Research on Data Encryption of Intelligent Internet-Connected Vehicle Terminals

Xiucheng Peng, Huayuan Liang, Xiuxian Li, Xiang Pan(✉), and Fei Liang

Guangxi Vocational Normal University, No. 105, East University Road, Xixiangtang District, Nanning, Guangxi, China
panxiang_px@126.com

Abstract. The rapid development of the intelligent terminal automobile industry has increased the demand for intelligent Internet-connected vehicle terminals, but there is the problem of data security not being guaranteed while the terminals realize traditional automobile networking and intelligence. Based on the FOTA technology architecture, the article investigates the application of optimized Bsdiff algorithm and hybrid encryption algorithm in the multi-module of smart Internet-connected vehicle terminal to improve the security of data transmission process in the vehicle terminal.

Keywords: Intelligent Networked Vehicle · Vehicle Mounted Terminal · Data Encryption · Information Security

1 Introduction

The rapid development of the smart connected vehicle industry in recent years has led to malicious attacks on vehicle manufacturers and connected vehicle information service providers [1], making it impossible to ensure data security. In this paper, we propose a data encryption transmission method based on Firmware-Over-the-Air (FOTA) software upgrade technology for mobile terminals by applying an optimised Bsdiff algorithm in combination with a hybrid encryption algorithm to improve the performance and security of in-vehicle terminals.

2 FOTA Technology Architecture

The FOTA technology architecture of the smart Internet connected vehicle terminal Fig. 1 consists of the server side, the vehicle FOTA terminal and the ECU side, and the core algorithm “hybrid encryption algorithm and optimised Bsdiff algorithm”. The FOTA technology architecture of the Smart Internet Connection Vehicle Terminal is shown in Fig. 1.

Server side: Through the wireless communication protocol, it receives the new version upgrade packets and analysis data released by the supplier and sends them to the terminal after packaging, and monitors the terminal status during the upgrade process.

D. Kumar et al. (Eds.): IEIT 2023, AHSSEH 10, pp. 1133–1139, 2023.
https://doi.org/10.2991/978-94-6463-230-9_135

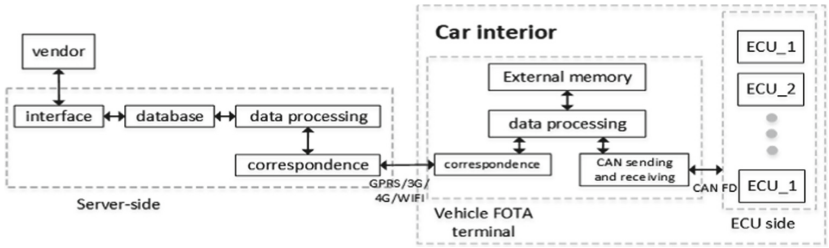

Fig. 1. FOTA technology architecture of intelligent Internet-connected vehicle terminal

The server can send and receive the upgrade packet data to the vehicle terminal when the communication is successful.

In-vehicle FOTA terminal: verify and receive the upgrade packet, make sure the upgrade packet is safe, and send the upgrade packet to the corresponding ECU terminal after obtaining the user's confirmation of upgrade instruction, and finally, through the CAN transceiver module, perform Bootloader brushing to the ECU terminal, and finally complete the upgrade.

ECU terminal: the control system of the intelligent networked car, mainly controls the driving status of the car and realizes its various functions. By updating the ECU of the whole car through the FOTA terminal, the overall performance of the ECU side in controlling the driving status and realizing the functions of the Internet-connected car can be improved.

3 FOTA Technology Based Encryption and Decryption System

3.1 Encryption and Decryption Module

Based on the symmetric key encryption security FOTA update technology, the smart Internet connected vehicle terminal to be upgraded encrypts the transmitted information with the public key and transmits it to the server, which receives the information and decrypts it with the private key, extracts the symmetric encryption algorithm and the symmetric key and then encrypts it, and then continues to operate using the symmetric encryption to achieve the purpose of data encryption research [2].

3.2 Transmission Module

The FOTA Smart Internet-connected Vehicle Terminal sends requests to the server via the HTTP protocol, the server receives the requests and processes the data by encryption and decryption, and then transmits the results back to the FOTA Smart Internet-connected Vehicle Terminal. The transmission module connects the FOTA device [3] to be upgraded and the server for communication, which ensures the security of the data transmission [4].

3.3 Detection Module

The detection module is connected to the vehicle-mounted terminal to be upgraded via the transmission module and is used to detect the pending upgrade status of the vehicle-mounted terminal to be upgraded. After receiving the instruction from the server, the vehicle-mounted intelligent Internet-connected terminal remotely connects to the server, at which time it only needs to detect that the vehicle-mounted intelligent Internet-connected terminal to be upgraded has good upgrade conditions and environment, and then the upgrade operation can be performed [5].

4 FOTA Data Encryption Algorithm and Its Application

4.1 Optimized Bsdiff Algorithm and Its Application

The optimized Bsdiff algorithm solves the problem of data transmission timeliness in the FOTA terminal, which uses the optimized Bsdiff algorithm to process data, shortening the problem of long data transmission and reception times in the FOTA terminal and improving the overall performance of the intelligent Internet-connected vehicle. The specific steps of the algorithm Fig. 2 are as follows:

Step 1: The smart Internet connected vehicle terminal obtains the upgrade package released by the server through the transmission module and sends a request to the ECU side. After the ECU side responds, the detection module detects the terminal version number and the upgrade package version number for comparison and confirms whether the version update is needed.

Step 2: After determining the version number, FOTA applies the optimized Bsdiff algorithm, compares the new file with the old file to generate the dictionary sequence I and then compares it with the new file to form a differential data packet, and sends it to the ECU side via CAN bus after applying bzip compression.

Step 3: The ECU side receives the differential packet and uses the diagnostic protocol service to clear the memory space, then decompresses the differential update packet using bzip and writes the data to external memory. The comparison with the old version of the file is continued to generate a topological ordering of the inserted blocks. With the optimized Bsdiff algorithm, the differential update operation of the bootloader is implemented on the ECU side. Once the data has been processed, FOTA sends control commands directly to the ECU side via the CAN bus. The specific application scheme of the optimized Bsdiff algorithm is shown in Fig. 2.

FOTA obtains historical and real-time position information by continuously recording the position information of the smart connected car via the internal memory unit. Based on the data information, it is quickly transmitted to the vehicle's speed control unit via the optimised Bsdiff algorithm to enable real-time control and adjustment of the car's speed for future autonomous driving purposes.

4.2 Hybrid Encryption Algorithm and Its Application

The hybrid encryption algorithm mainly solves the security of the in-vehicle FOTA terminal for data transmission and storage. The combined use of AES algorithm and

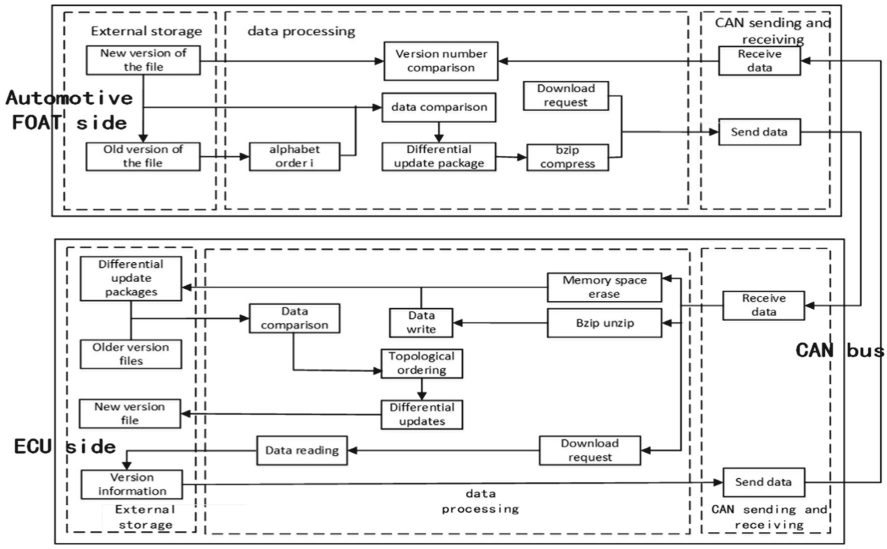

Fig. 2. Schematic diagram of the application of the optimized Bsdiff algorithm based on the in-vehicle FOTA terminal system

ECC algorithm [6] solves the problem of secure distribution of secret keys and improves the efficiency of encryption and decryption [7]. The algorithm-specific step aggregation Fig. 3 is as follows:

Step 1: FOTA, the smart Internet connected vehicle terminal, sends an encryption request to the ECU side, and generates the ECC private key and ECC public key after getting the response from the ECU side. The ECC public key is sent to FOTA, the vehicle terminal, through the CAN bus.

Step 2: FOTA processes its data using the optimized Bsdiff algorithm and encrypts it with AES encryption. The AES key is encrypted by the ECC public key, generates the differential packet cipher and AES key block, and transmits it to the ECU end.

Step 3: After receiving the data, the ECU side decrypts the AES key block using the ECC private key to get the AES key. Then the AES key decrypts the differential packet cipher text to get the complete differential packet and complete the update operation of FOTA to the ECU side [1, 8]. The specific hybrid encryption algorithm application schematic is shown in Fig. 3.

The hybrid encryption algorithm can be used in smart Internet-connected vehicles to encrypt and store data such as vehicle location information, historical track information, whole vehicle performance information monitoring and ECU software system upgrade. FOTA of Smart Internet connected vehicle terminal uses hybrid encryption algorithm to encrypt location information, historical track information and ECU software system upgrade data [9].

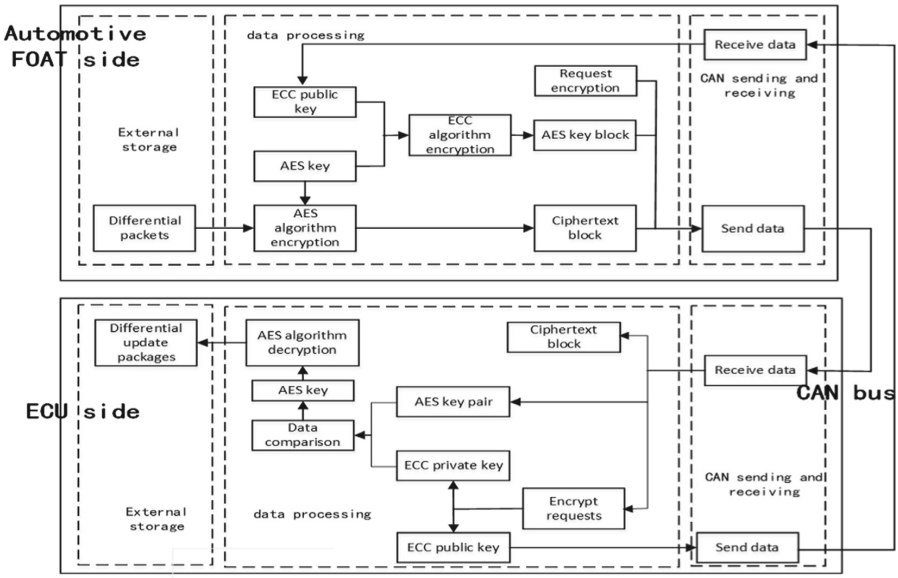

Fig. 3. Schematic diagram of hybrid encryption algorithm application based on in-vehicle FOTA terminal system

5 Experimental Verification

Test for optimized Bsdiff algorithm and hybrid encryption algorithm to check whether it meets the FOTA performance requirements of the intelligent networked vehicle terminal.

Based on the above test results Table 1, it is clear that the file size of the resulting differential repackage is not directly related to the size of the old and new files, but rather to the difference between the old and new files. The compression ratio of the resulting differential file compression packets varies depending on the degree of difference between the old and new file sizes.

According to the above test results Table 2, the hybrid encryption algorithm consumes about 1000 ms more time than if the hybrid encryption algorithm was not applied, and the time consumed for encryption and decryption is within 300 ms.

The analysis shows that the percentage of the new file size decreases as the new file size increases when the optimised Bsdiff algorithm and the hybrid encryption algorithm are applied to the intelligent Internet-connected vehicle terminal.

Table 1. Performance test table of optimized Bsdiff algorithm

Sample	Old file size (KB)	New file size (KB)	Differential file size (KB)	Compression rate	Upgrade time (s)	Traditional upgrade time
BCMV 1 > V 2	4.35	5.49	2.34	57%	10.233143	9
EPSV 1- > V 2	10.13	11.53	3.73	67%	10.667722	9.8
ACU Vl- > V 2	17.07	18.55	3.92	78%	10.958046	11
BMS V 1 > V 2	23.57	24.80	4.73	80%	11.157143	13
ACV 1- > V 2	30.22	31.56	3.88	87%	10.807258	14
ICV 1- > V 2	38.20	39.87	4.38	88%	11.080143	15

Table 2. Hybrid encryption algorithm performance test table

Documents	File Size (KB)	Encryptio time (ms)	Decryption time (ms)	Upgrade time (s)	Didn't use algorithm upgrade time
BCMV 2	5.49	146.21	102.24	9.871621	10.465712
EPS_V 2	11.53	146.54	102.37	10.507062	10.609813
ACU_V 2	18.55	151.83	108.64	11.696728	11.459452
BMS V 2	24.78	153.05	109.77	12.806394	11.945684
AC_V2	31.56	154.38	110.31	14.106208	13.096207
IC_V2	39.87	156.25	112.64	15.870657	14.800656

6 Conclusion

In order to solve the problem of data information leakage security risks of smart Internet connected vehicle terminals [10], the article proposes to combine the use of optimized Bsdiff algorithm and hybrid encryption algorithm based on FOTA technology to solve the data security and data transmission problems of smart Internet connected vehicle terminals.

Acknowledgements. This work was supported by Guangxi College Students' innovation and entrepreneurship training program under Grant No. 202214684004X.

References

1. Liu, X.D, Zhao, H.Q. (2023) Secure extraction technology of big data steganographic features based on hybrid cryptosystem[J/OL]. Journal of Nanjing University of Information Engineering (Natural Science Edition):1–9 [2023–03–12].
2. Yu, W.X, Zhang, P, Bi, C.R, et al. (2021) HTTP protocol-based data transmission program design and example [J]. Engineering and Experimentation, 2021, 61(04):89–90+98.
3. Yin, J. (2020) Analysis and design of data transmission method based on in-vehicle FOTA terminal [D]. Chongqing University of Posts and Telecommunications, 2020:1–44.
4. Zhang, H.Z, Zhang, Z.W. (2019) Research on information security based on HTTP protocol [J]. Computers and Networks, 2019, 45(17):69–71.
5. Li, R. (2019) Research and implementation of secure access technology for intelligent distribution network terminals [D]. North China Electric Power University, 2019:1–10.
6. Chen, X, Y. Lai, X, f. (2020) Research on hybrid cryptosystems based on AES and ECC algorithms. Journal of Beijing Printing Institute 2020, Vol. 3, No. 150–152, Total 3 pages.
7. Guan, Y.Z, Jiang, Y.X. (2020) Design of ciphertext loss prevention transmission system for communication networks based on hybrid encryption algorithm [J]. Modern Electronic Technology, 2020, 43(2):64–66.
8. Liu, H.Z. (2021) Research on the application technology of cryptographic algorithms for the field of intelligent networked vehicles[D]. Xi'an University of Electronic Science and Technology, 2021:1–10.
9. Chen, J.E, Chen, T., Tong, X.J. (2022) Design and implementation of a secure communication system based on hybrid encryption algorithm [J]. Journal of Lanzhou College of Arts and Sciences: Natural Science Edition, 2022, Vol. 5, No. 67–71,93, 6 pages
10. Zhang, X, Zhang, H.C, Liu, Z.L. (2021) Threat model and risk assessment of in-vehicle terminals of Internet-connected vehicles[J]. Automotive Practical Technology, 2021, 46(20): 26–30. DOI:https://doi.org/10.16638/j.cnki.1671-7988.2021.020.007.