Research on MAC Verification Code of Railway Signal Security Communication Protocol

Puwei Wu, Zhongdong Wu*, Liyun Li

School of Electronics and Information Engineering, Lanzhou Jiaotong University, No.88, Anning West Road, Lanzhou 730070, China

*2054802499@qq.com

Abstract. Aiming at the low security and low real-time performance of the message authentication security layer (MASL) message authentication code (MAC) algorithm in the railway signal security communication protocol RSSP-Ⅱ, the advanced encryption standard AES is used as the core algorithm of the MAC code and the ciphertext is used Packet link encryption and decryption of the message, simulation of the security protocol from the security-related key service process of the RSSP-Ⅱ communication protocol, verification of the confidentiality of the improved protocol, and optimization of the protocol key service process, that is, the key The center uses the advanced encryption standard AES algorithm to authenticate the vehicle equipment and the ground wireless block center, further strengthening the security of the protocol.

Keywords: RSSP-Ⅱ, AES, Message verification code (MAC), Verilog, QuartusⅡ, FPGA

1. Introduction

The railway communication environment has its particularity. The railway communication system generally adopts the existing transmission network[1], such as Ethernet, bus, etc. To ensure communication security, additional security communication protocols need to be loaded on these transmission networks to prevent high-speed railways. Data loss, insertion, tampering, and other threats faced by communications. The CTCS-3[2] train control system faces the speed limit server (TSRS), the dispatching centralized center (CTC), the radio block center (RBC), and the adjacent TSRS all adopt RSSP-Ⅱ[3]. The detailed structure of the RSSP-Ⅱ protocol is shown in Fig.1. In the message authentication security layer MASL (Message Authentication Safety Layer), user data is extended by the Message Authentication Code (MAC), that is, the security data must pass through the MAC of the MASL layer. Code protection to ensure the authenticity and integrity of the message before it is sent to the transport layer.
The message authentication code MAC of the MASL layer in RSSP-Ⅱ is mainly realized by performing triple DES encryption on data packets. Therefore, the DES algorithm is the core algorithm of the MASL layer MAC. However, with the improvement of computer processing speed and computing power, the DES algorithm has security risks. Guo[4] et al. studied the security of the core message authentication code MASL-MAC scheme of the RSSP-Ⅱ protocol, proposed a partial key recovery-forgery attack scheme, and proved that the algorithm has security flaws, in order to further improve the RSS-Ⅱ The overall security of the protocol is recommended to replace the existing 64-bit block cipher DES with the international or domestic standardized 128-bit block cipher AES. Zhang Yuanling [5] and others proposed a message authentication code algorithm based on AES and proved that the improved algorithm can overcome the security risks such as weak keys and semi-weak keys in the original algorithm through software implementation. The content of the RSSP-Ⅱ safety communication protocol is very large and complex. The analysis of its safety communication mechanism and the design of the simulation platform still need continuous exploration. Zhang Qihe [6] and others used FPGA design to realize the RSSP-Ⅱ protocol. The generation process of the MAC authentication code releases the CPU system resource occupation, improves the system operation efficiency, and has certain engineering significance. At the same time, foreign scholars have done further research and improvement on the AES algorithm. Harshali Zodpe et al. proposed an improved AES algorithm that uses a PN sequence generator to generate S-box values and initial keys. The avalanche effect verifies the improved AES algorithm. The algorithm has a significant improvement in encryption quality. This design is implemented on a field programmable logic gate array (FPGA) device and compared with the existing design, the throughput is significantly improved.

This article will start with the message authentication code scheme used in the RSSP-Ⅱ protocol, and conduct research on the security of the RSSP-Ⅱ protocol. In order to further improve the security performance of the protocol, this paper adopts the advanced encryption standard AES as the core algorithm of MAC, uses the ciphertext grouping link method to encrypt and decrypt the message, and performs the security protocol from the security-related key service process of the RSSP-Ⅱ communication protocol. Simulation, while optimizing the protocol key service process, that is, the key center uses the advanced encryption standard AES algorithm to authenticate the vehicle equipment and the ground wireless block center, which further strengthens the security of the protocol.

2. RSSP-Ⅱ security communication protocol message authentication security layer MASL

The functional modules of the RSSP-Ⅱ protocol can be divided into two categories, safety functional modules, and communication functional modules. RSSP -Ⅱ protocol detailed structure is shown in Fig.1. The main function of the message authentication security layer MASL is to attach the message authentication code MAC to the communication message, so as to realize the data source identification and integrity protection of the communication message and prevent possible forgery and tampering. The MAC scheme (MASL-MAC) adopted by the MASL layer is improved based on the CBC-MAC proposal 3 (ANSI Retail MAC) given by the ISO/IEC 9797-1 standard, and the underlying block cipher is the DES algorithm.
Retail MAC adds an additional round of DES decryption and another round of DES encryption operations, and uses different keys to complete the encryption and decryption operations respectively. The Retail MAC key is composed of two 56-bit DES keys, that is $K = (K_1, K_2)$, the input message $X$ is divided into 64-bit blocks $D_1, D_2, ..., D_n$. If the length of the last message $D_n$ after cutting is less than 64 bits, it will be filled with 0. Using the DES algorithm, the procedure $X$ for encrypting a 64-bit message block with a key is expressed as $DES(K_i, X)$, The decryption process is expressed as $DES^{-1}(K_i, X), \oplus$ represents the exclusive OR operation, and the final output MAC value is obtained by formula 1.

$$
\begin{align*}
H_0 &= 0; \\
H_i &= DES(K_i, h_{i-1} \oplus D_i) i = 1, 2, ..., q \\
MAC &= g(H_q)
\end{align*}
$$

The output transformation definition of Retail MAC is shown in formula 2,

$$
\begin{align*}
g(x) &= DES(K_1, DES^{-1}(K_2, x))
\end{align*}
$$

Based on Retail, the MASL-MAC algorithm adds a brand new key in the last round, expanding the DES key from 2 to 3, that is $K = (K_1, K_2, K_3)$. The difference with the standard Retail MAC is that the output transformation function at the end adds an extra key $K_3$ to replace the original encryption key $K_1$.

$$
\begin{align*}
g(x) &= DES(K_3, DES^{-1}(K_2, x))
\end{align*}
$$

MASL-MAC structure is shown in Fig.2.
3. Verify the security of the improved RSSP-II protocol

3.1. Key Service Process

The safety communication of the railway signal system relies on the RSSP-II communication protocol. The railway signal system equipment uses the RSSP-II communication protocol for signal interaction, and the entity authentication communication needs to be carried out through the key. Therefore, a special key server is required to implement key management for the communication participants. The main functions of the key server defined in SubSet038 include key generation, distribution, update, and query. The RSSP-II communication protocol specifies different key levels, which are divided into three levels: the first level is the session key (KAMAC), the second level is the authentication key (KMAC), and the third level is the transmission key (KTRANS).

3.2. Optimization of the key service process of the improved protocol

This article adopts an optimization method for the key center of the RSSP-II protocol. This method can optimize and improve the key center of key management during high-speed rail wireless communication. It specifically includes the following steps:

Step 1. Apply the public key encryption system to the railway communication key management system;

Step 2. Before the key center distributes the key to the vehicle-mounted equipment and the ground block center, the key center uses the public key system-based advanced encryption standard AES algorithm to authenticate the vehicle-mounted device and the ground wireless block center.

Step 3. The key center distributes the authentication key to the vehicle-mounted equipment and ground block center after communication encryption in step 2.

Among them, the specific process of step 2 is as follows:

The in-vehicle device is named device A; the key center M uses the AES encryption algorithm to authenticate the device A through the digital certificate of the device A as follows:

Step 2.1, device A sends a digital certificate to key center M, requesting identity verification;

Step 2.2, M sends a random string n to device A;
Step 2.3: Device A encrypts n with its own private key, and the ciphertext is N;

Step 2.4: The key center M uses A’s public key to decrypt N and compare it with n. If N and n are the same, it means that the identity of device A is legal and that the identity of device A is legal, which means that device A has passed the identity verification; otherwise, it means that device A is illegal, if the identity is illegal, it means that device A has not passed the identity verification;

In the same way, the ground wireless block center is named device B; the key center M uses the AES encryption algorithm to authenticate device B through the digital certificate of device B. The process is as follows:

Step 2.1: Device B sends a digital certificate to the key center M to request identity verification;

Step 2.2, M sends a random string n1 to device B;

Step 2.3: Device B uses its private key to encrypt n1, and the ciphertext is N1;

Step 2.4: The key center M uses B’s public key to decrypt N1 and compare it with n1. If N1 and n1 are the same, it means that the identity of device B is legal and that the identity of device B is legal, which means that device B has passed the identity verification; otherwise, it means device B Illegal, illegal identity means that device B has not passed the identity verification;

If N and n are consistent, the verification result is shown in Fig.3, indicating that device A has passed the identity verification and the optimized key service process is successfully verified; otherwise, as shown in Fig.4, device A has not passed the identity verification.

The security protocol is simulated from the security-related key service process of the RSSP-II communication protocol. The simulation result verifies the security attribute of the improved protocol’s confidentiality and optimizes the protocol key service process. Only through identity verification can The completion of the key service process further strengthens the security of the agreement.

4. Conclusion
Aiming at the low-security problem of the MASL layer message authentication code algorithm in the railway signal system RSS-II protocol, this paper uses the MASL-AES-MAC algorithm based on the advanced encryption standard AES algorithm, from the security-related key service process of the RSS-II communication protocol. The security protocol is simulated and the protocol key service process is optimized, so that the protocol has higher security and has certain engineering significance for the development of railway communication in the future.

References

[1] Zhangtai Z, Xu L and Wenyi J 2003 Railway Integrated Digital Mobile Communication System (GSM-R) M. China Railway Publishing House

[2] Liu Y and Zhao H Reliability 2019 Analysis of CTCS-3 Train Operation Control Systems via Binary Decision Diagrams Method C. 2018 IEEE International Conference on Information and Automation (ICIA). IEEE

[3] 2010 Ministry of Railways of the People’s Republic of China. CTCS-3 level train control specification: RSSP-Ⅱ Railway Signal Safety Communication Protocol V1.0 S. Beijing: Science and Technology Department of the Ministry of Railways, Yunji Signal 267, 11-53

[4] Wei G, Lianshan Y and Xiaomin W 2016 Security analysis of RSSP-Ⅱ railway signal safety communication protocol J. Journal of the China Railway Society, 38(8):50-56

[5] Yuanling Z, Zhongwei X and Yongbing W 2012 Improved MAC algorithm in railway signal security communication protocol J. Computer Engineering, 38(003):246-248

[6] Qihe Z Research on Railway Signal Safety Communication Protocol RSSP-Ⅱ and FPGA implementation of core algorithm