## RESEARCH

**Open Access** 



# An efficient anonymous batch authentication scheme based on priority and cooperation for VANETs

Tao Jing<sup>1</sup>, Yu Pei<sup>1</sup>, Bowu Zhang<sup>2</sup>, Chunqiang Hu<sup>3</sup>, Yan Huo<sup>1\*</sup>, Hui Li<sup>1</sup> and Yanfei Lu<sup>1</sup>

## Abstract

Vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communications have raised a series of challenges due to data security and user privacy. Vehicular ad hoc networks (VANETs) have become the target of malicious attacks. Authentication has been widely adopted in VANETs to guarantee secure communications. However, existing authentication schemes have failed to meet stringent time requirements of VANETs leading to information loss. In this paper, we propose an efficient anonymous batch authentication (EABA) scheme aiming to reduce the message loss rate of vehicles and roadside units (RSUs). In the EABA scheme, we introduce a message classification algorithm and allow receivers to authenticate messages based on the classification result so that messages with high priority will be authenticated preferentially. In addition, we propose a cooperative authentication mechanism, where RSUs and vehicles share authenticated messages to reduce the workload on RSUs when the network is saturated. The proposed method is evaluated by extensive simulations, and the results demonstrate that the EABA scheme can reduce the message loss significantly and guarantee information security.

Keywords: VANETs, Message authentication, Message classification, Reverse auction

## 1 Introduction

A vehicular ad hoc network (VANET) supports direct communication between vehicles and thus has wide applications in an intelligent transportation system (ITS) [1]. Vehicles in VANETs are typically equipped with mobile devices, following the dedicated short-range communication (DSRC) protocol [2-4]. Messages exchanged via the DSRC protocol include road condition [5], traffic events [6], advertisements, and weather condition [7], even video streams [8]. Upon receiving these messages, drivers can get a better understanding of road conditions and traffic reports and adjust their routing and velocity accordingly for safe and fast driving. In addition, messages in VANETs can also deliver value-added services, such as the commercials of nearby gas stations and restaurants. Besides the communication between vehicles, additional facilities such as a roadside unit (RSU), when connecting to

\*Correspondence: yhuo@bjtu.edu.cn

<sup>1</sup>School of Electronics and Information Engineering, Beijing Jiaotong

University, Shangyuancun, Beijing 100044, China

vehicles, can significantly enhance the performance of message exchanging due to its large computing capacity. For example, RSUs can disseminate messages to a large number of vehicles within seconds while it may take a greater amount of time for individual vehicles to receive messages then broadcast. In the presence of a traffic control center, RSUs can help gather messages from vehicles so that the control center has a full understanding of traffic on the road.

However, security concerns pose great challenges on communications in VANETs due to its unique characteristics (e.g., wireless communication, unbounded network size, frequent exchange of information, rapid changing network topology) [9–11]. Malicious users may intercept [12], poison [13], modify, and replay messages to interrupt communications or jam traffic. The attackers can even detect the identity of message sender and spoof as a legitimate user [14]. The integrity and authenticity of messages are seriously threatened [15]. To address these issues, some works design a secure routing path to isolate malicious nodes [16]. In addition, message authentication has been widely adopted in VANETs due to its reliability



© The Author(s). 2018 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Full list of author information is available at the end of the article

and easy implementation, where messages received must be authenticated before further being processed [17, 18]. While improving the communication security in VANETs, message authentication has introduced extra processing delay. Yet, most information in VANETs is time-sensitive. As vehicles move constantly in VANETs (typically 10 to 40 m/s or 36 to 140 km/h), messages are required to be processed in nearly real time so that drivers can be notified timely, i.e., before they enter the danger zone. As a result, messages in VANETs are often associated with a timer and will be discarded when the timer expires [19]. Consider a scenario that a vehicle receives multiple messages from vehicles nearby, and these messages will be placed in a queue based on their arrival time. Upon expiration of the timer, messages would be dropped immediately. Then, important information may be lost due to authentication delay when the network is congested. This situation is common in VANETs due to the possible data burst. Attackers may also take advantage and flood receivers with invalid messages [20, 21]. A wellrecognized solution for authentication in VANETs is to use the public key infrastructure (PKI)[22] to encrypt messages. However, most PKI-based approaches suffer from a significant amount of checking time for certificate revocation list (CRL)[22]. This may cause failure to meet the strict time requirements of VANET.

In order to address the problems outlined above, in this paper, we propose an efficient anonymous authentication scheme for VANETs based on message priority and vehicle cooperation. We adopt the elliptic curve digital signature algorithm (ECDSA) [23] for message encryption, as it requires less computation overhead with noticeably smaller keys compared with other existing algorithms. In addition, we employ the batch authentication in the proposed scheme that vehicles can authenticate multiple messages at a time to reduce the time for authentication [24]. We classify all received messages into multi-level priority queue (MLPQ) before authentication. Inspired by the observation that messages from vehicles nearby are more important, as they may contain information that immediately impacts the current vehicle, we group received messages based on the received signal strength. The messages sent from closer vehicles represent higher safety concern for ITS safety applications. Thus, our scheme enables these messages to be authenticated preferentially so as to retain important information. Moreover, we introduce a cooperative authentication mechanism, where RSUs and vehicles participate in cooperation, so that authenticated messages can be shared with low computation overhead. To encourage vehicles to participate in cooperation, we adopt a reverse auction mechanism to award vehicle participation.

Our contributions of this paper are summarized as follows:

- 1 We employ the elliptic curve cryptography and the batch authentication in our authentication algorithm, which can authenticate a set of messages simultaneously rather than one after another with low computational complexity. The proposed authentication algorithm can reduce the message loss rate significantly.
- 2 We classify received messages into different priority queues based on the received signal strength using Lloyd's algorithm, to prevent important messages (messages from nearby vehicles) from being dropped when the network is congested.
- 3 We propose a cooperative authentication method to allow vehicles to share authenticated messages with RSUs. An auction mechanism is included in the cooperative authentication method to encourage vehicles to help RSU select cooperators and calculate the reward for each. We have proven that the auction mechanism can guarantee truthful dealings.
- 4 The experiments of the proposed authentication scheme are carried out on MATLAB platform. The relevant parameters are set according to the real VANET scenario that is explained in Section 6. Simulation results show that the EABA scheme is safe and efficient. It can reduce the message loss rate of both vehicles and RSUs.

The rest of the paper is organized as follows. Section 2 reviews related work about message authentication in VANETs. Section 3 introduces the system model and preliminaries. Section 4 describes the cooperative message authentication scheme for VANETs. Section 5 analyzes the security, privacy, bid truthfulness, and authentication efficiency of our scheme. Section 6 demonstrates the simulation results and discusses the message loss rate of both vehicles and RSUs. Section 7 presents a conclusion.

## 2 Related work

There exist a number of works to address safety and privacy issues in VANETs. Raya and Hubaux [25] proposed a CPPA scheme based on PKI, which can achieve both security and privacy requirements of VANETs. However, it is time consuming because of the usage of a certificate revocation list (CRL). In addition, the size of the CRL is large, and it increases as the number of the revoked vehicles grows. The increasing number of CRL makes it hard for vehicles to authenticate messages in real time. Thus, checking against the CRL is bound to be a cause of authentication delay. In order to deal with the CRL problem in PKI-based schemes, elliptic curve-based schemes have been proposed due to its time efficiency. ECDSA is a main application of elliptic curvebased schemes. It is more computationally efficient than the commonly used PKI-based schemes [26]. It has been

recommended for message authentication by the current wireless access in vehicular environment (WAVE) standards. In addition, many authentication schemes have been proposed based on ECDSA. In [27], the authors proposed an efficient conditional privacy preservation (ECPP) protocol, which was a good implementation of ECDSA. However, the computational complexity of ECPP is heavy because of the usage of bilinear pairing. In order to improve the computation speed in message authentication, Zhang et al. introduced an identity-based batch verification (IBV) scheme in [28]. The IBV scheme still needs to use bilinear pairings and requires a special hash function known as the MapToPoint function, which is also time inefficient in VANETs. However, the IBV enables the received messages with signatures to be authenticated at the same time such that the total verification time could be reduced. To achieve better performance and reduce the computation cost, He et al. [29] and Lo and Tsai [30] proposed new efficient authentication schemes which did not use bilinear pairing under the premise of ensuring security and privacy. They presented a better performance in terms of computation cost. Shim in [31] proposed a conditional privacy preserving authentication scheme, called as CPAS. It reduced the computation time by canceling the use of MapToPoint function. In this paper, we mix together the advantages of both batch authentication and ECDSA without bilinear pairing and employ the MapToPoint to construct our authentication scheme.

Message authentication has been universally accepted to address security and privacy issues in VANETs. Based on the abovementioned schemes, they can be further classified into three categories: random authentication, cooperative authentication, and priority-based authentication. The most common is random authentication [29, 32]. In this way, all received messages with signatures are stored in the storage of queue according to their arrival order. They are picked randomly for authentication. However, a large amount of important messages from nearby vehicles will be lost in such a way because of the limited computational capability of vehicles.

Cooperative authentication has emerged as a promising approach to reduce the authentication overhead on individual vehicles and shorten the authentication delay [33, 34]. Vehicles cooperatively authenticate messages and share their authentication results to each other. Thus, the computation burden of them will be alleviated largely. Nevertheless, the implementation of this method is challenging due to the unique features of the VANETs, such as high mobility and real-time quality in data transmission.

Priority-based authentication is a new trend to solve problems in VANETs [20]. The main issue is that many important messages from neighbor vehicles may suffer from significant authentication delays. Different from previous approaches, all received messages in priority-based authentication schemes can be classified into MLPQ according to their importance. After that, messages will be authenticated in priority. Messages with great importance will be protected from authentication delay, and they will be authenticated in time. Therefore, we propose an authentication scheme based on priority in this paper. Hamida and Javed [23] used a direct *k*-means clustering method to do message clustering, while it is time consuming, especially in a dense traffic scenario. We use Lloyd's algorithm [35] in our paper, which performance is more superior than the direct *k*-means algorithm.

## 3 System model and preliminaries

## 3.1 System model

In this section, we present a general model for message exchange in VANETs as illustrated in Fig. 1. The notations used in this paper are listed in Table 1.

Consider a VANET *M* that consists of *n* vehicles, where every vehicle is equipped with an onboard unit (OBU) that can send and receive messages. In addition, each vehicle has a tamper-proof device (TPD) for data storage and processing. In this paper, we assume that the TPD is fully trusted and do not consider attacks towards the TPD. In other words, we believe data stored in the TPD are safe and free from attacks. Let  $V = \{v_i, i \in \{1, 2, ..., n\}\}$  be the set of vehicles in *M*.

Assume that there exists a trusted authority (TA). The TA is a trusted third party with a high level of computation performance. It is in charge of system initialization and the proposed authentication scheme implementation. Assume vehicles have registered at the TA in advance so that each vehicle will be assigned a unique identity (ID) and its account information will be copied and saved in its TPD as well. As a result, the TA has knowledge of the identity of all the vehicles in M. For the sake of simplicity, we assume that the TA is hard to be compromised by any adversary. Therefore, the TA is considered to be free of attacks as well. Let R be a RSU that works as an intermediary between the TA and vehicles. It can communicate with vehicles via radio signals and can also communicate with the TA through wired links.

Each vehicle  $v_i$  can broadcast messages to other vehicles when needed. The messages are links between nodes in M for communication. Denote a message by  $m_{mid} = \{b_{mid}, SV_{RID}, t_{mid}\}$  where  $b_{mid}$  represents the message body,  $SV_{RID}$  represents the vehicle ID of a sender, and  $t_{mid}$  is the message expiration time.

In particular, we consider a multi-sender-multi-receiver scenario that  $v_i$  may receive multiple messages at a time. Due to limited capacity of the TPD on  $v_i$ , received messages would be placed into a queue in order of their arrival time before they are processed.



Let  $q_t^i = [q_t^i[j]]^T$ ,  $j \in Z_+$ ,  $q_t^i[j] \in \{mid\}$  be the queue of messages to be processed in  $v_i$  at time *t*, and let  $|q_t^i|$  be the queue length. Let  $w_{mid}$  be the total time that a message  $m_{mid}$  stays in  $q^{l}$  (from the time it arrives to the time it gets processed), and it can be expressed as:

$$w_{mid} = \sum_{q_{t_{mid}}^i} w_{q_{t_{mid}}^i[j]} \tag{1}$$

Messages sent from closer vehicles deserve more attention as they may impact the current vehicle immediately. Inspired by this observation, we let  $v_i$  label messages with different priority tags based on the sender-receiver distance when processing messages.

For a particular message  $m_{mid}$ , the precise location of its sender SV cannot be inferred from  $m_{mid}$  itself. But fortunately, we can estimate the distance between SV and NVroughly by the received signal strength and then classify messages into k categories  $C_1, C_2, \ldots, C_k$  by their priority tag. Here, NV represents the message receiver. A clustering method [35] is adopted for message classification. Let  $d_{SV NV}^t$  represent the distance between the sender SV and a receiver  $NV \in V$  at time t. For example, we can classify all received messages into three categories at 100-m intervals:

- $C_1$ : if  $0 < d_{SV,NV}^t \le 100 \text{ m}$   $C_2$ : if  $100 < d_{SV,NV}^t \le 200 \text{ m}$   $C_3$ : if  $200 < d_{SV,NV}^t \le 300 \text{ m}$

Each of the messages in  $C_i$  needs to be authenticated by  $v_i$ . The authentication scheme will be described in the following section.

## 3.2 Security and privacy objective

The proposed cooperative authentication scheme is committed to protecting security and privacy of users in VANETs with a goal to ensure privacy preservation and bid truthfulness.

- Message authenticity and integrity: Due to intensive attacks in VANETs, messages during transmission can be intercepted and corrupted, and false information may be inserted to disturb traffic. Thus, it is important for receivers to verify the integrity of received messages making sure messages have not been tampered with during transit.
- Identity privacy preservation: As vehicles communicate over a public channel, messages transmitted in VANETs are vulnerable to tracking attacks where attackers could trace the targeted driver's activities based on the messages it broadcasted. For example, by monitoring broadcasted messages, an attacker can estimate the vehicle's location and trace the vehicle's traveling routes. The traveling routes expose the driver's privacy, which may be used for crimes. Thus, we let vehicles hide their real identity in this paper so that RSUs and other vehicles cannot distinguish a vehicle's real identity through the messages it sends.

RSUs. n

## Table 1 Notations

MA VANETVA set of vehicles in M $v_i$ A vehicle in VRA roadside unitSVA message senderNVA message receiver $m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $q_t^i$ The queue of messages to be processed in $v_i$ at time t $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time t $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $A$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^i$ The set of id of overlapped message $L_{RID}^i$ The set of id of overlapped message subtence $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ The lowest bidding value that a bidder can win	Symbol	Semantics	
VA set of vehicles in M $v_i$ A vehicle in VRA roadside unit $SV$ A message sender $NV$ A message receiver $m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $q_t^1$ The queue of messages to be processed in $v_i$ at time t $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^1$ The number of messages that $v_i$ has authenticated at time t $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system $P_{pub}$ The public key of the system $P_{pub}$ The password matched with vehicle's real identity $II$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^{i}$ The set of id of overlapped message subtenticated at $RSU$ at time t $e_{RDD}$ The set of id of overlapped message between $L_{RSU}^i$ and $a$ The vehicle's valuation of a single message $L_{RD}^{i}$ The set of id of overlapped message between $L_{RSU}^i$ and<	M	A VANET	
viA vehicle in VRA roadside unitSVA message senderNVA message receivermmidThe messagebmidThe message bodytrmidThe message expiration time $q_t^t$ The queue of messages to be processed in v <sub>i</sub> at time twmidThe total time that a message $m_{mid}$ stays in $q^i$ SmidA signature $z_t^i$ The number of messages that v <sub>i</sub> has authenticated at time tEA non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ pA large prime numberqA large prime numberGAn additive group of q orderPThe generator of GFpThe finite field over pH1A one-way hash functionH2A one-way hash functionsThe master key of the systemPpubThe public key of the systemPpubThe public key of the systemPpubThe password matched with vehicle's real identityI/IThe signal strengthTHThe threshold that will trigger the cooperative authentication $L_{RSU}^i$ The set of id of overlapped messages between $L_{RSU}^i$ and at time tentitoThe set of id of overlapped messages between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The set of id of overlapped message between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	V	A set of vehicles in M	
RA roadside unitSVA message senderNVA message receiver $m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $q_t^i$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $q$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_P$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^i$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID}$ The set of id of overlapped message $L_{RDU}^i$ The set of id of overlapped message between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message $h_{RDD}$ The bid price of a single message <td>Vi</td> <td colspan="2">A vehicle in V</td>	Vi	A vehicle in V	
SVA message senderNVA message receiver $m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $q_1^t$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_1^t$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The public key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $A$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^i$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID}$ The set of id of overlapped messages $L_{RID}^i$ The set of id of overlapped message between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	R	A roadside unit	
NVA message receiver $m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $d_t^1$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^1$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $H_3$ A vehicle's real identity $AlD$ A vehicle's real identity $AlD$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The step of id of messages waiting to be authenticated at RSU at time $t$ $R_{SU}$ The set of id of overlapped messages between $L_{RSU}^I$ and at time the messages authenticated by $v_{RD}$ . $b_{RID}$ The bid price of a single message $h_{RID}$ The bid price of a single message $h_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\sigma$ The bid price of a single message that a bidder can win	SV	A message sender	
$m_{mid}$ The message $b_{mid}$ The message body $t_{mid}$ The message expiration time $q_t^i$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authentication $L_{RSU}^{I}$ The set of id of overlapped messages between $L_{RSU}^{I}$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ The lowest bidding value that a bidder can win	NV	A message receiver	
$b_{mid}$ The message body $t_{mid}$ The message expiration time $q_t^i$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The public key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The set of id of messages waiting to be authenticated at RSU at time $t$ $RID$ The set of id of overlapped message $L_{RSU}^i$ The set of id of overlapped messages between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	m <sub>mid</sub>	The message	
$t_{mid}$ The message expiration time $q_t^i$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve; $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RJD}^i$ The set of id of overlapped messages between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message	b <sub>mid</sub>	The message body	
$q_t^i$ The queue of messages to be processed in $v_i$ at time $t$ $w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The threshold that will trigger the cooperative authentication $L_{RSU}^i$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RID}^i$ The set of id of overlapped messages between $L_{RSU}^i$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message $b_{RID}$ The bid price of a single message	t <sub>mid</sub>	The message expiration time	
$w_{mid}$ The total time that a message $m_{mid}$ stays in $q^i$ $S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RID}^i$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	$q_t^i$	The queue of messages to be processed in $v_i$ at time $t$	
$S_{mid}$ A signature $z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system $P_{pub}$ A vehicle's real identity $AlD$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	W <sub>mid</sub>	The total time that a message $m_{mid}$ stays in $q^i$	
$z_t^i$ The number of messages that $v_i$ has authenticated at time $t$ $E$ A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RD}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RD}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	S <sub>mid</sub>	A signature	
EA non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$ $p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authenticated at RSU at time $t$ $RID$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	$Z_t^i$	The number of messages that $v_i$ has authenticated at time $t$	
$p$ A large prime number $q$ A large prime number $G$ An additive group of $q$ order $P$ The generator of $G$ $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The set of id of messages waiting to be authenticated at $RSU$ at time $t$ $e_{RID$ The set of id of overlapped message $L_{RSU}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	Ε	A non-singular elliptic curve: $y^2 = x^3 + ax + b \mod p$	
qA large prime numberGAn additive group of q orderPThe generator of G $F_p$ The finite field over p $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash functionsThe master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID$ The set of id of overlapped messages $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	р	A large prime number	
GAn additive group of $q$ orderPThe generator of G $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time $t$ $e_{RID$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	9	A large prime number	
PThe generator of G $F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authenticated at RSU at time $t$ $R_{RD}$ The set of id of messages waiting to be authenticated at RSU at time $t$ $R_{RD}$ The set of id of overlapped message $L_{RD}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RD}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	G	An additive group of <i>q</i> order	
$F_p$ The finite field over $p$ $H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	Ρ	The generator of G	
$H_1$ A one-way hash function $H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authenticated at RSU at time t $e_{RID}$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	Fp	The finite field over <i>p</i>	
$H_2$ A one-way hash function $H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The set of id of overlapped message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	$H_1$	A one-way hash function	
$H_3$ A one-way hash function $s$ The master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RJD}^{t}$ The set of id of overlapped messages between $L_{RSU}^{t}$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	$H_2$	A one-way hash function	
sThe master key of the system $P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	H <sub>3</sub>	A one-way hash function	
$P_{pub}$ The public key of the system, $P_{pub} = s \times P$ $RID$ A vehicle's real identity $AID$ A vehicle's anonymous identity $PAD$ The password matched with vehicle's real identity $I$ The signal strength $TH$ The threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	S	The master key of the system	
RIDA vehicle's real identityAIDA vehicle's anonymous identityPADThe password matched with vehicle's real identityIThe signal strengthTHThe threshold that will trigger the cooperative authenticationCPThe amount that a RSU can afford for entire authenticated at RSU at time te_{RIDThe vehicle's valuation of a single message $L_{RJD}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	P <sub>pub</sub>	The public key of the system, $P_{pub} = s \times P$	
AIDA vehicle's anonymous identityPADThe password matched with vehicle's real identityIThe signal strengthTHThe threshold that will trigger the cooperative authenticationCPThe amount that a RSU can afford for entire authenticated at RSU at time te_{RIDThe vehicle's valuation of a single messageLt RIDThe set of id of orverlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ .b_{RIDThe bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	RID	A vehicle's real identity	
PADThe password matched with vehicle's real identityIThe signal strengthTHThe threshold that will trigger the cooperative authenticationCPThe amount that a RSU can afford for entire authenticated at RSU at time te_{RIDThe vehicle's valuation of a single messageL_{RIDThe set of id of or entire authenticated by $v_{RID}$ .b_{RIDThe set of a single message that $v_{RID}$ .b_{RIDThe bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	AID	A vehicle's anonymous identity	
IThe signal strengthTHThe threshold that will trigger the cooperative authenticationCPThe amount that a RSU can afford for entire authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for The lowest bidding value that a bidder can win	PAD	The password matched with vehicle's real identity	
THThe threshold that will trigger the cooperative authentication $CP$ The amount that a RSU can afford for entire authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$	1	The signal strength	
CPThe amount that a RSU can afford for entire authentication $L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ $\alpha$ The lowest bidding value that a bidder can win	TH	The threshold that will trigger the cooperative authenticatio	
$L_{RSU}^t$ The set of id of messages waiting to be authenticated at RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ $\alpha$ The lowest bidding value that a bidder can win	СР	The amount that a RSU can afford for entire authentication	
RSU at time t $e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ $\alpha$ The lowest bidding value that a bidder can win	L <sup>t</sup> <sub>RSU</sub>	The set of id of messages waiting to be authenticated at	
$e_{RID}$ The vehicle's valuation of a single message $L_{RID}^t$ The set of id of overlapped messages between $L_{RSU}^t$ and at time the messages authenticated by $v_{RID}$ . $b_{RID}$ The bid price of a single message that $v_{RID}$ asks for $\alpha$ The lowest bidding value that a bidder can win		RSU at time t	
L <sup>t</sup> <sub>RID</sub> The set of id of overlapped messages between L <sup>t</sup> <sub>RSU</sub> and at time the messages authenticated by v <sub>RID</sub> .         b <sub>RID</sub> The bid price of a single message that v <sub>RID</sub> asks for         α       The lowest bidding value that a bidder can win	e <sub>RID</sub>	The vehicle's valuation of a single message	
at time the messages authenticated by v <sub>RID</sub> .b <sub>RID</sub> The bid price of a single message that v <sub>RID</sub> asks forαThe lowest bidding value that a bidder can win	L <sup>t</sup> <sub>RID</sub>	$_{D}$ The set of id of overlapped messages between $L_{RSU}^{t}$ and	
b <sub>RID</sub> The bid price of a single message that v <sub>RID</sub> asks forαThe lowest bidding value that a bidder can win		at time the messages authenticated by $v_{RID}$ .	
lpha The lowest bidding value that a bidder can win	b <sub>RID</sub>	The bid price of a single message that $v_{RID}$ asks for	
	α	The lowest bidding value that a bidder can win	
$r(b_{RID})$ The ranking order of received bids	r(b <sub>RID</sub> )	The ranking order of received bids	
$T_p$ The time for performing a bilinear pairing operation	$T_p$	The time for performing a bilinear pairing operation	
T <sub>MP</sub> The execution time of a scale multiplication point operation	T <sub>MP</sub>	The execution time of a scale multiplication point operation	
T <sub>MTP</sub> The execution time of a MapToPoint operation	T <sub>MTP</sub>	The execution time of a MapToPoint operation	

*Traceability*: Even with identity privacy-preserving methods implemented in VANETs, malicious users could find ways to interrupt traffic and cause information lost. For example, malicious users could send false messages which could result in accidents, and they can escape their punishment by hiding their real identity. To solve this problem, we allow the TA to track malicious vehicles and publish them when necessary. That is, the TA can extract the vehicles' real identity by analyzing the messages they sent.

## 4 Cooperative message authentication scheme

In this section, we propose a message authentication scheme that aims to reduce message loss rate by introducing cooperative authentication among vehicles and

## 4.1 Scheme overview

In EABA, we adopt the public key cryptography for message authentication. Note that different from classical public key cryptosystems, all legitimate vehicles in M share the same public key, while each vehicle has a unique private key, and the private key is known only to the vehicle itself. This public-key-private-key distribution is made possible thanks to the presence of the TA. In our scheme, the TA is in charge of initializing authentication settings (i.e., choosing the prime number for public key), and keys are generated and assigned to vehicles when they register at the TA. As a result, we can easily let all vehicles have the same public key.

Figure 2 illustrates message authentication of the proposed scheme. Before sending a message  $m_{mid}$ , SV would sign the message with its private key. The message would then be broadcast with SV's signature  $S_{mid}$  to other vehicles and RSUs in M. Upon receiving  $m_{mid}$ , NV and RSUs would use the shared public key to examine the signature to make sure the integrity of the message (i.e., the message is not altered or tampered with during transmission). A message would be accepted for further applications if it passes authentication, rejected otherwise.

In particular, when a message  $m_{mid}$  arrives at a vehicle, it would be placed into a queue and would be processed in order as messages arrive. It takes time for an individual vehicle  $v_i$  to authenticate all the messages received. Thus, in the presence of burst traffic, a message may get dropped before it could be authenticated, as its timer  $t_{mid}$ expires. The message authentication on a RSU is quite similar. When a vehicle in M broadcasts a message, a copy of that message would be sent to the RSU. The RSU needs to authenticate received messages before forwarding them to other RSUs or vehicles. In order to speed up the authentication of messages, we let the RSU first broadcast to all the vehicles in M for cooperation, so that vehicles willing to participate can share their own authenticated messages



with the RSU. The RSU then can notify all the vehicles in M about authenticated messages it collects such that vehicles can remove these messages. This is because that they have been proven trusted by some vehicles already and there is no need to verify the message again. As a result, the time that a message  $m_{mid}$  stays in  $q^i$  (Eq. (1)) would be reduced. The reason is that either there would be less messages before it in the queue or the message  $m_{mid}$  itself has been authenticated at some other vehicle; in turn, less messages would be dropped due to timer expiration. Specifically, as RSUs are connected via wired links, authenticated messages from different VANETs can also be exchanged. This ensures that vehicles on the border of M would not be disadvantaged when exchanging messages with the current RSU.

Note that the RSU needs to authenticate the authenticated messages from cooperating vehicles before broadcasting them to other vehicles. As more vehicles participate in the cooperation scheme, the workload on the RSU rises quickly. Thus, in our scheme, instead of authenticating received messages one by one, the RSU would verify an integrated signature of messages from each participating vehicle so as to improve authentication efficiency.

The proposed EABA scheme consists of seven phases, i.e., system initialization, vehicle registration, key and anonymous identity creation, message signing, message classification, individual message authentication and batch authentication, and auction-based cooperative authentication. We will describe each phase in detail in the following subsections.

### 4.2 System initialization

In the first phase of EABA scheme, we let the TA initialize system parameters:

- The TA chooses a large prime number *p* and creates a non-singular elliptic curve *E* on the prime filed  $F_p$ ,  $E: y^2 = x^3 + ax + b \pmod{p}$  [36].
- The TA chooses a generating point *P* with *q* order of the group *G*. Here, *q* is a large prime number, *G* is an additive group that contains all of the points on the *E* and a point-at-infinity *O*, and *P* is used for generating the public key and private key [36].
- The TA chooses a random number *s* ∈ Z<sup>\*</sup><sub>q</sub> as the master key of the system and calculates the system public key P<sub>pub</sub> = *s* × P which will be shared by all the vehicles and RSUs in *M*.
- The TA chooses tree one-way hash functions:  $H_1: G \to Z_q, H_2: G \to Z_q, H_3:$  $\{0, 1\}^* \times \{0, 1\}^* \times G \times \{0, 1\}^* \to Z_q.$

During the first phase, the TA will generate parameters for message signing and authentication: *params* =  $\{p, q, a, b, P, P_{pub}, H_1, H_2, H_3\}$ , which would be shared with all RSUs and vehicles (these parameters will be loaded into a vehicle when registering).

## 4.3 Vehicle registration

Every vehicle in the VANET *M* needs to register at the TA in order to participate in message exchange. Assume that each vehicle has a TPD installed, and let the TPD serve as a PKG (private key generator) because of its good security performance.

During registration, each vehicle will receive an unique identity *RID* and a password *PAD*, which would be stored in the TPD. The TA will pre-load public system parameters { $p, q, a, b, P, P_{pub}, H_1, H_2, H_3$ } and the master key *s* into the TPD of each vehicle as well, for message signing and authentication.

#### 4.4 Key and anonymous identity creation

After registration at the TA, every vehicle will start generating its private key and anonymous identity.

Given *RID*, the TPD will choose a random number  $\delta_i \in Z_q^*$  and compute the vehicle's anonymous identity *AID* [29].

$$AID_1 = \delta_i \times P \tag{2}$$

$$AID_2 = RID \oplus H_1(\delta_i \times P_{pub}) \tag{3}$$

The anonymous identity (*AID*) of  $v_{RID}$  can be calculated based on Eqs. (2) and (3), which is expressed as

$$AID = \{AID_1, AID_2\} \tag{4}$$

We adopt the key generation method in [37]. Let  $sk_i$  denote the private key of  $v_{RID}$ . Then, the  $sk_i$  can be computed as:

$$sk_i = \delta_i + s \times H_2(AID) \mod q$$
 (5)

## 4.5 Message signing

In this phase, we adopt the signature generation method in [37]. A vehicle  $v_{RID}$  signs a message with

$$S_{mid} = H_3(AID \parallel t_{mid} \parallel \lambda_i \parallel b_{mid}) \cdot r_i + sk_i \mod q$$
(6)

where

$$\lambda_i = r_i \times P,\tag{7}$$

and  $r_i \in Z_q^*$  is a random number. Then,  $v_{RID}$  will broadcast the signed message  $m_{mid} = \{b_{mid}, AID, t_{mid}, \lambda_i, S_{mid}\}$  to all vehicles nearby.

#### 4.6 Message classification

We assume that all received messages would be pushed into the message queue. Each queue has a threshold which is relevant to the number of messages. If the number of the messages on the queue is beyond the threshold, we consider that it is beyond the vehicle's processing capacity, and this phase will be triggered.

Messages sent from closer vehicles deserve more attention as they may impact the current vehicle immediately. For example, in case of accidents, vehicles near the site will be affected right away, while vehicles far away from the site have more time to take actions (e.g., change the route). Inspired by this observation, we can group messages into different categories according the sender-receiver distance and push them into corresponding priority queues. We adopt Lloyd's algorithm for clustering. Given *n* messages, Lloyd's algorithm can partition them into *k* categories [35]. Assume that the vehicle  $v_{RID}$ has a training data set with *n* received messages' signal strength, denoted as  $I = \{I_1, I_2, ..., I_n\}$ ,  $I_i$  denotes the signal strength of *i*th message,  $(1 \le i \le n)$ . This training phase can be performed based on messages received during the last period of time in a dense traffic scenario.

We use Lloyd's algorithm to classify them into k categories. The objective function is to minimize the mean squared distance from each data point to its nearest center. It can be denoted as follows [35],

$$\underset{C}{\arg\min} \sum_{i=1}^{k} \sum_{I \in C_{i}} \| I - w_{i} \|^{2}$$
(8)

where  $w_i$  denotes the mean value of signal intensity in  $C_i$  (i.e.,  $w_i$  is the centroid).

After classification, messages can be authenticated in order of priority, from the highest to the lowest. Note that if received message signal strength  $I_m$   $(1 \le m \le n)$  is not within the training set I, we assume that the message comes from a vehicle far away. This message will be assigned with the lowest priority.

#### 4.7 Individual authentication and batch authentication

In this phase, each vehicle authenticates messages in order of priority independently. Given a received message  $m_{mid} = \{b_{mid}, AID, t_{mid}, \lambda_i, S_{mid}\}$ , a receiver (vehicle or RSU) would use system parameters *params* =  $\{p, q, a, b, P, P_{pub}, H_1, H_2, H_3\}$  received during registration, to verify its integrity.

Before authenticating a message, the receiver would examine its expiration time  $t_{mid}$  and continue the authentication process if it does not expire, otherwise drop the message.

A message  $m_{mid}$  is valid if the following equation holds:

$$S_{mid} \cdot P = H_3(AID \parallel t_{mid} \parallel \lambda_i \parallel b_{mid}) \cdot \lambda_i + AID_1 + H_2(AID) \cdot P_{pub}$$
(9)

The above equation can authenticate  $m_{mid}$  by its signature  $S_{mid}$  with authentication parameters obtained from the TA when registered. Using (9), messages that cannot pass authentication will be rejected and the message sender will be reported to the TA.

Furthermore, to speed up message authentication, we adopt a batch authentication method [28] that allows a receiver to authenticate multiple messages simultaneously. Thus, the total time for a receiver to authenticate all received messages can be significantly reduced.

Given *n* received messages, we extract their signatures  $S_{mid} = \{S_{mid}^1, S_{mid}^2, ..., S_{mid}^n\}$ . Then, we can authenticate them simultaneously by checking the following equation:

$$\begin{pmatrix}
\sum_{i=1}^{n} S_{mid}^{i} \\
= \left( \sum_{i=1}^{n} H_{3} \left( AID^{i} \parallel t_{mid} \parallel \lambda_{i} \parallel b_{mid} \right) \cdot \lambda_{i} \right)$$

$$+ \left( \sum_{i=1}^{n} AID_{1}^{i} \right) + \left( \sum_{i=1}^{n} H_{2} \left( AID^{i} \right) \right) \cdot P_{pub}$$
(10)

The receiver would accept these messages, if Eq. (10) holds and reject otherwise.

## 4.8 Auction-based cooperative authentication

In order to ease the heavy burden on the RSU, we introduce an auction-based cooperative authentication mechanism. The cooperative authentication will be triggered once the number of the RSU's received messages is beyond a threshold TH. First, the RSU calculates a cost price CP (CP is the amount that the RSU can afford for the entire authentication service)[38] and then broadcasts a request message to all vehicles in M for cooperation. Let the set of ID of messages waiting to be authenticated at RSU at time t be  $L_{RSU}^t$ ,  $L_{RSU}^t = \{mid\}$ . For the sake of communication efficiency, the RSU will only include  $L_{RSU}^{t}$  in the request message instead of the entire message contents. Vehicles that have received the request message will decide whether or not to participate in cooperative authentication. Each vehicle  $v_{RID}$  will cross-check the ID of its authenticated messages and  $L_{RSU}^{t}$  to see whether there exists overlap. If there happens to exist messages in  $L_{RSII}^t$  authenticated by  $v_{RID}$ ,  $v_{RID}$  will calculate a valuation price  $e_{RID}$  ( $e_{RID}$  is the vehicle's valuation of a single message). There are many factors affecting the valuation price  $e_{RID}$  of a vehicle, such as the resource consuming and privacy exposing. Here, we omit the details of pricing scheme and follow the mainstream work [38, 39]. Let  $L_{RID}^{t}$ be the set of ID of overlapped messages between  $L_{RSU}^{t}$  and the messages authenticated by  $v_{RID}$ . Let  $b_{RID}$  be the bid price of a single message that  $v_{RID}$  asks for. Thus,  $v_{RID}$  will participate in auction announcing that it can authenticate messages in  $L_{RID}^t$  with a price  $b_{RID}$  for each message. In order to prevent market distortion, we assume that each vehicle uses its true valuation in the auction, i.e.,  $b_{RID} =$  $e_{RID}$ . In addition, we assume that each vehicle can only bid once at an auction. After receiving bids from vehicles, the RSU will select vehicles for cooperation and compute the corresponding payment.

In particular, for each message *mid* in  $L_{RSU}^t$ , the RSU sorts received bids in increasing order of  $b_{RID}$  if *mid*  $\in L_{RID}^t$ . The RSU purchases the cooperation service starting with the lowest bid. If the message with the lowest bid has been purchased, the RSU will skip and look for the next lowest bid until the total payment goes over *CP* or there are no more bids available.

In [40], the critical value  $\alpha$  means the lowest bidding value that a bidder can win. Here, the RSU calculates the payments for winners according to the critical value  $\alpha$  and the RSU pays  $\alpha$  for one of the cooperators. Then, the RSU sends the purchase decision to all participants. Finally, vehicles whose messages are purchased will sign these messages in an integrated signature [33] and send the authentication result to the RSU. The RSU will pay cooperative vehicles after receiving the result.

## 5 Theoretical analysis

In this section, we analyze the security, privacy, truthfulness, and individual rationality of our proposed EABA scheme.

#### 5.1 Message authenticity and integrity

In the proposed EABA scheme, the message signing and authentication are based on ECDSA [26], whose security depends on the difficulties of discrete logarithm problem. It has been proven that there does not exist polynomial adversary that can forge a valid message and convince receivers that a false message is valid [26]. Thus, false messages and tampered messages will be identified by receivers and not be accepted during authentication examining the validity and integrity of messages. Therefore, the message authenticity and integrity can be guaranteed in our proposed EABA scheme.

## 5.2 Privacy preserving

The EABA scheme can preserve the privacy of message senders. The EABA scheme can protect the identity of message senders from being known by adversaries, while it can also reveal the real identity of vehicles when necessary. In the EABA, vehicles sign messages with their anonymous identity so that the real identity can be hidden.

Thus, no one can trace a sender's real identity by analyzing its messages due to the anonymous identity except the TA.

The TA holds the master key *s* and recovers the sender's true identity by:

$$RID = AID_2 \oplus H_1(\delta_i \times P_{pub}). \tag{11}$$

$$\delta_i \times P_{pub} = \delta_i \times P \times s = AID_1 \times s \tag{12}$$

As a result, if a malicious user generates false messages deliberately to damage or disturb traffic order, the TA can discover its real identity by using (11) and (12) and make punishment.

## 5.3 Bid truthfulness

In this subsection, we prove that the proposed EABA scheme obeys bid truthfulness.

As discussed in [40], an auction mechanism is truthful if it satisfies both monotonicity and critical value payment. *Proof* Let  $r(b_{RID})$  be the ranking order of received bids and  $r(b'_{RID})$  be the ranking order of bid  $b'_{RID}$ .  $b'_{RID} = b_{RID} - \sigma(\sigma > 0)$ , where  $\sigma$  is a random small value. Obviously,  $b'_{RID} < b_{RID}$ . We allocate bids in increasing order of bid price  $b_{RID}$ ,  $r(b'_{RID}) < r(b_{RID})$ . Thus, if  $b'_{RID}$  is denied by the auctioneer,  $b_{RID}$  must be also denied by the auctioneer. On the other hand, if vehicle  $v_{RID}$  wins the auction,  $v'_{RID}$  must also win the auction. As a result, the auction mechanism in EABA is monotonic.

## Theorem 1 The EABA is bid-truthful.

*Proof* In **Lemma 1**, we have proven that the EABA is monotonic. Since the RSU pays for cooperative vehicles in increasing order, the critical value as a result is the highest bid price that can win the auction.  $\Box$ 

Therefore, as the EABA both satisfies monotonicity and critical value payment, it is truthful [40].

#### 5.4 Authentication efficiency

In this subsection, we analyze the authentication efficiency of the EABA scheme.

Authentication efficiency is defined as how fast an authentication algorithm runs, and it can be measured by evaluating computation overhead of the authentication algorithm [41]. It is one of the most important performance indexes, because low authentication efficiency can result in long authentication delay and increase the workload of vehicles or RSUs. We compare the computation overhead of the EABA with two state-of-the-art works [29-31], IBV and CPAS. The result is shown in Table 2. Here, n is the number of signatures,  $T_p$  is the time for performing a bilinear pairing operation,  $T_{MP}$  is the execution time of a scale multiplication point operation, and  $T_{MTP}$  is the execution time of a MapToPoint operation, since the time for performing  $T_p$  or  $T_{MTP}$  is typically far greater than that of  $T_{MP}$ . Therefore, our EABA scheme works best in terms of authentication efficiency among the abovementioned schemes.

#### 5.5 Computation and communication overhead

In EABA, extra message transmission and cost are introduced due to message authentication and exchange. The

Table 2 Running time

Scheme	Signature authentication	n signature batch authentication
IBV	$3T_P + T_{MP} + T_{MTP}$	$3T_P + nT_{MP} + nT_{MTP}$
CPAS	$3T_P + 2T_{MP}$	$3T_P + (n+1)T_{MP}$
EABA	3T <sub>MP</sub>	$(n + 2)T_{MP}$

authentication methods used in the EABA including public key cryptography without certificates and parings, and batch authentication are standard and lightweight [30]. In addition, the majority of authentication computation, such as ID generation and key generation, is done in phase 1, i.e., system initialization by the TA. Thus, we believe that the computation required by the EABA in general is within the RSU and vehicle (OBU)'s capacity.

The communication overhead mainly comes from the message exchange between a RSU and vehicles in auctionbased cooperative authentication (Section 4.8). Participating vehicles share with RSU their authenticated messages, which later will be sent to all vehicles within RSU's transmission range. To reduce the communication overhead, we let the RSU and vehicles only exchange the id, *mid*, of authenticated messages rather than the entire message. As a result, the communication efficiency would be greatly improved.

## 6 Results and discussion

In this section, we validate the performance of our proposed EABA scheme in terms of authentication delay through a simulation study.

## 6.1 Simulation setup

We simulate a VANET that consists of *n* vehicles, a RSU, and a TA. Each vehicle is equipped with an OBU that broadcasts messages every 100 ms based on the DSRC protocol [2]. Following the mainstream work [3, 42], we set the received messages' signal strength in our simulation between -80 and -55 dBm. Every message sent in our VANET includes a timer, and messages will be dropped if timer expires. In the simulation, we let the expiration time be 5 s, the transmission range of each vehicle be 350 m, and the transmission radius of the RSU be 1000 m.

Define vehicle density as the average number of vehicles within a receiver's (vehicle or RSU) communication range. Intuitively, the higher the density, the more the vehicles nearby. This represents the vehicle will receive more messages. In our simulation, we vary the vehicle density of vehicles between 0 and 300 and the vehicle density of the RSU between 0 and 1000. Also, we define the message loss rate as the fraction of the total received messages that are dropped by the receiver.

Simulations in this section are conducted using MAT-LAB over Windows 7, dual core with 4 G memory. Note that results are average of 50 runs.

## 6.2 Discussion of vehicle's message loss rate

Figure 3 describes the average message loss rate of vehicles in M versus vehicle density when the vehicle density varies between 0 and 300. We can observe that the message loss rate increases as the number of vehicles increases. As



the number of vehicles increases, for each vehicle, it will receive more messages, in turn increasing the waiting time for a message to be authenticated. As a result, more messages will be dropped due to expiration. In addition, we can find that the proposed EABA scheme achieves less message loss than the other two state-of-the-art message authentication methods. This is because the time spent for message authentication in the EABA is less than that for the others.

Next, we evaluate the performance of our EABA scheme under the dense traffic scenario. As mentioned in Section 4, in case of burst traffic/messages, the message classification will be triggered in order to authenticate messages more efficiently. In our simulation, we set the threshold of classification to be 224. This means that if a vehicle has more than 224 messages in its queue, the classification will be triggered. Figure 4 reports the result of message classification when the traffic density is set to be 250. In Fig. 4, every point represents a received message, and different colors represent different message categories. Messages in different categories will be dispatched into different priority queues as described in Section 4. We divide messages into five categories. This is because if the number of categories is too small (e.g., 2), there will be a lot of important messages dispatched into low priority at higher risk of being lost. Considering the vehicle's communication range and vehicle's distribution in the VANET, we set the range of the number of categories from 3 to 6 (We have tested 3, 4, and 6 categories too. The results are similar).

Figure 5 displays the message loss rate with and without message classification when the vehicle density is 250. In particular, C1, C2, ..., C5 represent five categories, where messages are clustered based on the signal strength (C1)is centered at -62 dB, C2 is centered at -74 dB, and so on). The centroid value is calculated by Lloyd's algorithm, and all received messages are directed to corresponding categories. Inspired by the observation that messages sent from closer vehicles deserve more attention as they may impact the current vehicle immediately, we believe messages in C1 are more important than other categories. Thus, C1 should be processed with higher priority. Similarly, C2 should be processed before C3, C4, and C5 as it contains more important messages. In Fig. 5, with classification, we can see that the loss rate of important messages (C1, C2, C3) is largely reduced, close to zero, compared to that without classification. This is because messages with higher priority are authenticated preferentially, while messages with lower priority will be authenticated lastly. Thus, we can protect the important message from being lost with message classification.

## 6.3 Discussion of RSU's message loss rate

Figure 6 reports the message loss rate of a RSU with and without cooperative authentication when the traffic density is between 800 and 1000. CP is varied between 20 and 60, and CP is virtual currency. The bid price for a single message at each vehicle is set randomly between 0.06 and 0.08. As can be seen in Fig. 6, the message loss rate is large without cooperation. This is because in dense



traffic, messages cannot be authenticated timely when the number of received messages is large. Thus, the non-cooperation may result in a large loss rate. In addition, the message loss rate of the RSU is reduced as the cooperation authentication is introduced and decreases as the *CP* increases. This is because as *CP* rises, the RSU pays higher. It can purchase more cooperative authentication service and more authenticated messages from cooperative vehicles. Therefore, there will be less messages for the RSU to

authenticate. From the above simulations, we can see that our proposed EABA scheme can largely reduce the massage loss rate of both vehicles and RSUs. And it is suitable for VANETs.

## 6.4 Discussion for the future work

The cooperative authentication may increase the risk of privacy exposure. The reason is that malicious nodes can detect vehicles' presence and track their locations





by monitoring message flow when vehicles communicate with each other over a public wireless channel. We will target these security concerns in our future work.

In addition, we only employ numerical analysis to evaluate the proposed scheme in this paper. An actual VANET system may have many complicated scenarios such as straight roads, corners, intersections, and communication blind spots. How to achieve cooperative authentication for such multi-scenario system is also the main work in the future.

## 7 Conclusion

In this paper, we propose an EABA scheme based on priority and cooperation for VANETs. In order to improve authentication efficiency, the function of batch authentication of multiple messages is included in our EABA scheme. In addition, messages sent from nearby vehicles can be given high priority, such that vehicles can authenticate all received messages in priority and the loss rate of important messages can be largely reduced. With the proposed cooperation and auction mechanism, the EABA is able to lighten the burden of RSUs. We analytically prove that the EABA not only satisfies the security and privacy requirements of VANETs, but also can guarantee bid truthfulness. Through abundant simulation analysis, we demonstrate that our EABA scheme has low computation complexity on message clustering and message authentication. The authentication delay can be largely reduced, and the message loss rate can be also reduced at the same time.

#### Abbreviations

CRL: Certificate revocation list; DSRC: Dedicated short-range communication; EABA: Efficient anonymous batch authentication; ECDSA: Elliptic curve digital signature algorithm; IBV: Identity-based batch verification; ITS: Intelligent transportation systems; MLPQ: Multi-level priority queue; OBU: Onboard unit; PKI: Public key infrastructure; RSUs: Roadside units; TA: Trusted authority; TPD: Tamper-proof device; V2V: Vehicle-to-vehicle; V2R: Vehicle-to-roadside; VANETs: Vehicular ad hoc networks; WAVE: Wireless access in vehicular environment

#### Acknowledgements

Not applicable.

#### Funding

This work was financially supported by NSFC 61571010 and 61471028 and the Fundamental Research Funds for the Central Universities 2017JBM004 and 2016JBZ003.

#### Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

#### Authors' contributions

The authors have contributed jointly to the manuscript. All authors have read and approved the final manuscript.

#### **Competing interests**

The authors declare that they have no competing interests.

#### Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

#### Author details

<sup>1</sup> School of Electronics and Information Engineering, Beijing Jiaotong University, Shangyuancun, Beijing 100044, China. <sup>2</sup>Department of Computer Science, Marist College, Poughkeepsie, New York 12601, USA. <sup>3</sup>School of Big Data and Software Engineering, Chongqing University, Shapingba, Chongqing 401331, China.

## Received: 24 November 2017 Accepted: 12 November 2018 Published online: 04 December 2018

#### References

- K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, Y. Zhou, Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions. IEEE Commun. Surv. Tutor. 17(4), 2377–2396 (2015)
- J. B. Kenney, Dedicated short-range communications (DSRC) standards in the United States. Proc. IEEE. 99(7), 1162–1182 (2011)
- D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich, Design of 5.9 GHz DSRC-based vehicular safety communication. IEEE Wirel. Commun. 13(5), 36–43 (2006)
- J. Qian, T. Jing, Y. Huo, H. Li, Z. Li, Energy-efficient data dissemination strategy for roadside infrastructure in VCPS. EURASIP Wirel, J., Commun. Netw. 2016(1), 148 (2016). https://doi.org/10.1186/s13638-016-0650-0
- Y. Liu, X. Weng, J. Wan, X. Yue, H. Song, A. V. Vasilakos, Exploring data validity in transportation systems for smart cities. IEEE Commun. Mag. 55(5), 26–33 (2017)
- C. Chen, T. H. Luan, X. Guan, N. Lu, Y. Liu, Connected vehicular transportation: data analytics and traffic-dependent networking. IEEE Veh. Technol. Mag. 12(3), 42–54 (2017)
- Y. Lu, Z. Zhao, B. Zhang, L. Ma, Y. Huo, G. Jing, A context-aware budget-constrained targeted advertising system for vehicular networks. IEEE Access. 6, 8704–8713 (2018)
- J. Qiao, Y. He, X. S. Shen, Improving video streaming quality in 5G enabled vehicular networks. IEEE Wirel. Commun. 25(2), 133–139 (2018)
- M. A. Elsadig, Y. A. Fadlalla, VANETs security issues and challenges: a survey. Indian Sci. J. Technol. 9(28), 1–8 (2016)
- A. Boualouache, S. M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun. Surv. Tutor. 20(1), 770–790 (2018)
- H. Li, R. Lu, J. Misic, M. Mahmoud, Security and privacy of connected vehicular cloud computing. IEEE Netw. 32(3), 4–6 (2018)
- J. M. Moualeu, W. Hamouda, F. Takawira, Intercept probability analysis of wireless networks in the presence of eavesdropping attack with co-channel interference. IEEE Access. 6, 41490–41503 (2018). https://doi. org/10.1109/ACCESS.2018.2854222
- Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, Z. Liang, Man-in-the-browsercache: persisting HTTPS attacks via browser cache poisoning. Comput. Secur. 55, 62–80 (2015). https://doi.org/10.1016/j.cose.2015.07.004
- Y. Huo, C. Hu, X. Qi, T. Jing, Lodpd: A location difference-based proximity detection protocol for fog computing. IEEE Internet Things J. 4(5), 1117–1124 (2017)
- J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, J. Liu, A position-aware Merkle tree for dynamic cloud data integrity verification. Soft. Comput. **21**(8), 2151–2164 (2017). https://doi.org/10.1007/s00500-015-1918-8
- M. Wang, J. Liu, J. Mao, H. Cheng, J. Chen, C. Qi, Routeguardian: constructing secure routing paths in software-defined networking. Tsinghua Sci. Technol. 22(4), 400–412 (2017). https://doi.org/10.23919/ TST.2017.7986943
- F. Qu, Z. Wu, F. Y. Wang, W. Cho, A security and privacy review of VANETs. IEEE Trans. Intell. Transp. Syst. 16(6), 2985–2996 (2015)
- M. Azees, P. Vijayakumar, L. J. Deboarh, EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. 18(9), 2467–2476 (2017)
- M. R. Asaar, M. Salmasizadeh, W. Susilo, A. Majidi, A secure and efficient authentication technique for vehicular ad-hoc networks. IEEE Trans. Veh. Technol. 67(6), 5409–5423 (2018)
- Z. Li, C. Chigan, in *Communications (ICC), 2010 IEEE International Conference On*. On resource-aware message verification in VANETs, (2010), pp. 1–6. https://doi.org/10.1109/ICC.2010.5502129
- M. U. Tariq, J. Florence, M. Wolf, Improving the safety and security of widearea cyber-physical systems through a resource-aware, service-oriented development methodology. Proc. IEEE. **106**(1), 144–159 (2018)
- A. Wasef, X. Shen, EMAP: Expedite message authentication protocol for vehicular ad hoc networks. IEEE Trans. Mob. Comput. 12(1), 78–89 (2013)
- E. B. Hamida, M. A. Javed, in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). Channel-aware ECDSA signature verification of basic safety messages with k-means clustering in VANETs (IEEE, Crans-Montana, 2016), pp. 603–610

- J.-L. Huang, L.-Y. Yeh, H.-Y. Chien, ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans. Veh. Technol. 60(1), 248–262 (2011)
- M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks. Comput, J., Secur. 15(1), 39–68 (2007)
- S. Lamba, M. Sharma, in Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference On. An efficient elliptic curve digital signature algorithm (ECDSA) (IEEE, Katra, 2013), pp. 179–183
- R. Lu, X. Lin, H. Zhu, P. H. Ho, X. Shen, in *INFOCOM 2008. The 27th* Conference on Computer Communications. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications (IEEE, Phoenix, 2008). https://doi.org/10.1109/INFOCOM.2008.179
- C. Zhang, R. Lu, X. Lin, P. H. Ho, X. Shen, in *INFOCOM 2008. The 27th Conference on Computer Communications*. An efficient identity-based batch verification scheme for vehicular sensor networks (IEEE, Phoenix, 2008). https://doi.org/10.1109/INFOCOM.2008.58
- D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensic Secur. 10(12), 2681–2691 (2015)
- N. W. Lo, J. L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. 17(5), 1319–1328 (2016)
- K. A. Shim, cal CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. 61(4), 1874–1883 (2012)
- H. Zhu, T. Liu, G. Wei, H. Li, PPAS: privacy protection authentication scheme for VANET. Clust. Comput. 16(4), 873–886 (2013)
- X. Lin, X. Li, Achieving efficient cooperative message authentication in vehicular ad hoc networks. IEEE Trans. Veh. Technol. 62(7), 3339–3348 (2013). https://doi.org/10.1109/TVT.2013.2257188
- Y. Hao, T. Han, Y. Cheng, in *Global Communications Conference* (*GLOBECOM*), 2012 IEEE. A cooperative message authentication protocol in VANETs, (2012), pp. 5562–5566. https://doi.org/10.1109/GLOCOM.2012. 6504006
- 35. S. Lloyd, Least squares quantization in PCM. IEEE Trans. Inf. Theory. 28(2), 129–137 (1982)
- S. Lamba, M. Sharma, in *Machine Intelligence and Research Advancement* (*ICMIRA*), 2013 International Conference On. An efficient elliptic curve digital signature algorithm (ECDSA), (2013), pp. 179–183. https://doi.org/ 10.1109/ICMIRA.2013.41
- C.-P. Schnorr, Efficient signature generation by smart cards. Cryptol, J. 4(3), 161–174 (1991)
- L. Licai, Y. Lihua, G. Yunchuan, F. Bingxing, in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference On.* Bargaining-based dynamic decision for cooperative authentication in MANETs (IEEE, Beijing, 2014), pp. 212–220
- G. Yunchuan, Y. Lihua, L. Licai, F. Binxing, in *INFOCOM*, 2014 Proceedings *IEEE*. Utility-based cooperative decision in cooperative authentication (IEEE, 2014), pp. 1006–1014
- T. Jing, F. Zhang, L. Ma, W. Li, X. Chen, Y. Huo, TORA: a truthful online reverse auction scheme for access permission transaction in macro-femtocell networks. Adhoc Sensor Wirel. Netw. 28, 347–362 (2015)
- 41. A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, extensible, and efficient VANET authentication. Commun. J. Netw. **11**(6), 574–588 (2009)
- M. Boban, W. Viriyasitavat, O. Tonguz, in ACM International Workshop on Vehicular Inter-Networking (VANET), Poster. Modeling vehicle-to-vehicle line of sight channels and its impact on application-level performance metrics (ACM, Taipei, 2013)