Efficient Secure and Privacy-Preserving Route Reporting Scheme for VANETs

Yuanfei Zhang, Qianwen Pei, Feifei Dai and Lei Zhang
Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, China
Email: 51151500152@stu.ecnu.edu.cn, 51164500231@stu.ecnu.edu.cn, 51151500011@stu.ecnu.edu.cn, leizhang@sei.ecnu.edu.cn

Abstract. Vehicular ad-hoc network (VANET) is a core component of intelligent traffic management system which could provide various of applications such as accident prediction, route reporting, etc. Due to the problems caused by traffic congestion, route reporting becomes a prospective application which can help a driver to get optimal route to save her travel time. Before enjoying the convenience of route reporting, security and privacy-preserving issues need to be concerned. In this paper, we propose a new secure and privacy-preserving route reporting scheme for VANETs. In our scheme, only an authenticated vehicle can use the route reporting service provided by the traffic management center. Further, a vehicle may receive the response from the traffic management center with low latency and without violating the privacy of the vehicle. Experiment results show that our scheme is much more efficiency than the existing one.

1. Introduction
Nowadays, vehicles bring much convenience for modern life. But with the increasing amount of vehicles, urban transportation system suffers many challenges. Traffic congestion happens in big cities during rush hours everyday, which has negative effects on traffic efficiency of the cities. Air pollution and low traffic efficiency caused by traffic congestion are serious problems for traffic management department. Also the complexity of the traffic environment makes drivers difficult to make decisions and could easily lead to accidents. Therefore, government focuses on technologies that can be used to resolve traffic problems. Vehicular ad-hoc network (VANET) is proposed recently to improve traffic efficiency. It has attracted more and more attention from both industry and academic community. A VANET usually consists of vehicles and infrastructures including roadside units (RSUs). Each entity in VANET is equipped with on-board unit (OBU) which has communication module and computation module. A VANET enables vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and infrastructure to vehicle (I2V) communications based on dedicated short range communication (DSRC) protocol [1].

VANET is a core component of intelligent traffic management system. With the knowledge of traffic information, intelligent traffic management system could be applied to control traffic situation directly or indirectly. For example, according to traffic flow, intelligent traffic management system can adjust traffic light to improve traffic efficiency [2]. As traffic congestion wastes much time of drivers and passengers, route reporting schemes supported by intelligent traffic management system would be a solution. Route reporting schemes require drivers to report their future routes to traffic management center so that possible traffic congestion could be predicted by analysing each vehicle's route information. According to the route information, drivers can change their routes to avoid traffic jam.
Although great convenience is provided by route reporting, it also suffers from several security and privacy issues that must be taken into consideration. In route reporting schemes, vehicles need to broadcast messages which contain their location, future routes, etc. If an attacker may learn a vehicle’s location or travel plan, then driver’s privacy would be violated. Pseudonyms are generally used to protect vehicles’ privacy. But most of the existing route reporting schemes using pseudonyms cannot meet the privacy requirements of drivers, because the reported information can be used to link pseudonyms [3]. In addition, an attacker can forge messages to mislead other vehicles or send fake messages to RSUs. Authentication mechanism should be provided to guarantee the security of the messages in VANETs. Digital signatures can be employed to provide authentication of the messages. To avoid the certificate management problem, identity-based signature is an ideal option.

Besides security and privacy, efficiency is a crucial concern for a route reporting scheme. When vehicles are driving at high speed, the entities in VANETs should react quickly so that vehicles can get response in real-time. A route reporting scheme should have low computation and communication overheads. In existing secure and privacy-preserving route reporting schemes, however, RSUs need to verify a mass of signatures to achieve authentication. If the signatures are verified one by one, it could not achieve expected efficiency requirement. To satisfy the efficiency requirement, an efficient batch verification technique should be employed in route reporting schemes. By using the batch verification technique, a set of signatures could be verified in a short period of time.

Recently, a scheme called privacy-preserving route reporting for infrastructure-based VANETs (PRIB) was proposed [3]. PRIB protects vehicles’ privacy by using pseudonyms to hide vehicles’ identities and using homomorphic encryption to hide vehicles’ travel plans. In PRIB, the traffic management center can only learn the total number of vehicles in each road segment. A vehicle’s travel plan will not be leaked to other entities.

1.1. Related Work
The concept of intelligent traffic management system was proposed in [4]. Intelligent traffic management system can be employed to define and apply traffic management decisions. Many intelligent traffic management schemes have been studied recently. Salama et al. proposed an intelligent cross road traffic management system which can control traffic lights by using photoelectric sensors to monitor traffic density [5]. Based on the radio frequency identification (RFID) technology, a scheme that collects and calculates average traffic flow information on each road to get latest congestion messages was proposed in [6]. Recently, Liu et al. proposed an intelligent traffic light control scheme which is secure, privacy-preserving and fog device friendly [2].

Route guidance is a valuable application in intelligent traffic management system. Khosroshahi et al. proposed an optimal route search algorithm for dynamic route guidance [7]. Hajiahmadi et al. proposed a high-level scheme for optimal dynamic route guidance using macroscopic fundamental diagram [8]. Wang et al. proposed a real-time path-planning algorithm based on a hybrid-VANET-enhanced intelligent transportation system, which takes advantages of VANETs and transportation system [9]. Lin et al. introduced a scheme that can be used to predict traffic conditions and determine alternative optimal routes based on shared traffic information [10]. Rabieh et al. proposed a privacy-preserving route reporting scheme, in which attackers cannot link pseudonyms [3].

The security and privacy issues in VANETs have been studied for a long time [11]-[14]. Pseudonyms are commonly applied to achieve vehicles’ privacy. Chaurasia et al. proposed a privacy sustaining strategy based on appropriate pseudonym update for VANETs [15]. Chim et al. proposed a VANET-based privacy-preserving navigation scheme based on anonymous credential [16]. Wei et al. proposed an RSU aided beacon-based trust management system which aims to thwart internal malicious attackers by using beacon messages and event messages [17]. Recently, Song et al. realized security requirements in VANETs by using secure multiparty computation and homomorphic encryption [18].

1.2. Our Work
In this paper, we propose an efficient secure and privacy-preserving route reporting scheme. Our scheme has five stages: setup, initialization, route request and reporting, batch verification and route
aggregation, traffic guidance. In setup and initialization stages, system parameters and entities' private-public keys are generated. In route request and reporting stage, a vehicle who wants to use the route reporting service has to connect to service provider, i.e., traffic management center, via an RSU. It has to verify the RSU's signature at first and then generate a route request which contains its signature and encrypted route. Batch verification and route aggregation is an important stage which is mainly executed by RSUs. In this stage, RSUs verify signatures from nearby vehicles and aggregate encrypted routes. Compared with a recent proposal, our main improvement is that we reduce the computation overhead of this stage. In traffic guidance stage, the traffic management center receives aggregated routes and generates traffic guidance for the vehicles. Performance evaluation is also given to show the efficiency of our scheme.

The remainder of this paper is organized as follows. Section II is the background which introduces our network model, design goals and related techniques. In section III, we give a high-level review of the PRIB scheme and discussion the efficiency of the scheme. In section IV, the improved scheme is proposed in detail. In section V, the performance evaluation and security analysis are presented. The last section is the conclusion.

2. Background

2.1 Network Model
As shown in Figure 1, a route reporting scheme consists of vehicles, RSUs, traffic management center (TMC), department of motor vehicles (DMV).

![Figure 1 Network model.](image)

- Vehicles: Vehicles run on the road and send route request packets when enter into the communication range of the RSUs. Vehicles also can use computation modules to encrypt and sign messages with issued credentials by DMV.
- RSUs: RSUs are deployed along the roads and also equipped with computation modules. RSUs can communicate with vehicles and TMCs. RSUs are responsible for route aggregation, traffic guidance forwarding, etc.
- TMCs: Each TMC is connected to a group of RSUs which are located in the TMC's monitoring area. TMCs generate traffic guidance for vehicles by using traffic information analysis algorithm.
- DMV: DMV is a trust agency that manages registration for vehicles and RSUs. Typically, DMV is responsible for generating public-private key pairs and certified pseudonyms for vehicles.

2.2 Design Goals
- Vehicle Privacy: The location privacy of the vehicles should not be leaked to other entities. Specifically, if the future route of a vehicle is leaked, an attacker can conduct monitoring which could impact the safety of the driver.
• Authentication: Authentication must be concerned in VANETs. If authentication is not supported, entities cannot detect whether the messages received have been modified or even malicious attackers may forge traffic guidance which would threaten the driver's safety.

• Computation efficiency: As we mentioned, computation efficiency is closely related to the latency of the route reporting scheme. Our scheme mainly focuses on the computation overhead to help drivers get route guidance in time.

2.3 Bilinear Maps
Bilinear map has been applied in various VANETs' schemes [19], [20] with its excellent cryptographic properties.
Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two cyclic additive groups of prime order $q$, and $\mathbb{G}_T$ be a cyclic multiplicative group of the same order. Let $P$ be a generator of $\mathbb{G}_1$, $Q$ be a generator of $\mathbb{G}_2$. A map $\hat{\epsilon}: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear map with following properties:

- Bilinearity: $\hat{\epsilon}(aP, bQ) = \hat{\epsilon}(P, Q)^{ab}$ for all $a, b \in \mathbb{Z}_q^*$.
- Non-degeneracy: $\hat{\epsilon}(P, Q) \neq 1$.
- Computability: There exists an efficient algorithm to compute $\hat{\epsilon}(U, V)$ for any $U \in \mathbb{G}_1, V \in \mathbb{G}_2$.

2.4 Homomorphic Encryption
Homomorphic encryption is a form of encryption that allows performing computation on ciphertext. The decrypted result matches the result that the same operation performed on the plaintext. Here is a form of homomorphic encryption:

$\mathbb{E}(m_1) \cdot \mathbb{E}(m_2) = \mathbb{E}(m_1 \cdot m_2)$

Paillier cryptosystem is applied in this paper because of its additive homomorphic properties.

3. The PRIB scheme
In this section, we describe PRIB briefly and give a discussion of PRIB.

3.1. Review of PRIB
In PRIB, roads are divided into segments and each segment has a unique identifier. DMV generates a public-private key pair and a secret for each vehicle. Each TMC generates a public-private key pair and publishes the public key. The RSU broadcasts route request packet to vehicles in its communication range. Vehicle verifies the signature of the RSU then reports its encrypted route if the signature is valid. Vehicle sends back packet containing its encrypted route by using Paillier homomorphic encryption [21]. After the RSU receives a certain number of route packets, it verifies the vehicles' signatures by leveraging batch verification technique [22], [23]. If the signatures are valid, the RSU aggregates the vehicles' routes and send aggregated route ciphertext to the TMC. TMC verifies the signature of aggregated route packet and decrypt the ciphertext. After decryption, the TMC gets the total number of vehicles that will drive in each road segment. Due to the homomorphic encryption, the TMC cannot acquire any vehicle's routes separately. With the number of vehicles in each road segment and traffic information, the TMC sends traffic guidance to vehicles through RSUs. So vehicles can easily avoid traffic congestion by the route reporting.

3.2. Discussion of PRIB
PRIB scheme aims to achieve privacy-preserving in route reporting scheme. To prevent attackers from using reported information to link pseudonyms, PRIB uses homomorphic encryption and route aggregation to protect vehicles' privacy. It's a valid approach for TMCs to analyse traffic condition and generate traffic guidance without leakage of vehicles' route information. However, more aspects should be concerned in traffic management system such as efficiency. Apparently, time overhead in PRIB needs to be low enough so that the drivers can make decisions timely. RSU plays an important role in PRIB, it sends requests, verifies signatures, aggregates routes, forwards routes. However, when RSU verifies the signatures of vehicles' routes, the verification of $n$ vehicles' route reporting packets needs $n+1$ times of pairing operations in PRIB. So the pairing operations in PRIB increases linearly with the
number of route reporting packets. As we know, pairing operations consume much of time in cryptography computation. If many vehicles are sending route reporting packets, drivers would spend much time waiting for traffic guidance. A technique that has lower time overhead should be employed to shorten the latency of traffic guidance.

4. Our Scheme

As shown in Figure 2, our improved scheme have five stages: setup, initialization, route request and reporting, batch verification and route aggregation, traffic guidance. In setup stage, DMV generates system parameters and publishes them to other entities. In initialization stage, DMV generates keys for vehicles and RSUs. In route request and reporting stage, the RSU sends route request to the vehicles in its communication range. After receiving request, the vehicle generates route reporting packet and sends it to the RSU. In batch verification and route aggregation stage, the RSU verifies route reporting packets using batch verification technique, then sends aggregated routes to the TMC. In traffic guidance stage, TMC decrypts aggregated routes and analyse routes to provide traffic guidance for vehicles.

| Notations | Descriptions |
|-----------|--------------|
| $s$       | The master private key of DMV |
| $P_0$     | The master public key of DMV |
| $V_i$     | The $i$th vehicle |
| $R_i$     | The $i$th RSU |
| $T_i$     | The $i$th TMV |
| $PID_i$   | The pseudo identity of $V_i$ |
| $v_{si}$  | The private key of $V_i$ |
| $r_{si}$  | The private key of $R_i$ |
| $r_{pi}$  | The public key of $R_i$ |
| $||$       | Message concatenation operation |
| $\oplus$ | A bitwise XOR operation |

Figure 2 System description.
4.1. Setup
At this stage, DMV generates the public parameters for the whole system. It does the following:

- Choose two cyclic additive groups $\mathbb{G}_1$, $\mathbb{G}_2$ and a cyclic multiplicative group $\mathbb{G}_T$ of prime order $q$, let $\hat{e}$ be a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. $P$ is a generator of $\mathbb{G}_1$.
- Choose cryptographic hash functions $H_0(\cdot) : \{0, 1\}^* \rightarrow \mathbb{G}_1$, $H_1(\cdot) : \{0, 1\}^* \rightarrow \mathbb{G}_2$, $H_2(\cdot) : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_3(\cdot) : \{0, 1\}^l \rightarrow \{0, 1\}^l$, where $l$ is the length of the pseudo-identities.
- Randomly pick $s \in \mathbb{Z}_q^*$ as its master private key, and computes $P_0 = sP$ as its master public key.
- Publish the system parameters as $\text{params} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, P_0, H_0(\cdot) \sim H_3(\cdot))$.

where $\text{params}$ are prestored in each entity in the system.

4.2. Initialization
At this stage, DMV generates private keys for vehicles and each RSU generates its private-public key pair. This stage is generally the same as that in PRIB [3].

- DMV generates private key $\nu_i$ for vehicle $V_i$ by computing $\nu_i = sH_1(PID_i)$, $PID_i$ is pseudonym of $V_i$. DMV sends $\nu_i$ and $PID_i$ to $V_i$ through secure channel.
- $R_i$ generates its private key by choosing $rs_i \in \mathbb{Z}_q^*$ and generates public key by computing $rP_i = rs_iP$.
- TMC generates $x$ as private key and $(m, \mu)$ as public key. TMC publishes the public key.

4.3. Route Request and Reporting
At this stage, the RSU sends route request to vehicles, the vehicle verifies the RSU’s signature then sends reporting packet to the RSU.

- $R_i$ generates the signature $\sigma_i = rs_iH_1(M \parallel ID_i \parallel \tau)$, where $M$ is the list of road segments that the RSU queries, $ID_i$ is the RSU’s identity, $\tau$ is the timestamp.
- The RSU send route request packet $M \parallel ID_i \parallel \tau \parallel \sigma_i$ to the vehicles nearby.
- Each vehicle checks the equation $e(P, \sigma_i) = e(rp_i, H_1(M \parallel ID_i \parallel \tau))$ to verify the signature of the RSU. If the equation holds, go next step, otherwise abort. The following is the proof of the equation.

\[
e(P, \sigma_i) = e(P, rs_iH_1(M \parallel ID_i \parallel \tau)) = e(rs_iP, H_1(M \parallel ID_i \parallel \tau)) = e(rp_i, H_1(M \parallel ID_i \parallel \tau))
\]

- For $1 \leq j \leq t$, $L_{i,j} \in \{000, 001\}$ represents whether $V_i$ will run on the $j$th road segment. $V_i$ chooses a random number $\eta_i$ and encrypts the route by computing $\xi_i = \mu^{(L_{i,1} + L_{i,2} + \cdots + L_{i,t})\eta_i^m} \bmod m^2$.
- $V_i$ selects a random number $\alpha_i$ and computes $X_i = \alpha_iP'$, $Y_i = \alpha_iP_0 + H_2(\xi_i, X_i)\nu S_i$, where $P' = \varphi(P)$ and $P_0 = \varphi(P_0)$, $\varphi$ is a mapping from $\mathbb{G}_1$ to $\mathbb{G}_2$.
- $V_i$ picks a random number $\beta_i$ and computes $V_i = \beta_iP$, $C_i = PID_i \oplus H_3(\beta_i rP_i)$.
- $V_i$ sends route reporting packet $\psi_i = (V_i, C_i, \xi_i, \omega_i)$ to $R_i$, where $\omega_i = (X_i, Y_i)$.

4.4. Batch Verification and Route Aggregation
At this stage, we modify the verification method of RSUs. When the RSU receives vehicles’ reporting routes, the RSU uses batch verification techniques to verify multiple signatures. The underlying signature scheme used here is [24]. Then the RSU aggregates encrypted routes which is same as PRIB’s aggregation.

- After $R_i$ receives $n$ route reporting packets, for $1 \leq i \leq n$, it computes $PID_i = C_i \oplus H_3(rs_iV_i)$.
- $R_i$ picks $n$ random numbers $r_1, r_2, \ldots, r_n \in \mathbb{Z}_q^*$, computes $Q_i = r_iH_2(\xi_i, X_i)H_1(PID_i)$, $X_i = r_iX_i$, $Y_i' = r_iY_i$.
- $R_i$ verifies the packets by checking the equation $e(P, \sum_{i=1}^n Y_i') = e(P_0, \sum_{i=1}^n (X_i' + Q_i))$
If the equation holds, go next step, otherwise abort. The following is the proof of the equation.
\[ e(P, \sum_{i=1}^{n} Y_i) = e(P, \sum_{i=1}^{n} r_i Y_i) = e(P, \prod_{i=1}^{n} r_i (\xi_0 X_i + VS_i)) = e(P, \prod_{i=1}^{n} r_i (\xi_0 X_i + HS_i(ID_i))) = e(P, \prod_{i=1}^{n} (r_i \alpha_i P_i + r_i H_2(\xi_0 X_i) H_1(ID_i))) = e(P_0, \prod_{i=1}^{n} (X_i + Q_i)) \]

- We use PRIB’s method to aggregate encrypted routes and generate signature. The aggregated routes is \( \Lambda = \prod_{i=1}^{n} \xi_i \mod m^2 \). The signature is \( q_i = rs_i H_1(\Lambda \parallel ID_i \parallel \tau) \).
- \( R_i \) sends aggregated route packet \( \Lambda \parallel ID_i \parallel \tau \parallel q_i \) to TMC.

### 4.5 Traffic Guidance

At this stage, TMC verifies the signature of aggregated route packet from RSUs and generate traffic guidance for vehicles. This stage is the same as that in PRIB.

- After the TMC \( T_i \) receives aggregated route packet, \( T_i \) checks
  \[ e(P, q_i) = e(rP_i, H_1(\Lambda \parallel ID_i \parallel \tau)) \]
  If the equation holds, go next step, otherwise abort. The following is the proof of the equation.
  \[ e(P, q_i) = e(P, rs_i H_1(\Lambda \parallel ID_i \parallel \tau)) = e(rs_i P, H_1(\Lambda \parallel ID_i \parallel \tau)) = e(rP_i, H_1(\Lambda \parallel ID_i \parallel \tau)) \]
- \( T_i \) computes \( (L(\Lambda^x \mod m^2)/L(\mu^x \mod m^2)) \mod m \) to get \( \sum_{i=1}^{n} L_{i,1} \parallel \sum_{i=1}^{n} L_{i,2} \parallel \cdots \parallel L_{i,t} \).
- \( T_i \) uses collected traffic information to generate traffic guidance and send it to vehicles through RSUs.

### 5 Evaluation

#### 5.1 Computation Overhead

The main difference between our scheme and PRIB is signature batch verification of reporting routes. So in this section, we focus the computation overhead of RSUs and show the efficiency of our improved scheme. Our experiments were implemented on a Linux machine with Intel Core i7-4790 at frequency of 3.60 GHz by using MIRACL library.
As shown in Figure 3, PRIB's verification time increases faster than ours and always longer than ours. In PRIB, when the RSU verifies the signatures of vehicles' routes, the verification of n vehicles' route reporting packets needs n+1 times of pairing operations. Pairing operations are time consuming cryptographic computations. However, in our scheme, we reduce the times of pairing operations into only 2. Also, the number of pairing operations in our scheme doesn't increase with the number of signatures. So in Figure 3, the verification time of our scheme is much lower than PRIB's time.

5.2. Security Analysis
In this section, we show that our scheme satisfies security requirements such as privacy-preserving and authentication.

- Vehicle privacy: With homomorphic encryption, each vehicle's future route is transmitted in the form of ciphertext. $V_i$ encrypts its route under the TMC's public key, so $R_i$ cannot recover $V_i$'s route. Furthermore, when TMC decrypts aggregated routes which are in form of $\sum_{i=1}^{n} L_{i,1} \| \sum_{i=1}^{n} L_{i,2} \| \ldots \| \sum_{i=1}^{n} L_{i,t}$, it means that only the number of vehicles that will drive on the segment would be achieved. So even TMC cannot get knowledge of each vehicle's future route.

- Authentication: Authentication is achieved by digital signatures. $R_i$ uses batch verification to verify multiple signatures of vehicles. The basic signature scheme in the paper is transformed from Hess's signature scheme [24]. The security of the signature scheme relies on Diffie-Hellman hard problem. The random numbers used in batch verification make the signatures unforgeable.

6. Conclusion
In this paper, we propose an improved route reporting scheme which is more practical than existing one. Our scheme uses the batch verification technique which can verify multiple route reporting packets in a short period of time. Compared to PRIB, our scheme not only achieves required security properties, but the computation overhead has been reduced. Both theoretical analysis and experiments show that our scheme is valid and meets the efficiency for traffic management system in VANETs. We will focus on more techniques to improve traffic management system by enhancing safety and efficiency.

7. Acknowledgment
This work is supported in part by the national key research and development program of China under grant 2017YFB0802004, the NSF of China under Grants 61572198, 61632012, Shanghai high technology field project under grant 16511101400.

8. References
[1] S. Al-Sultan, M. Al-Doori, A. Al-Bayatti and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” Journal of Network and Computer Applications, vol 37, pp 380-392, 2014.
[2] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng and J. Shen, “Secure intelligent traffic light control using fog computing,” Future Generation Computer Systems, Feb. 2017.
[3] K. Rabieh, M. M. E. A. Mahmoud and M. Younis, “Privacy-Preserving Route Reporting Schemes for Traffic Management Systems,” IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2703-2713, Mar. 2017.
[4] H. Kirschfink, J. Hernandez, M. Boero and M. Gmbh. “Intelligent traffic management models,” Seventh World Congress on Intelligent Transport Systems, Nov. 2000.
[5] A. Salama, B. Saleh and M. Eassa, “Intelligent cross road traffic management system (ICRTMS),” 2nd International Conference on Computer Technology and Development, pp. 27-31, 2010.
[6] W. Wen, “An intelligent traffic management expert system with RFID technology,” Expert Systems with Applications, vol. 37, no. 4, pp. 3024-3035, 2010.
[7] A. Khosroshahi, P. Keshavarzi, Z. KoozehKanani and J. Sobhi, “Acquiring real time traffic information using VANET and dynamic route guidance,” IEEE 2nd International Conference on Computing, Control and Industrial Engineering, pp. 9-13, 2011.
[8] M. Hajiahmadi, V. Knoop, B. Schutter and H. Hellendoorn, “Optimal dynamic route guidance: A model predictive approach using the macroscopic fundamental diagram,” 16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013), pp. 1022-1028, 2013.

[9] M. Wang, H. Shan, R. Lu, R. Zhang, X. Shen and F. Bai, “Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System,” IEEE Transactions on Vehicular Technology, vol. 64, no. 5, pp. 1664-1678, May 2015.

[10] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu and W. Zhao, “A Real-Time En-Route Route Guidance Decision Scheme for Transportation-Based Cyberphysical Systems,” IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2551-2566, March 2017.

[11] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer and B. Liu, “Practical secure and privacy-preserving scheme for value-added applications in VANETs,” Computer Communications, vol. 71, pp 50-60, 2015.

[12] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin and C. Hu, “Distributed Aggregate Privacy-Preserving Authentication in VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516-526, Mar. 2017.

[13] L. Zhang, “OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks,” IEEE Transactions on Information Forensics and Security, DOI: 10.1109/TIFS.2017.2730479.

[14] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, “APPA: Aggregate Privacy-Preserving Authentication in Vehicular Ad Hoc Networks,” The 14th Information Security Conference (ISC 2011), vol. 7001, pp. 293-308, 2011.

[15] B. Chaurasia, S. Verma, G. Tomar and S. Bhaskar, “Pseudonym Based Mechanism for Sustaining Privacy in VANETs,” First International Conference on Computational Intelligence, Communication Systems and Networks, pp. 420-425, 2009.

[16] T. Chim, S. Yiu, L. Hui and V. Li, “VSPN: VANET-Based Secure and Privacy-Preserving Navigation,” IEEE Transactions on Computers, vol. 63, no. 2, pp. 510-524, Feb. 2014.

[17] Y. Wei and Y. Chen, “An Efficient Trust Management System for Balancing the Safety and Location Safety and Location Privacy in VANETs,” 2012 IEEE 11th International Conference on Trust, pp. 393-400, 2012.

[18] J. Song, C. He, F. Yang and H. Zhang. “A privacy-preserving distance-based incentive scheme in opportunistic VANETs,” Security and Communication Networks, vol. 9, no. 15, pp. 2789-2801, Oct. 2016.

[19] B. Liu and L. Zhang, “On the Security of a Privacy-preserving Key Management Scheme for Location Based Services in VANETs,” Sixth International Symposium on Foundations & Practice of Security (FPS 2013), vol. 8352, pp. 323-335, 2014.

[20] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, “A Scalable Robust Authentication Protocol for Secure Vehicular Communications,” IEEE Transactions on Vehicular Technology, vol. 59, no. 4, pp. 1606-1617, May 2010.

[21] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” Adv. Cryptology EUROCRYPT, vol. 1592, pp. 223–238, Apr. 1999.

[22] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, “EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621-1631, Sept. 2012.

[23] L. Zhang, B. Qin, Q. Wu, F. Zhang, “Efficient Many-to-One Authentication with Certificateless Aggregate Signatures,” Computer Networks, vol. 54, no. 14, pp. 2482–2491, 2010.

[24] F. Hess, “Efficient identity-based signature schemes based on pairings,” in Proc. 9th Annual International Workshop Selected Areas in Cryptography (SAC’02), vol. 2595, pp. 310-324, 2002.