed scheme can work under very sparse RSUs environment and the computation involved in signing and verification for message authentication is only one HMAC, so the proposed scheme outperforms previously schemes.

References

[1] R. Uzcategui, A. J. D. Sucre, G. Acosta-Marum, Wave: A tutorial, *IEEE Communications Magazine*, Vol. 47, No. 5, pp. 126-133, May, 2009.

[2] X. F. Chen, F. Zhang, W. Susilo, Y. Mu, Efficient Generic On-Line/Off-Line Signatures Without Key Exposure, in: J. Katz, M. Yung (Eds.), *Applied Cryptography and Network Security, Lecture Notes in Computer Science*, Vol. 4521, Springer, 2007, pp.18-30.

[3] J.-P. Hubaux, S. Capkun, J. Luo, The Security and Privacy of Smart Vehicles, *IEEE Security and Privacy*, Vol. 2, No. 3. pp. 49-55, May, 2004.

[4] C. X. Zhang, X. D. Lin, R. X. Lu, P. H. Ho, X. M. Shen, An Efficient Message Authentication Scheme for Vehicular Communications, *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 6, pp. 3357-3368, November, 2008.

[5] A. Wasef, Y. X. Jiang, X. M. Shen, DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks, *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 2, pp. 533-549, February, 2010.

[6] Y. P. Sun, R. X. Lu, X. D. Lin, X. M. Shen, J. S. Su, An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications, *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 7, pp. 3589-3603, September, 2010.

[7] C. Y. Chen, T. C. Hsu, H. T. Wu, J. Y. Chiang, W. S. Hsieh, Anonymous Authentication and Key-Agreement Schemes in Vehicular Ad-Hoc Networks, *Journal of Internet Technology*, Vol. 15, No. 6, pp. 893-902, November, 2014.

[8] Y. H. Huang, K. H. Fan, W. S. Hsieh, Message Authentication Scheme for Vehicular Ad-Hoc Wireless Networks without RSU, *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 6, No. 1, pp. 113-122, January, 2015.

[9] M. W. Huang, H. T. Wu, G. J. Hong, W. S. Hsieh, Using BDH for the Message Authentication in VANET, *Mathematical Problems in Engineering*, Vol. 2014, pp. 1-13, September, 2014.

[10] W. S. Li, C. W. Tsai, W. S. Hsieh, C. S. Yang, M. C. Chiang, A Key Management Scheme for Dense Wireless Sensor Networks, *Journal of Information*, Vol. 14, No. 7, pp. 2459-2470, July, 2011.

[11] A. D. G. Yein, C. Y. Chen, T. C. Hsu, W. S. Hsieh, J. A. Lin, Attack Wireless Sensor Network Using Compromised Key Redistribution, *International Journal, Applied Mechanics and Materials, The Special Issue of Information Technology Applications in Industry*, Vol. 263-266, pp. 920-925, December, 2012.

[12] A. D. G. Yein, Y. H. Huang, C. H. Lin, W. S. Hsieh, C. N. Lee, Z. T. Luo, Using a Random Secret Pre-Distribution Scheme to Implement Message Authentication in VANETs, *Applied Sciences*, Vol. 5, No.4, pp. 973-988, October, 2015

[13] M. Scott, Implementing Cryptographic Pairings, *Proceedings of the First International Conference on Pairing-Based Cryptography*, Tokyo, Japan, 2007, pp. 177-196.

[14] M. Long, C. H. J. Wu, J. D. Irwin, Reducing Communication Overhead for Wireless Roaming Authentication: Methods and Performance Evaluation, *International Journal of Network Security*, Vol. 6, No.3, pp. 331-341, May, 2008.

[15] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, M. K. Khan, Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANETs, *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 4, pp. 3235-3248, April, 2017.

[16] M. R. Asaar, M. Salmasizadeh, W. Susilo, A. Majidi, A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks, *IEEE Transactions on Vehicular Technology*, Vol. 67, No. 6, pp. 5409-5423, June, 2018.

[17] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, *Proceeding of INFOCOM 2008. The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 2008, pp. 1229-1237.

[18] H. Krawczyk, T. Rabin, Chameleon Hashing and Signatures, *Proceeding of the 7th Annual Network and Distributed System Security Symposium*, San Diego, CA, USA, 2000, pp. 143-154.

[19] C. H. Lin, W. S. Hsieh, F. Mo, M. H. Chang, A PTC Scheme for Internet of Things: Private-Trust-Confidentiality, *Proceeding of 2016 30th IEEE International Conference on Advanced Information Networking and Applications*, Crans-Montana, Switzerland, 2016, pp. 969-974.

[20] W. S. Hsieh, S. Y. Liao, A. D. G. Yan, The Random Secret Pre-distribution for Wireless Sensor Network, *Proceedings of the Conference on Information Technology and Applications in Outlying Islands*, Kinmen, Taiwan, 2013, pp. 844-846.

[21] P. C. Kuo, *Chameleon Hash Based Message Authentication for VANET in Sparse RSU Environment*, Master Thesis, Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, 2015.

Biography

Chih-Hsueh Lin was born in Kaohsiung, Taiwan in 1977. He received the Ph.D. degree in computer science and engineering from National Sun Yat-sen University, Kaohsiung, Taiwan in 2006. From 2009 to 2018, he was an Assistant Professor with the computer and communication department, Shu-Te University, Kaohsiung, Taiwan. From 2018 to date, he was an Assistant Professor with the electronic engineering department, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan. His research interests include machine learning; information security; biomedical signal processing and data mining.