Appl. Sci. **2015**, *5*, 973-988; doi:10.3390/app5040973

OPEN ACCESS

applied sciences

ISSN 2076-3417

www.mdpi.com/journal/applsci

Article

Using a Random Secret Pre-Distribution Scheme to Implement Message Authentication in VANETs

Alan Dahgwo Yein [1], Yu-Hsiu Huang [2,3], Chih-Hsueh Lin [4,*], Wen-Shyong Hsieh [2,4], Chung-Nan Lee [2] and Zhong-Ting Luo [2]

[1] Department of Information Management, Shu-Te University, Kaohsiung 82445, Taiwan; E-Mail: alanyein@stu.edu.tw

[2] Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan; E-Mails: yhhuang@csu.edu.tw (Y.-H.H.); wshsieh@stu.edu.tw (W.-S.H.); cnlee@cse.nsysu.edu.tw (C.-N.L.); m013040085@student.nsysu.edu.tw (Z.-T.L.)

[3] Department of Computer Science and Information Engineering, Cheng-Shiu University, Kaohsiung 83347, Taiwan

[4] Department of Computer and Communication, Shu-Te University, Kaohsiung 82425, Taiwan

* Author to whom correspondence should be addressed; E-Mail: josuslin@stu.edu.tw; Tel.: +886-7-615-8000 (ext. 4800).

Academic Editor: Takayoshi Kobayashi

Received: 30 July 2015 / Accepted: 16 October 2015 / Published: 30 October 2015

Abstract: In recent years, the development of the Intelligent Transportation System (ITS) has increased the popularity of vehicular *ad hoc* networks (VANET). A VANET is designed to enable vehicles to exchange information about traffic or vehicle conditions to help other vehicles avoid traffic accidents or traffic jams. To resist malicious attacks, all vehicles must be anonymous and their routings must be untraceable, but still verifiable. The vehicles must trust each other and communicate confidentially. In a VANET, Road Side Units (RSU) are installed on traffic signs or streetlights to help vehicles maintain anonymity, to authenticate messages, or to support confidentiality. However, the coverage of an RSU is limited and the cost of widespread installation is high. RSU installations are incremental, so messages must be authenticated using dense RSUs or sparse RSUs. In this paper, the concept of random key pre-distribution that is used in Wireless Sensor Networks (WSN) is modified to random secret pre-distribution (RSP), which integrates identity-based cryptography (IBC) to produce a message authentication scheme for VANETs in a sparse RSU environment. In the proposed scheme, vehicles follow a process to determine a common secret, allowing them to

authenticate each other and obtain the pairing value as a key for use in message authentication and private communication. Evaluation results show that the proposed scheme outperforms related schemes.

Keywords: VANET; RSP; IBC; anonymity; message authentication; private communication

1. Introduction

A general VANET has a three-tier structure [1], which comprises a trusted authorizer (TA), many road side units (RSUs), and vehicles. The TA is the central trust tier, and it is connected to the RSU via a wired network. The communication between the RSUs and vehicles uses the wireless communication protocol IEEE 802.11p. IEEE 802.11p is a revision of 802.11 with the addition of Wireless Access in the Vehicular Environment (WAVE) [2]. All RSUs (second tier) and vehicles (third tier) must register with the TA to obtain initial certification, identities or common secrets to enable them to make requests anonymously. RSUs are installed at the side of the road to help vehicles maintain anonymity and authenticate messages. The vehicles can broadcast, exchange, or receive messages about road conditions, traffic conditions, their positions, or their speed to avoid accidents and worsening traffic jams. Malicious attackers [3,4] may collect transmitted messages in VANETs to obtain the private information of users. To resist malicious attacks and maintain the privacy of the vehicles, each vehicle must remain anonymous, and its messages must be sent anonymously, so the authentication of messages in VANETs is an important issue.

In a VANET, communications can be classified into two types—without RSU and with RSU. In communication of the first type, each vehicle broadcasts messages to other vehicles or communicates confidentially with specific vehicles. In this scenario, vehicles must ensure their privacy, their confidentiality and the authentication of messages by themselves. In the second scenario, an RSU supports the privacy and confidentiality of vehicles, and message authentication.

In a VANET, messages are authenticated to ensure that received messages are valid and have been sent by a legal source. To preserve privacy, the real identity of a vehicle cannot be exposed or traced. In this paper, the concept of random key pre-distribution that is used in Wireless Sensor Networks (WSN) is modified to random secret pre-distribution (RSP) that integrates identity-based cryptography (IBC), to build an environment in which vehicles can maintain anonymity, communicate confidentially, authenticate messages, and resist malicious attacks with the assistance of RSUs or by themselves in a sparse RSU environment. In the proposed scheme, the TA maintains a large pool of secrets that will be pre-distributed randomly to all RSUs and vehicles as the original registration set. All RSUs have a pseudo random generator (PRNG) and the same seed value that is provided periodically by the TA, so they have the same secret pool from which to issue the randomly selected secret to vehicles. Based on the common secrets held in common either between RSUs and vehicles or among vehicles under an RSU, entities of both types can authenticate each other, authenticate messages, and communicate confidentially following the pairing process. The proposed scheme satisfies the security requirements of a VANET, including message authentication, identity verification, non-repudiation, confidentiality, conditional anonymity, and un-traceability.

In this paper, Section 2 introduces related works and techniques that are used herein. Section 3 describes the proposed schemes. Section 4 analyzes the security and performance of the proposed schemes. The final section draws conclusions and provides suggestions for future works.

2. Related Works and Techniques

According to Hubaux *et al.* [5], a smart vehicle can record, compute, and specify its position. It uses the traditional public-key infrastructure (PKI). The complexity of computation is increased if the vehicle uses PKI to encrypt the messages. The computation overhead of the communication step is also then increased. Moreover, for privacy and un-traceability, the vehicle must frequently change its certificate, imposing a burden on the TA.

Zhang *et al.* [6] proposed a scheme in which RSUs were used to support message authentication by vehicles. When a vehicle enters the coverage range of an RSU, it establishes a secret key after mutual authentication. The vehicle will then generate a short message authentication code (MAC) using this secret key. The RSU will verify the authentication of MAC. However, exposure of the certificate creates the problem that the vehicles will become traceable.

In 2010, Wasef *et al.* [7] proposed the RSU-aided distributed certificate service (DCS), which enables vehicles to update their certificates from an RSU. A vehicle can update its certificate from any RSU, even when it is not in the coverage range of that RSU. The performance of the DCS depends on the density of the RSUs.

Sun *et al.* [8] proposed a pseudonymous authentication scheme with privacy preservation (PASS), which supports the DCS. The scheme can reduce the certificate-updating overhead and the revocation overhead. Attackers cannot trace legitimate vehicles, even when they compromise the RSU. However, the DCS has the loading of certificate and it can not work in sparse RSU environment.

Chen *et al.* [9] used chameleon hash values to perform anonymous authentication and used ID-based cryptography (CH-IBC) to perform key agreement. In this scheme, vehicles use a chameleon hash value as a disposable alias. They can verify message authentication and message integrity, but it still needs the assistance of an RSU.

Hung *et al.* [10] proposed a chameleon hash function-based message authentication scheme without RSUs, but they did not solve the problem of malicious revocation. Hung *et al.* [11] used the bilinear Diffie-Hellman method (BDH) to propose a message authentication scheme for a dense RSU environment, which involves certificate request RSU by RSU. Kuo [12] proposed a message authentication scheme that can get pairing value to establish mutual trust in intra- and inter-RSU environments based on the chameleon hash function, but this scheme suffers from malicious revocation.

Section 4 will compare DCS [7], PASS [8], CH-IBC [9], BDH [11] and the proposed scheme in terms of functionality and performance.

Two problems are evident in all of the listed schemes. First, RSUs perform the most important roles in message authentication, but their performance worsens as they become sparser. The second problem concerns the certification base. The privacy of vehicles is maintained by making their identities and routes non-traceable. Accordingly, identities must be anonymous and changed frequently, generating heavy loads that are associated with certificate changing and informing of revoked certification.

To solve the two aforementioned problems, we propose a secure scheme for VANET. The installation of RSUs can be increased even in very sparse environment, and the vehicles establish mutual trust and obtain the pairing value based on the secret that is embedded in their anonymous identities instead of by certification. The following section presents in the scheme in detail.

In a WSN, the random key pre-distribution (RKP) [13] is used to perform mutual authentication using a common secret key. A random subset of keys in the pool will be embedded into the sensor nodes before node deployment. The nodes in the WSN can authenticate each other if they have common secret keys. The plain secret keys in the nodes make RKP vulnerable to compromise attacks [14]. When some nodes are compromised, the attacker can make malicious nodes using the fake subset of secret keys that were collected from the compromised nodes. Hsieh *et al.* [15] modified RKP to RSP, in which the common secret is embedded in the private key. Pairing the private key [16] with the public key, nodes mutually authenticate using the common pairing value if their private key includes the common secret.

3. Proposed Scheme: RSP-Based Message Authentication for VANET

In the proposed scheme, one day is split into n time slots ($T_1 \sim T_n$), and the TA maintains a large secret pool that will be pre-distributed randomly to all RSUs and vehicles as information about the original registration set (ORG) at T_0. With a pseudo random generator and the same seed value that is provided by the TA in $T_1 \sim T_n$, all RSUs have the same secret pool from which to issue the random secret in response to registration requests from vehicles. Every day, in T_1 or the first time slot (T_t), a vehicle enters the coverage of an RSU, and requests the new registration set (NRG) using the information in its ORG. In another time slot, the vehicle can request the new registration set using the information in its NRG; set this NRG as its previous registration set (PRG), and set the new registration as its new NRG. Accordingly, the ORG, PRG and NRG that are maintained by a vehicle are requested at $T_0, T_{t-1}\ and\ T_t$, respectively. The information of the registration set includes issuer, time slot, set of identities, set of secret indices and set of private keys. The public key can be derived from the identity and the time slot, and in the public keys are embedded the indexed secret value to form the private keys. At any time, a vehicle can choose randomly one of its identities in ORG, PRG or NRG as its identity and announce this anonymous identity to all neighbors. An anonymous identity has the form (issuer, time slot, identity, set of secret indexes). Based on the information in a vehicle's anonymous identity, neighboring vehicles can find the common secret, calculate the pairing value, or find a neighbor that can help with message authentication or confidential communication. This section will describe this process in detail. Table 1 presents the associated notation and definitions.

Table 1. Notation and definitions.

Z_q	Z_q is a finite field that is formed by mod q, where q is a large prime number.
G,P, P^x	G is an EC addition group with mod q; P is the generator of G. P^x is the value 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.
ê (Q,R)	ê (Q,R) is a bilinear pairing function that pairs Q and R in G with a value in Z_q. ê (Q,R) satisfies the functions of pairing. ê (Q,R) = ê (R,Q), ê (aQ,bR) = ê (bQ,aR) = ê $(Q,R)^{ab}$
ID_{TA}, ID_{Ra}	ID_{TA} and ID_{Ra} are the IDs of the TA and RSUa.
SP_{TA}	SP_{TA} is the secret pool of the TA that is generated by a pseudo random generator with seed S_{do}; SP_{TA} has R_{TA} secrets. SP_{TA} = $\{SP_{TA}(d_i) \mid SP_{TA}(d_i) \in PRNG(S_{do}), d_i = 1\sim R_{TA}\}$ SP_{TA} (d_i) is the d_{ith} secret in SP_{TA}
SP_{Rt}	SP_{Rt} is the secret pool of RSUs , which is generated by $PRNG(S_{dt})$, where S_{dt} is sent by TA at T_t. All RSUs have the same SP_{Rt} at T_t; R_R is the size of SP_{Rt} and SP_{Rt} = $\{SP_{Rt}(d_j) \mid SP_{Rt}(d_j) \in PRNG(S_{dt}),\ d_j = 1\sim R_R\}$
DS_{Ra}, DS_{V_i}	DS_{Ra} and DS_{V_i} are the set of secret indexes of Ra and V_i. DS_{Ra} = $\{d_{Ray} \mid d_{Ray} \in_R (1\sim R_{TA}), y = 1\sim N_R\}$, N_R is the number of the index in DS_{Ra}, $N_R \ll R_{TA}$ DS_{V_i} = $\{d_{V_ix} \mid d_{V_ix} \in_R (1\sim R_{TA})$, or $d_{V_ix} \in_R (1\sim R_R), x = 1\sim N_V\}$. The secret of V_i can be issued by the TA or RSU; N_V is the number of the index in DS_{V_i}, $N_V < N_R$
PK_n	PK_n is the public key of node n , which may be an RSU or a vehicle. PK_n= $H(ID_i \parallel ID_n \parallel T_t)\ P$, ID_n is the ID of node n; T_t is the time slot in which the ID is assigned by issuer ID_i.
IDS_{V_i}	IDS_{V_i} is the set of identities of vehicle i; IDS_{V_i} = $\{ID_{V_ix} \mid ID_{V_ix} \in M , x = 1\sim N_V\}$. Every vehicle ($V_i$) has N_V anonymous IDs, assigned by an issuer or chosen by itself.
PRS_{V_i}	PRS_{V_i} is the set of private keys of V_i. PRS_{V_i}= $\{PR_{V_ix} \mid SP(d_{V_ix})\ PK_{V_ix}, x = 1\sim N_V\}$ If the private keys are assigned by the TA, then SP is SP_{TA} and PK_{V_ix} = $H(ID_{TA} \parallel ID_{V_ix} \parallel T_0)\ P$. If the private keys are assigned by R_a , then SP is SP_{Rt} and PK_{V_ix} = $H(ID_{RA} \parallel ID_{V_ix} /\!/ T_t)\ P$; T_t is the time slot in which the identities are assigned.
XRG_n	XRG_n is the registration set of node n ; X may be "O" for original registration, "P" for previous registration at T_{t-1} , or "N" for new registration at T_t. Node n may be an RSU or a vehicle. XRG_n = {*Issuer ID , Time slot,* IDS_n, DS_n, PRS_n}
ORG_{Ra}, ORG_{V_i}	ORG_{Ra} and ORG_{V_i} are the original registration sets of RSU a and Vehicle i that are issued by the TA at T_0. ORG_{Ra} = $\{ID_{TA}, T_0, ID_{Ra}, DS_{Ra}, PRS_{Ra}\}$ DS_{Ra} = $\{d_{Ray} \mid d_{Ray} \in_R (1\sim R_R), y = 1\sim N_R\}$ PRS_{Ra} = $\{PR_{Ray} \mid PR_{Ray} = SP_{TA}(d_{Ray})\ PK_{Ra}, y = 1\sim N_R\}$ SP_{TA} (d_{Ray}) is the d_{Ray}^{th} secret in SP_{TA}. PK_{Ra} = $H(ID_{TA} \parallel ID_{Ra} \parallel T_0)\ P$; R_a has one ID (ID_{Ra}) but N_R private keys. ORG_{V_i} = $\{ID_{TA}, T_0, IDS_{V_i}, DS_{V_i}, PRS_{V_i}\}$; IDS_{V_i} = $\{ID_{V_ix} \mid$ the anonymous ID (ID_{V_ix}) , $x = 1\sim N_V\}$ DS_{V_i} = $\{d_{V_ix} \mid d_{V_ix} \in_R (1\sim R_{TA}), x = 1\sim N_V\}$; PRS_{V_i} = $\{PR_{V_ix} \mid PR_{V_ix} = SP_{TA}(d_{V_ix})\ PK_{V_ix}, x = 1\sim N_V\}$; PK_{V_ix} = H($ID_{TA} \parallel ID_{V_ix} \parallel T_0$) P; V_i has IDS_{Vi}, DS_{Vi} and PRS_{Vi} that have N_V items in the set.
PRG_{V_i}, NRG_{V_i}	PRG_{V_i} and NRG_{V_i} are the previous (T_{t-1}) and new (T_t) registration sets of V_i; PRG_{V_i} = $\{ID_{Rx}, T_{t-1}, IDS_{V_i}, DS_{V_i}, PRS_{V_i}\}$; Here, the secret pool is SP_{Rt-1} and DS_{Vi} is the set of secret indexes in SP_{Rt-1}. NRG_{V_i} = $\{ID_{Ry}, T_t, IDS_{V_i}, DS_{V_i}, PRS_{V_i}\}$. The secret pool for NRG_{V_i} is SP_{Rt}.
ID_{V_i}	ID_{V_i} is the anonymous ID of V_i At any time, V_i can randomly choose one of IDS_{V_i} and claim to be ID_{V_i}.
$C(a, b)$	b elements taken from a elements, the number of combinations of b elements that may arise as $C(a, b)$
$E_k(m)$	Symmetric encryption of m using key k.

3.1. Original Registration Set (ORG)

All RSUs and vehicles must register with the TA to receive the original registration set (ORG_R or ORG_V). The TA will record the original information, including the original ID and the information about the original registration set, as in Table 2.

Table 2. Information about the original registration set in TA.

Entity Type	Real ID of Entity	Original Registration Set	Revoked?
RSU	Real ID of RSU_A	$\{ID_{TA}, T_0, ID_{Ra}, DS_{Ra}, PRS_{Ra}\}$	No
⋮	⋮	⋮	No
Vehicle	Real ID of Vehicle i	$\{ID_{TA}, T_0, IDS_{V_i}, DS_{V_i}, PRS_{V_i}\}$	No
⋮	⋮	⋮	No

3.2. Obtaining New Registration with ORG_{Vi}

At T_1 or the first time (T_t), a vehicle enters the coverage of an RSU, and requests the new registration set from that RSU (Ra). The steps are as follows.

S1. V_i randomly chooses one of its IDS_{V_i} in ORG_{V_i}, ID_{V_i}, to form the information of its anonymous identity and selects N_V new anonymous ID_S (IDS'_{V_i}) , before sending the request to R_a.

$$V_i \rightarrow R_a: (ID_{TA}, T_0, ID_{V_i}, DS_{V_i}),(IDS'_{V_i})$$

S2. After receiving the request, R_a compares DS_{V_i} with DS_{Ra} in ORG_{Ra} , and checks that if any $d_{V_ix}{}'$ in DS_{V_i} equals $d_{Ray}{}'$ in DS_{Ra}.

S2.1. If the equality holds, then R_a randomly chooses a subset of (1~R_R) to be the new DS'_{V_i}; sets new PRS'_{V_i}; makes the pairing value P_{Ra,V_i}; returns these message to V_i, and records information that includes the anonymous identity and new registration information.

$$R_a \rightarrow V_i: (ID_{TA}, T_0, ID_{Ra}), (DS'_{V_i}), (d_{V_ix}{}'), (E_{P_{Ra,V_i}}(PRS'_{V_i}))$$

where $d_{V_ix}{}' = d_{Ray}{}'$, $P_{Ra,V_i} = \hat{e}\ (PR_{Ray}{}', PK_{V_i})$

$$PRS'_{V_i} = \{PR'_{V_ix} \mid PR'_{V_ix} = SP_{Rt}\ (d'_{V_ix})\ H\ (ID_{RA} \parallel ID'_{V_ix} \parallel T_t)\ P, d'_{Vix} \in DS'_{Vi}, x = 1 \sim N_V\}$$

S2.2. Otherwise, R_a passes the request to its neighbor, R_b.

R_b processes step 2 in a manner similar to the processing by R_a until the positive response is sent back from R_x to R_a; then, the response is returned to V_i.

$$R_x \rightarrow R_b \rightarrow R_a \rightarrow V_i : (ID_{Ta}, T_0, ID_{Rx}), (DS'_{V_i}), (d_{V_ix}{}'), (E_{P_{Ra,V_i}}\ (PRS'_{V_i}))$$

S3. V_i receives the response , and then sets

$$NRG_{V_i} = \{ID_R, T_t, IDS'_{V_i}, DS'_{V_i}, PRS'_{V_i}\}$$

where ID_R may be ID_{Ra} or ID_{Rx}

Now, V_i receives its NRG_{Vi} , and R_a or R_x records the corresponding registration information, including NRG_{Vi} and the anonymous identity in ORG_{Vi}, as in Table 3.

Table 3. Recorded information about the anonymous identity and the new registration set (NRG_{Vi}) in RSU_A.

Anonymous Identity	New Registration Set	Revoked?
$\{ID_{TA}, T_0, ID_{V_i}, DS_{V_i}\}$	$\{ID_{Ra}, T_t, IDS_{V_i}', DS_{V_i}', PRS_{V_i}'\}$	No
⋮	⋮	No
$\{ID_{Rx}, T_{t-1}, ID_{V_i}, DS_{V_i}\}$	$\{ID_{Ra}, T_t, IDS_{V_i}', DS_{V_i}', PRS_{V_i}'\}$	No
⋮	⋮	No

3.3. Requesting New Registration Set with NRG_{Vi}

At T_{t+1}, RSUs generate a new secret pool SP_{Rt+1} for T_{t+1}, and the vehicle will request a new registration set, as follows.

S1. V_i randomly chooses one of its identities, the secret index, and the private key (ID_{V_ix}, d_{V_ix}, PR_{V_ix}) in NRG_{V_i}. V_i selects N_v new IDs to be IDS'_{Vi} and sends the request to Ra (which is in communicating range of V_i).

$$V_i \rightarrow R_a: (ID_{RX}, T_t, ID_{V_i}, DS_{V_i}), (IDS'_{V_i})$$

S2. After receiving the message, R_a randomly chooses a subset of (1~R_R) to be the new secret index set, DS'_{V_i}; sets a new set of private keys as PRS'_{V_i}, and selects one index in $DS_{V_i}(d_{V_ix})$

$$PRS'_{V_i} = \{PR'_{V_ix} \mid PR'_{V_ix} = SP_{Rt+1}\,(d'_{V_ix})\,H\,(ID_{Ra} \parallel ID'_{V_ix} \parallel T_{t+1})\,P, x = 1\text{~}N_V\},$$

making $P_{Ra,V_i} = \hat{e}\,(SP_{Rt}\,(d_{V_ix})\,H\,(ID_{TA} \parallel ID_{Ra} \parallel T_0)\,P,\,H\,(ID_{Ra} \parallel ID_{V_i} \parallel T_t)\,P)$, and then returns the message , before recording information that includes the anonymous identity and the new NRG_{Vi}.

$$R_a \rightarrow V_i: (ID_{TA}, T_0, ID_{Ra}, d_{V_ix}), (\,DS'_{V_i}), (\,Ep_{Ra,V_i}\,(PRS'_{V_i}))$$

S3. V_i receives the message; decrypts the attached PRS_{Vi} with $P_{Vi,Ra}$, sets $PRG_{Vi} = NRG_{Vi}$ and lets $NRG_{Vi} = \{ID_{Ra}, T_{t+1}, IDS'_{Vi}, DS'_{Vi}, PRS'_{Vi}\}$.

The pairing, $P_{Vi,Ra} = \hat{e}(SP_{Rt}\,(d_{V_ix})\,H\,(ID_{Ra} \parallel ID_{V_i} \parallel T_t)\,P,\,H\,(ID_{TA} \parallel ID_{Ra} \parallel T_0)\,P)$ equals P_{Ra,V_i}

Now, V_i receives its NRG_{Vi} and sets PRG_{Vi}; R_x records the corresponding registration information, including NRG_{Vi} and the anonymous identity in PRG_{Vi} as in Table 3, but the anonymous identities in PRG_{Vi}.

3.4. Constructing Set of Neighbors

At any time in T_t, the time slots in the *PRG* and the *NRG* in a vehicle may be (T_{t-1}, T_t) or (T_{t-2}, T_{t-1}). To construct the set of neighbors, every vehicle will say "hello" to all neighbors to announce its presence, and will periodically disclose its anonymous identity. Every vehicle must maintain a set of neighbors, which includes information about the neighbors and the expiration time. When V_i receives a hello message from V_j, V_i will determine whether V_j is in the set of neighbors; if it is, then V_i presets the expiration time of V_j. If V_j is a new vehicle, then V_i will set the $V_j's$ information in the neighbor set and preset the expiration time. The expiration time will be counted on continuously. When the expiration time of V_j is reached, the information of V_j will be removed.

Hello message

$$V_i \rightarrow \text{all: “Hello”}, (ID_{Ra}, T_t, ID_{Vi}, DS_{Vi}), \text{where } ID_{Vi} \in_R IDS_{Vi}$$

Construction of Set of Neighbors

V_i collects hello messages of all neighbors, and then builds the set of neighbors as follows.

V_i has the information of V_j, (ID_{Rb}, T_t, ID_{Vj} , DS_{Vj}), and V_j has the information of V_i, (ID_{Ra}, T_t, ID_{Vi}, DS_{Vi}). V_i generates the pairing value $P_{Vi,Vj}$ with V_j, and V_j generates the pairing value $P_{Vj,Vi}$ with V_i, consistent with Equations (1) and (2).

$$P_{\text{Vi,Vj}} = \hat{e}\left(\frac{H(ID_{Ra} \| ID_{Vi} \| T_t)}{H(ID_{Ra} \| ID_{Vix} \| T_t)} PR_{\text{Vix}}, PK_{\text{Vj}}\right) = \hat{e}\left(PK_{Vi}, PK_{Vj}\right)^{dvix} \quad (1)$$

$$P_{\text{Vj,Vi}} = \hat{e}\left(\frac{H(ID_{Rb} \| ID_{Vj} \| T_t)}{H(ID_{Rb} \| ID_{Vjy} \| T_t)} PR_{\text{Viy}}, PK_{\text{Vi}}\right) = \hat{e}\left(PK_{Vj}, PK_{Vi}\right)^{dviy} \quad (2)$$

If any d_{Vix} in DS_{Vi} equals d_{Vjy} in DS_{Vj}, then $P_{Vi,Vj}$ will equal $P_{Vj,Vi}$. $P_{Vi,Vj}$ is the pairing value of V_i and V_j that is used for mutual authentication. If no $d_{Vix} = d_{Vjy}$, then V_i checks for another vehicle in the set of neighbors (V_l) whose DS_{V_l} has a common index with DS_{Vj} and DS_{Vi} , and then puts “ID_{Vl}” in the pairing value field , enabling V_l to help V_i to authenticate with V_j . The information of V_k is taken at T_{t-1}, and V_i will use PRG_{Vi} to make a pairing with V_k in a pairing process that is similar to the process described above. In Table 4, V_i has a common secret with V_j and V_k, and V_j can help V_i and V_l to perform authentication.

Table 4. Set of neighbors.

Neighbor Vehicle	Pairing Value	Expiration Time
$(ID_{Rb}, T_t, ID_{Vj}, DS_{Vj})$	$P_{Vi,Vj}$	ET_j
$(ID_{Rc}, T_{t-1}, ID_{Vk}, DS_{Vk})$	$P_{Vi,Vk}$	ET_k
$(ID_{Rd}, T_t, ID_{Vl}, DS_{Vl})$	ID_{Vj}	ET_l

3.5. Message Authentication

For V_i, the neighbor set lists information about all neighbors, including their anonymous identities, pairing values, and the other vehicles that can help to pass messages. When V_i wants to broadcast a message, it will generate a polynomial function with all pairing values and a random key K, and then make the HMAC of the message and the time stamp with key K.

$F(x) = K + \prod(x - P_{Vi,Vj})$, where V_js are the neighbors of V_i, and the pairing values are $P_{Vi,Vj}$.

S1. $V_i \rightarrow$ all: (ID_{Ra}, T_t, ID_{Vi}),(M, T_s),$(F(x), HMAC(M \| T_S)_K)$,(List of ID_{Vk}) where ID_{Vk} is the ID of the vehicle that is in the pairing value field of the neighbor set, and can help V_i to rebroadcast this message.

S2. After V_j receives the message, V_j takes $P_{Vj,Vi}$ from the neighbor set of V_j; calculates $F(P_{Vj,Vi})$ to obtain K', and checks whether the $HMAC(M \| T_S)_{K'}$ equals $HMAC(M \| T_S)_K$; if it does, then Vj authenticates this message; otherwise, V_j rejects this message.

If V_j is in the list of ID_{Vk}, then V_j will rebroadcast this message by a similar process.

3.6. Communicating Confidentially

Two neighbors (V_i, V_j) can communicate confidentially using $P_{Vi,Vj}$ as an encryption key to encrypting the message and the time stamp. If V_i and V_j have no common secret but do have a common neighbor (V_k), then V_k has a common secret with V_i and V_j. V_i can communicate confidentially with V_j passing to the common neighbor V_k.

3.7. In a Sparse RSU Environment

A vehicle is associated with two sets of registration information (PRG and NRG). This information can be used for message authentication or confidential communication. If the longest distance between two neighboring RSUs is less than the distance through which a vehicle moves in two time slots, then a vehicle can always receive new registration information before the NRG expires. Therefore, RSUs can be incrementally deployed. Since all RSUs have the same SP_{Rt}, the concept of the RSP can be applied to all vehicles even if they register with different RSUs. If the vehicle cannot find any RSU to request the new registration, it still can use its ORG for message authentication.

3.8. Revocation

At any time, if a malicious vehicle is found using the information of anonymous identity that is claimed by the malicious vehicle, and the registration table is recorded in all RSUs, then the ORG, PRGs and NRGs of the malicious vehicle will be explored and revoked by the TA and all RSUs, so the malicious vehicle will not be able to request any new registration information in the next time slot. Only ORG revocation must always be recorded. Revoked PRGs and NRGs can be withdrawn in the next two time slots. Thus, the overhead of the revocation list is small. To trace the original registration information, all RSUs must keep a record of registration information for one day. The overhead of recording the registration table is also light.

For example, vehicle *i* registers its original registration set in TA with its real identity as the information in Table 5.1. At T_{t-2}, it registers a new registration set in RSU_a, $\{ID_{Ra}, T_{t-2}, IDS'_{vi}, DS'_{vi}, PRS'_{vi}\}$ with its anonymous identity, $\{ID_{TA}, T_0, ID_{vi}, DS_{vi}\}$ as the information in Table 5.2. Then, the vehicle obtains a new registration set from RSU_b and RSU_c at T_{t-1} and T_t as the information in Tables 5.3 and 5.4. When it was found that it use the anonymous identity $\{ID_{Rc}, T_t, ID'''_{vi}, DS'''_{vi}\}$ to perform a malicious attack in time slot T_t. According to the information in anonymous identity, Table 5.4 will be checked, and be traced back from Tables 5.4, 5.3, and 5.2 to Table 5.1 in TA. TA will revoke the right of vehicle *i*, and inform the information about the original registration set and the new registration sets in Tables 5.3 and 5.4 to all RSUs to deny the new anonymous request from vehicle *i*.

Table 5. Example of request for anonymous identities.

Table 5.1. Recording table in TA.

Real ID	Original Reg. Set
⋮	⋮
Real ID of vehicle i	$\{ID_{TA}, T_0, IDS_{vi}, DS_{vi}, PRS_{vi}\}$
⋮	⋮

Table 5.2. Recording table in RSU_a.

Anonymous ID	New Reg. Set
⋮	⋮
$\{ID_{TA}, T_0, ID_{vi}, DS_{vi}\}$	$\{ID_{Ra}, T_{t-2}, IDS'_{vi}, DS'_{vi}, PRS'_{vi}\}$
⋮	⋮

Table 5.3. Recording table in RSU_b.

Anonymous ID	New Reg. Set
⋮	⋮
$\{ID_{Ra}, T_{t-2}, ID'_{vi}, DS'_{vi}\}$	$\{ID_{Rb}, T_{t-1}, IDS''_{vi}, DS''_{vi}, PRS''_{vi}\}$
⋮	⋮

Table 5.4. Recording table in RSU_c.

Anonymous ID	New Reg Set
⋮	⋮
$\{ID_{Rb}, T_{t-1}, ID''_{vi}, DS''_{vi}\}$	$\{ID_{Rc}, T_t, IDS'''_{vi}, DS'''_{vi}, PRS'''_{vi}\}$
⋮	⋮

3.9. Broadcasting of Seed Value from TA to All RSUs

In every time slot, TA must broadcast a seed value to all RSUs to generate a new secret pool. Based on the same secret pool, all of new registration set requested in the same time slot will have the same properties of random secret pre-distribution. However, when an RSU is found to be performing a malicious attack, its right to respond to a new registration request in the following time slots must be suspended. To revoke the right of a malicious RSU to respond, the secret index of the malicious RSU is appended to the set of revoking secret indexes (DS_{vk}), and DS_{br} is made the set of secret indexes for broadcasting the new seed value. DS_{br} will be used by the TA to broadcast the seed value , as follows.

TA receives DS_{vk} and sets DS_{br} as an empty set.

S1. For all valid RSUs, R_i,

TA selects any one new secret index in DS_{Ri}, but not in DS_{vk} and DS_{br}; this new secret index is added to DS_{br}.

S2. TA sets $F1(x)=k1+\prod(x-d_i)$ and $F2(x) = k2+\prod(x-(SP_{TA}(d_i)P)^x)$, for all di in DS_{br}.

Now, TA can use DS_{br}, $F_1(x)$ and $F_2(x)$ to broadcast a new seed value, as follows.

S3. TA→ all: $ID_{TA}, T_t, n, F1(x)$, $HMACK1(ID_{TA} \| T_t \| n)$, $F2(x)$, $Ek2$(new seed value)

S4. RSU(*Ra*) receives the broadcast message.

Calculates $K_{1y} = F_1(d_{Ray})$, $d_{Ray} \in DS_{Ra}$, $y = 1 \sim N_R$

Checks whether any K_{1y}' exists such that $HMAC_{K1y'}(ID_{TA} \parallel T_t \parallel n)$ equals $HMAC_{k1}(ID_{TA} \parallel T_t \parallel n)$.

If K_{1y}' is exist, takes d_{Ray}', that K_{1y}' is equal to $F_1(d_{Ray}')$, calculate $K_2' = F_2\left(\left(\frac{PR_{Ray'}}{H(ID_{TA} \| T_0 \| ID_{Ray'})}\right)^x\right)$ and decrypt $E_{k2}'(.)$ to retrieve the new seed value to generate a new secret pool in time slot T_t.

Because the secret indexes of malicious RSU are not included in DS_{br}, even it quests the secret index in DS_{br}, but it has not the respective private key, so it can not get the decrypted key k_2' to retrieve the new seed value.

4. Analysis of Security and Performance

A VANET is vulnerable to various malicious attacks, including masquerading attacks, forgery attacks and reply attacks. To ensure the privacy of vehicles, the proposed scheme must support anonymity, confidential communication, and conditional un-traceability. When a legal vehicle makes a malicious attack, it will be traced and revoked.

4.1. Security Analysis

In the proposed schemes, the public key is formed by the hash value of the identity of the issuer, an anonymous identity, and the time slot, according to Equation (3). Any vehicle's public key can be calculated by any other vehicle. A vehicle's private keys are formed by the indexing secret and the vehicle's public key, according to Equation (4). Vehicles know the secret index but cannot retrieve the indexing secret because the ECDLP (Elliptic Curve Discrete Logarithm Problem) is hard. The pairing values are used to establish mutual trust and perform negotiation. The pairing values are bilinear mappings of one vehicle's private key and another vehicle's public key, which can be calculated by a vehicle without any negotiation. In the processes of requesting a new registration and building a neighbor set, the only exposed information is anonymous identity $\{ID_{Ra}, T_t, ID_{vi}, DS_{vi}\}$. ID_{Ra}, T_t *and* ID_{vi} can not be fake because they will be used to calculate the public key and the associated private key. DS_{vi} is exposed but does not include any information of secret value in secret pool. The information that is involved in message authentication is the message and pairing values that are derived by the vehicle. The following section discusses security in greater detail.

4.1.1. Masquerading Attacks

In the proposed scheme, one vehicle (V_i) uses the information of anonymous identity included (ID_{Ra}, T_X, ID_{Vi}, DS_{Vi}), to say "hello", and it uses PRS_{Vi} to generate a pairing value for message authentication or communication. ID_{Vi}, which is one IDS_{Vi}, can be used only in T_t. For any ID_{Vix} in IDS_{Vi}, the public key and private key are as follows.

$$PK_{Vix} = H(ID_{Ra} \parallel ID_{Vix} /\!/ T_t)\, P \quad (3)$$

$$PR_{Vix} = SP_{Rt}\,(d_{Vix})\, PK_{Vix} \quad (4)$$

V_i knows ID_{Vix}, d_{Vix} and PR_{Vix} but it cannot retrieve SP_{Rt} (d_{Vix}) because the ECDLP (Elliptic Curve Discrete Logarithm Problem) is a hard problem. Therefore, V_i cannot masquerade as having another anonymous ID without information of the secret pool. In message authentication and the construction of a set of neighbors, the only exposed information is ID_{Vi} , DS_{Vi}, $F(x)$ and $HMAC(M \parallel T_S)_K$, so an attacker cannot retrieve any private information about the private keys. Therefore, masquerading attacks are impossible.

4.1.2. Forgery Attacks

In a broadcast message, (ID_{Rt} , T_X, ID_{Vi}), (M, T_S) and ($F(x)$, $HMAC(M \parallel T_S)_K$), constitute the identity (ID_{Vi}), the broadcast message (M), and the polynomial function ($F(x)$) that is embedded the *HMAC* key K, and the *HMAC* of message. Without the pairing value that is derived with the common secret that is embedded in the private key, the *HMAC* key cannot be retrieved, and without the *HMAC* key, an attacker cannot forge a message that can pass the *HMAC* check. In the "hello" message, DS_{Vi} are broadcast with ID_{Vi} attached so, without the secret pool (SP_{TA} or SP_{Rx}), an attacker cannot obtain the pairing values with other vehicles.

4.1.3. Replay Attacks

The "hello" message is used to claim that the vehicle is present, and neighboring vehicles use the "hello" message to generate pairing value. Hence, replaying the hello message affects one more neighbor, but this neighbor cannot perform a mutual pairing to perform any attack without the private keys. The time stamp in the *HMAC* of a broadcast message and a communicated message can resist the replay attack.

4.1.4. Anonymity and Conditional Un-Traceability

In ORG, PRG or NRG, N_V anonymous IDs can be used for anonymity. At any time, a vehicle can randomly choose one of them to claim an identity. Since the identity can be changed at any time, the running path of the vehicle will be untraceable. However, since ORG, PRG, or NRG information is recorded in the TA or RSUs, the real identity of a vehicle that makes a malicious attack can be traced.

4.1.5. Message Authentication and Confidential Communication

In the construction of a set of neighbors, the pairing value between two vehicles that have a common secret is calculated mutually. The pairing value is calculated as $\hat{e}(PR_{Vix}, PK_{Vj})$ or $\hat{e}(PR_{Viy}, PK_{Vi})$, where PR_{Vix} and PR_{Viy} have a common secret. The pairing value will be used for message authentication or confidential communication. Based on the ECDLP, they know d_{Vix} or d_{Viy}, but they do not know the value of $SP(d_{Vix})$ or $SP(d_{Viy})$ in the secret pool of TA or RSU. If two vehicles do not have a common secret, but they have a common trusted neighboring vehicle, then they can communicate confidentially through the mutually trusted vehicle, or make message authentication from rebroadcasting message.

4.1.6. Revocation

The TA maintains all ORGs for the vehicles. RSUs maintain the registration PRG and NRG information for one day. Every T_l, or the first vehicle registration, the ORG information is used for new registration requests, and the registration information is recorded in an RSU. 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. PRG or NRG information can be used for two time slots, but malicious vehicles cannot use it to become newly registered.

4.2. Performance Analysis

This section will discuss the possibilities of obtaining pairing values and authenticating messages. The proposed scheme will be compared to DCS [7], PASS [8], CH-IBC [9] and BDH [11] with respect to functions and performance in message authentication.

4.2.1. Probability of Obtaining Pairing Value and Authenticating Messages

As described in Section 3, R_R is the size of the secret pool in an RSU; N_V is the number of secrets in a vehicle that has been assigned by an RSU. Let the number of neighboring vehicles be N_B. P_{NP} is the probability that two vehicles have no common secret. P_P is the probability that two vehicles have a common secret and so can generate a pairing value for message authentication or confidential communication. P_{RP} is the probability that two vehicles do not have a common secret and a common trusted neighbor, so a broadcast message cannot be authenticated.

$$P_{NP} = C\,(R_R - N_V, N_V)/C\,(R_R, N_V)$$

$$P_P = 1 - P_{NP}$$

$$P_{RP} = P_{NP}\,{P_{NP}}^{N_B P_P} = {P_{NP}}^{(1 + P_P N_B)}$$

When V_i broadcasts a message, V_j has a probability P_P of being directly authenticated. In P_{RP}, 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). P_{NP} is small, so the probability that a message cannot be authenticated is very small.

4.2.2. Functionality Comparison

The functions of message authentication schemes are anonymous, conditional un-traceability, message authentication in sparse RSU, or needing certification. Table 6 compares schemes in terms of functionality, and the proposed scheme fits all functional requirements.

Table 6. Comparison of functionality.

Functions \ Scheme	DCS [7]	PASS [8]	CH-IBC [9]	BDH [11]	Proposed Scheme
Anonymity	√	√	√	√	√
Conditional un-traceability	√	√	√	√	√
Authentication in sparse RSU environment	×	×	√	×	√
Does not need certification	×	×	√	×	√

4.2.3. Performance Analysis

The construction of a neighbor set is performed offline, so the load associated with pairing is ignored. During message authentication, the message must be signed to show that it has been sent by a legal vehicle and the signature must be verified. The numbers of computations in message signing and verification are measured. The computations may be bilinear pairing (T_P), EC multiplication (T_m), exponential (T_e) or *HMAC*. The computation times for T_P, T_m, T_e and *HMAC*, measured on a 3 GHZ Pentium 4 PC [16,17] are 4.5 ms, 0.6 ms, 0.54 ms and 0.002 ms, respectively. Table 7 shows the number 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 *HMAC* key K are computations of a polynomial function. The computing time can be ignored, so the computations that are involved in signing or verifying in the proposed scheme are *HMAC* computations only.

Table 7. Comparison of schemes in terms of number of computations and time required.

Phase \ Method	DCS [7]	PASS [8]	CH-IBC [9]	BDH [11]	Proposed Scheme
Signing	$2\,T_m$	$1\,T_m$	$2\,T_e$	$2\,T_m$	*HMAC*
Verification	$5\,T_P + 3\,T_m$	$3\,T_P + 4\,T_m$	$2\,T_e$	$T_P + T_m$	*HMAC*
Total Number of Computations	$5\,T_P + 5\,T_m$	$3\,T_P + 5\,T_m$	$4\,T_e$	$T_P + 3\,T_m$	2*HMAC*
Required Time	25.5 ms	16.5 ms	2.16 ms	6.3 ms	0.004 ms

5. Conclusions and Future Work

This paper proposed the concept of the RSP for constructing a message authentication scheme for use in VANETs. In the proposed scheme, all RSUs and vehicles must register with the TA to receive the original registration set (ORG). At any time, all RSUs have a common secret pool that is generated by a PRNG with a common seed value that is sent by the TA in every time slot. The RSUs act as issuers that can assign a sub-set of secrets to any vehicles that have been authenticated with their ORG or NRG, which were obtained in the previous time slot. For every T1, or whenever vehicles enter the VANET for the first time, vehicles request the new registration set (NRG) with the information in ORG. In other time slots, the vehicles can obtain the new registration set with the information in NRG to generate a new NRG. In the proposed scheme, vehicles randomly choose one of their IDs in NRG and the set of secret index to announce their presence periodically. Using the ID and secret index set,

neighboring vehicles can compute the mutual pairing value or find vehicles that can help them with message authentication.

In message authentication, a polynomial function is formed by the pairing values and the *HMAC* key. The *HMAC* of the message with the key will be attached to the broadcast message. Vehicles that receive a broadcast message use their pairing value to retrieve the *HMAC* key and to authenticate the message. Some vehicles are asked to rebroadcast the message for vehicles that do not have a common secret with the sender. The proposed scheme is very simple but satisfies all the requirements of a VANET, such as defense against masquerade, forgery and replay attacks, anonymity, un-traceability, message authentication, confidential communication, and a light revocation list. The only computation that is involved in signing and verification for message authentication is that associated with *HMAC*, so the proposed scheme outperforms previously proposed schemes.

In message authentication, the index-set of a secret sub-set must be broadcast, potentially leaking information of the secret pool, so future work should seek to hide the index set while ensuring that the load associated with message authentication is light.

Acknowledgments

This paper is the partial result of projects NSC101-2221-E366-003-MY3, MOST103-2632-E366-001 and MOST104-2632-E366-001. The authors thank the Ministry of Science and Technology, R.O.C., for its support.

Author Contributions

Alan Dahgwo Yein proposed the original idea and wrote the first draft. Yu-Hsiu Huang set up the main structure and the detail processes. Chih-Hsueh Lin revised the article and response the reviewer's comment. Wen-Shyong Hsieh leaded the supporting project. Chung-Nan Lee advised the manuscript. Zhong-Ting Luo proposed the basic concept in his master thesis.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Lu, R.; Lin, X.; Zhu, H.; Ho, P.; Shen, X. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. In Proceedings of the INFOCOM 2008, the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
2. Uzcategui, R.; Acosta-Marum, G. Wave: A tutorial. *Commun. Mag.* **2009**, *47*, 126–133.
3. Lin, X.D.; Sun, X.T.; Ho, P.H.; Shen, X.M. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
4. Raya, M.; Hubaux, J.-P. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, Alexandria, VA, USA, 7–10 November 2005.

5. Hubaux, J.; Capkun, S.; Luo, J. The Security and privacy of Smart Vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55.
6. Zhang, C.X.; Lin, X.D.; Lu, R.X.; Ho, P.H.; Shen, X.M. An efficient message authentication scheme for vehicular communications. *IEEE Trans. Veh. Technol.* **2008**, *57*, 3357–3368.
7. Wasef, A.; Jiang, Y.X.; Shen, X.M. DCS: An efficient distributed-certificate-service scheme for vehicular networks. *IEEE Trans. Veh. Technol.* **2010**, *59*, 533–549.
8. Sun, Y.P.; Lu, R.X.; Lin, X.D.; Shen, X.M.; Su, J.S. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3589–3603.
9. Chen, C.Y.; Hsu, T.C.; Wu, H.T.; Chiang, J.Y.; Hsieh, W.S. Anonymous authentication and key agreement schemes in vehicular ad-hoc networks. *J. Internet Technol.* **2014**, *15*, 896–902.
10. Huang, Y.H.; Fan, K.H.; Hsieh, W.S. Message authentication scheme for vehicular ad-hoc wireless networks without RSU. *J. Inf. Hidding Multimedia Signal Process.* **2015**, *6*, 113–122.
11. Huang, M.W.; Wu, H.T.; Hong, G.J.; Hsieh, W.S. Using BDH for the message authentication in VANET. *Math. Probl. Eng.* **2014**, *2014*, 1–13.
12. Kuo, P.C. Chameleon Hash Function Based Message Authentication for VANETs in sparse RSU Environment. Master Thesis, National Sun Yat-sen University, Kaohsiung, Taiwan, 2015.
13. Li, W.S.; Tsai, C.W.; Hsieh, W.S.; Yang, C.S.; Chiang, M.C. A Key Management scheme for dense wireless sensor networks. *Inf. J. Int. Interdiscip. J.* **2011**, *14*, 2459–2470.
14. Yein, A.D.-G.; Chen, C.Y.; Hsu, T.C.; Hsieh, W.S.; Lin, J.A. Attack wireless sensor network using compromised key redistribution. *Int. J. Appl. Mech. Mater. Spec. Issue Inf. Technol. Appl. Ind.* **2012**, *263–266*, 920–925.
15. Hsieh, W.S.; Yan, D.G.; Liao, S.Y. The Random Secret Pre-distribution for Wireless Sensor Network. In Proceedings of the Conference on Information Technology and Applications in Outlying Islands, Kinmen, Taiwan, 18 May 2013; pp.844–846.
16. Scott, M. Implementing cryptographic pairings. *Lect. Notes Comput. Sci.* **2007**, *4575*, 177–196.
17. Long, M.; Wu, C.-H.J.; Irwin, J.D. Reducing communication overhead for wireless roaming authentication: Methods and performance evaluation. *Int. J. Netw. Secure* **2008**, *6*, 331–341.

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).