Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(10):105-109**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Internet of vehicles data encryption transmission and security authentication scheme

Zouyu Xie, Guowei Lin, Yufang Liang, Shujian Yu, Liugfen Li*

Artificial Intelligence Key Laboratory of Sichuan Province, School of Mathematics and Statistics, Sichuan University of Science & Engineering, P. R. China
liliufen@suse.edu.cn

Abstract In order to improve the safety level of automobile information transmission and enhance the safety certification ability of smart cars in complex network systems, the research and results of vehicle network security and blockchain identity authentication are analyzed and summarized. In the Internet of Vehicles environment, the encryption algorithm and the blockchain authentication mechanism are combined, and the data encryption transmission and authentication scheme based on Diffie-Hellman algorithm, ElGamal algorithm and blockchain technology is proposed and designed. It is of great significance.

Keywords blockchain, data encryption, Diffie-Hellman, authentication mechanism, ElGamal

1. Introduction

With the popularity of smart cars, the security issues of information transmission such as information tampering and network monitoring are more prominent. In 2015, Ponemon [1-2], a US research institute, said that 60% to 70% of vehicles in the future will be recalled due to information transmission security vulnerabilities, and the chances of cars being attacked by information security will gradually increase. When the vehicle terminal and the server perform two-way data transmission, there are two major security risks. One is authentication, there is no verification of the sender's identity information; the second is that data encryption security is not enough. In terms of identity authentication mechanism: In 2016, Abboud [3] and others proposed a radio frequency identification-based vehicle identity authentication scheme. During the driving process, the vehicle transmits data through the electronic tag and the server, and the vehicle data and the server are mutually Authentication. Under V2X communication, a scheme of interworking between DSRC and cellular network technology is proposed to achieve efficient V2X communication. In 2017, Ying et al. [4] proposed an anonymous and lightweight authentication based on ASC protocol to solve the authentication problem in VANET. It is capable of reducing communication and computational overhead by 50% compared to existing methods. In 2018, Ni et al. [5] proposed a scheme for secure authentication using public key infrastructure, which can meet the data transmission requests of different vehicle users in different driving scenarios. In 2014, Liu et al. [6] proposed an agent-based distributed computing authentication scheme, which enables agent vehicles to use the authentication function to simultaneously authenticate multiple messages. However, it can't resist fake and modified attacks and incorrectly accept batch invalid signatures. Therefore, in 2018 Rajabzadeh et al. [7] proposed an identity-based new message authentication using proxy tool (ID-MAP). Under the random language model, It proves that the scheme can meet the certification requirements of batch messages. The literature [8-9] is a safety certification scheme based on the theory of group signature.

In terms of encryption algorithm: In 2014, Ding Min [10] improved the large prime number generation and large power model operation in Elgamal algorithm, and proposed an improved dynamic password authentication mechanism. In 2015, Su Yunna [11] designed the Elgamal algorithm based on the semi-group nature based on the generalized Fibonacci sequence. The algorithm was validated by numerical examples. In 2016, Jiang Lili [12] analyzed the security threats faced by the Elgamal algorithm, constructed an Elgamal algorithm based on the generalized conic curve on the ring Zn, and proved the correctness of the improved public key cryptography. In 2017, Toan et al. [13] proposed a new encryption scheme based on the difficulty of Elgamal encryption algorithm and discrete logarithm problem to reduce the risk of key leakage. In 2018, Rachmawati et al. [14] proposed an encryption scheme combining the triple DES algorithm with the Elgamal algorithm. But its efficiency decreases as the size of the encrypted message increases.

2. Prerequisite Knowledge

2.1. Diffie-Hellman algorithm

The Diffie-Hellman algorithm is a key exchange algorithm that relies on the difficulty of computing discrete logarithms so that both users can securely exchange a key to encrypt subsequent messages.

Algorithm Description:

Suppose users A and B want to exchange a pair of keys, A is the initiator and B is the receiver.

I. Algorithm disclosure parameters: a larger prime number p and one of its original roots a;

II. A select a large random integer X_A $(1 \le X_A \le p-1)$, calculate

$$Y_A = a^{X_A} \bmod p$$

X_A save itself, Y_A sends to B;

III. B select a larger random integer X_B $(1 \le X_B \le p-1)$,calculate

$$Y_B = a^{X_B} \bmod p$$

X_B save itself, Y_B is sent to A;

IV. User A, B gets a common key. According to the modulo operation rule, the obtained public key is:

$$k = Y_B^{X_A} \bmod p = Y_A^{X_B} \bmod p .$$

2.2. ElGamal algorithm

The ElGamal algorithm is an asymmetric encryption algorithm based on Diffie-Hellman key exchange proposed by Taher in 1984. It is a successful application of the one-way trapdoor function, which converts the function into a public key encryption system.

Select prime number p and two random numbers g, Prk $(g < p; Prk < p)$.

Generates a key:

$$Puk = g^{Prk} \bmod p$$

The company is Puk. The private key is Prk.

Suppose the message that needs to be encrypted is M $(M < p)$, Then randomly select a number k $(k < p \; and \; (k, p-1) = 1)$.

Encryption:

$$a = g^k \bmod p$$

$$b = Puk^k \; M \bmod p$$

Get ciphertext (a, b)

Decrypt:

$$M = b \; / \; a^{Puk} \; (\bmod p)$$

2.3. Digital signature and verification mechanisms in blockchains:

Blockchain Bitcoin uses digital signatures to ensure that data is not modifiable throughout the system and that the identity of both parties is authentic.

Digital signature process description:

Suppose A is the sender and B is the receiver; A sends a transaction message Q to B.

I. Before A sends information Q to Party B, a pair of public and private keys are generated in Party A's system.

II. When A sends information Q, A first hashes Q to generate a ciphertext A, and then uses A's key to encrypt A to generate digital fingerprint P. Finally, A sends information Q, digital fingerprint P and public key. Send it to B together.

III. B performs hash operation on the received information Q to generate another ciphertext A', and decrypts the digital fingerprint P into ciphertext A by using the public key generated by A; compares A and A', if they are equal, Prove that the transaction information Q has not been tampered with, and the identity of Party A is confirmed.

3. System Design

3.1. Preset Information

Before the smart car leaves the factory, a large prime number p greater than 1024 bits and two random numbers $g, x(g < p, x < p)$ are preset.

3.2 Sender verification module (Fig. 1)

I. The smart car end performs a HASH operation on the message C to obtain a digital summary $NA1$ of C;

II. Using the ELGamal encryption algorithm to generate a key pair (public key Puk, private key Prk);

III. The car end regenerates a random number C, where

$$K = \{t \mid 1 < t < p-1 \, and \, t \in Z\}$$

and calculates

$$C1 = g^K \bmod p$$

$$C2 = g^{K \times NA1} \bmod p$$

where $(C1,\ C2)$ is the ciphertext of the digital digest $NA1$;

IV. Packet C, public key Puk and ciphertext $(C1,\ C2)$ are packaged and sent to the receiver (cloud server).

3.3 Cloud Verification Module (Fig. 2)

I. The cloud successfully receives the message C, the public key Puk and the ciphertext $(C1,\ C2)$;

II. Using the public key Puk to decrypt the ciphertext $(C1,\ C2)$ to obtain a digital digest $NA1$;

III. Perform HASH operation on message C again to obtain digital summary $NA2$;

IV. If $NA1 \equiv NA2$, the verification passes and proceeds to the next stage; otherwise, the verification fails, and the information is sent back to the sender (such as issuing a warning, etc.).

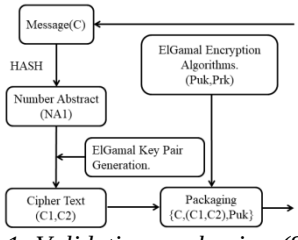

Figure 1: Validation mechanism (Sender)

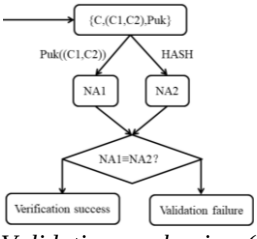

Figure 2: Validation mechanism (Recipient)

3.4. Key Exchange Module (Fig. 3)

I. After the cloud verification is passed, the car end generates a random number α and calculates

$$X = g^{\alpha} \bmod p;$$

II. Packing $\{X, g, p\}$ and sending it to the cloud server through the sender verification module;

III. Verify the $\{X, g, p\}$ through the cloud verification module, if passed:

Step 1: The cloud server generates a random prime number β;

Step 2: Calculate

$$Y = g^{\beta} \bmod p;$$

Step 3: Send Y to the smart car through the sender verification phase.

IV. If the verification of $\{X, g, p\}$ fails, feedback warning information is sent to the smart car end;

V. The smart car end uses the received Y to calculate the key

$$K = Y^{\alpha} \bmod p;$$

3.5. Information Transmission Phase (Fig. 4)

I. The smart car uses the key K to encrypt the plaintext information M to be sent to obtain the ciphertext C.

II. Send $\{C, Puk, (C1, C2)\}$ to the server through the sender verification module;

III. Verify the received $\{C, Puk, (C1, C2)\}$ through the cloud verification module;

IV. If the verification is passed, the ciphertext C in $\{C, Puk, (C1, C2)\}$ is decrypted with the key K to obtain the plaintext information M, and the information M is processed accordingly; if the verification fails, then The user issues a warning.

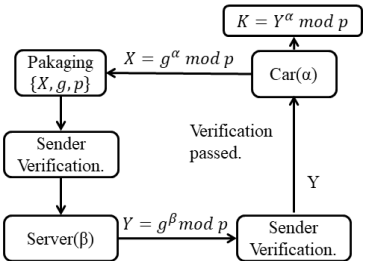

Figure 3: Key exchange

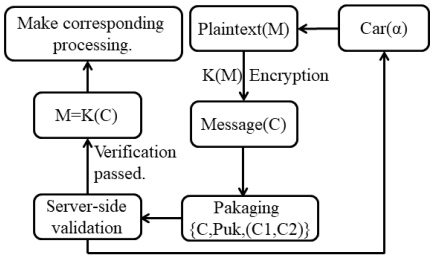

Figure 4: Send a message

4. Summary

The program is designed to securely transmit messages over the vehicle and the cloud without being monitored and attacked. The scheme combines the ELGamal encryption verification mechanism and the Diffie-Hellman key exchange protocol to perform key exchange under the condition that the identity of both parties is determined, which overcomes the high-risk vulnerability of the man-in-the-middle attack in the Diffie-Hellman protocol, and makes the keys of both parties Exchange is more secure and confidential. At the same time, the information encrypted by the key must be decrypted by the key used for encryption and the inverse algorithm of the same algorithm. Combined with multiple authentication, the information transmission is more secure.

Acknowledgements

This work was supported by the Talent Project of Sichuan University of Science & Engineering (2017RCL23); the Science Founding of Artificial Intelligence Key Laboratory of Sichuan Province (2017RZJ03); the Opening Project of Sichuan Province University Key Laboratory of Bridge Non-destruction Detecting and Engineering Computing (2017QYJ03); the college students' innovation and entrepreneurship training project (cx201912).

References

[1]. H. Stubing and A. Jaege~ "Secure beamforming for weather hazard warning application in Car-to-X communication", Lecture Notes in Electrical Engineering, 78: l 87-206, 2010.
[2]. S. Hameed, O. Khalifa and M. Ershad, "Car Monitoring, aerting and tracking model, enhancement with mobility and database facilities", in Proc. International Conference on Computer and Communication Engineering (ICCCE'I, 2010.
[3]. Abboud K., Omar H., Zhuang W. Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey [J]. IEEE Transactions on Vehicular Technology, 2016: 1-1.
[4]. Ying B., Nayak A. Anonymous and Lightweight Authentication for Secure Vehicular Networks [J]. IEEE Transactions on Vehicular Technology, 2017: 1-1.
[5]. Ni J., Lin X., Shen X. Efficient and Secure Service-oriented Authentication Supporting Network Slicing for 5G-enabled IoT [J]. IEEE Journal on Selected Areas in Communications, 2018:1-1.
[6]. Liu Y., Wang L., Chen H. H. Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks [J]. IEEE Transactions on Vehicular Technology, 2014: 1-1.
[7]. Rajabzadeh Asaar M, Salmasizadeh M, Susilo W, et al. A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks [J]. IEEE Transactions on Vehicular Technology, 2018:1-1.
[8]. Cao J., Ma M., Li H. G2RHA: Group-to-Route Handover Authentication Scheme for Mobile Relays in LTE-A High-Speed Rail Networks [J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 9689-9701.
[9]. Zhang A., Chen J., Hu R. Q., et al. SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks. [J]. IEEE Transactions on Vehicular Technology, 2016, 65(4): 2659-2672.
[10]. Ding Min. Research and Design of a Dynamic Identity Authentication Mechanism Based on Digital Signature [D]. Hebei University of Technology, 2014.
[11]. Su Yunna, Liao Xingwei. Design of Cryptographic System Based on Generalized Fibonacci Sequences [J]. Journal of Southwest China Normal University (Natural Science), 2015, 40(11): 61-66.
[12]. Jiang Lili. Research on generalized conic curve public key cryptography on ring Z_n [D]. Harbin Engineering University, 2016.
[13]. Toan Nguyen Duc, Hong Bui The. Building Background to the Elgamal Algorithm [J]. IJMSC-International Journal of Mathematical Sciences and Computing (IJMSC), 2017, 3(3).
[14]. D Rachmawati, A S Harahap, R N Purba. A hybrid cryptosystem approach for data security by using triple DES algorithm and ElGamal algorithm [J]. IOP Conference Series: Materials Science and Engineering, 2018, 453(1).