Design and Implementation of AES Symmetric Encryption Algorithm Based on In-Vehicle CAN Network Communication Data

Yuanyuan Li, Qi Yu [a] and Anyu Cheng

School of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China.

[a] yuqi@sumarte.com

Abstract

Aiming at the problem of more and more external interfaces added to vehicle, malicious intrusion into in-vehicle CAN network and stealing and tampering with CAN network data, this paper uses AES symmetric encryption algorithm to encrypt and decrypt data with high speed and high encryption strength. AES symmetric encryption algorithm to encrypt the data of in-vehicle CAN network and design the symmetric key library and key update mechanism to ensure the secure transmission of in-vehicle CAN network communication data and establish the hardware simulation platform to verify the reliability of AES symmetric encryption algorithm.

Keywords

AES Symmetric Encryption, In-Vehicle CAN Network, Symmetric key library, Rekeying.

1. Introduction

With the rapid development of information technology, in-vehicle electronic systems are experiencing a qualitative change, more and more, more and more rich in-vehicle entertainment systems, interactive systems of people and vehicles, smart devices appear in the vehicle, but at the same time, the vehicle adds many external interfaces, These additional external interfaces can be the entrance of an attacker to invade the in-vehicle network. The attacker invades the in-vehicle CAN network through numerous external interfaces and steals and tampers the CAN network communication data, which will seriously threatens the driving safety of the vehicle .

Famous white hat hackers Miller and Valasek, Ph.D., have published research reports on the safety of internet of vehicle for three consecutive years since 2013 in the world's top security conferences [1-3]. The attacks covered in these reports, whether adopted direct connection, or adopted remote attacks on entertainment system vulnerabilities, the ultimate goal was to control the vehicle by sending a forged command message to the in-vehicle electronic control unit (ECU) through the in-vehicle CAN network. Miller et al. Used the Jeep Cherokee WI-FI open port to intrude into the Uconnect system and reprogram the ECU's firmware and then control key functions by intruding the vehicle's CAN network [3], causing 1.4 million vehicles to be recalled.

At present, there are many companies and agencies on the in-vehicle network security conducted in-depth study. The EVITA (E-Safety Vehicle Intrusion Protected Applications) project [4] focused on solving hardware security issue. The AUTOSAR (Automotive Open System Architecture) architecture proposed Secure On-Board Communication to regulate the secure transmission between the ECUs [5]. Some security companies have proposed the integration of security modules in the gateway to intrusion detection of security threats [6]. In addition, some experts and scholars are also thinking about the data encryption algorithm applied to the automotive network security [8].

In this paper, we use AES symmetric encryption algorithm to encrypt the in-vehicle CAN network communication data and design a symmetric key library of AES symmetric encryption algorithm and key updated mechanism to ensure the in-vehicle CAN network communication data to securely transmit in the in-vehicle CAN network Security.

2. Based on the In-Vehicle CAN network AES algorithm principle

AES is an iterative block cipher algorithm, the packet length and key length can be changed, according to the selected number of bits, the encryption of the wheel constant is also different. In this paper, AES symmetric encryption algorithm based on the in-vehicle CAN network communication data is studied based on the 128-bit key length AES algorithm. In the following, the AES symmetric encryption algorithm based on the in-vehicle CAN network communication data is represented by AES-128. The main algorithm flow shown in Fig. 1.

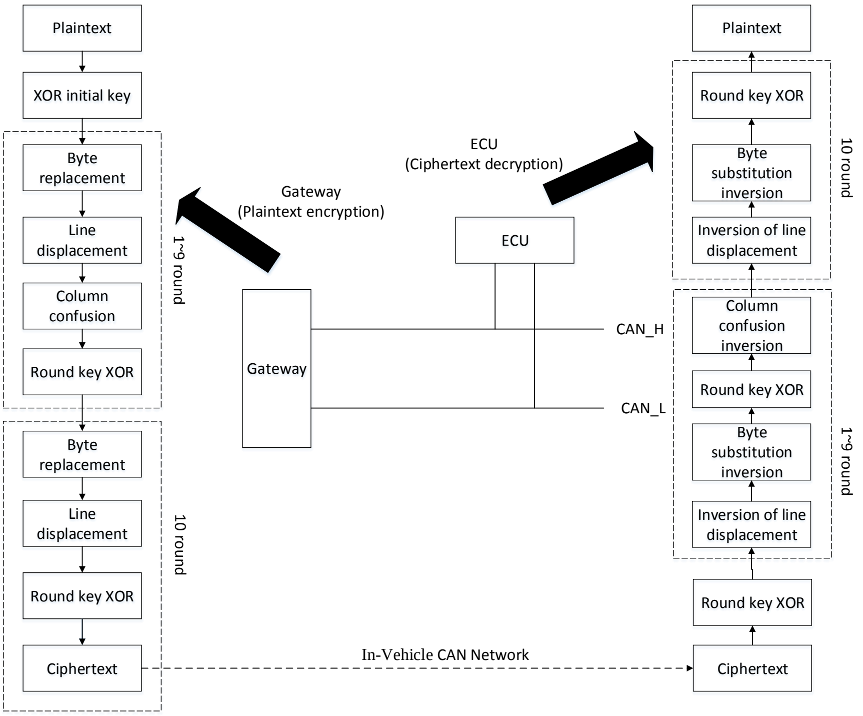


Fig. 1 AES encryption and decryption based on in-vehicle CAN network

In in-vehicle CAN network, plaintext information is transformed into ciphertext information at the gateway by 10 rounds of AES algorithm. The ciphertext information is transmitted to the ECU node and restored to plaintext by 10 rounds of inverse transformation.

3. Based on the In-Vehicle CAN network AES algorithm design

In this paper, AES symmetric encryption algorithm is applied to the encryption of in-vehicle CAN network communication data. Based on the research results of AES symmetric encryption algorithm, the following two parts are carried out according to the characteristics of CAN network: symmetric key library design and key update mechanism design.

3.1 Symmetric key library design

In the in-vehicle CAN network, it is extremely unsafe to use the same key for all data packets in the encryption process. A key is cracked will lead to the entire in-vehicle CAN network data security is a great threat. Therefore, aiming at the problem that the key is too single, this paper designs a symmetric key library containing multiple keys of AES symmetric encryption algorithm, so as to ensure the security of the communication data of the in-vehicle CAN network to the maximum extent.

Symmetric key library based on in-vehicle CAN network is shown as in Fig. 2, set up the symmetric key library of AES symmetrical encryption algorithm in gateway and ECU node, there are 6 different key stores in key library, namely Key1, Key2, Key3, Key4, Key5, Key6.

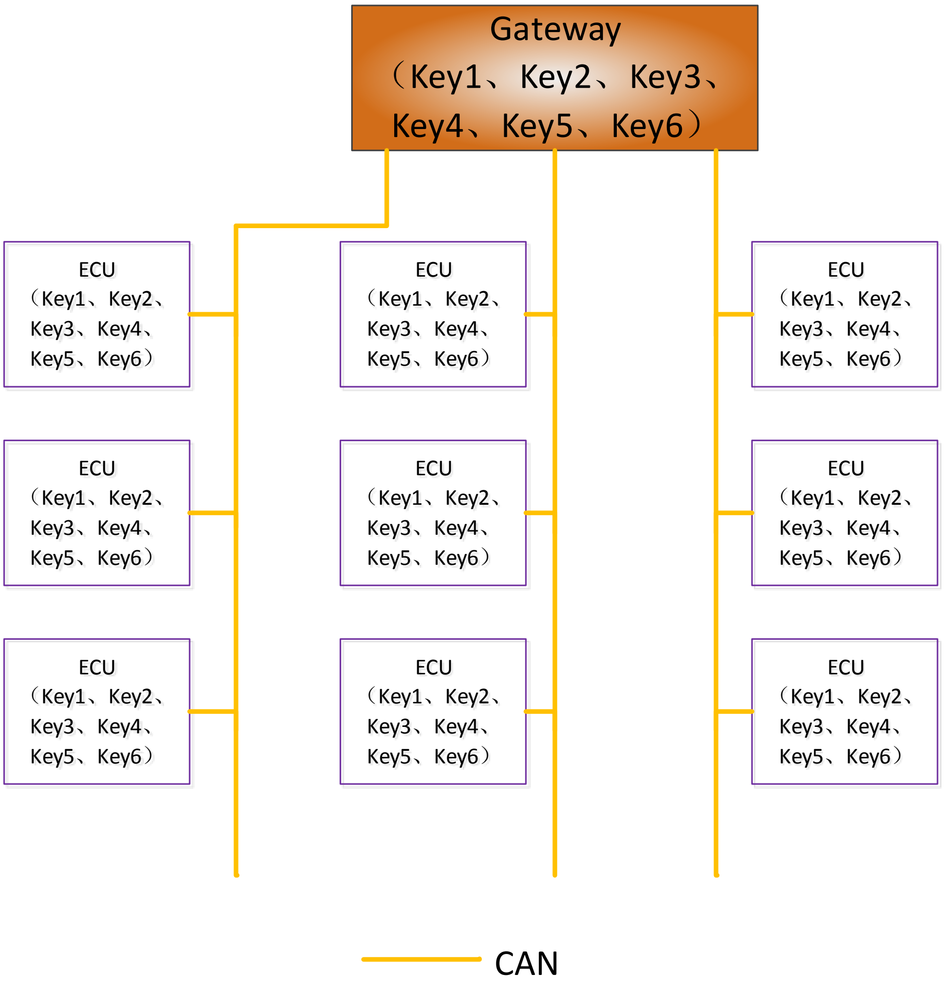


Fig. 2 Symmetric key library

In the symmetric keystore, a key is randomly selected to encrypt the pivotal information of the data message to form a ciphertext. When the ciphertext is transmitted to the ECU node, the corresponding decryption key is selected in the symmetric key repository at the ECU node to decrypt the ciphertext into plaintext. Select the key in the symmetric key library to process the data encryption and decryption process as shown in Fig. 3.

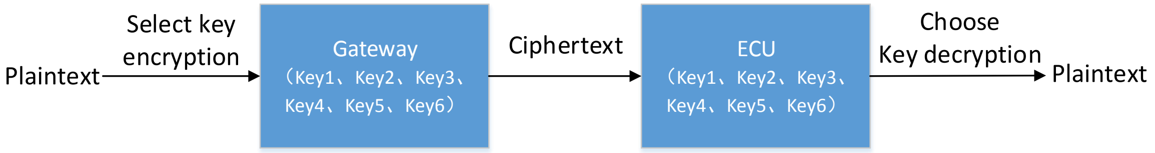


Fig. 3 Symmetric key library encryption and decryption process

3.2 Key Update Mechanism Design

In-Vehicle CAN network communication data unit for the frame, the gateway sends the data frame to each node to control node to work, and receive data frames from the node. CAN-bus standard frame structure by the seven segments, namely the beginning of the frame, the arbitration section, the control section, the data section, CRC section, ACK section, the end of the frame. The data segment of CAN communication contains 8 bytes. In order to improve the resource utilization rate and ensure the communication rate, this paper applies the AES symmetric encryption algorithm to encrypt / decrypt the data segment of CAN message. The AES-128 symmetric encryption algorithm encrypts plaintext information to form a ciphertext. The length of the data is 16 bytes. Therefore, the first 8 bytes of ciphertext data are placed in a CAN-bus standard frame until the first frame of ciphertext After the message is sent, the last 8 bytes of ciphertext data are placed in the CAN-bus standard frame of the same ID and sent out. After these two CAN messages are received by the ECU, they are combined into a complete ciphertext message and decrypt into a plaintext message. The frame structure of ciphertext is shown in Fig. 4.

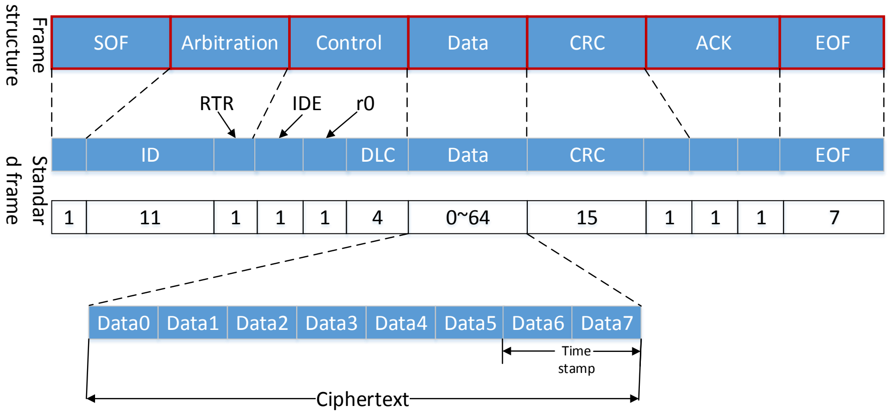


Fig. 4 Ciphertext frame structure

CAN message at the gateway by randomly selected encryption key to encrypt the CAN message, and select the corresponding decryption key at the ECU node to decrypt the ciphertext. During encryption and decryption, the encryption key and decryption key are the same key and stored in the respective symmetric key library. Therefore, a key update mechanism needs to be designed so that randomly selected encryption keys and decryption keys correspond one-to-one to ensure data communication security. This paper uses a key array mechanism, the six keys are placed in the key array, the gateway and the ECU node set 0.1ms timer, synchronization update the gateway and the network node at the key selection, so that at the gateway The selected key is the same as the key selected at the network node, so as to solve the problem that the encryption key and the decryption key correspond one-to-one. The timer work flow chart is shown in Fig. 5. The key update mechanism is shown in Fig. 6.

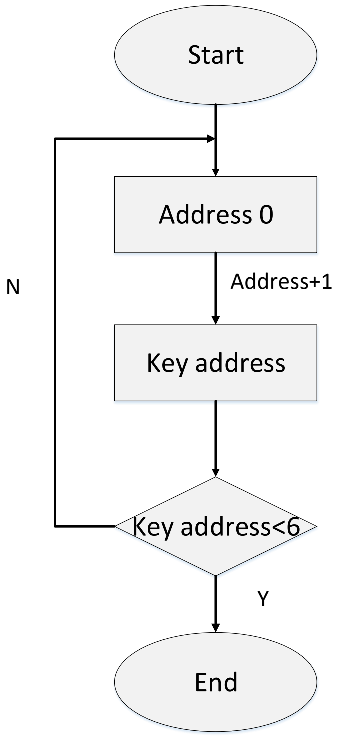


Fig. 5 Timer flow chart

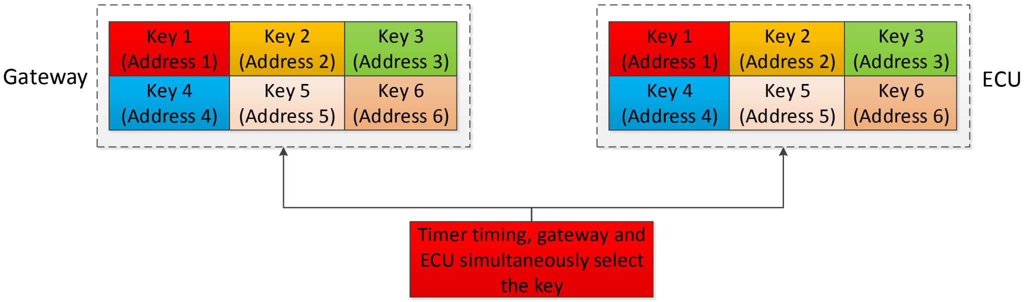


Fig. 6 Key Update Mechanism

4. AES algorithm in the In-Vehicle CAN bus implementation and results analysis

In the experiment, the gateway and the network node both used a NXP company with a two-CAN communication microcontroller - LPC1768, CAN transmission rate up to 1Mbit / s. In the experiment, the same key library is set up at the gateway and at the network node. When the plaintext is encrypted, the same key is selected through the synchronization of the timer set at the gateway and the ECU node, and the key at the gateway is used as the encryption key , The key at the ECU node acts as a decryption key. Experiments AES encryption algorithm to encrypt CAN network communication data. The plaintext, key, ciphertext, and plaintext after decryption are as follows:

Event message:

plaintext message: 0XAA,0X02,0X03,0X02,0X05,0X07,0X08,0XAA

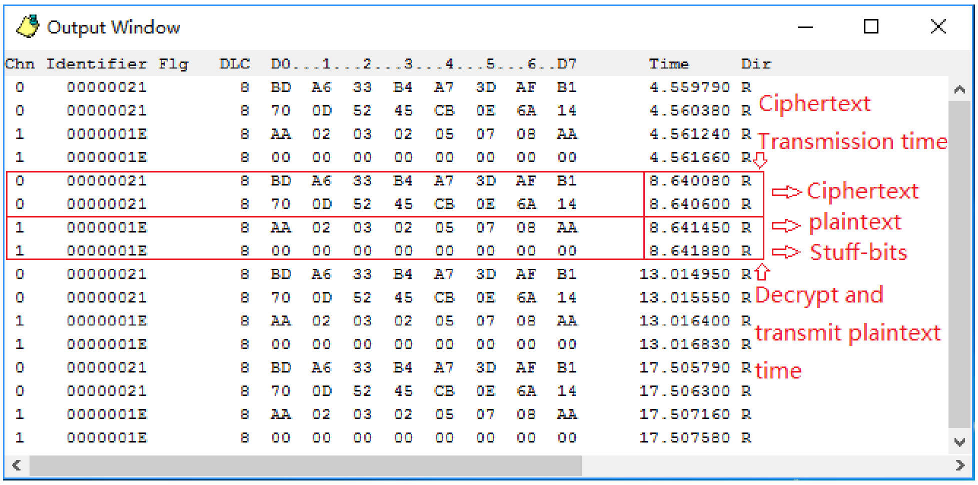
(2)Key: 0X01,0X02, 0X03,0X04,0X05,0X06,0X07,0X08,

0X01,0X02,0X03,0X04,0X05,0X06,0X07, 0X08

(3)Ciphertext information: 0XBD, 0XA6, 0X33, 0XB4, 0XA7, 0X3D,0XAF,0XB1,

0X70,0X0D,0X52,0X45,0XCB,0X0E,0X6A,0X14

After AES encrypts and decrypts the event message, the ciphertext and decrypted plaintext acquired by Kvaser tool are shown in Fig. 7.



```
Output Window

Chn Identifier Flg   DLC  D0...1...2...3...4...5...6..D7      Time      Dir
 0     00000021        8  BD  A6  33  B4  A7  3D  AF  B1      4.559790 R
 0     00000021        8  70  0D  52  45  CB  0E  6A  14      4.560380 R
 1     0000001E        8  AA  02  03  02  05  07  08  AA      4.561240 R
 1     0000001E        8  00  00  00  00  00  00  00  00      4.561660 R
 0     00000021        8  BD  A6  33  B4  A7  3D  AF  B1      8.640080 R
 0     00000021        8  70  0D  52  45  CB  0E  6A  14      8.640600 R
 1     0000001E        8  AA  02  03  02  05  07  08  AA      8.641450 R
 1     0000001E        8  00  00  00  00  00  00  00  00      8.641880 R
 0     00000021        8  BD  A6  33  B4  A7  3D  AF  B1     13.014950 R
 0     00000021        8  70  0D  52  45  CB  0E  6A  14     13.015550 R
 1     0000001E        8  AA  02  03  02  05  07  08  AA     13.016400 R
 1     0000001E        8  00  00  00  00  00  00  00  00     13.016830 R
 0     00000021        8  BD  A6  33  B4  A7  3D  AF  B1     17.505790 R
 0     00000021        8  70  0D  52  45  CB  0E  6A  14     17.506300 R
 1     0000001E        8  AA  02  03  02  05  07  08  AA     17.507160 R
 1     0000001E        8  00  00  00  00  00  00  00  00     17.507580 R
```

Fig. 7 AES Encrypts and decrypts plaintext

As shown in the figure above, when the CAN network baud rate is 500kbs, the transfer time of a ciphertext is 520μs. The ciphertext is transmitted to the node via the CAN network and decrypted into the plain text at the node. The decrypted plaintext messages, this process takes 1.28ms. Under the condition of 10% network load, the maximum communication delay time of CAN network event type message is 1.950 ms [7]. The transmission time of the plaintext information of in-vehicle CAN network communication data in this paper after being encrypted by AES symmetric encryption algorithm is shown in the following Table 1.

Table 1 Ciphertext transmission time

Nature of the message	A ciphertext transmission time	Ciphertext transmission and decryption time	Maximum communication delay requirements
Event message	520μs	1.28ms	1.950ms

As shown in the above experimental results, the plaintext message is encrypted by the AES encryption algorithm to form a 16-byte ciphertext. The 16-byte ciphertext is decrypted at the ECU node and then restored to a 16-byte plaintext message. The first 8 The bytes are plain text, the last 8 bytes are padded bits. From the experimental results, it can be seen that after the data message is encrypted at the gateway by the AES encryption algorithm, the data message is transmitted in ciphertext through the CAN bus network, thereby preventing the network threat from being externally threatened at the external interface of the vehicle and stealing and tampering with the data message. The security of data transmission in CAN network is consistent with the plain text before decryption at the network node. At the same time, the ciphertext transmission time of AES-128 symmetric encryption algorithm satisfies the requirements. Therefore, the verification of AES symmetric encryption algorithm reliability.

5. Conclusion

In this paper, the working principle of encryption and decryption of AES symmetric encryption algorithm is studied. According to the characteristics of CAN network in vehicle, it is applied to the data encryption of in-vehicle CAN network communication data. At the same time, symmetric key library and key update mechanism to ensure the safety of in-vehicle CAN network communication data in the transmission of in-vehicle CAN network. Finally, a hardware simulation platform is set up to test the design scheme. The experimental results show that the design of this paper meets the real-time requirements of in-vehicle CAN network while ensuring the safety of in-vehicle CAN network communication data during transmission. Based on the existing research, this design uses data encryption algorithm to encrypt the important data, so as to protect the important data from the risk of intrusion and tampering. It is of great significance for the research and development of in-vehicle network data security.

References

[1] Miller C, Valasek C. Adventures in automotive networks and control units[J]. DEF CON, 2013, 21: 260-264.

[2] Miller C, Valasek C. A survey of remote automotive attack surfaces[J]. Black Hat USA, 2014.

[3] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015.

[4] Apvrille, L., El Khayari, R., Henniger, O., Roudier, Y., Schweppe, H., Seudié, H., ... & Wolf, M.: Secure automotive on-board electronics network architecture. In FISITA 2010 world automotive congress, Budapest, Hungary (Vol. 8) (2010).

[5] Specification of Module Secure Onboard Communication AUTOSAR Release 4.2.2, https://www.autosar.org/standards/classic-platform/release-42/software-architecture/general/, last accessed 2017/8/03.

[6] Symantec Anomaly Detection for Automotive, https://www.symantec.com/products/anomaly-detection-for-automotive, last accessed 2017/7 /29.

[7] Li Jia, Zhu Yuan, Tian Guangyu. Analysis of CAN and TTCAN Communication Delay [J]. Journal of Tsinghua University: Natural Science, 2006, 46 (2): 261-265.

[8] Siddiqui A S, Plusquellic Y G J, Saqib F. Secure communication over CANBus[C]// IEEE, International Midwest Symposium on Circuits and Systems. IEEE, 2017:1264-1267.