2022 10th International Conference on Intelligent Computing and Wireless Optical Communications (ICWOC) | 978-1-6654-7153-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICWOC55996.2022.9809903

Path Privacy-Preserving Scheme Based on Oblivious Transfer Protocol

Zian Yan
North China University of Technology
Beijing, China
17792617793@163.com

Jianhong Zhang
North China University of Technology
Beijing, China
jhzhangs@163.com

***Abstract*—Vehicular ad hoc networks (VANETs) can provide information and technical support for vehicles connected to the Internet, improving driving efficiency. However, VANETs requires drivers to disclose their specific driving paths to the server, and this measure increases the risk of leaking privacy. Honest but curious service providers may want to know customers' other private messages by collecting information about vehicle paths. Therefore, we propose an architecture based on the oblivious transport protocol to solve the above problems. In this architecture, the driver can obtain the required RSU messages without revealing the specific route information to the server. At the same time, our scheme uses the Chinese residual theorem to revoke malicious users, protecting the legitimate interests of service providers and RSUs. Finally, AES achieves fast authentication between the vehicle and the RSU, ensuring that the user can obtain real-time information while driving. Experiments show that our system can reduce computational costs compare to other methods.**

Keywords—VANETs, RSU, the Chinese residual theorem, oblivious transfer protocol

I. INTRODUCTION

With the continuous increase in the number of cars, road traffic problems such as congestion and safety accidents have become more and more serious. Autonomous driving technology can help vehicles plan their routes, reduce safety hazards such as fatigued driving, and improve driving safety. High-performance autonomous driving technology requires much environmental information, such as vehicle status, road conditions, weather, etc.

The V2X architecture is an architecture of autonomous driving technology, which usually includes vehicles, servers provider (SP) and RSUs. On the user side of V2X, the vehicle is equipped with a TPD module and an OBU module. The TPD module is responsible for the calculation; the OBU module is used to communicate and store messages. In VANETs, road condition information is directly collected by RSUs, uploaded to the server, and sent to the corresponding vehicle within its coverage. Vehicles can optimize and adjust their paths based on the received information, improve transportation efficiency and reduce the traffic accident rate.

This research was supported in part by the Natural Science Foundation of Beijing (no. 4212019, M22002), the National Natural Science Foundation of China (no. 62172005), the Guangxi Key Laboratory of Cryptography and Information Security (no. GCIS201808), the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province (No. ZCL 21014) and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (no. 2019BDKF JJ012).

However, some privacy issues exist on the Internet of Vehicles: the communication between entities is connected through wireless channels. The adversary can obtain the user's identity information through eavesdropping and other methods, which will damage the rights and interests of the user.

Angermeier et al. [1] proposed a scheme based on anonymous identity to address these problems. The network server generates an anonymous token for the vehicle; the user accesses the server with the anonymous token to obtain the required information. However, under this scheme, the server can obtain other information about the client, such as the vehicle's driving route, and use the collected data to infer the user's real identity. Digital signature [2]-[4] can solve the above problems, but digital signature needs to use PKI to generate public and private key pairs for each vehicle. On the one hand, the generation and verification of public and private key pairs require a lot of communication consumption; on the other hand, the expensive PKI increases the cost of server deployment. Lv *et al*. [5]. proposed a scheme based on BGN homomorphic encryption, which hides the trace information of the vehicle in a matrix. They Use matrix transformation to hide vehicle trajectory information. However, the amount of calculation on the client-side in this solution far exceeds the amount on the server, increasing the user's calculation burden, which is not feasible.

This paper proposes a path privacy protection method based on the k-out-of-n oblivious transmission protocol. The vehicle will generate its route information before departure and hide its path messages through oblivious transmission protocols. The protocol effectively reduces the amount of calculation for the client. For different RSUs, the keys are different, which improves the system's security level. Fast identity authentication based on AES encryption ensures that the information obtained by the driver is the latest. In addition, the agreement can also revoke malicious users through China's remaining theorem, which protects the interests of service providers.

The rest of the paper is organized as follows. Section II introduces the preliminaries, system modules, and designed goals. Our scheme is proposed in Section III. The analysis of Security, calculation evaluation, and comparison are shown in Section IV. Section V concludes the article.

II. PRELIMINARIES

We first give our network architecture, threat model, and design goals in this part. Then some relevant theoretical knowledge is introduced.

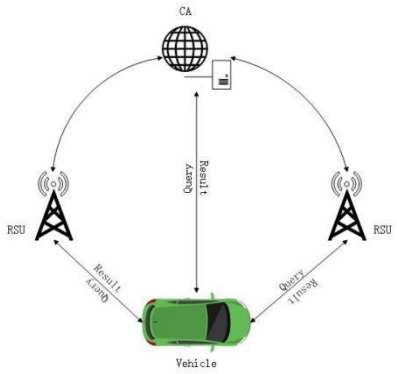

Fig. 1. System model.

- **CA:** CA is a semi-trusted party that is curious about the vehicle's tracks while complying with the execution of the protocol. In addition, the CA stores RSU's information and sends the information to the vehicle when it receives a query request from the vehicle.
- **RSU**: RSU collects traffic information within its coverage and sends it separately to the CA and the vehicles.
- **Vehicle**: The vehicle is equipped with OBU and TPD modules. The OBU is responsible for information exchange between the vehicle and RSU, CA, and the TPD stores information and security calculation.

A. Hilbert Curve

The space-filling curve can transform the two-dimensional data into one-dimensional data, reducing space complexity and computational overhead. As a spatially filled curve, the Hilbert curve preserves the adjacent nature of the original curve, with data traversing all the elements distributed over the square grid. In addition, the Hilbert curve can also be constructed according to different starting and ending points, increasing the convenience of spatial construction.

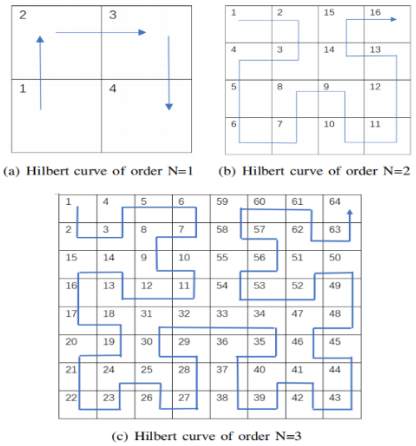

Fig. 2. Hilbert curve.

B. k-out-of-n Oblivious Protocol

The protocol is a two-party protocol [6] that allows the requester to select K RSU information from the CA. This protocol ensures that the server does not know the specific information chosen by the requester.

- **Requster:** If the requester wants to get messages $\{\gamma_1,\gamma_2,\ldots,\gamma_n\}$, the requester needs to construct two k-degree polynomials:

  1) $e(x)=\sum_{i=0}^{k-1}b_i x^i+x^k$, where $e(i)=0$, if $i\in\{\gamma_1,\gamma_2,\ldots,\gamma_n\}$

  2) $f(x)=\sum_{i=0}^{k-1}a_i x^i+x^k$, which is used to mask e(x) coefficient.

  3) The requester calculates $I_i=g^{a_i}h^{b_i}$ and sends the information $I=[I_0,\ldots,I_{k-1}]$ to the server.

- **Server**: The server computes $r_i=I_0 I_1^i\ldots I_{k-1}^{i^{k-1}}(gh)^{i^k}$, generates a secret key k_i, then encrypts each massage m_i by the ElGamal cryptosystem, the result is $c_i=(g^{k_i},m_i r_i^{k_i})$.

- **Requester:** For each RSU_i in $\{\gamma_1,\gamma_2,\ldots,\gamma_n\}$, the requester can get the plaintext m_i by computing

$$\begin{aligned} V_{\gamma_i}/U_{\gamma_i}^{f(\gamma_i)} &= m_{\gamma_i}\cdot(g^{f(\gamma_i)}h^{e(\gamma_i)})^{k_{\gamma_i}}/g^{k_{\gamma_i}f(\gamma_i)} \\ &= m_{\gamma_i}\cdot(g^{f(\gamma_i)}\cdot 1)^{k_{\gamma_i}}/g^{k_{\gamma_i}f(\gamma_i)} \\ &= m_{\gamma_i} \end{aligned}$$

C. Chinese Remainder Theorem

Assuming that there exist positive integers $p_1,\ldots,p_k$ which are mutually prime. For any integer, the congruence equations $c\equiv\sum_{i=0}^{k}y_i P_i M_i\equiv y_1P_1M_1+y_2P_2M_2+\ldots+y_kP_kM_k(\mathrm{mod}\,M)$ can be solved, where $M=p_1p_2\ldots p_k=p_1M_1=p_2M_2=\cdots=p_kM_k, M_i=\frac{M}{p_i}$, and M_i satisfies the solution of the congruence equation $M_iP_i\equiv 1(\mathrm{mod})p_i$.

$$\begin{cases} c\equiv y_1(\mathrm{mod}\,p_1) \\ c\equiv y_2(\mathrm{mod}\,p_2) \\ \cdots \\ c\equiv y_k(\mathrm{mod}\,p_k) \end{cases}$$

D. Elliptic Curve Cryptosystem

There exists a finite field F_p, where p is a prime number. A set of elliptic curve points E is defined as follows: $y^2=x^3+ax+b(\mathrm{mod}\,p)$, where $a,b\in F_p$ and $(4a^3+27b^2)\bmod p\neq 0$.

- Multiplication Properties: The multiplication properties of E are defined as $nP=p+\ldots+p$ (n times), where $n\in Z_q^*$, $n>0$.
- ECDLP: There exist two random points $P,Q\in G$ on curve E, where $Q=xP, x\in Z_q^*$. It is difficult to calculate x from Q.

E. Design Goals

The objectives of the scheme are as follows:

- Anonymity: the attacker cannot obtain the vehicle's real identity by attacking the RSU.
- Efficiency: After the vehicle enters RSU coverage, the RSU can quickly authenticate the vehicle's pseudo-identity and provide information for the certified vehicle.
- Route Privacy Protection: Assuming there is no collusion between CA and RSU, CA cannot obtain the trajectory of any vehicle.
- Unlinkability: The adversary cannot associate different pseudonyms from the exact vehicle.
- Revocation: CA can revoke a malicious user who does not comply with the User Agreement.

III. Our Scheme

This section proposes an efficient scheme to protect the privacy of the vehicle's path, which combines the k-out-of-n oblivious protocol and the Chinese remainder theorem. This scheme includes the **initialization**, **registration**, **query**, and **authentication** stages. The k-out-of-n oblivious protocol can help the vehicle obtain the symmetric keys of the relevant RSUs, but the server can not learn which symmetric keys the vehicle has received. The Chinese remainder theorem can realize the revocation of the malicious user. The details of the scheme are as follows:

A. Initial Phase

1) CA generates a public/secret key pair (PK_{CA}, SK_{CA}) and issues NO_{RSU_i} to RSU_i.

2) RSU_i selects its symmetric encryption key K_{RSU_i}, then sends K_{RSU_i} and identity certificate to CA. K_{RSU_i} is updated periodically, such as every day.

3) CA checks the identity certificate. If it is correct, CA uses the points in the Hilbert curve to represent the different geographic locations of the RSU in reality, RSU_i as shown in Fig. 2. CA sets the information vectors m_i.

TABLE I. RSUs Information

	Number	Symmetric key	Information
m_1	NO_{RSU_1}	K_{RSU_1}	$info_1$
m_2	NO_{RSU_2}	K_{RSU_2}	$info_2$
...	...	...	...
m_i	NO_{RSU_i}	K_{RSU_i}	$info_i$
...	...	...	...
m_n	NO_{RSU_n}	K_{RSU_n}	$info_n$

The road information RSU_i is donated as $info_i$, K_{RSU_i} is the symmetric key, NO_{RSU_i} corresponds to each grid RSU_i.

4) The CA publishes the actual map using Hilbert Curve and PK_{CA} to other entities, keeps K_{RSU_i} and m_i privately.

B. Registration Phase

1) The vehicle V_i sends the RID_i (the vehicle's real identity) and related information to CA.

2) CA verifies the vehicle's identity. If the verification is successful, CA generates an integer p_i for the vehicle RID_i, where $\gcd(p_i, p_j) = 1, i \neq j$. Then CA computes $M = p_1 p_2 \ldots p_k = p_1 M_1 = p_2 M_2 = \cdots = p_k M_k, M_i = \frac{M}{p_i}$, where $\varphi_i = M_i P_i \equiv 1 (\bmod p_i)$.

3) CA randomly chooses a new domain key $k_d \in Z_q^*$, and calculates $c = k_d \varphi_1 \ldots \varphi_n$, $c = k_d \varphi_1 \ldots \varphi_n$, where P is a random point on Elliptic Curve E.

4) CA returns φ_i to the vehicle V_i, chooses a random number $\mu \in Z_q^*$ and two secure one-way hash functions $H_i : \{0,1\} \to Z_q^* (i = 1,2)$, and calculates $P_{CA} = sP$. Finally, CA publishes the parameter $(q, E, P, P_{pud}, P_{CA}, H_1, H_2)$

C. Query Phase

Each vehicle's TPD uses the Dijkstra algorithm to predict its path on the actual map. If an RSU is passed, it will be put into the set P; otherwise, it will be discarded. Then TPD uses Hilbert Curves to transform the map into a sequence P, donates as $P = \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$, where n is equal to the total number managed by the CA.

To prevent CA from obtaining specific information about the vehicle's driving route, TPD initiates oblivious transfer protocol as follows:

1) The TPD generates the system parameters g, h and G_p. Then TPD constructs a polynomial function of degree $k : e(x) = \sum_{i=0}^{k-1} b_i x^i + x^k$, where e(i)=0, if $i \in \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$. Then, TPD generates a random polynomial $f(x) = \sum_{i=0}^{k-1} a_i x^i + x^k$,which is used to compute $I = [l_0, \ldots, l_{k-1}]$, where $l_i = g^{a_i} h^{b_i}$. TPD sends I to the CA.

2) For each RSU's information m_i, the server computes $r_i = l_0 l_1^i \ldots l_{k-1}^{i^{k-1}} (gh)^{i^k}$, and generates a secret key k_i. Then the server encrypts each massage m_i by the ga cryptosystem. The result is $c_i = (g^{k_i}, m_i r_i^{k_i})$ .Then, the CA sends the encrypted message c_i to the vehicle.

3) The TPD can get the plaintext m_i by computing $m_{\gamma_i} = m_{\gamma_i} r_{\gamma_i}^{k_{\gamma_i}} / g^{k_{\gamma_i} f(\gamma_i)}$ for each RSU_i in $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$.

D. Authentication Phase

1) TPD selects a random nonce $r_i \in Z_q^*$, and generates a pseudo-identity. $PID_i = H_1(r_i \cdot P_{CA}) \oplus RID_i$.

2) TPD obtains the domain key k_d by computing $c \bmod p_i = k_d$, then calculates $\alpha_i = H_2(PID_i \| T_1 \| a)$ and $P_V = r_i \cdot P$, where T_1 is the current timestamp. The signature is calculated as $\sigma_i = \alpha_i \cdot k_d \bmod q$.

3) OBU sends the encryption message $M_1 = \{\sigma_i, E_{K_{RSU_i}}(a), PID_i, P_V, T_i\}$.

4) RSU decrypts $E_{K_{RSU_i}}\{a\}$ and obtains σ_i, a, PID_i, T_i. Then it computes $\alpha_i^{'} = H_2(PID_i \| T_i \| a)$, and verifies whether the formula $\sigma_i \cdot P \overset{?}{=} \alpha_i^{'} \cdot P_{pud} \bmod q$ is established. It proves that the message M_1 comes from a legitimate user if it holds.

5) RSU authenticates the vehicle and sends $M_2 = \{H_1(a+1), E_{K_{RSU_i}}(info_i)\}$ to it.

6) The vehicle receives M_2 and checks $H_1(a+1)$ right. If it is correct, the TPD decrypts and obtains $info_i$; otherwise, it fails.

IV. Analysis

A. Security Analysis

1) **Anonymity**: According to the content of the previous section, we can learn the vehicle' real identity $RID_i = PID_i \oplus H_1(r_i \cdot P_{CA}) = PID_i \oplus H_1(\mu \cdot P_V)$. No adversary can solve the ECDLP problem in the given polynomial time.

2) **Efficiency:** When RSU certifies the vehicle, it only needs to perform 4 hash operations, 3 multiplication operations on the elliptic curve, and 1 AES operation, which takes about 0.0564ms.

3) **Route privacy protection**: We donate each RSU_i with γ_i. There is a group $(a_0^{'}, a_1^{'}, \ldots, a_{k-1}^{'})$ that satisfies every group $(b_0^{'}, b_1^{'}, \ldots, b_{k-1}^{'})$ representing the vehicle's path selection $(\gamma_0^{'}, \gamma_1^{'}, \ldots, \gamma_{k-1}^{'})$. The server can not distinguish $l_i = g^{a_i} h^{b_i}$ and $l_i^{'} = g^{a_i^{'}} h^{b_i^{'}}$ according to the DDH assumption.

4) **Unlinkability**: The vehicle uses pseudo-identity when sending a message signature. In the query phase, a random number is used in the process of constructing a pseudo-identity, which will change after sending a signed message. Thus, no adversary can associate the exact vehicle with the signature messages.

5) **Revocation**: The CA can restore the user's real identity by calculating the formula $RID_i = PID_i \oplus H_1(\mu \cdot P_V)$ when the vehicle violates the user agreement. Then, CA calculates $c_{new} = k_d^{'} \varphi_1 \ldots \varphi_{i-1} \varphi_{i+1} \ldots \varphi_n$.

B. Evaluation Analysis

In the query phase, the number of RSUs required by the vehicle is equal to the order of the polynomial k, and k determines the amount of TPD calculation. Meanwhile, The computation amount of CA is related to the order of the polynomial K, and the total number (denoted as n) of RSUs managed by CA. The computational amount of CA increases linearly with the total number of RSUs when the highest power of the polynomial k is fixed. In practice, an RSU can communicate over 500 meters directly and cover an area of 1 square kilometer. Shanghai's urban area is about 660 square kilometers. Approximately 1,000 RSUs are needed to ensure that the vehicle can receive the information in complex situations.

Our simulation was performed on a laptop computer equipped with I5-7300HQ 2.5GHz, 8G RAM. In addition, the k-out-of-n oblivious transfer protocol uses C based Miracl library.

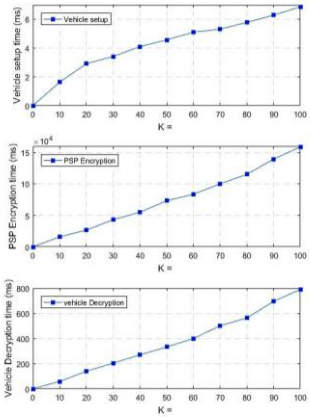

Fig. 3. Calculate Consumption.

1)TPD initializes the oblivious transfer protocol and computes the parameter of g, h and G_p, where the length of p is 1024bits, g and h are 512bits.

2) TPD's set up computing cost in generating e(x), f(x) and r_i is shown in Vehicle set up Computation;

3)CA generates a secret key k_i for each message m_i, then encrypts each message m_i by ElGamal encryption. The encryption result is $c_i = (g^{k_i}, m_i r_i^{k_i})$. The computational overhead of the CA generating ciphertext is shown in PSP Encryption

4)TPD decrypts the m_i by computing $m_{\sigma_i} = m_{\sigma_i} r_{\sigma_i}^{k_{\sigma_i}} / g^{k_{\sigma_i} f(\sigma_i)}$.TPD's decryption time is shown in Vehicle Decryption time.

C. Evaluation Comparison

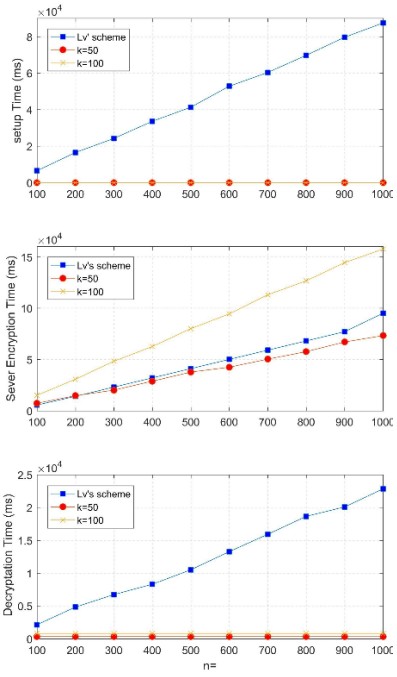

Fig. 4. Evaluation Compare.

We make a comparison with Lv's scheme. In the setup phase, our calculation efficiency mainly depends on the construction of polynomials e(x), f(x) and l_i. The efficiency of Lv's is based on the pre-encryption and shift matrix. In the encryption stage, our calculations are mainly reflected in the index calculation of NO_{RSU_i} and the parameter generation of ElGamal encryption; the calculation amount of the Lv's scheme is determined by BGN encryption parameter generation and matrix multiplication. In the decryption stage, our efficiency depends on the calculation of f(x) and the decryption of ElGamal; the Lv's scheme is based on the decryption speed of the BGN algorithm. The decryption speed of ElGamal is much better than that of the BGN algorithm.

In Fig.4, the computational cost of our scheme on the user side is much lower than that of Lv's scheme. On the server side, when k=50, our computational cost is slightly lower than the Lv's scheme. When k=100, our computational cost is approximately twice Lv's scheme. In reality, the server's computing power is much higher than that of the experimental platform; the computing consumption requirements of the client are as low as possible. Thus the above situation is acceptable.

TABLE II. OPERATION TIME

Operations	Symbol	Times(ms)
Pairing operation	T_{pa}	3.6631
Hash	T_h	0.001
AES encryption and decryption	T_{AES}	0.011
Multiplication of eliptic curve	T_{mul}	0.383
Modular operation	$T_{e\cdot m}$	0.4420
Multiplication of eliptic curve	$T_{e\cdot sm}$	0.0138

TABLE III. EXECUTION TIME COMPARISON

Scheme	Verify a vehicle	Verify n vehicle
Teng's scheme	$2T_{pa}+T_{mul}$	$2T_{pa}+T_{mul}$
Zhu's scheme	$2T_{pa}+13T_{mul}+2T_h$	$2T_{pa}+(6n+7)T_{mul}+2nT_h$
Our sheme	$4T_h+3T_{e\cdot sm}+T_{AES}$	$n(4T_h+3T_{e\cdot sm}+T_{AES})$

At the certification stage, the efficiency of our scheme also improved. Our calculations are mainly manifested in the multiplication operation of elliptic curves, encryption and decryption of AES, and hash function calculations in the authentication phase.

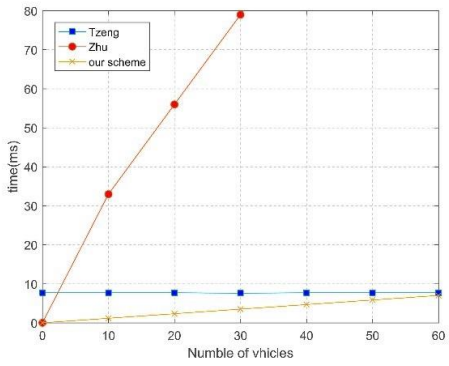

Fig. 5. Authentication Time.

The efficiency of TZENG [7] depends on batch verification. The timing of the pairing operation determines the efficiency of EAAP [8]. The approximate times for the various operations are shown in Table II. In Table III, we compare the verification time of TZENG, EAAP, and our scheme.

V. CONCLUSION

In this article, we introduced a protocol to protect the privacy of vehicle paths. With the help of the k-out-of-n oblivious transfer protocol, users can obtain the RSU information on the route while ensuring the confidentiality of the travel route. At the same time, the rapid authentication between the vehicle and the RSU can help users obtain the latest road condition information and improve the user travel experience. In addition, fast certification can also help RSU update road information within its coverage area, such as congestion conditions, in a timely and effective manner. Nevertheless, the protocol is not perfect. In future work, we hope to use short-term keys [9] to ensure that users can replace their pseudonyms, which can effectively prevent external adversaries from using link attacks [10] and motion tracking attacks [11] to infer users' real identity.

REFERENCES

[1] D. Angermeier, A. Kiening, and F. Stumpf, "PAL—Privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication," in Proc. ACM VANET, 2013, pp. 1–10.

[2] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[3] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[4] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 907–919, Feb. 2014.

[5] Songzhan Lv and Yining Liu, "PLVA: Privacy-Preserving and Lightweight V2IAuthentication Protocol," in IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS,24 February 2021, pp. 1 - 7.

[6] Youssef Khazbak, Junpeng Qiu, Tianxiang Tan, and Guohong Cao, "Target Finder: A Privacy Preserving System for Locating Targets through IoT Cameras," in ACM Transactions on Internet of Things Volume 1Issue 3July 2020 Article No.: 14pp 1–23https://doi.org/10.1145/3375878

[7] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," IEEE Trans. Veh. Technol., vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[8] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[9] K. J. Ahmed and M. J. Lee. "Secure LTE-based V2X service," IEEE Internet Things J., vol. 5, no. 5, pp. 3724–3732, Oct. 2017.

[10] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," Int. J. Distrib. Sens. Netw., vol. 12, no. 3, p. 6138251, 2016.

[11] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.