Information Transmission Scheme between Train and RBC Based on AES-ECC Algorithm

Zhang Junjie¹,a, Zheng Yunshui²,b

¹College of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou, China
²College of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou, China
aemail:0219400@stu.lzjtu.edu.cn,bemail:0619427@stu.lzjtu.edu.cn

Abstract: The existing information encryption scheme between the Radio Block Center (RBC) and the ground has problems such as weak keys, and the vehicle-ground information has a potential threat of being stolen. In order to ensure the safety of driving, on the basis of ensuring the correct transmission of train and ground information, research on more efficient encryption schemes has become the focus of work. In response to this trend, a hybrid encryption scheme based on AES and ECC encryption algorithms is proposed. The AES algorithm replaces the original 3DES algorithm, and the elliptic curve encryption algorithm ECC is used to encrypt the session key to improve the encryption security level. The encryption simulation, avalanche effect verification and execution efficiency test of fixed-length data are completed on Visual Studio 2013 platform, and compared with the original encryption scheme. The results show that the scheme can meet the avalanche effect and the accuracy of data transmission, and it takes less time than the original encryption scheme, and is more suitable for two-way large-capacity information transmission between vehicles and ground.

1. Introduction

In recent years, with the improvement of real-time requirements for information interaction between trains and the ground, the Chinese Train Control System (CTCS)-3 level has been widely used in my country's existing passenger dedicated lines. As the core ground equipment of CTCS-3, RBC is a signal control system based on a fail-safe computer platform. It is a collection and interaction center for ground signal system information and instructions. It can generate control information such as train permits and pass the global railway-oriented The mobile communication GSM-R (Global System for Mobile communications-Railway) is sent to the on-board equipment to ensure that the train runs safely, reliably and efficiently within its control range. As an important channel to realize this mechanism, the safety and reliability of the wireless transmission of vehicle-ground information is particularly important.

At present, the session key in Railway Signal Safety Protocol-II (RSSP-II) is a mode of Data Encryption Standard (DES), namely Triple DES(3DES) . However, 3DES has weak protection against specific selected plaintext attacks and known plaintext attacks, and 3DES may have security risks due to its algorithm structure. Therefore, it is imperative to study the new encryption scheme for the secure transmission of information between vehicles and ground. M. Aguado proposed to use 128-bit key AES for message verification and integrity check for the European Train Control System (ERTMS), as well as the use of public key facilities for key distribution. Xia Haonan et al. studied the secure transmission of RBC messages in the train control system, and proposed to use the AES algorithm to
encrypt the data transmission process, and use the colored Petri net simulation tool to apply for the movement authority (MA) and RBC of the train. The information interaction process of sending and encrypting MA was simulated, and the end-to-end encryption of vehicle equipment and RBC was realized, providing a theoretical basis for software design. J. Raigoza[4] evaluates the performance of the AES algorithm, measures the execution time of different types of data string values, and provides experimental ideas for the performance evaluation of encryption algorithms.

According to the encryption characteristics of symmetric and asymmetric encryption algorithms, this paper selects AES [5] which has faster encryption speed in symmetric encryption algorithm and ECC which has higher security level in asymmetric encryption algorithm. AES is used to encrypt a large number of vehicle ground information plaintext data, and ECC is used to encrypt AES session key.

2. Vehicle and ground information encryption

The hybrid encryption scheme is divided into two parts: plaintext encryption and key encryption. The block diagram of the overall encryption scheme is shown in Figure 1:

![Figure 1 Overall encryption scheme](image)

2.1 plaintext encryption

Encrypting the plaintext can ensure that an attacker cannot obtain effective information through eavesdropping during data transmission. Plain text messages refer to control information such as driving permits generated by RBC. The plaintext message encryption uses the AES algorithm with a packet length of 128bit, and the key also uses a 128bit key. The encryption process of the sender is designed as follows:

Process: Input parameters include plaintext $M$ and session key $K_S$, are expressed as $E(M, K_S)$.

1) Set the direction flag of message $M$. If the party is the message sender, the flag bit is set to '0', and the message receiver is set to '1'.

2) Attach the destination address (DA) before the message $M$: $DA|M$, calculate the length $L$ (16 bits) of $DA|M$ and append it to the front, namely $L|DA|M$, in order to calculate the ciphertext $C$.

3) It is judged whether the length of $L|DA|M$ is an integer multiple of 128, and if it is not satisfied, it is filled. The additional padding data is $P$, the length of the padded message $L|DA|M|P$ becomes a multiple of 128bit, and then AES encryption is performed on the filled sequence to generate a ciphertext $C$.

4) The elliptic curve encryption algorithm is used to encrypt the session key $K_S$, generate $K_e$, and add it to the end of the ciphertext $C$.

2.2 Key Encryption

ECC is an asymmetric cryptographic algorithm based on elliptic curve. By comparison with other algorithms, ECC can provide higher security with smaller key sizes. ECC with a 256 bit key size can achieve the same level of security as the RSA algorithm using the larger key size (3072 bits). The encryption of the session key $K_S$ with a fixed length is as shown in Figure 2, the specific encryption process:
Fig.2 Encryption process of session key block

Step1: Select the elliptic curve \( y^2 \equiv x^3 + ax + b \), denote as \( E(a,b) \), \( a,b \in \mathbb{Z}_p \).

Step2: Select random number \( r \), and base point \( G \) as the public parameters.

Step3: Block coding with 128bit key \( K_S \), and then map \( K_S \) to the elliptic curve to get the plaintext point \( P(x,y) \).

Step4: Block coding with 128bit key \( K_S \), and then map \( K_S \) to the elliptic curve to get the plaintext point \( P(x,y) \).

Use the public key \( Q \) of the receiver and the random number \( r \) of the sender to calculate \( C_i = M + r \) and \( C_i + l = rG \) to obtain the encryption key \( K_e \). At the receiving end, decryption of the encryption key \( K_e \) is the key point, and the processing process is as follows:

- At the receiving end, decryption of the encryption key \( K_e \) is the key point, and the processing process is as follows:

  - Use the receiver's private key to decrypt the ciphertext, separate the AES key part of the received data, get \( C_1, C_2, \ldots, C_{32} \), calculate \( C_2 - dC_1 \), where \( d \) is the private key that the receiver does not disclose to the outside world, after the plaintext points are obtained, the \( m \) points are separated first, and then decoded, and finally the session key \( K_S \) is decrypted for decryption of the ciphertext.

3. Results analysis and discussion

3.1. Correctness verification

In order to verify the correctness of the proposed algorithm, the following information packets are selected for processing: the most important vehicle-to-ground communication with the most frequently used vehicle permission message, the emergency stop message with the shortest message length, and the MA message after splicing message packets 21, 27, 72 with the longest message length.

The simulation test is carried out on PC. The key used by both communication parties is set to 128bit. The input string includes the plaintext to be encrypted and the session key \( K_S \). Firstly, the plaintext data of the sender is processed by 128bit grouping, and the plaintext is encrypted with the session key shared by both parties to obtain ciphertext \( C \). After encrypting \( K_S \), you get \( K_e \). When decrypting, decrypt \( K_e \) first and get \( K_S \), then the ciphertext \( C \) is decrypted to get the decrypted character sequence, which is compared with the input character sequence to verify its correctness.

Perform the same processing on the three different types of messages, observe the input and output parts, and compare them with the plaintext data sent by the sender, which shows that the algorithm has good accuracy for the three representative types of messages. It can meet the basic encryption and decryption requirements.
3.2. Validation of avalanche effect

According to the design requirements of the encryption algorithm, meeting the avalanche effect can prevent an attacker from speculating on the input from the output result and causing the algorithm to crack. In order to test whether the encryption scheme satisfies the strict avalanche effect, that is, if one bit of the input sequence is changed arbitrarily, whether more than half of the output bits are changed in the statistical output. This article uses two experiments to verify.

Set the plaintext packet size to 128bit, and fix the plaintext unchanged. First, encrypt with a 128bit initial key $K_s$ to obtain the initial ciphertext $C$, then encrypt the key $d$ to obtain $Ke$, and obtain the splicing sequence $S$. Invert each bit in the initial key $K_s$ in turn to obtain 128 keys, respectively perform 128 times of encryption to obtain 128 sequences of $S_i(C||Ke)$, $(1<i<128)$, then XOR the $S_i$ with the initial ciphertext $S$, and count the number of 1 in each comparison result. After the same operation, the ciphertext sequence $S_i'(C||Ke')$, $(i=1,2,3,...,8)$ is obtained, and the occurrence times of 1 after the bit by bit XOR between the ciphertext sequence $S_i'$ and the initial ciphertext sequence $S$ are counted. For the change of the same key, the XOR operation is repeated three times, and the average value is taken as the final result.

![Avalanche effect verification diagram](image)

Table 1 Statistics of the number of change bits of output result

| Number of bits | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   |
|----------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Number of runs | 1   |     |     |     |     |     |     |     |
|                | 854 | 713 | 817 | 810 | 700 | 852 | 849 | 736 |
|                | 2   |     |     |     |     |     |     |     |
|                | 743 | 865 | 795 | 825 | 790 | 845 | 756 | 712 |
|                | 3   |     |     |     |     |     |     |     |
|                | 895 | 787 | 813 | 759 | 820 | 786 | 791 | 801 |
| The average    | 830.7 | 788.3 | 808.3 | 798.0 | 770.0 | 827.7 | 798.7 | 749.7 |

The output results in the two cases are shown in Figure 3 and table 1. Each point in Figure 3 represents the number of times 1 appears in the result when a bit of plaintext and key changes. After 128 encryption operations, the average values are 789.9, which are greater than half of the output bit value of ciphertext sequence. In Table 1, the average change of ciphertext bits is 796.4, so the scheme satisfies the key avalanche effect and plaintext avalanche effect.

3.3 Execution efficiency.

The encryption time of three encryption algorithms is measured:

For 3DES and AES encryption, the encryption time includes the plaintext encryption time $T_m$. The encryption time of hybrid encryption consists of two parts: plaintext encryption time $T_m$ and session
key encryption time $T_{KS}$. For the improved scheme, the fixed symmetric key $K_S$ and elliptic curve encryption key size are 128 bit and 8 bit respectively, the session key size of 3DES is 64 bit, and the session key length of AES encryption is 128 bit. Change the type of input vehicle ground information, perform 20 times of time measurement for the same type of data, take the average value, and get the encryption time-consuming parameters of three encryption algorithms under different data types, as shown in Table 2.

We can see that for different test data, the hybrid encryption algorithm shows good encryption efficiency and shorter encryption time compared with the original scheme.

| Test Data | Data size /bit | Encryption time /ms |
|-----------|----------------|---------------------|
|           | 3DES          | AES    | AES+ECC |
| Test data 1 | 435           | 1.8    | 1.3    | 1.4    |
| Test data 2 | 307           | 1.4    | 1.1    | 1.3    |
| Test Data 3 | 2739          | 12.4   | 11.1   | 12.3   |

### 4. Conclusion

In the hybrid encryption algorithm, encrypted ciphertext is used for data transmission and ECC is used for symmetric key transmission. After simulation test, the data received by the receiver is consistent with that of the sender, which verifies the accuracy and security of the hybrid encryption. Through the simulation on VS platform, the results show that the proposed hybrid encryption method is reasonable and has better real-time performance, and has high theoretical value and practical application prospect.

### Acknowledgments

This work was supported by the Project of Regional Science Foundation of National Natural Science Foundation of China (61763023).

### References

[1] YANG Jie. Three kinds of symmetric encryption algorithm application in the center of the wireless occlusion[J]. Automation & Instrumentataion, 2017(4):135–137.

[2] I. Lopez and M. Aguado, Cyber security analysis of the European train control system[C]//IEEE Communications Magazine, vol.53, no. 10, pp.110-116, October 2015.

[3] Xia Haonan, Dai Shenghua. Security encryption with radio block center Colored Petrinet.[J]. Journal of Computer Applications, 2018,38(12):3476-3480.

[4] J. Raigoza and K. Jituri, Evaluating Performance of Symmetric Encryption Algorithms[C].//2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp.1378-1379.

[5] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan. New Comparative Study Between DES, 3DES and AES within Nine Factors [C]//Journal of computer, volume2,issue3,march 2010.