A GROUP MANAGEMENT SCHEME OF VEHICLE NETWORKING BASED ON HIERARCHICAL DISTRIBUTION

X. WANG[†‡], H. YUE[†] and X. SHE[†]

† *Hunan University of Science and Technology & School of Computer Science and Engineering, CA 411201, China.*
‡ *CONNECT, fengwxl@163.com*

***Abstract*— We introduce and implement a new centralized distribution algorithm and applied it to the vehicle networking environment, and the principle is to reconstruct the principal structure of a one-way function binary tree based on the Chinese remainder theorem, and generate the final group key from the bottom up.**

The analysis shows that the final data distribution can be reduced to the logarithmic level of the traditional centralized distribution data. In the aspect of authentication, we use the elliptic curve signature algorithm (ECDSA). It is more lightweight than Rivest Shamir Adleman(RSA) and the traditional Digital Signature Algorithm(DSA). The authentication and management of the vehicles in the coverage area can be faster and more convenient. Thus, it is more suitable for the fast-moving vehicle network environment.

Experiments shows the scheme can be applied to mobile and large number of nodes environments. Besides,it can realize efficiency, anonymity, traceability, non-repudiation and backward security in terms of security.

***Keywords*— Chinese remainder theorem, elliptic curve signature algorithm (ECDSA), Internet of vehicles, Anonymity, groups**

I. INTRODUCTION

With the rapid development of the automobile industry and economy, the explosive growth of the number of vehicles makes the potential safety problems occur frequently. The Internet of Vehicles (Hasrouny *et al*., 2017; Waqas *et al.*, 2020) is an emerging technology that ensures safe driving through real-time information sharing.

The way of the Internet of Vehicles is through a wireless connection. Due to the openness of wireless communication, it is more likely to be attacked (Waqas *et al.*, 2020).

The Internet of Vehicles has unique characteristics: a) complex topology variability; b) massive vehicles; c) can withstand higher power consumption; d) fast movement. Our goal is to reduce the delay as much as possible while ensuring the basic operation. Because of this, we cannot copy the original methods in wireless ad hoc networks and sensor networks. The large-scale multiple-input multiple-output technology in the 5G network architecture and the way of device-to-device communication can reduce the communication delay. (Gupta and Jha, 2015; Choi *et al.*, 2018). At the same time, batch operation, real-time and lightweight considerations are also the directions of our choice (Rai *et al.*, 2018; Minghui *et al.*, 2018).

The batch operation can reduce the number of communications between vehicles and servers during authentication. Furthermore, the effect can be accumulated with the effect of real-time and lightweight methods, so the concepts of aggregate authentication (Zhang and Zhang, 2009; Shim, 2010; Cheng *et al.*, 2015) and group authentication (Mahalle *et al*., 2014) are gradually proposed. Group authentication means that the members in the same group use a unified key to sign and authenticity. Every qualified member can sign on behalf of the group and the signature is valid. The realization of group authentication is to extract a public group key from the private key of the group, so now part of group authentication is to realize the member key through the Chinese remainder theorem (Zhang *et al.*, 2019). Finally, the extracted group key can be used as the key of traditional or new signature authentication schemes (Liu *et al.*, 2018). The group key is used as the key value of symmetric signature authentication schemes, elliptic curve (Zheng *et al*., 2020), bilinear mapping (Islam *et al.*, 2018) and DSA (Cui *et al.*, 2018) to achieve group authentication. It is not difficult to see from the experimental results that these schemes can reduce the total authentication time of vehicle nodes to a certain extent. However, because group authentication is a batch authentication method for nodes, its security requirement will be higher than that of single node authentication. And the experiment verifies the necessity of identity trust in group management, and finally concludes: in the absence of a reliable trust model, malicious nodes can deny the group key signature information in some specific ways (Zeng *et al.*, 2020). After that, the trust model is improved by different methods, such as 1) By adding the detection of behaviour, the improper behavior can be detected at the beginning (Hasrouny *et al.*, 2019); 2) In the scheme, the ability to resist key destruction is increased (Alfadhli *et al.*, 2019). 3) The scheme of hiding and protecting location information (Poongodi *et al.*, 2018). However, with the improvement of the trust model, the authentication scheme will inevitably become more and more bloated, so many scholars put forward some lightweight schemes (Kou *et al.*, 2019; Kou *et al.*, 2020). For example, a) In order to relieve the pressure of the team leader, a concept of trust agent is proposed, which manages the trust model through an agent (Kanchan and Chaudhari, 2019). b) Or the authentication nodes are divided into different regions to facili tate management and handoff (Kalil *et al.*, 2020; Lai and Ding, 2019; Jiang and Shen, 2020); c)

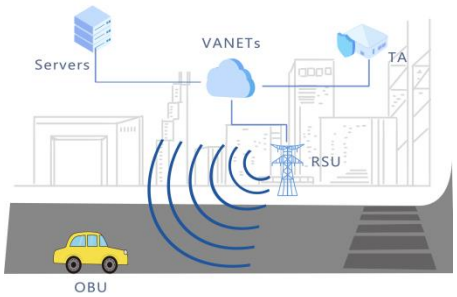

Figure 1: System structure diagram.

Group authentication is implemented based on Zero-Knowledge Proof, which is more lightweight because there is no power operation (Rasheed *et al.*, 2019). d) The symmetric encryption and asymmetric signature authentication algorithm are combined to achieve a lower communication overhead than the original pure asymmetric signature authentication scheme (Bunese *et al.*, 2020). With the popularity of 4G and the arrival of 5g, scholars have realized the need to combine 5g or cellular data network with vehicle network authentication, and the cooperation between the two can achieve higher efficiency and security. The corresponding authentication scheme is proposed for 5g environment (Lai *et al.*, 2018; Ouaissa *et al.*, 2020; Liu *et al.*, 2018; Tan and Chung, 2019).

There is still a massive challenge in group authentication, which is the need to distribute the relevant information of the group key. This paper refers to the key management and distribution methods in large-scale networks, such as key tree distribution and mapping. This paper reconstructs the formation of the key tree.

Our work reduces the delay on the premise of ensuring the normal operation of the basic group authentication operation, introduces batch operations, improves real-time performance, light weight, and improves security, and proposes corresponding solutions for the upcoming 5G technology.

II. SYSTEM STRUCTURE AND PRELIMINARY KNOWLEDGE

A. System structure

In this paper, the model used includes TA (trusted institution), fixed RSU (roadside device), and mobile OBU (on-board device). The structure is shown in the figure below:

The on-board unit (OBU) carried by the vehicle regularly broadcasts its own speed and direction information, and the RSUs) Road location and safety information broadcast to vehicles regularly, so that other OBUs can quickly obtain useful information on the road. RSU can broadcast and receive some signature information in the group, provide various services for OBU, broadcast the identity information of revoked vehicles, and assist TA to reveal the real identity of some illegal vehicles. Each RSU has its own storage space and computing power.

B. Group authentication

Group authentication is a solution to a large number of vehicle node authentication, which can be used to reduce the number of communication between OBU and the authentication server.

Elliptic Curve Digital Signature Algorithm (ECDSA) :
Elliptic curve cryptography (ECC) is a public key cryptosystem based on elliptic curve algebra over finite fields. One of its greatest advantages is that the key size is much smaller than the traditional public key cryptosystem, which makes the algorithm based on elliptic curve suitable for resource constrained devices. And it can also be used in the Internet of Vehicles. Moreover, because it is based on elliptic curve discrete logarithm problem (ECDLP), elliptic curve cryptosystem has high security.

An elliptic curve over a finite field F_q (a finite field of order q) consists of all points (x, y), where $x, y \in F_q$, infinity O satisfy the *Weierstrass* form of length:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where $a_i \in F_q$, $a, b \in F_p$ and $4a^3 + 27b^2 = 0 \bmod p$.

There are two finite fields: the prime field F_p and the binary field F_{2m}. When the field of prime number ($p > 3$) is used, the above formula can be simplified as:

$$y^2 = x^3 + ax + b \quad (2)$$

For other related operations such as addition, multiplication and more, please refer to (Johnson *et al.*, 2001).

For digital signature schemes, ECDSA is widely used. Many studies have proved that the algorithm is suitable for a limited source environment (Wander *et al.*, 2005). In fact, compared with other public key cryptography algorithms such as RSA, DSA and ElGamal (Al-Zubaidie *et al.*, 2019), ECDSA provides authentication, integrity and non-repudiation with lower computational cost. For example, ECDSA with 256-bit key provides the same level of security for the RSA algorithm with 3072 bit key.

Key tree structure composed of Chinese remainder theorem:
The definition of Chinese remainder theorem (Sorbi *et al.*, 2009) is as follows:

$$\begin{cases} y \equiv y_1 (\bmod\ m_1) \\ y \equiv y_2 (\bmod\ m_2) \\ \vdots \\ y \equiv y_k (\bmod\ m_k) \end{cases} \quad (2)$$

when $k \geq 2$, let $M = m_1 m_2 \cdots m_k$, $M_i = \coprod_{j \neq i} m_j$. Then we can get $y \equiv x_1 M_1 M'_1 + x_2 M_2 M'_2 + \cdots + x_k M_k M'_k$. Where $MM'=1$.

C. Key tree generation and construction

We regard k actual node values as a tree structure of leaf nodes. Through the combination of two to form an internal node, the node of the upper layer is generated. Continue the above operation until the number of nodes in the generated layer is 1, and then a binary key tree is generated. As follows:

The square node represents the actual node, while the circle represents the internal node. Two child nodes construct a parent node, and the corresponding relationship is:

$$y_{ij} = y_i M_i M'_i + y_j M_j M'_j \quad (3)$$

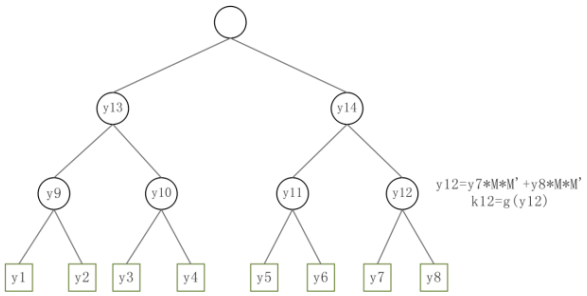

Figure 2: Chinese Remainder Theorem of tree structure

The key distribution method in the key tree: $g(y_i)$ represents the mapping function, which can map the secret to the domain corresponding to the symmetric key, and this value can be used to encrypt the spread secret value. In the key tree structure, each actual node only needs to keep the secrets of the sibling node and the ancestor's sibling node to get the final group key. Just because the secrets of the sibling node and the ancestor's sibling node are kept, the processing centre only needs to broadcast and update the changed node secrets encrypted by the sibling node's $g(y_i)$. Unicast is used to join a new node because the new node needs to know the secret value in the original key tree, so it is only necessary to unicast the secret value to the new node.

III. PROPOSED SCHEME

In this part, we propose a novel group signature scheme for VANETs privacy protection. In this scheme, Ta is responsible for the registration, identity authentication, certificate issuance and revocation of OBU and RSU, and RSU is responsible for group management. Let us assume that TA is fully trusted and RSU is honest and curious. The scheme is as follows:

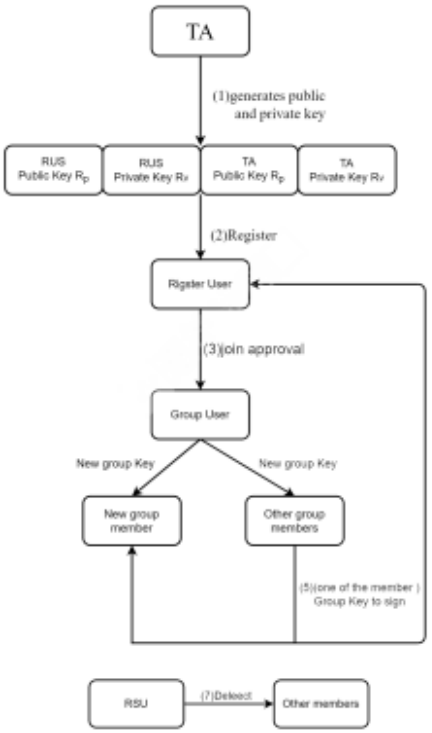

Figure 3: Scheme processing flow chart

The processing flow of group signature is as follows:

- Initialization: TA selects system parameters and generates its key and TA's key to prepare for the next step.
- Registration: the vehicle node applies for registration with TA, and TA generates a pseudonym after receiving the registration application information, and then goes to the next step.
- Join: the new member applies to the group administrator for a license, and the group administrator sends the license to the new member after approval and goes to the next step
- Generate group key: the group manager generates a group key for the new members and distributes the group key to each member user.
- Signature: any group member signs information with the group key.
- Confirmatory signature: any group member in the group will verify the information signed with the group key after receiving it.
- Delete (cancel): when a member needs to exit, the RSU will change the key of the new node to an invalid state, and then the group key will change accordingly.
- Tracking: when RSU finds malicious information or when there is a dispute among nodes, it will open the signature through RSU and recover the real identity of the user node. Then, the malicious node is marked and added to the database of the malicious node. In the future, the malicious node will never be added to the network.

A. Initialization

TA uses the following algorithm to generate its own public-private key pair: TA is mainly responsible for generating a series of pseudonym parameters.

TA needs to generate some coefficients (RSA encryption) for kana generation. Based on the selected elliptic curve, TA selects two random numbers s, r. The product of s and r is n, and G is a prime number less than n. TA performs the following calculation, and takes (R, X, G) as public key information and (x, r) as private key information,

$$R = r.G \quad (4)$$

$$X = x.G \quad (5)$$

B. Register

In this paper, when RSU and OBU want to join VANETs, TA will generate the corresponding certificates and pseudonyms for them. When RSU receives the certificate, it can verify whether the new group member is legal. Finally, RSU will broadcast users' pseudonyms through hierarchical distribution, so that other legitimate users can know the legitimacy of new users.

TA evenly selects random number r, calculates $R = r.\dot{G}$, and then sends it to the user applying for registration. The user generates a pseudo-random number $e = hash(R||ID_i)$ by selecting a hash function and sends it to ta. TA calculates $UID = r + e.x$ and $X = x.\dot{G}$, and sends (UID, X) to the registered user. When the user

receives the registration information, it means that the registration phase is completed and the next step is started.

C. Join

After RSU receives the registration information and the certificate, after RSU confirms the certificate, it means that the user is legal and can be allowed to join the group. At this time, the join operation is finished and the next step is started. The confirmation algorithm is as follows:

$$UID = r.G + e.x.G = R + e.X \quad (6)$$

When the equation is true, and $T' - T \leq \Delta T$ (ΔT means freshness), it means that the certificate is legal and does not time out, and the certificate is confirmed successfully. Therefore, through the confirmation of the certificate and whether the timeout is used as the certificate of whether the member joins the group, the certificate will be saved into the database after obtaining the certificate.

D. Generate the corresponding group key

The required information is distributed by generating a binary tree structure. The distribution methods include multicast and unicast. As shown in Fig. 1, when a node broadcasts information, it only needs to encrypt the key of its sibling node and the key of the sibling node of its ancestor node with the key of its own node, so that the node can get the necessary group key information.

The vehicle node U_i randomly selects a prime number b_i to send to RSU; RSU randomly selects a prime number d, $1 \leq d \leq n-1$ as the private key, then calculates $D = (x, y) = dG$, then takes D as the public key and d as the private key. Calculate as follows:

$$\begin{cases} d = d_1 (\text{mod } b_1) \\ d = d_2 (\text{mod } b_2) \\ \quad \vdots \\ d = d_r (\text{mod } b_r) \end{cases} \quad (8)$$

1. Group initialization:

Firstly, RSU distributes the initial key information k_i and secret d_i to the authenticated nodes. The steps are as follows:

- Key sharing: the secret value d_i (leaf node's secret value) is transmitted between RSU and the single vehicle by DH exchange.
- Establish the tree pointing relationship: establish a binary tree relationship for the nodes of the initial group, and transfer the pointing relationship of each node to each node.
- Broadcast key information: broadcast the internal node information of each leaf, and finally each vehicle node obtains the secrets of the sibling node and the ancestor's sibling node (that is, the necessary information to obtain the group key);

2. Group Join:

When the vehicle node joins the group, it only needs to broadcast the node secret of each node corresponding to the new blind node. Of course, when broadcasting, it is encrypted by the key of its brother node. As shown in the figure, it only needs to broadcast the secret of the new 9, 13, 15 and 16 nodes. ($E_{k_1}(d_{16})$, $E_{k_2}(d_9)$, $E_{k_{10}}(d_{15})$, $E_{k_{14}}(d_{13})$) can unicast the brother node 1 and the ancestor's brother node (2, 10, 15) required by (16 nodes, 14). The secret of ($E_{k_{16}}(d_1, d_2, d_{10}, d_{14})$).

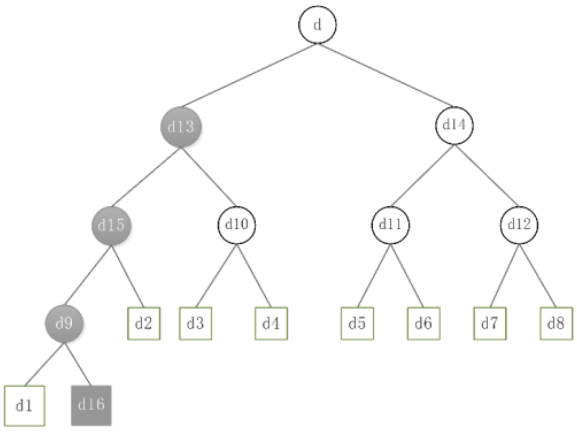

Figure 4: Schematic diagram of node joining.

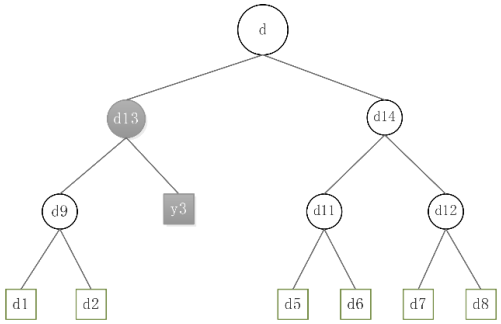

Figure 5: Schematic diagram of node deletion

3. Group deletion:

When the vehicle node applies to RSU to leave the group, RSU needs to update the change of the group key after the node leaves by broadcasting. It only needs to encrypt and broadcast the changed node secret information through the brother node key, as shown in the figure below, and only needs to broadcast the $E_{k_9}(d_3)$, $E_{k_{14}}(d_{13})$ information to each node.

E. Signature

We compared RSA, DSA and ECDSA signature authentication algorithm, and finally concluded that ECDSA can provide identity, integrity and non- repudiation. ECDSA with 256 bit key provides the same level of security for RSA algorithm with 3072 bit key. User U1 selects a message M and a public-private key pair ($d, Q = dG$), so the signature steps are as follows:

- Randomly select a prime number k, the value range is $1 \leq k \leq n-1$, calculate $(x, y) = kG$.
- Calculate k^{-1} mod n.
- Calculate $e = HASH(m)$.
- Calculate $s = k^{-1}(e + d.(D_i \ mod \ b_i)) mod \ n$, so the final signature information is (x, s).

F. confirm

- Confirm that R and s are in $[1, n-1]$.
- Calculation $HASH(m)$.

- Calculation $w = s^{-1} \ mod \ n$.
- Calculation $u_1 = ew \ mod \ n$and $u_2 = xw \ mod \ b_i$.
- Calculate $(x_i, y_i) = u_1 G + u_2 Q$. If $(x, y) = O$ the signature is illegal.
- If and only if $x_i = mod \ n == x$ accepts the signature.

G. Delete

When the node needs to leave the area covered by the group, the node needs to be deleted. It only needs to delete the group.

H. Trace

When RSU finds a malicious node or two nodes have a dispute, RSU and TA will open the signature to show the real identity of the vehicle user. RSU can calculate the known group public key x and the congruence equation $x = D_i (mod \ b_i)$, then RSU can obtain the certificate of the malicious node, and TA can obtain the real identity of the malicious node by calculating $UID = r + hash(R||ID_i).x$ through the private key T_s.

IV. SAFETY AND PERFORMANCE ANALYSIS

A. **Correctness analysis**

The correctness of this article involves the correctness of identity information, RSU public parameters and signature.

1. Correctness of identity information:

RSU receives the vehicle U_i identity information ID_i and generates the time stamp T'. RSU uses (m, X, R) to calculate $UID.G = r.G + e.x.G = R + e.R$ to confirm the legitimacy of the identity without a timeout.

2. Correctness of identity information:

RSU judges whether $x_i = mod \ n == x$ is true by calculating the equation $(x_i, y_i) = u_1 G + u_2 Q$ and indicates that the signature is correct when M2 is true.

B. **safety analysis**

Through mathematical analysis, we conclude that our scheme can meet the following characteristics.

- Anonymity: due to the use of certificate signature technology and timing update strategy (when the user applies to TA for registration, TA will generate a pseudonym for the user and update it every other time), the attacker cannot infer the real identity of the vehicle.
- Traceability: when a malicious node is found on the Internet of vehicles, the real information of the malicious node can be traced and marked through the cooperation between RSU and TA.
- Non-repudiation: non repudiation means that no member of a group can generate a signature. In our scheme, if an attacker participates in the forgery of information signature (R, s), because it cannot directly calculate d through Q, then it will choose a random number d to forge the original d value, so the final signature $s' = k^{-1}(e + d'D_i) mod b_i$ is not equal to the original signature $s = k^{-1}(e + dD_i) mod b_i$ of the member, which proves its non-repudiation.
- Backward security: it indicates that the revoked vehicle node cannot obtain the subsequent node, which is guaranteed by the binary tree structure based on the Chinese remainder theorem. When the node is deleted, its direction will be changed, and the group key is generated by deleting the remaining nodes of the node.
- Mutual concealment in a group: members in a group cannot access the private key information of other members, but can only access their public information. In the process of key distribution, users only receive their own private key and cannot access other members' private keys.

C. **Performance analysis and performance**

We compare the time cost and the number of key distributions between the key distribution scheme 1 (Liu *et al.*, 2018) using the same structure and scheme 2 (Zheng *et al.*, 2020) using the synchronization factor. The experimental environment is implemented in the veins (vehicle network simulation environment), and its configuration is shown Table 1.

We set up such a scene, as shown in the figure below. An RSU device is distributed at a crossroad, which assists the verification server in vehicle authentication. Next to the intersection are 11 vehicles (all carrying vehicle units for communication). The vehicle sends the group joining requests to RSU one after another. RSU verifies the identity legitimacy of the vehicle to ta. If the verification is legal, RSU will join the group and update the group key and issue the group key to the vehicle. The vehicle is signed with the group key, while other vehicles or RSUs verify it. At the same time, we record the time cost of vehicle signature verification and the number of data distribution when joining the group. As shown in Fig. 7, 8, 9 and 10.

The figure below shows the time cost comparison of scheme 1, scheme 2 and this scheme in single vehicle verification. It can be seen that the delay of this scheme for scheme 1 is significantly reduced, which is consistent

Table1. Experimental environment parameter table

Device information	Parameter
CPU	Intel(R) Core(TM) i5-3337U at 1.80GHz
RAM	4GB
Operating system	Ubuntu (R) 16.04 (virtual machine)

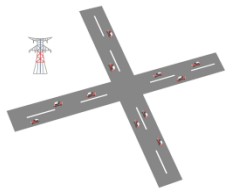

Figure 6: Scene diagram

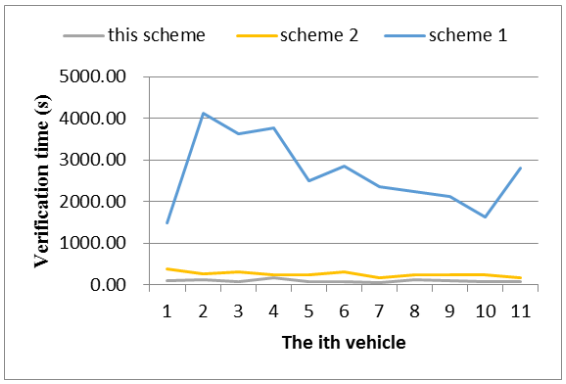

Figure 7: Verification time for a single vehicle

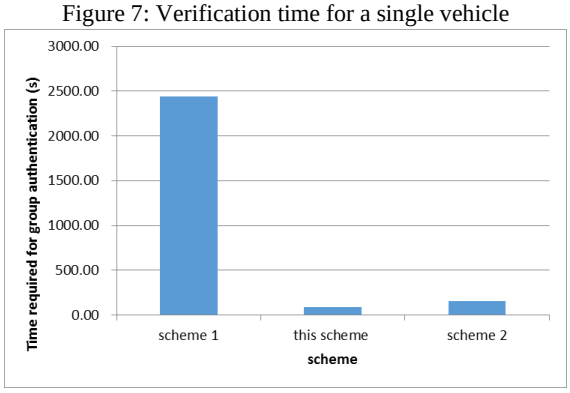

Figure 8: Comparison of time required in RSU coverage area

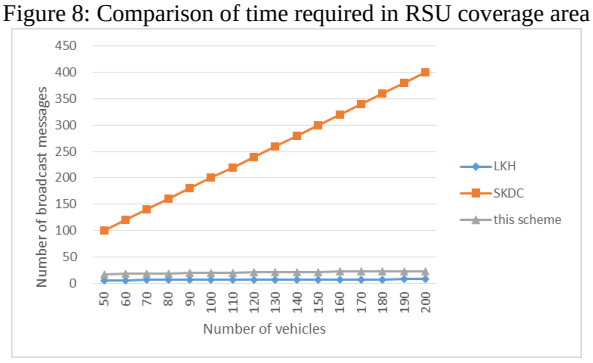

Figure 9: The number of broadcasts required to join a node

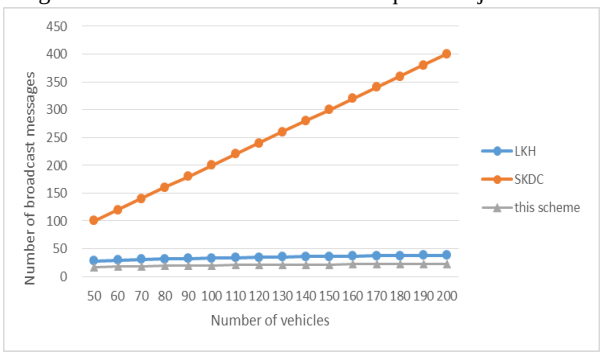

Figure 10: The number of broadcasts required to delete a node

with our expectations. This is due to the reason that we convert the signature verification scheme from DSA signature authentication scheme to ECDSA signature authentication scheme, which is mainly due to the low cost of elliptic curve algorithm The reason why scheme 2 has a slight advantage is that it adopts the structure of key tree, which has lower overhead than scheme 2 which uses complex operations to complete group authentication. Here we have a more detailed analysis in the data distribution comparison chart.

Next, we compare the number of broadcasts needed by the key distribution scheme with SKDC and LKH (Wong *et al*., 2000), which are the traditional distribution scheme based on the center and the top-down hierarchical distribution scheme. It can be seen that both this scheme and LKH are better than the traditional distribution scheme SKDC in terms of the number of distributed data. The number of distributed data of SKDC increases linearly with the number of nodes, and the number of distributed data of this scheme is slightly more than that of LKH. However, LKH needs to carry out encryption operations when encrypting data, which is more expensive than this scheme. Overall, we get the conclusion that the communication cost of this scheme is optimal, and the number of data distribution is slightly less than that of LKH.

V. CONCLUSION

In the environment of the Internet of vehicles, a large number of car certifications makes the pressure of the certification management center suddenly soar. At the same time, the topological changes caused by vehicle movement also make the work of certification management center more difficult. Therefore, it is necessary to have a scientific key management and lightweight authentication scheme. In this article, the elliptic curve algorithm is used as the authentication scheme. Through the experiment, it is found that it only takes milliseconds to complete the authentication. Through the investigation of the actual situation, the coverage of an RSU is about 500 meters, and the authentication scheme designed in this paper can be completed at normal speed. Besides, the key distribution method in this paper is achieved through the key tree. And when deleting users, the number of information distribution is greatly reduced. According to the section of "safety and performance analysis", we can also see that the scheme can meet the required security.

REFERENCES

Alfadhli, S.A., Alresheedi, S., Lu, S., Fatani, A. and Ince, M. (2019) ELCPH: An Efficient Lightweight Conditional Privacy-Preserving Authentication Scheme Based on Hash Function and Local Group Secrete Key for VANET. *The World Symposium*. Wuhan, China, 32-36.

Al-Zubaidie, M., Zhang, Z. and Zhang, J. (2019) Efficient and secure ECDSA algorithm and its applications: a survey. *arXiv*. **1902**, 10313-10344.

Blum, J.J., Eskandarian, A. and Hoffman, L.J. (2004) Challenges of intervehicle ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*. **5**, 347-351.

Bunese, E.E., Todt, E. and Albini, L.C.P. (2020) Vanet security through group broadcast encryption. *Journal of Computer and Communications*. **08**, 22-35.

Cheng, L., Wen, Q., Jin, Z., Zhang, H. and Zhou, L. (2015) Cryptanalysis and improvement of a certificateless aggregate signature scheme. *Information Sciences*. **295**, 337-346.

Choi, G., Jung, J., Moon, H., Kim, Y. and Pan, S. (2018) User authentication system based on baseline-corrected ecg for biometrics. *Intelligent Automation and Soft Computing*. **25**, 193-204.

Cui, J., Tao, X., Zhang, J., Xu, Y. and Zhong, H. (2018) HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for vanets. *Vehicular Communications*. **14**, 15-25.

Hasrouny, H., Samhat, A.E., Bassil, C. and Laouiti, A. (2017) VANet security challenges and solutions: A survey. *Vehicular Communications*. **7**, 7-20.

Hasrouny, H., Samhat, A.E., Bassil, C. and Laouiti, A. (2018). Trust model for secure group leader-based communications in VANET. *Wireless Networks*. **25**, 4639–4661.

Isam, S.K.H., Obaidat, M.S., Vijayakumar, P., Abdulhay, E., Li, F. and Reddy, M.K.C. (2018) A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets. *Future Generation Computer Systems*. **84**, 216-227.

Jiang, Y., Ge, S. and Shen, X. (2020) Aaas: an anonymous authentication scheme based on group signature in vanets. *IEEE Access*. **8**, 98986-98998.

Johnson, D., Menezes, A. and Vanstone, S. (2001) The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*. **1**, 36-63.

Kalil, H.E.H., Kora, A.D. and Boumerdassi, S. (2020) Security in VANETs: Lightweight Protocol for Group-of-Vehicles Masters (LPGVM). *22nd Int. Conf. on Advanced Communication Technology (ICACT)*. Phoenix Park, PyeongChang, Korea (South). 6-11.

Kanchan, S. and Chaudhari, N.S. (2019) Signcrypting the group signature with non-transitive proxy re-encryption in vanet. *Recent Findings in Intelligent Computing Techniques*. Singapore, 15-23.

Kou, J., He, M., Xiong, L., Ge, Z. and Xie, G. (2020) Efficient hierarchical multi-server authentication protocol for mobile cloud computing. *Computers, Materials and Continua*. **64**, 297-312.

Kou, L., Shi, Y., Zhang, L., Liu, D. and Yang, Q. (2019) A Lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT. *Computers, Materials and Continua*. **58**, 545-565.

Lai, C. and Ding, Y. (2019) A Secure Blockchain-Based Group Mobility Management Scheme in VANETs. *IEEE/CIC Int. Conf. on Commun-ications in China (ICCC)*. Changchun, China. 340-345.

Lai, C., Zheng, D., Zhao, Q. and Jiang, X. (2018) SEGM: A secure group management framework in integrated VANET-cellular networks. *Vehicular Communications*. **11**, 33-45.

Liu, P., Liu, B., Sun, Y., Zhao, B. and You, I. (2018) Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET. *IEEE Access*. **6**, 20795-20806.

Liu, X., Jia, Z., Xu, E., Gong, B. and Wang, L. (2018) A privacy protection scheme in vanets based on group signature. In Chinese Conf. on Trusted Computing and Information Security. Singapore, 286-300.

Mahalle, P.N., Prasad, N.R., and Prasad, R. (2014) Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT). *4th Int. Conf. on Wireless Communications*. Aalborg, Denmark, 1-3.

Minghui, Z., Yangyang, D., Hanxiao L., Infoeng S.O. and Nationalities U.F. (2018) Research on Identity Authentication Protocol Group Signature-based in Internet of Vehicles. *Journal of Guiyang College Natural Sciences.* **10**, 30-32.

Ouaissa, M., Houmer, M. and Ouaissa, M. (2020) An Enhanced Authentication Protocol based Group for Vehicular Communications over 5G Networks. *3rd Int. Conf. on Advanced Communication Technologies and Networking (CommNet)*. Marrakech, Morocco, 1-8.

Poongodi R.K. and Sivakumar T. (2018) Enhanced Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks Using Authentication Group Key. *Bonfring International Journal of Software Engineering and Soft Computing*. **8**, 26-30.

Rai, K.M., Yadav, A., Sagar, A.K. and Gupta, A., and Jha, R.K. (2015) A survey of 5g network: architecture and emerging technologies. *IEEE Access*. **3**, 1206-1232.

Rasheed, A.A., Mahapatra, R.N. and Hamza-Lup, F.G. (2019) Adaptive Group-Based Zero Knowledge Proof-Authentication Protocol in Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*. **21**, 867-881.

Sagar, S (2018) Security Provision In VANETs Using Group Based Key Share Algorithm. *Int. Conf. on Advances in Computing*. Greater Noida (UP), India, 261-266.

Shim, K.A. (2010) An id-based aggregate signature scheme with constant pairing computations. *Journal of Systems and Software*. **83**, 1873-1880.

Sorbi, A., Wu, G. and Yang, Y. (2009) High minimal pairs in the enumeration degrees. 6th *Annual Conference on Theory and Applications of Models of Computation.* Changsha, China.

Tan, H. and Chung, I. (2019) A Secure Cloud-Assisted Certificateless Group Authentication Scheme for VANETs in Big Data Environment. *Int. Conf. on Big Data Engineering*. New York, United States. 107-113.

Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C. (2005) Energy analysis of public-key cryptography for wireless sensor networks. *Third IEEE Int. conf. on pervasive computing and communications.* Kauai Island, 324-328.

Waqas, M., Tu, S., Rehman, S.U., Halim, Z. and Rehman, O.U. (2020) Authentication of Vehicles and Road

Side Units in Intelligent Transportation System. *CMC -Tech Science Press*. **64**, 359-371.

Wong, C.K., Gouda, M. and Lam, S.S. (2000) Secure group communications using key graphs. *IEEE/ACM transactions on networking*. **8**, 16-30.

Zhang, J., Cui, J., Zhong, H., Chen, Z. and Liu, L. (2019) PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks. *IEEE Transactions on Dependable and Secure Computing*. **14**, 1545-1559.

Zhang, L. and Zhang, F. (2009) A new certificateless aggregate signature scheme. *Computer Communications*. **32**, 1079-1085.

Zheng, Y., Chen, G., and Guo, L. (2020) An Anonymous Authentication Scheme in VANETs of Smart City Based on Certificateless Group Signature. COMPLEXITY. **2020**, 1-8.

Received: March 31, 2021
Sent to Subject Editor: April 14, 2021
Accepted: January 29, 2023
Recommended by Subject Editor Jose Guivant