Computing (2016) 98:685–708
DOI 10.1007/s00607-014-0393-x

LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication

Mingzhong Wang · Dan Liu · Liehuang Zhu · Yongjun Xu · Fei Wang

Received: 29 March 2013 / Accepted: 10 March 2014 / Published online: 25 March 2014

Abstract Authentication in vehicular ad-hoc network (VANET) is still a research challenge, as it requires not only secure and efficient authentication, but also privacy preservation. In this paper, we proposed a lightweight and efficient authentication scheme (LESPP) with strong privacy preservation for secure VANET communication. The proposed scheme utilizes self-generated pseudo identity to guarantee both privacy preservation and conditional traceability, and it only requires a lightweight symmetric encryption and message authentication code (MAC) generation for message signing and a fast MAC re-generation for verification. Compared with currently existing public key based schemes, the proposed scheme significantly reduces computation cost by 10^2–10^3 times and decreases communication overhead by 41.33–77.60 %, thus achieving resilience to denial of service (DoS) attack. In LESPP, only key management center can expose a vehicle's real identity from its pseudo identity, therefore, LESPP provides strong privacy preservation so that the adversaries cannot trace any vehicles, even if all roadside units are compromised. Furthermore, vehicles in LESPP need not maintain certificate revocation list (CRL), so any CRL related overhead is

M. Wang · D. Liu (✉) · L. Zhu
School of Computer Science, Beijing Institute of Technology, Beijing, People's Republic of China
e-mail: liudanking@126.com; liudanking@bit.edu.cn

M. Wang
e-mail: wangmz@bit.edu.cn

L. Zhu
e-mail: liehuangz@bit.edu.cn

Y. Xu · F. Wang
Institute of Computing Technology, Chinese Academy of Sciences, Beijing, People's Republic of China
e-mail: xyj@ict.ac.cn

F. Wang
e-mail: wangfei@ict.ac.cn

avoided. Extensive simulations reveal that the novel scheme is feasible and has an outstanding performance of nearly 0 ms network delay and 0 % packet loss ratio, which are especially appropriate for realtime emergency event reporting applications.

Keywords Secure VANET communication · Lightweight authentication · Strong privacy preservation · Conditional traceability · DoS resilience

Mathematics Subject Classification 90B18

1 Introduction

Vehicular ad hoc network (VANET) causes close attention from government, academia and motor industry in recent years. VANET is a promising approach to enhancing transportation safety and efficiency, and are the key technology for intelligent transportation system (ITS) [1–3]. In VANETs, each vehicle is equipped with an onboard unit (OBU), together with RSUs, a large scale self-organized network can be constructed by utilizing dedicated short-range communications (DSRC) [4] for vehicle-to-vehicle (V2V) and vehicle-to-roadside unit (V2R) data exchange. VANET is a green computing system. It not only increases the efficiency and effectiveness of the whole traffic electronic system. But also decreases vehicles' green-house gas emissions. Through VANET communications, road safety and driving experience can be improved, infotainment services [5] can be provided to bring much convenience to both drivers and passengers.

The creation of VANET is really a significant plus to transportation management and road safety. Nevertheless, VANET meets a set of unique challenges. On the one hand, the wireless communication in VANET is broadcasting in essence, which makes the data can be easily monitored, altered and forged. So the network security must be guaranteed. On the other hand, vehicles are located in an open physical space, privacy (e.g., driver's identity, license plate, position, travel route) leaking [38–40] in VANET not only exposes privacy information, but also brings threat to the lives and properties of drivers and passengers. For example, malicious vehicles or adversaries can use legitimate vehicles identity information to track the vehicles travel route and analyze drivers habit, then theft or other crime may be implemented by abusing VANET communications. So the privacy of each vehicle needs special consideration. In addition, the privacy preservation in VANET is conditional, i.e., the authorities can reveal the identity and other privacy information of the vehicle, in case of crime/car accident scene investigation and other disputes.

The basic idea to insure the security of VANET and privacy of vehicles is privacy preserving authentication. Up to now, researchers have suggested many privacy preserving authentication schemes for VANET. However, most of them are based on public key infrastructure (PKI) by employing traditional digital signature to authenticate message which leads to some drawbacks: (1) according to DSRC, every vehicle sends a message with a time interval about 100–300 ms and the communication range is about 300 m. A typical OBU with a 400 MHz processor requires about 20 ms to verify one signature [37]. Message verification is not an issue when the vehicle density keeps low. But when vehicle density is high, e.g., 200–1,000 vehicles are in the communication range, each vehicle needs to verify 2,000–10,000 messages per second

which causes significant computation overhead for vehicles and is far beyond OBU's capacity. Furthermore, the computational DoS attack can be effortlessly implemented and the availability of VANET is decreased. (2) Digital signature together with the corresponding certificate always take a significant portion of the packet size which causes additional bandwidth consumption and higher packet loss ratio. (3) In consideration of large scale and conditional privacy preservation feature of VAVETs, certificate updating and revocation generate a significant cost for certificate authority. Although there are some schemes [23,34] trying to combine digital signature with hash function and message authentication code to ease above shortcomings, the essence of the problem is still unsolved.

In this paper, we proposed a lightweight and efficient strong privacy preserving (LESPP) authentication scheme by mainly utilizing message authentication code (MAC) and symmetric encryption. To the best of our knowledge, LESPP is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication. The proposed scheme has the following unique features:

1. DoS resilience authentication: LESPP only requires a lightweight symmetric encryption and MAC generation for message signing and a fast MAC re-generation for verification. Compared with currently existing privacy preserving authentication schemes, LESPP significantly reduces computation cost by 10^2–10^3 times, which makes the scheme resilient to DoS attack. This feature makes the scheme especially suitable for large scale VANET.
2. Strong privacy preservation: Tamper-proof device (TPD) [7,12,36] is employed to protect cryptographic materials and generate pseudo identity to sign/verify messages, so vehicle privacy is preserved. In addition, only trust authority KMC can disclose vehicles' real identities with the system key (for vehicles, system key is protected by TPD, and vehicles can only do limited operations indirectly with system key), so LESPP provides strong privacy preservation, i.e., even if all RSUs are compromised, adversaries still do not know the real identities of vehicles.
3. Low certificate management overhead: In LESPP, vehicles no longer hold certificates, the certificate authority do not need to manage thousands of certificates compared with the PKI based schemes. In addition, with CRL abolished, any CRL related overhead is removed.
4. Low bandwidth consumption: For message signing, message packet carries a short MAC and pseudo identity instead of long digital signature and certificate. Besides, identity-based digital signature is utilized in process of signing hereby makes it no necessary to transmit certificate with signature, thus reducing the attached communication overhead. Compared with other schemes, LESPP decreases communication overhead by 41.33–77.60 %.
5. Low network delay: Benefitting from efficient authentication and low bandwidth consumption in LESPP, the network delay caused by security protocol is very low. This makes the scheme especially appropriate for real-time emergency event reporting applications.
6. RSU-aided system key updating: RSUs are employed to speed up system key updating, which shortens the key updating cycle.

The rest of the paper is organized as follows. Section 2 presents the research work related to privacy authentication in VANET. Section 3 defines the system model. Then the 4th section presents the scheme parts in detail. Section 5 gives scheme security analysis. Section 6 describes the experimental datasets, parameter settings and shows the details of our experimental results. In Sect. 7, we conclude the paper and discuss the future work.

2 Related work

Numerous of schemes have been suggested to tackle the issues of security and conditional privacy preservation in VANETs. The classification of these schemes can be divided into three types: (1) pseudonymous authentication based schemes; (2) group based schemes; (3) hybrid schemes.

Pseudonymous authentication based schemes employ anonymous private key to sign messages and the corresponding pseudonymous certificate to verify messages. As each $\{privatekey, pseudonymouscertificate\}$ pair are linked to a pseudo identity, the real identity of a vehicle is preserved. In [6], Raya et al. proposed a scheme named BP by pre-distributing a number of anonymous private keys and the corresponding certificates (e.g., 43,800 certificates in [6]) for each vehicle. Message is signed with a randomly chosen private key, and be verified by the corresponding anonymous certificate. As the anonymous certificate is generated according to a pseudo identity, real identity of a sender is not revealed and privacy is protected. The list of anonymous certificates related to the real identity of the drivers are kept by the authority to provide conditional traceability. In [7], Raya et al. introduced TPD to the scheme to take care of storing cryptographic material and operations to enhance the security. However, this kind of scheme have some obvious shortcomings: (1) the CRL increases quickly which will take a large storage to store CRL and a long time to do CRL checking before message verification. (2) When the authority need to revoke a vehicle, it has to revoke all the anonymous certificates that are hold by the vehicle. It causes a lot of bandwidth consumption and increases authority's certificate management overhead. In [8], Sun et al. optimized traditional pseudonymous authentication schemes by using hash chains [9] to reduce CRL size and employing proxy re-signature [10] to improve certificate-updating efficiency. In [11], Lu et al. introduced an efficient conditional privacy preservation (ECPP) scheme by generation of on-the-fly short-time anonymous keys between OBUs and RSUs which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys. Nevertheless, this scheme requires that RSUs are always reachable otherwise certificate updating will fail. In [12], Zhang et al. introduced an identity-based batch verification [13,14] scheme for privacy preserving authentication by utilizing TPD to generate random pseudo identities and corresponding private keys. Batch verification improves efficiency but is still not efficient enough compared with symmetric cryptography authentication schemes, and vulnerable to DoS attack.

The basic thought of group based schemes is employing a group to hide the group member, then the real identity is covered and privacy is protected. In [15], Lin et al. suggested a privacy preserving authentication scheme based on group signature

[16,17] and identity (ID)-based signature [18] (GSIS). In group signature, a message is anonymously signed by private key of a sender and verified by the group public key, while identities of senders can only be recovered by authorities. ID-based signature is applied by RSUs to digitally sign each message launched by RSUs to ensure its authority, where the signature overhead can be greatly reduced. CRL size of group signature is linear with the number of revoked vehicles, but CRL checking operation involves two paring calculations, which would take about 10^4 times computation cost than a string comparison [19]. In [20], Zhang et al. employed each RSU to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast V2V messages, which can be instantly verified by the vehicles in the same group (and neighbor groups). Due to numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET. But this scheme needs RSU to be pervasive otherwise the scheme is ineffective. In [21], Sampigethaya et al. proposed a scheme that dynamically forms a group, and each group has a group key and group leader. For group members in the same group communication, group key is used for signing and authenticating messages; for group to group or group to infrastructure communication, group leader acts as a proxy to send/request data instead of group members. The idea of group navigation of vehicles provides nature anonymity, but it may cost a lot of group leader's communication energy and computation resource, and makes the group leader become bottleneck of the system.

Hybrid schemes combine pseudonymous authentication protocol, digital signature, MAC and other authentication technologies to make a tradeoff between computation efficiency, CRL size, bandwidth consumption, verification delay, and so on. Calandriello et al. [22] proposed a hybrid scheme by combining pseudonym scheme with group signature. Each vehicle V is equipped with a group signing key gsk_v and group public key pgk_{CA}. A vehicle can issue a "self-cerfity" certificate for itself by gsk_v and then signing its message using private key corresponding to the "self-cerfity" certificate. In such a way, the average overhead of message authentication can be reduced, but the expensive group signature CRL checking still remains a problem. Studer et al. [23] introduced VAST scheme based on Elliptic Curve Digital Signature Algorithm (ECDSA) and modified version of Timed Efficient Stream Loss-Tolerant Authentication (TESLA++) [24]. ECDSA signature provides fast authentication and non-repudiation, and TESLA++ provides data integrity. The scheme is flexible, extensible and efficient, but it does not provide privacy preservation and conditional traceability. In [25], Lin et al. suggested a similar scheme with [23]. Lin's scheme utilizes pseudonymous authentication instead of direct using ECDSA for non-repudiation. So Lin's scheme offers privacy preservation and conditional traceability. But, the TESLA is directly used in Lin's scheme, which makes the scheme vulnerable to memory DoS attack and increased verification delay.

All of the above schemes are directly or indirectly based on the digital signature technology for message signing and verification, none of them are efficient enough for numerous message verification and appropriate for real large scale VANET deploying. In this paper, we address lightweight and efficient privacy preserving authentication and introduced a conditional privacy preserving authentication scheme based on message authentication code and symmetric encryption. Note that digital signature is only

utilized for TPD access authentication and system key management in our scheme. As intervals of TPD access authentication and system key management are quite long (e.g., once a year for system key updating when vehicle annual inspection), the computation and communication overhead can be ignored. To the best of our knowledge, the proposed scheme is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication.

3 System model and security notions

In this section, system model (network model and attack model) and design goals are presented.

3.1 Network model

We consider V2V and V2R communications based on DSRC protocol in VANET. There are three types of network entities: key management center (KMC), RSUs, vehicles.

- KMC: KMC is a trust authority and is fully trusted by all the other entities. It is powered with sufficient computation and storage resources and is in charge of (1) RSUs and vehicles registration, (2) vehicle information (including vehicle's real identity, owner information) and system key management (including key initiation, key updating and key revocation) and (3) message non-repudiation verification and conditional traceability.
- RSU: RSU is a kind of infrastructure deployed on the roadside and can communicate with KMC directly. It has a powerful communication capability with transmission range of 1–3 km. The chief duties of RSU are message forwarding and distributed RSU aided key updating.
- Vehicle: Each vehicle in VANET is equipped with an OBU and TPD. The OBU is used to communicate with each other by sending messages (local traffic information, traffic light information, emergency warning) and TPD is employed to store cryptographic materials and process cryptographic operations. TPD is secure against any compromised attempt in any circumstance. All the data stored in TPD cannot be extracted by an adversary, including cryptographic material, data and code [7,12,36].

3.2 Attack model

We assume the adversary can control the whole communication channel and it can monitor all the data pass through the channel and can also tamper the message, drop some packets and even replace the original message. Furthermore, the adversary can also capture and compromise small part of RSUs and vehicles. All the data transmit to/through compromised RSUs and vehicles can be obtained and analyzed by the adversary. The purpose of the adversary is to induce the legitimate vehicles to accept false or harmful messages without being detected and abuse the VANET to maximum

its gains (e.g., cheating neighboring vehicles to make a clear path to greedy driver's destination regardless of the cost to the system, snooping legitimate users' privacy).

3.3 Design goals

The proposed scheme has the following security design goals:

- DoS resilience authentication: All the messages should be authenticated to ensure these messages are indeed sent unaltered by legitimate vehicles in VANET. If the message is altered, the receiver can detect this modification. Furthermore, the authentication should be efficient (low storage cost and computation overhead) to avoid possible performance bottleneck and DoS attack.
- Identity privacy preserving: Privacy leaking in VANET stems from vehicle's real identity leaking. If authentication scheme employs traditional digital signature, the identity information is easily leaked [26] due to broadcasting nature in vehicular communication. So, identity privacy must be protected during V2V and V2R communication.
- Unlinkability: Schemes that use pseudo identity as a mask to cover the real identity provide anonymity, but do not guarantee unlinkability. The outside observer can link multiple messages to one vehicle through traffic analysis, which enables the adversary to trace a particular vehicle and incurs location privacy violation [27] problem. In [11], the author defines three levels of user privacy. In this paper, we aim to achieve the level 3 privacy: authentication, anonymity, unlinkability.
- Conditional traceability: For vehicles and RSUs, V2V and V2R communications are anonymous and unlinkable. But the KMC have the ability to verify non-repudiation of a message to ensure that no vehicles can deny the message generated by itself, and retrieve a vehicle's real identity when the message is in dispute.
- Strong privacy preservation: Even if all RSUs are compromised, the adversary cannot obtain vehicles' real identities and privacy information.

4 The proposed LESPP authentication scheme

In this section, we proposed a lightweight and efficient privacy preserving authentication scheme for secure VANET communication. The proposed scheme includes the following six phases:

1. KMC initiation and vehicle registration: KMC generates its private/public keys and system parameters, vehicles register themselves to KMC to configure their TPDs and apply for access tokens.
2. Message signing: Before sending a message, a vehicle signs the message with the self-generated pseudo identity by TPD.
3. Message verification: Vehicle verifies the received message with the corresponding pseudo identity to determine accept/reject the message.
4. System key updating: KMC broadcasts the key updating information to vehicles to update system key.

5. Vehicle revocation: KMC broadcasts the revocation information to vehicles to revoke vehicles.
6. Message tracing: KMC traces the original of the message with the system key.

In VANET, each vehicle is equipped with a TPD which consists of four modules: (1) authentication module, (2) message signing module, (3) message verification module, (4) key updating module, which are shown in Fig. 1. Any TPD related operations must pass authentication module first, therefore, an adversary cannot take advantage of the TPD even if the vehicle is stolen. For convenience, the notations throughout this paper are listed in Table 1:

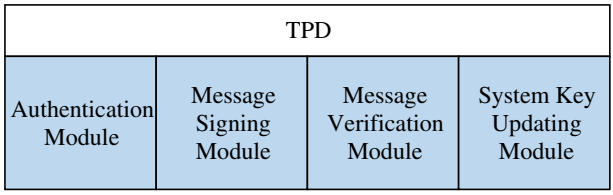

Fig. 1 Modules of TPD

Table 1 Notations

Notations	Descriptions
KMC	Key management center, a trust authority
$Vehicle_i$	The ith vehicle
TPD_i	TPD of $Vehicle_i$
$\mathbb{G}$	A cyclic additive group
V	A cyclic multiplicative group
k_m	The system key
ts	Timestamp
m	A message
ID_i	The real identity of $Vehicle_i$
ID_{KMC}	The identity of KMC
$PID_{i,ts}$	Pseudo identity of $Vehicle_i$ at ts
$Info_i$	Vehicle information of $Vehicle_i$
$h(.)$	Hash function $h : \{0,1\}^* \times V \rightarrow \mathbb{Z}_q^*, \mathbb{Z}_q^* = \{x \in \{1,\ldots,q-1\} \mid gcd(x,q) = 1\}$
$h_k^1(.)$	Hash function $h_k^1 : \{0,1\}^* \rightarrow \{0,1\}^n$
$H(.)$	Hash function $H : \{0,1\}^* \rightarrow \mathbb{G}^*, \mathbb{G}^* = \mathbb{G} \backslash \{0\}$ [31]
$Enc_k(.)$	Encryption function using k as the encryption key, such as AES [28]
$MAC_k(.)$	MAC computation function using k as a key, such as HMAC [29]
$mac_{m,ts}$	Message authentication code of message m at ts
$Sign_k(.)$	Identity-based message signing function [30]
$Verify_{id}(.)$	Identity-based message verification function [30]
$\|\|$	Message concatenation operation

4.1 KMC initiation and vehicle registration

At the stage of KMC initiation and vehicle registration, KMC initiates system parameters and vehicles register themselves to KMC. Let $\mathbb{G}$ be a cyclic additive group of order q, $P \in \mathbb{G}$ a generator of $\mathbb{G}$ and let $e : \mathbb{G} \times \mathbb{G} \rightarrow V$ be a bilinear map which satisfies following conditions [30]:

1. Bilinear: $e(x_1 + x_2, y) = e(x_1, y)e(x_2, y)$ and $e(x, y_1 + y_2) = e(x, y_1)e(x, y_2)$.
2. Non-degenerate: There exists $x \in \mathbb{G}$ and $y \in \mathbb{G}$ such that $e(x, y) \neq 1$.

Then KMC initiates system parameters and vehicles register themselves to KMC as follows:

- KMC initiation:
  1. KMC randomly picks integer $\alpha \in \mathbb{Z}_q^*$ as system private key, and computes $\beta = \alpha P$ as system public key.
  2. KMC computes $S_{ID_{KMC}} = \alpha H_{ID_{KMC}}$ as its identity secret key and generates system key $k_m = \{k_m^1, k_m^2\}$, where $k_m^1 \in \{0, 1\}^a$, a is the key length of $Enc_k(.)$; $k_m^2 \in \{0, 1\}^b$, b is the key length of $h_k^1(.)$.
  3. KMC publishes $\{\beta, ID_{KMC}\}$, and keeps α, k_m, $S_{ID_{KMC}}$ secret.
- Vehicle registration:
  1. For each vehicle, represent as $Vehicle_i$, firstly, it submits its real identity ID_i and vehicle information $Info_i$ (e.g., engine serial number, date of manufacture, vehicle owner) to the KMC through secure channels (e.g., drive to KMC to submit information personally).
  2. Then KMC checks the correctness of these information (usually with assistance of national vehicle management department). If the information is valid, KMC randomly picks $PID_i \in \mathbb{Z}_q^*$ as $Vehicle_i$'s initial pseudo identity, and generates the signature $\sigma_i = Sign_{S_{ID_{KMC}}}(ID_i)$. The signature generation is computed as follows:
     (a) KMC chooses an arbitrary $P_1 \in \mathbb{G}^*$, picks a random integer $k \in \mathbb{Z}_q^*$;
     (b) $r = e(P_1, P)^k$, $v = h(ID_i, r)$, $u = vS_{ID_{KMC}} + kP_1$;
     (c) $\sigma_i = \{u, v\}$.
  3. Finally, KMC saves $Vehicle_i$'s registration information, preloads $\{\{\beta, ID_{KMC}\}, \{ID_i, \sigma_i\}, ts, k_m, PID_i\}$ on the TPD of $Vehicle_i$ and sends the vehicle owner $\{ID_i, \sigma_i\}$ as the access token. Access token is kept secret by $Vehicle_i$. Vehicle registration procedure is shown in figure 2.

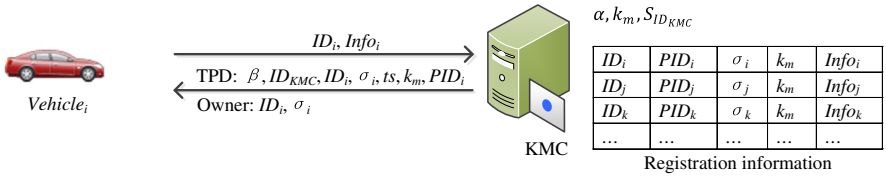

Fig. 2 Modules of TPD

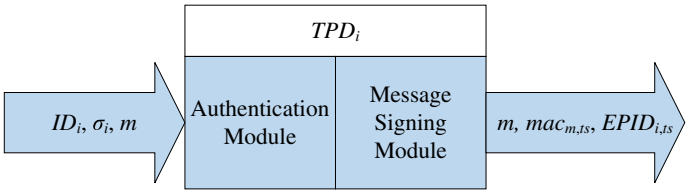

Fig. 3 Message signing process

4.2 Message signing

When a vehicle generates a message, it has to sign the message before sending it to other vehicles. The original message format is $\{timestamp, message\ type, message\ content\}$. Message signing phase can be divided into two steps: (1) access token verification, (2) message signing, and it utilizes authentication module and message signing module of TPD to process the task as shown in Fig. 3.

- Access token verification: In order to prevent abuse of TPD, any TPD related operation must pass access token verification first.
  1. Compare $\{ID_i, \sigma_i\}$ with access token stored in the TPD, if they are not equal, return *invalid* and exit verification.
  2. Query that whether $\{ID_i, \sigma_i\}$ have been verified, if they have already been verified since vehicle started, return *valid* and exit verification.
  3. Authentication module verifies $1? = Verfifry_{ID_KMC}(ID_i, \sigma_i)$. If ID_i,σ_i passes verification, record $\{ID_i, \sigma_i\}$ and return *valid*. Signature verification is computed as follows:
     (a) $\sigma_i = \{u, v\}, r = e(u, P) \cdot e(H(ID_{KMC}), -\beta)^v$;
     (b) If $v == h(ID_i, r)$, return 1; otherwise return 0.
- Message signing. If access token verification returns *valid*, TPD signs a message m as follows:
  1. Message signing module generates $Vehicle_i$'s current pseudo identity $EPID_{i,ts} = Enc_{k_m^1}(PID_{i,ts})$, where $PID_{i,ts} = PID_i||ts$;
  2. Computes $mac_{m,ts} = MAC_{k_{ts}}(m)$ as message authentication code of m where $k_{ts} = h^1_{k_m^2}(EPID_{i,ts})$.

After the vehicle signs the message, it sends $\{m, mac_{m,ts}, EPID_{i,ts}\}$ to other vehicles.

4.3 Message verification

When $Vehicle_j$ receives message $\{m, mac_{m,ts}, EPID_{i,ts}\}$ from $Vehicle_i$, it verifies message as follows before accept it. Message verification phase can be divided into two steps: (1) access token verification, (2) message verification, and it utilizes authentication module and message verification module of TPD to process the task as shown in Fig. 4.

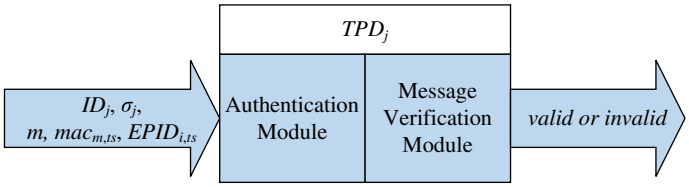

Fig. 4 Message verification process

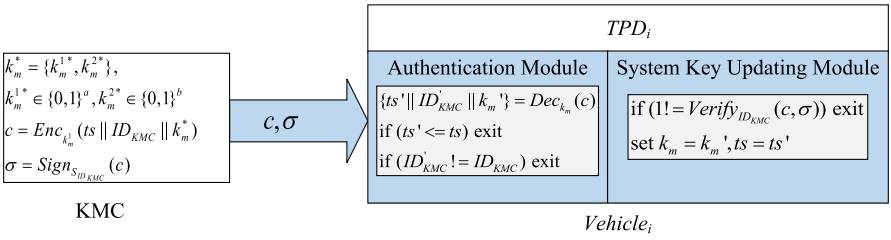

Fig. 5 System key updating process

- Access token verification: Authentication module verifies $\{ID_j, \sigma_j\}$ just like in the message signing phase.
- Message verification: Message verification module computes $mac'_{m,ts} = MAC'_{k'_{ts}}(m)$ where $k'_{ts} = h^1_{k^2_m}(EPID_{i,ts})$, if $mac'_{m,ts} == mac_{m,ts}$, $Vehicle_j$ accepts message m, otherwise rejects it.

4.4 System key updating

System key k_m is protected by TPD, and any TPD related operation must pass authentication module first. Thus an adversary cannot take advantage of the TPD even if the vehicle is stolen. In order to further enhancing the system security, we introduce system key updating strategy to update k_m periodically. The system key updating process is shown in Fig. 5.

System key updating is carried out by KMC, distributed RSUs and vehicles: KMC broadcasts system key updating information $\{c, \sigma\}$, then RSUs re-broadcasts this information to vehicles to aid system key updating, when a vehicle finishes system key updating, it broadcasts the information to its neighbor vehicles to speed up system key updating phase.

It should be noted that system key updating in VANET does not require synchronization. When a legitimate vehicle finds that its system key is expired, it sends a key updating request to KMC through the nearest RSU to obtain $\{c, \sigma\}$ to update system key.

4.5 Vehicle revocation

Revoking $Vehicle_i$ in LESPP is really straightforward: KMC broadcasts $\{PID_i, \sigma_i\}$ where PID_i is the initial pseudo identity of $Vehicle_i$, and $\sigma_i = Sign_{S_{IDKMC}}(PID_i)$.

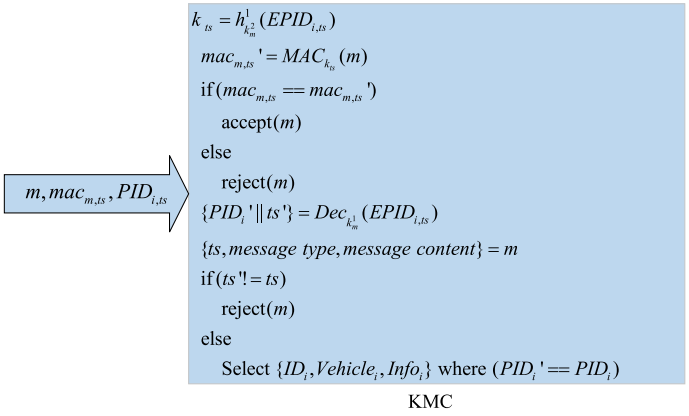

Fig. 6 Message tracing process

When $Vehicle_i$ receives $\{PID_i^{'}, \sigma_i^{'}\}$, TPD verifies $PID_i^{'}? = PID_i$ and $1? = Verify_{ID_{KMC}}(PID_i^{'}, \sigma_i^{'}$. If $\{PID_i^{'}, \sigma_i^{'}\}$ passes verification, TPD of $Vehicle_i$ deletes all the cryptographic material (e.g., PID_i, k_m) stored in TPD to make the TPD invalid. As a result, $Vehicle_i$ is revoked and can no longer generate valid traffic messages. PID_i is the pseudo identity of $Vehicle_i$, so the adversary is unable to link the history messages to $Vehicle_i$, and the backward security is guaranteed.

4.6 Message tracing

When a message is in dispute, KMC can trace the original message sender by the following steps as shown in Fig. 6. Through message tracing, KMC can verify non-repudiation of the message and track the message's original sender.

5 Security analysis

According to the design goals in Sect. 3.3, the security analysis is discussed in the following paragraph. In discussion, we also analyze some representative authentication schemes (e.g., BP, GSIS, VAST) introduced in Sect. 2 to compare with LESPP. The comparison result of different security properties that schemes fulfill is demonstrated in Table 2.

– DoS resilience authentication: In LESPP, message authentication code is utilized to guarantee the integrity of the message. KMC can disclose the original sender of the message with system key k_m to provide non-repudiation. Only symmetric encryption, MAC and hash function which are at least 2–3 orders of magnitude faster than public key based operations [32] are used for message signing and verification, so the proposed authentication scheme is lightweight and efficient. It should be noted that although access token verification requires an identity-based signature verification, it only happens once when the vehicle just starts

Table 2 Comparison of different security properties schemes fulfill

Property	Scheme			
	BP	GSIS	VAST	LESPP
Integrity	✓	✓	✓	✓
Non-repudiation	✓	✓	✓	✓
Level 3 unlinkability				
Authentication	✓	✓	✓	✓
Anonymity	✓	✓	×	✓
Anonymity	×	✓	×	✓
Conditional traceability	✓	✓	×	✓
Strong privacy preservation	×	×	×	✓
DoS attack prevention	×	×	✓	✓

up. So it does not affect the performance of the scheme. KMC is responsible for RSUs/vehicles registration and system information management which only require a small amount of computation and storage overhead. Furthermore, KMC is powered with sufficient resources, so it will not be the bottleneck of the while system even if the scale of VANET becomes very large. While for public cryptography based authentication schemes, such as BP, GSIS, authentication causes high computation overhead, which makes them vulnerable to DoS attack, especially when vehicles are intensive in a relative small area.

– Identity privacy preserving: Pseudo identity is utilized for V2V and V2R communication. Pseudo identity is encrypted with system key k_m, which prevents real identity leaking and pseudo identity spoofing attack. Therefore, the real identity of a vehicle is preserved, and any attacking based on the identity tracking will fail no matter how many messages the adversary collects. System key k_m is protected by TPD, and can not be used directly by vehicles. Thus, even if the vehicle is stolen, the identity privacy is still preserved. KMC stores system key and vehicle's privacy information. Based on our system model, it is a trust authority and secure against adversary's all kinds of attack. So adversaries could not take any advantage of KMC to obtain vehicles' privacy. VAST scheme combines improved TESLA protocol with digital signature, and are resilient to DoS attack, but it utilizes vehicle's real certificate for authentication, the identity privacy is not preserved.
– Unlinkability: Pseudo identity varies as time changes, which avoids the adversary link multiple messages to one vehicle and replay attack. Message signing module generates message authentication code and message verification module can verifies message without knowing sender's identity privacy, so the proposed scheme achieves *level 3 privacy*: authentication, anonymity, unlinkability. BP scheme uses a number of pseudo certificates to mask the real identity of the vehicle, however, during the short life time of a special pseudo certificate, the linkability between messages and the particular vehicle is still kept.
– Conditional traceability: Only KMC can disclose original sender of a message with system key k_m when a message is in dispute. We emphasize that the property

of traceability must be conditional, because if the traceability is unconditional, the property of unlinkability will becomes meaningless. Obviously, VAST scheme only guarantees unconditional traceability, which makes the adversary can trace a particular vehicle and incurs location privacy violation problem.
– Strong privacy preservation: In LESPP, RSUs are responsible for traffic message forwarding and distributed RSU-aided system key updating. RSUs do not have any knowledge of vehicles' real identities and privacy. In additional, Traffic message is protected by message authentication code, and system key updating message is signed by KMC. So, any modification or forging will be detected. Even if all RSUs are compromised, the adversary still cannot obtain vehicles' real identities and privacy information.

6 Performance evaluation

In this section, we evaluate the performance of the proposed LESPP with BP, GSIS, VAST schemes. Tate pairing [33] is adopted in our evaluation, where $\mathbb{G}$ is represented by 161 bits, and the order q is represented by 160 bits. Moreover, we utilize AES-128 as $Enc_k(.)$, HMAC as $MAC_k(.)$, SHA-1 as $h_k^1(.)$. Let N_{crl} denote the number of CRL items, T_{mul} denote the time to compute one point multiplication, T_{par} denote the time to perform one pairing operation, T_h denote the time of one hash function operation, T_{mac} denote the time of one message authentication code operation, T_{enc} denote the time of one encryption operation. T_{mul}, T_{par}, T_h, T_{mac}, T_{enc} dominate the computation performance of schemes, for simplicity, we only consider these operations for authentication overhead evaluation, certificate updating overhead evaluation and vehicle revocation overhead. We run 100 times point multiplication, tate pairing, SHA-1 hash function, AES-128 encryption on a machine equipped with an Intel Core (TM) 2 Duo CPU @ 2.4GHz respectively, and the average operation times are 5.4 ms, 40.7 ms, 6 μs, 16.7 μs, 40.7 μs respectively. The following simulation adopts the measured processing time based on these data. The certificate validity period $\triangle T = 60$s, and vehicles broadcasts a message every 300 ms according to DSRC.

6.1 Authentication overhead

6.1.1 Communication overhead

Communication overhead for authentication one message consists of the attached certificate and signature. In BP, the certificate is 63 bytes, and the signature is 42 bytes, therefore the communication overhead of BP for one message is 105 bytes. The signature length of GSIS is 192 bytes. Group signature utilizes group public key to verify messages, so there is no need to attach certificate with the signature. Communication overhead of VAST includes 63 bytes certificate, 20 bytes message authentication code, 42 bytes signature, 16 bytes symmetric key and 4 bytes index ID. In LESPP, there is no certificate communication overhead, its communication overhead is 20 bytes message authentication code and 23 bytes pseudo identity. So

Table 3 Communication overhead of sending one message

	BP	GSIS	VAST	LESPP
Communication overhead (byte)	105	192	145	43

Table 4 Message signing cost

	BP	GSIS	VAST	LESPP
Computation cost	T_{mul}	$3T_{par} + T_h$	$T_{mul} + T_{mac}$	$T_h + T_{mac} + T_{enc}$

the communication overhead of LESPP is 43 bytes. Table 3 shows communication overhead of sending one message.

It can be seen that, compared with BP, GSIS, VAST, the proposed LESPP causes the lowest bandwidth consumption, and it significantly decreases communication overhead by 41.33–77.60 %.

6.1.2 Message signing cost

In BP, message signing requires one point multiplication, so the cost is T_{mul}. Message signing cost is shown in Table 4. According to our former experiment, BP can sign $1/0.0054 \approx 185.2$ messages every second. Figure 7 illustrates the number of messages that the scheme can sign per second. It can be seen that, LESPP is the fastest scheme for message signing, and can sign 14,347.2 messages per second.

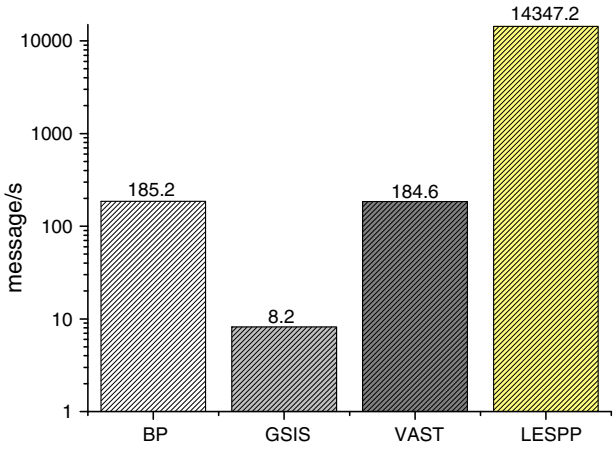

Fig. 7 Message signing speed

Table 5 Message verification cost

	BP	GSIS	VAST	LESPP
CRL checking	0	$2N_{crl}T_{par}$	0	–
Certificate verification	$2T_{mul}$	0	$2T^*_{mul}$	–
signature verification	$2T_{mul}$	$5T_{par} + T_h$	$2T^*_{mul} + 2T_{mac}$	$T_h + T_{mac}$
Total	$4T_{mul}$	$2N_{crl}T_{par} + 5T_{par} + T_h$	$4T^*_{mul} + 2T_{mac}$	$T_h + T_{mac}$

In VAST, certificate and digital signature verification is only performed when non-repudiation is necessary

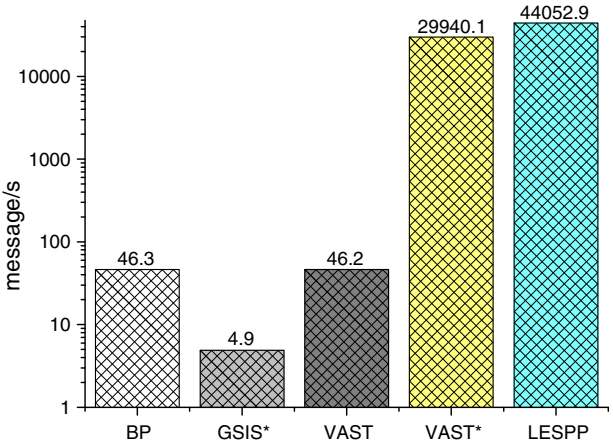

Fig. 8 Message verification speed. GSIS* represents the best performance of GSIS, i.e., $N_{crl} = 0$; VAST* is the performance result when non-repudiation is not necessary, i.e., $T^*_{mul} = 0$

6.1.3 Message verification cost

For BP, GSIS and VAST, message verification includes CRL checking, certificate verification and signature verification. In BP and VAST, CRL checking is simple string comparison, the computation cost can be ignored. While GSIS needs two paring operations for each CRL item, and the CRL checking cost is $2N_{crl}T_{par}$. Table 5 shows message verification cost. Together with the message signing cost, we can figure out that LESPP significantly reduces computation cost by 10^2–10^3 times compared with BP, GSIS, VAST.

Figure 8 illustrates number of messages that the scheme can verify per second. Obviously, LESPP is the most efficient scheme for message verification. Consider an extremely case: there are 1,000 vehicles in the 300 m communication range, and each vehicle generates a massage every 100 ms. Thus the verification speed must equal or greater than 10,000 message/s. Only LESPP and VAST* still works well under this situation and are resilient to DoS attack. Although VAST scheme also has a very high computation performance for message verification when non-repudiation is not necessary, VAST requires global time synchronization which increases message delay and decreases feasibility of the scheme.

Table 6 Certificate/key updating overhead

	BP	GSIS	VAST	LESPP
Communication overhead (byte)	3,076,290	$41N_{crl}$	63	88
Computation cost	$2T_{mul}$	T_{par}	T_{mul}	$T_{enc} + 2T_{par} + T_h$

6.2 Certificate/key updating overhead

In BP, when a vehicle used up all of the pseudo certificates, it needs to update its 48,830 pseudo certificates according to [7]. The communication overhead is $48,830 \times 63$ bytes and the computation cost for a vehicle is $2T_{mul}$. In GSIS, trust authority (TA) sends all the revocation list to every vehicle to update group key, the communication overhead is $41N_{crl}$ bytes, the computation cost for a vehicle is T_{par}. Certificate updating in VAST is similar with BP, but it only needs to update one certificate at a time. In LESPP, system key is updated according to Sect. 4.4. Table 6 shows the certificate/key updating overhead of different schemes.

Usually, GSIS, VAST and LESPP update certificate/key annually with assistance of national vehicle management department, while BP has to update pseudo certificates once the certificates are used up (about once a month). Certificate/Key updating overhead of GSIS grows linearly with N_{crl}, so when N_{crl} is large, the overhead may be very high. Both VAST and LESPP have an extremely low certificate/key updating overhead, but VAST does not provide identity privacy preservation and unlinkability.

6.3 Vehicle revocation overhead

In BP, when TA needs to revoke a vehicle, it has to insert all the public keys of valid pseudo certificates the vehicle holds into CRL. The average number of valid pseudo certificates a vehicle possesses is 48,830/2. So the communication overhead is $24,415 \times 21 + 105$ bytes. The 105 bytes overhead is the attacked certificate and signature. For GSIS, VAST and LESPP, to revoke a vehicle only needs to insert one item into the CRL. Vehicle revocation overhead is shown in Table 7.

It can be seen that, LESPP has the lowest communication overhead for revoking a vehicle. Furthermore, LESPP employs TPDs to revoke vehicles, then vehicles in LESPP do not need to maintain a CRL to record the revoked vehicles. This unique property makes LESPP especially suitable for large scale VANET.

Table 7 Vehicle revocation overhead

	BP	GSIS	VAST	LESPP
Communication overhead	512,715 + 105	41 + 192	21 + 105	21 + 42
Computation cost	$2T_{mul}$	$5T_{par} + T_h$	$2T_{mul}$	$2T_{par}$
CRL size	$512715N_{crl}$	$41N_{crl}$	$21N_{crl}$	0

Fig. 9 City street scenario corresponding to a roughly square are of size 2,250 × 2,250 m^2

6.4 Scheme simulation

In this subsection, we simulate BP, GSIS, VAST (VAST*), LESPP with opportunistic networking environment (ONE) [35]. Aiming at estimating real world road system properly, we select a part from real map of Beijing (northeast corner of area surrounded by the No.2nd Ring Road of Beijing) using OpenJump and import it into ONE as a city street scenario. The adopted map and the user interface of ONE in this paper is presented in Figs. 9 and 10.

All vehicles are distributed deliberately on the roads of the map at the beginning of each simulation. Each of them would choose one casual point separately on roads and moves towards it following some kind of movement model, at a random speed generated from a range of 10 km/h centered at a velocity value configured in advance. ONE provides several advanced practical movement models to imitate different actual scenarios in life. Hereby we cautiously equip every vehicle with ShortestPathMap-BasedMovement in which Dijkstra's algorithm is used to find shortest path along connected road between two random map nodes. Having arrived at destination, a carriage waits for a short time, then it would pick next random target on some road of the grids and repeat the aforementioned moving process till the end of this round of simulation. Other essential parameters are listed in Table 8.

Metrics for performance evaluation in this paper are the average message delay, average message loss ratio and percentage of signature verified, which are represented as $avgD_{msg}$, $avgLR$ and $avgPerSV$ [18], correspondingly, and are stated as follows:

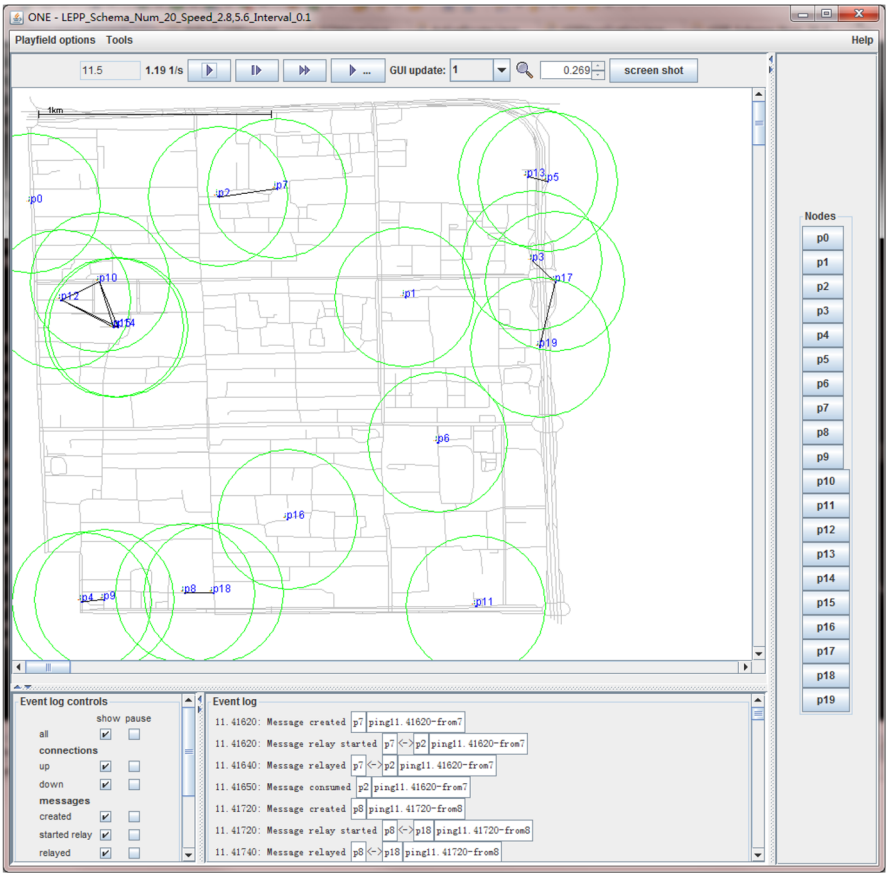

Fig. 10 ONE user interface

Table 8 Simulation configuration

Simulation scenario	City streets
Communication range	300 m
Simulation time	100 s
Channel bandwidth	6 Mbps
Wait time	0–5 s
Buffer size	1 M bytes
Broadcast Interval	0.3 s
Speed	(20 km/h,100 km/h]

$$avgD_{msg} = \frac{1}{N_D \cdot M_{sent_n} \cdot K_n} \sum_{n \in D} \sum_{m=1}^{M_{sent\_n}} \sum_{k=1}^{K_n} (T_{sign}^{n\_m} + T_{transmission}^{n\_m\_k}) \cdot (L_{n\_m\_k} + 1) \tag{1}$$

where D is the simulation district, N_D is the total number of vehicles in D, M_{sent_n} is the number of messages sent by vehicle n, K_n is the number of vehicles within the

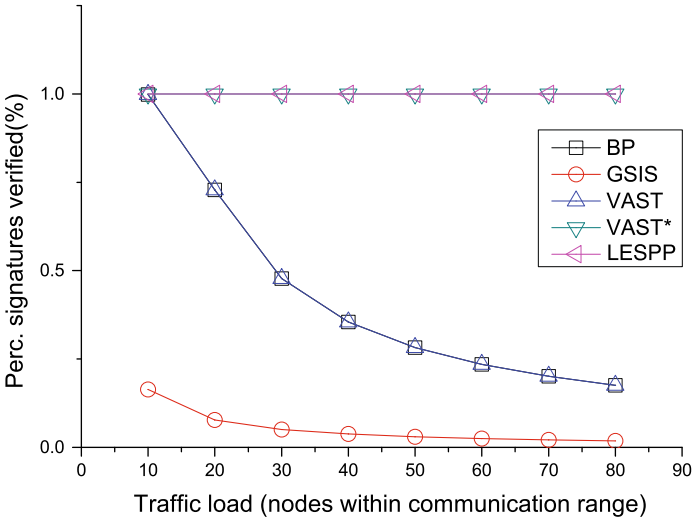

Fig. 11 Impact of traffic load on message delay

one-hop communication range of vehicle n, $T_{sign}^{n\_m}$ represents the time consumed for signing message m by vehicle n, n_m_k is one message sent by vehicle n and received by vehicle k, and $L_{n\_m\_k}$ is the length of buffer queue equipped in vehicle k when n_m_k is received by vehicle k.

$$avgLR = \frac{1}{N_D} \sum_{n=1}^{N_D} \frac{M_{dropped}^{n}}{\sum_{k=1}^{K_n} M_{arrived}^{n}} \tag{2}$$

where $M_{dropped}^{n}$ means the total of dropped messages by vehicle n in application layer, and $M_{arrived}^{n}$ the number of received messages in network layer by vehicle n. Here consideration of message loss caused by wireless transmission is excluded, as leaving only message loss by security protocol due to full buffer space.

$$avgPerSV = \frac{1}{N_D} \sum_{n=1}^{N_D} \frac{M_{consumed}^{n}}{\sum_{k=1}^{K_n} M_{arrived}^{n}} \tag{3}$$

where $M_{consumed}^{n}$ means the total of consumed messages by vehicle n in application layer. In the following, we conduct a set of experiments to analyze the impacts of different traffic loads. Simulation results are shown in Figs. 11, 12 and 13.

It could be seen that, with the growth of traffic load, the average message delay decreases all the time for GSIS. As for BP, VAST and VAST* it increases when traffic load is lower than 40, yet decreases after that. This is mainly because that the buffering mechanism produces a time point at which the buffer space is exactly full, resulting in the fact that older unverified messages are dropped yet newer ones are verified and counted into statistics. The proposed LESPP scheme keeps 0 at this

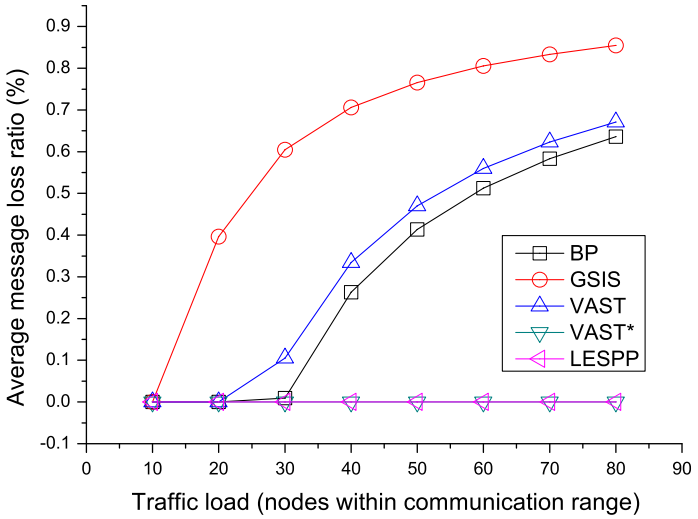

Fig. 12 Impact of traffic load on message loss ratio

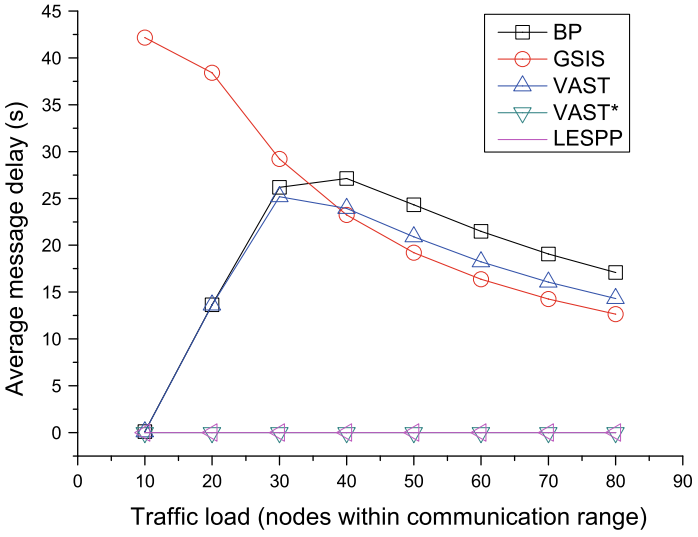

Fig. 13 Impact of traffic load on percentage of signatures verified

metric which is absolutely lower than all other schemes, and is extremely appropriate for real-time emergency event reporting applications. Moreover, as vehicle number in communication range getting larger, average message loss ratio turns out an increasing trend for nearly all schemes except VAST* and LESPP, which keep almost 0 even when the traffic load climbs up to 80. It is remarkable that when the traffic load reaches 80, average message loss ratio is higher than 63 % for BP, GSIS and VAST. Such kind of situations exist only in severe traffic jams in which vehicles' buffer space are filled rapidly, and would harm VANET application dramatically. Percentages of signature

verified for both of VAST* and proposed LESPP are nearly 100 % , while for the other three schemes are decreasing as traffic load getting larger and arriving at lower than 40 % when traffic load passes 40. The properties of 0 message loss ratio and about 100 % signatures verified reveal that LESPP is resilient to DoS attack, which significantly increases availability and stability of the VANET. Considering the above analysis of simulations, LESPP turns out to have the lowest average message delay, the lowest message loss ratio and the highest of signature verified percentage. Although VAST* also produces a good performance, but it does not provide some essential security, such as unlinkability, conditional traceability, non-repudiation.

7 Conclusion

In this paper, we have proposed a lightweight and efficient authentication scheme for secure VANET communication. The proposed scheme mainly employs symmetric operations for message signing and verification, which reduces both computation and communication overhead. Identity based signature used by KMC to sign messages does not need to transmit certificate along with the message, which further reduces communication overhead and avoids certificate management. Extensive simulation reveal that the novel scheme is feasible and has an outstanding performance on message signing/verification, message loss ratio and network delay. To the best of our knowledge, LESPP is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication. The KMC stores vehicles real identity and other vehicle information and is responsible for system key updating. So KMC becomes the center of VANET and the security of whole system relies greatly on KMC. If the KMC is compromised, the whole scheme is no longer effective. In our future work, we will focus on the lightweight and efficient authentication scheme based on decentralized KMC.

Acknowledgments This paper is supported by Program for New Century Excellent Talents in University (NCET-12-0046), National Natural Science Foundation of China No.61272512, Beijing Municipal Natural Science Foundation No.4121001, and DNSLAB, China Internet Network Information Center, Beijing 100190.

References

1. Weiland RJ, Purser LB (2000) Intelligent transportation systems. Transportation in the new millennium. http://trid.trb.org/view.aspx?id=639268
2. Taylor MAP (2001) Intelligent transport systems. Handbook of transport systems and traffic control. p 461. http://scholar.google.com/scholar?q=Handbook+of+transport+systems+and+traffic+control+TAYLOR&btnG=&hl=en&as_sdt=0%2C5
3. Wang F, Zeng D, Yang L (2006) Smart cars on smart roads: an IEEE intelligent transportation systems society update. IEEE Pervasive Comput 5(4):68–69
4. Dedicated Short Range Communications (DSRC) Home. http://trid.trb.org/view.aspx?id=725762. Accessed 31 Dec 2002
5. Msn, TV. http://www.msntv.com/. Accessed 20 May 2007
6. Raya M, Hubaux J (2005) The security of vehicular ad Hoc networks. In: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks, pp 11–21

7. Raya M, Papadimitratos P, Hubaux JP (2006) Securing vehicular communications. IEEE Wirel Commun 13(1):8–15
8. Sun Y, Lu R, Lin X, Shen XS (2010) An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans Veh Technol 59(1):3589–3603
9. Mao W (2003) Modern cryptography: theory and practice. Prentice-Hall, Englewood Cliffs
10. Libert B, Vergnaud D (2008) Multi-use unidirectional proxy re-signatures. In: Proceedings of ACM CCS, Alexandria, pp 511–520
11. Lu R, Lin X, Zhu H, Ho P, Shen XS (2008) ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of 2008 INFOCOM, pp 1229–1237
12. Zhang C, Lu R, Lin X, Ho P, Shen XS (2008) An efficient identity-based batch verification scheme for vehicular sensor networks. In: Proceedings of 2008 INFOCOM, pp 246–250
13. Fiat A (1990) Batch RSA. In: Proceedings of CRYPTO'89, pp 175–185
14. Camenisch J, Hohenberger S, Pedersen M (2007) Batch verification of short signatures. In: Proceedings of EUROCRYPT'07, pp 246–263
15. Lin X, Sun X, Ho P, Shen XS (2007) GSIS: a secure and privacy preserving protocol for vehicular communications. IEEE Trans Veh Technol 56(1):3442–3456
16. Cham D, Heyst EV (1991) Group signatures. In: Proceedings of 1991 advances in cryptology- EUROCRYPT, pp 257–265
17. Boneh D, Boyen X, Shacham H (2004) Short group signatures. In: Proceedings of 2004 CRYPTO, pp 227–242
18. Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Proceedings of 1984 advances in CryptologyCrypto. Springer, New York, pp 47–53
19. Wang F, Xu YJ, Wu L, Dan Liu, Zhu LH (2013) Authenticating and tracing biological anonym of VANET based on KMC decentralization and two-factor. In: Proceedings of the 11th annual international conference on mobile systems, applications, and services (MobiSys '13). ACM, New York, pp 519–520
20. Zhang L, Wu Q, Solanas A, Domingo FJ (2010) A scalable robust authentication protocol for secure vehicular communications. IEEE Trans Veh Technol 59(1):1606–1617
21. Sampigethaya K, Li M, Huang L, Poovendran R (2007) AMOEBA: robust location privacy scheme for VANET. IEEE J Sel Areas Commun 25(1):1569–1589
22. Calandriello G, Papadimitratos P, Hubaux J, Lioy A (2007) Efficient and robust pseudonymous authentication in VANET. In: Proceedings of 2007 the fourth ACM international workshop on Vehicular, ad hoc networks, pp 19–28
23. Studer A, Bai F, Bellur B, Perrig A (2008) Flexible, extensible, and efficient VANET authentication. J Commun Netw 11(6):574–588
24. Perrig A, Canetti R, Tygar JD, Song D (2002) The TESLA broadcast authentication protocol. In: Proceedings of RSA CryptoBytes'02
25. Lin X, Sun X, Wang X, Zhang C, Ho P, Shen XS (2008) TSVC—timed efficient and secure vehicular communications with privacy preserving. IEEE Trans Wirel Commun 7(1):4987–4998
26. Ren K, Lou W, Deng RH, Kim K (2006) A novel privacy preserving authentication and access control scheme in pervasive computing environments. IEEE Trans Veh Technol 55(4):1373–1384
27. Sampigethava K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K (2006) CARAVAN: providing location privacy for VANET. In: Proceedings of International workshop on vehicular ad hoc networks
28. Daemen J, Rijmen V (1998) AES Proposal: Rijndael. In: Proceedings of the first advanced encryption standard candidate conference, National Institute of Standards and Technology (NIST)
29. Bellare M, Canetti R, Krawczyk H (1996) Message authentication using hash functions the HMAC construction. RSA Lab CryptoBytes 2(1):12–15
30. Hess F (2003) Efficient identity based signature schemes based on pairings. Sel Areas Cryptogr 2595:310–324
31. Boneh D, Lynn B, Shacham H (2001) Short signatures from the Weil pairing. In: Proceedings of 2001 ASIACRYPT, pp 514–532
32. Katz J, Lindell Y (2007) Introduction to modern cryptography: principles and protocols. Chapman & Hall/CRC, Boca Raton, Florida
33. Scott M (2007) Efficient implementation of cryptographic pairings. http://www.pairing-conference.org/2007/invited/Scott_slide.pdf
34. Zhang C, Lin X, Lu R, Ho P, Shen XS (2008) An efficient message authentication scheme for vehicular communications. IEEE Trans Veh Technol 57(1):3357–3368

35. Keranen A, Ott J, Karkkainen T (2009) The ONE simulator for DTN protocol evaluation. In: Proceedings of the 2nd international conference on simulation tools and techniques
36. Papadimitratos P, Levente B, Schoch E, Freudiger J, Raya M, Ma Z (2008) Secure vehicular communication systems: design and architecture. Commun Mag IEEE 46(1):100–109
37. Hsiao H, Studer A, Chen C, Perrig A, Bai F, Bellur B (2011) Flooding-resilient broadcast authentication for VANETs. In: Proceedings of the 17th annual international conference on mobile computing and networking, pp 193–204
38. Zhang X, Liu C, Nepal S, Pandey S, Chen J (2013) A privacy leakage upper-bound constraint based approach for cost-effective privacy preserving of intermediate datasets in cloud. IEEE Trans Parallel Distrib Syst 24(6):1192–1202
39. Zhang X, Yang LT, Liu C, Chen J (2014) A scalable two-phase top-down specialization approach for data anonymization using MapReduce on cloud. IEEE Trans Parallel Distrib Syst 25(2):363–373
40. Zhang X, Liu C, Nepal S, Chen J (2013) An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud. J Comput Syst Sci 79(5):542–555