Message Authentication Scheme for VANET Based on Proxy Re-Signature

Xiaodong Yang¹, Faying An¹, Ping Yang¹, Xiaobo Wu², Yutong Li¹ and Likun Xiao¹

1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou, Gansu 730070, China
2. School of Software, Yantai Vocational College, Yantai, Shandong 264670, China
Email: y200888@163.com

Abstract. To solve the problems of privacy protection and low efficiency of signature verification in vehicle ad-hoc networks, a new message authentication scheme based on proxy re-signature technology is proposed. The new scheme can transform the signature on the message from the roadside into the signature on the same message signed by the trusted authority by using the proxy re-signature, and achieves the anonymity of vehicle identity and traceability of the communication message. The server is introduced into the signature verification of the message, which reduces the computational cost of the verifier, and effectively improves the signature verification performance. The analysis results show that the proposed scheme not only has higher security, but also has lower computational overhead.

1. Introduction
Vehicle ad-hoc networks (VANETs) are self-organizing networks for communication between vehicles and roadside infrastructure [1, 2]. The vehicle ad-hoc networks can effectively manage the vehicle’s driving information and traffic conditions. In addition, it can provide intelligent traffic services. As an important support for intelligent transportation systems, the vehicle ad-hoc networks is increasingly attracting attention from countries around the world. However, the vehicle ad-hoc networks faces many information security issues, among which the message authentication and identity privacy protection issues are particularly prominent [3, 4].

Raya et al. [5] proposed a vehicle ad-hoc networks privacy protection scheme, but the key storage overhead was too large. To overcome the shortcomings of Raya et al.’s scheme, Lin et al. [6] designed a new message authentication scheme based on a group signature algorithm, but the cost of vehicle revocation was relatively large. Chim et al. [7] proposed another scheme which effectively improved the authentication efficiency and reduced the communication overhead, but their scheme did not consider the problems of privacy protection. Although Shim [8], Rajput et al. [9] proposed privacy-preserving authentication scheme in vehicle ad-hoc networks, respectively. However, their schemes have deficiencies in the efficiency of signature verification.

To address the problems such as privacy protection and computation overhead in existing schemes, we propose a new message authentication scheme for VANETs based on proxy re-signature in this paper. The proposed scheme achieves the privacy protection of the vehicle’s identity, reduces the storage cost of the vehicle unit, and improves the service capacity of the roadside unit. Meanwhile, the server is introduced into the signature verification process of the message, which effectively reduces
the signature verification overhead of the verifier. Hence, our scheme is very suitable for vehicle units with limited computing resources.

2. Preliminaries

2.1. Bilinear Pairing
Let \( G_1 \) and \( G_2 \) be two multiplicative cyclic groups of prime order \( p \), and let \( g \) be a generator of \( G_1 \). A map \( e: G_1 \times G_1 \rightarrow G_2 \) is said to be a bilinear pairing if \( e \) satisfies the following property:

a) Bilinear: \( e(g^a, g^b) = e(g, g)^{ab} \) for \( a, b \in \mathbb{Z}_p^* \).

b) Non-degeneracy: \( e(g, g) \neq 1 \).

c) Computability: There exists an efficient algorithm to compute \( e(g^a, g^b) \) for \( a, b \in \mathbb{Z}_p^* \).

2.2. Complexity Assumption
Given a tuple \((g, g^a, g^b) \in G_1^3\) for unknown \( a, b \in \mathbb{Z}_p^* \), the Diffie-Hellman problem is to compute \( g^{ab} \).

The CDH assumption holds if the probability that any polynomial-time algorithm solves the discrete logarithm problem in \( G_1 \) is negligible.

2.3. Proxy Re-signature
A bidirectional proxy re-signature scheme consists of the following five algorithms:

- **Key**: On input \( \text{param} \), this algorithm outputs a public and private key pair \((pk, sk)\).
- **ReKey**: On input two private keys \((sk_A, sk_B)\), this algorithm outputs a re-signing key \(rk_{A\rightarrow B}\) for the proxy.
- **Sign**: On input a private key \( sk \) and a message \( m \), this algorithm outputs a signature \( \sigma \) on \( m \).
- On input a re-signing key \( rk_{A\rightarrow B} \) and a signature \( \sigma_A \) on a message \( m \) under the public key \( pk_A \), this algorithm outputs a signature \( \sigma_B \) on \( m \) under the public key \( pk_B \).
- **Verify**: On input a public key \( pk \), a message \( m \) and a signature \( \sigma \), this algorithm outputs 1 if \( \sigma \) is valid and 0 otherwise.

3. Our Message Authentication Scheme for VANETs

3.1. System Initialization
Assume that \( G_1 \) and \( G_2 \) are two groups of prime order \( p \), \( g \) is a generator of \( G_1 \), and \( e: G_1 \times G_1 \rightarrow G_2 \) is a bilinear paring. The trusted authority (TA) selects \( n_0 + 2 \) random numbers \((g_2, u', u_1, \ldots, u_{n_0})\) from \( G_1 \), and selects the random number \( \alpha \in \mathbb{Z}_p^* \) as its private key \( sk_{TA} \). After that, the trusted authority calculates the corresponding public key \( pk_{TA} = g^\alpha \), and publishes the system parameter \( \text{param} = (G_1, G_2, e, g_2, u', u_1, \ldots, u_{n_0}) \). Note that TA’s public key/private key pair is \((pk_{TA}, sk_{TA}) = (g^\alpha, \alpha)\).

3.2. Vehicle’s Key Generation
The on-board unit (OBU) randomly selects \( k \in \mathbb{Z}_p^* \) as its private key \( sk_A \) and computes corresponding public key \( pk_A = g^k \). Note that OBU mainly includes on-board equipment such as vehicles.

3.3. Vehicle Registration
Each vehicle submits information such as unique identity \( ID \) and public key \( pk \) to the trusted authority. After the authenticity of vehicle identity information is verified, the trusted authority stores vehicle information \((ID, pk)\) in the user registry list.
3.4. Re-Signing Key Generation
To convert the communication message signature of vehicle OBU to a signature of TA on the same message, the roadside unit (RSU) computes re-signing key $r_{k_{A \rightarrow T_A}}$ between OBU and TA as follows:

a) RSU randomly selects $\lambda \in Z_p^*$ and sends $\lambda$ to OBU.

b) OBU calculates $\lambda_i = k\lambda \pmod{p}$ from private key $sk_i = k$ and sends $(ID, \lambda_i)$ to TA.

c) If TA does not find a corresponding tuple $(ID, \lambda_i)$ for $ID$ in the user registry list, indicating that OBU is an unregistered vehicle, then TA sends an unregistered message to OBU. Otherwise, TA calculates $\lambda_2 = \alpha / \lambda_1 \pmod{p}$ from $sk_{T_A} = \alpha$ and then sends $\lambda_2$ to RSU.

d) RSU computes a re-signature key $r_{k_{A \rightarrow T_A}} = \lambda_2 \alpha = (\alpha \lambda_1) \lambda = (\alpha / (k \lambda)) \lambda = \alpha \lambda (\pmod{p})$.

3.5. Signature Generation
To sign a message $m = (m_1, ..., m_n) \in \{0,1\}^n$, OBU randomly chooses $r \in Z_p^*$ and uses its private key $k$ to compute a signature $\sigma_A = (\sigma_{A1}, \sigma_{A2})$ on $m$, where $\sigma_{A1} = g_r^i \cdot w'$, $\sigma_{A2} = g^r$ and $w = u' \cdot \prod_{i=1}^n u_i^m$. Then, OBU sends message $m$, public key $pk_A$, and corresponding signature $\sigma_A = (\sigma_{A1}, \sigma_{A2})$ to the nearby RSU.

3.6. Signature Conversion
After receiving the tuple $(m, pk_A, \sigma_A = (\sigma_{A1}, \sigma_{A2}))$, the RSU first checks whether $e(\sigma_{A1}, g) = pk_A \cdot e(w, \sigma_{A2})$. If it does not hold, RSU refuses to forward the message $m$ to the recipient. Otherwise, RSU uses its re-signing key $r_{k_{A \rightarrow T_A}} = \alpha / k \pmod{p}$ to compute $\sigma_B = (\sigma_{B1}, \sigma_{B2}) = \sigma_A^{r_{k_{A \rightarrow T_A}}} = (g_{r}^i \cdot w'^{u/rk}, g^{u/k}) = (g_{r}^i w', g')$, where $r' = ra / k$. Then, RSU sends $(m, pk_{T_A}, \sigma_B)$ to other recipients, and stores $(m, pk_A)$ in the message forwarding list.

3.7. Message Verification
The receiver checks the authenticity and integrity of the message by verifying the validity of the signature on the message. The receiver randomly selects $x \in Z_p^*$ as a secret string and computes $pk = (g_r, pk_A)^x$. For the received a message/signature pair $(m, \sigma_B = (\sigma_{B1}, \sigma_{B2}))$ from RSU, the receiver and the server perform the following operations:

a) The receiver calculates $\sigma^* = (\sigma_{B1}, \sigma_{B2}) = (\sigma_{B1})^{x'}$ and sends $(m, \sigma^*)$ to the server.

b) The server calculates $\eta_i = e(\sigma_{B1}, g)$ and $\eta_i = e(w, \sigma_{B2})$, then sends $(\eta_i, \eta_z)$ to the receiver.

c) After receiving the $(\eta_i, \eta_z)$, the receiver calculates $\eta = pk \cdot \eta_i$ and checks whether the equation $\eta_i = \eta \cdot \eta_z$ holds. If this equation holds, the receiver is sure that $\sigma_B$ is a valid signature on $m$ and accepts the message $m$; otherwise, the receiver rejects $m$.

3.8. Vehicle Revocation
When a malicious vehicle unit sends a fake message $m$, RSU searches the message forwarding list to find the corresponding record $(m, pk_A)$ and then sends $(m, pk_A)$ and the signature $\sigma_A$ to the TA. After verifying the validity of the signature $\sigma_B$, TA confirms that the fake message $m$ is indeed sent by $pk_A$, and then searches the user registry list to find the entry $(ID_A, pk_A)$. At last, the real identity $ID_A$ of the vehicle is added to the user revocation list, and the information that the vehicle $ID_A$ is revoked is broadcast to all RSUs.

4. Security Analysis
4.1. Unforgeability
The security of our scheme is based on Yang et al.’s proxy re-signature scheme [10]. In addition, Yang et al. [10] have shown that their scheme is unforgeable in the standard model, and its security can be
reduced to the CDH assumption. Therefore, our scheme satisfies unforgeability, and an attacker cannot forge a valid signature of any message sent by the vehicle.

4.2. Revocability
In our scheme, the revocation of the vehicle is achieved mainly through the user revocation list maintained by the TA. When the malicious vehicle unit sends a false message, there are two ways of revocation. One is that TA determines the real identity of the malicious vehicle unit by looking up the user registry list. The other is that TA determines the real identity through the message forwarding list stored by the roadside unit. After the TA accurately locates the identity of the malicious vehicle unit and executes the corresponding punitive measures.

4.3. Identity Privacy
In order to protect the identity privacy of the vehicle, RSU forwards the message sent by the OBU during each communication, and the signature of OBU is converted into the signature of TA. As a result, the verifier of the message only needs to know the TA's public key to verify the legitimacy of the signature without knowing the OBU's public key or other related identity information. Other participating entities can’t infer the real identity of the vehicle unit from the communication message except TA. During every communication process, the identity of the sender is verified, and each illegal user can’t communicate with the legitimate user who has been verified. After passing the authentication, the vehicle unit can communicate with other roadside units and vehicle units. Therefore, the scheme proposed in this paper makes the communication between OBUs anonymously, and effectively protects the identity privacy of the transmission vehicle.

5. Performance Analysis
In our scheme, the verifier delegates most of the computational tasks of signature verification to a server, and performs a few calculations to verify the validity of the signature. In the signature generation phase, OBU requires 3 exponentiations to generate a signature. In the signature conversion phase, RUS needs 2 exponentiations to transform a signature. In the message verification phase, the receiver requires 1 bilinear pairing and 2 exponentiations to complete the validity of the signature. As for the communication costs, OBU sends only two elements in \( G_1 \) to complete a communication. To further demonstrate the efficiency of our scheme, we compare the verifier’s computation cost of our scheme with the other two schemes, and the results are shown in Table 1. The computational overhead of bilinear pairing and exponentiation is much greater than other cryptographic operations, so we mainly consider bilinear pairing and exponentiation operations.

| Scheme           | Exponentiation | Bilinear pairing |
|------------------|----------------|------------------|
| Rajput’s scheme  | 3              | 3                |
| Shim’s scheme    | 4              | 3                |
| Our scheme       | 2              | 1                |

From Table 1, we can see that our scheme greatly reduces the computational cost of the verifier and efficiently improves the response time of message verification. Therefore, our scheme outperforms other schemes in the efficiency of signature verification.

6. Conclusions
In this paper, a message authentication scheme for vehicle ad-hoc networks based on proxy re-signature is proposed. Our scheme uses proxy re-signature technology to achieve the authentication of communication messages, and ensure the privacy and revocability of vehicle identity in the communication process. However, the security of the proposed scheme depends on the assumption of CDH problem and can’t resist the attack of quantum computation. Therefore, it is a challenging but
meaningful work to design a message authentication scheme in vehicular ad hoc networks against quantum computation attacks.

7. Acknowledgments
This work was partially supported by the National Natural Science Foundation of China (61662069), China Postdoctoral Science Foundation (2017M610817), Science and Technology Project of Lanzhou City of China (2013-4-22), Foundation for Excellent Young Teachers by Northwest Normal University (NWNU-LKQN-14-7), Project of Shandong Province Higher Educational Science and Technology Program (No. J16LN61).

8. References
[1] Qiu T, Chen N, Li K, et al. Heterogeneous Ad hoc networks: architectures, advances and challenges. Ad Hoc Networks, 2017, 55: 143-152.
[2] Zhang F, Liu H, Leung Y W, et al. CBS: community-based bus system as routing backbone for vehicular ad hoc networks. IEEE Transactions on Mobile Computing, 2017, 16 (8): 2132-2146.
[3] Li P, Zhang T, Huang C, et al. Rsu-assisted geocast in vehicular ad hoc networks. IEEE Wireless Communications, 2017, 24(1): 53-59.
[4] Gao T H, LI Y Q. Survey on anonymous authentication mechanisms of VANET. Chinese Journal of Network and Information Security, 2017, 2 (8): 10-16.
[5] Raya M, Hubaux J P. The security of vehicular ad hoc networks. Proc. Int. Conf. on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 2005: 11-21.
[6] Lin X, Sun X, Ho P H, et al. GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Transactions on vehicular technology, 2007, 56(6): 3442-3456.
[7] Chim T W, Yiu S M, Hui L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks, 2011, 9(2): 189-203.
[8] Rajput U, Abbas F, Eun H, et al. A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access, 2017, 5: 12014-12030.
[9] Shim K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.
[10] Yang X, Li Y, Gao G, et al. Sever-aided verification proxy re-signature scheme in the standard model. Journal of Electronics & Information Technology, 2016, 38(5): 1151-57.