2021 2nd International Conference on Computer Communication and Network Security (CCNS) | 978-1-6654-2711-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCNS53852.2021.00016

Analysis of the influence of CAN bus encryption and decryption on real time performance

Tonghong Chong
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
chongtonghong@catarc.ac.cn

Tianyu Liu
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
liutianyu@catarc.ac.cn

Yanan Zhang
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
zhangyanan@catarc.ac.cn

Chao Ma
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
machao@catarc.ac.cn

Xianfeng Jia
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
Jiaxianfeng@catarc.ac.cn

Zhi Wu
Networking Technology Research Office
China Automotive Technology & Research Center Automotive Data Co, Ltd
Tianjin, China
wuzhi@catarc.ac.cn

***Abstract*—With the rapid development of intelligent network connected vehicle, information security has been paid more and more attention. In order to solve the problem that the vehicle bus information is transmitted directly without encryption, which is easy to be illegally monitored and maliciously cracked, it is planned to encrypt the vehicle bus information before transmission. Sender and receiver use the same encryption algorithm and key. The sender encrypts the data before sending the message, while the receiver decrypts the data after receiving it. In order to study the influence of CAN bus encryption and decryption on transmission efficiency, taking TC299 chip as an example, different encryption and decryption algorithms are used to encrypt and decrypt data with different lengths. The research shows that the time of symmetric encryption is much less than that of asymmetric encryption; With the increase of the length of the data to be encrypted and decrypted, the time required for encryption and decryption also increases; The time of encryption and decryption is microseconds, which will not affect the real-time performance of the bus.**

Keywords- Cyberseurity; CAN-BUS; Encryption and decryption scheme; Encryption and decryption algorithm; Realtime

I. INTRODUCTION

A. Intelligent networked car development status

With the diversification of automotive networking technology and the continuous improvement of networking rate, the market potential of automotive networking services will be gradually released. Intelligent Connected Vehicle (ICV) is equipped with advanced on-board sensors, controllers, actuators and other devices, and integrates modern communication and network technologies to realize intelligent information exchange and sharing between vehicles and X (vehicles, roads, people, clouds, etc.).With the functions of complex environment perception, intelligent decision-making, collaborative control, etc., it can realize safe, efficient, comfortable and energy-saving driving, and finally it can realize a new generation of cars that can replace people to operate[1].

From a global perspective, countries and regions such as the United States, Europe and Japan started earlier, and governments of various countries issued corresponding policies and plans to plan the development of intelligent networked vehicles and intelligent transportation.

Automobile intelligent network connection technology has triggered a new round of international scientific and technological competition. Mercedes-Benz, Ford, Toyota, Volvo and other top automobile manufacturers in the world have carried out research and development on the technology of autonomous vehicles of different grades. At the same time, in recent years, IT giants represented by Google, Apple, Intel and other companies in the United States have spared no effort to invest in the field of auto-driving technology. The acquisition of Mobileye Company by Intel for US$ 15.3 billion is the embodiment of this fierce competition and an important part of its overall strategy of establishing auto-driving.

In the long run, the technology development of intelligent Internet connected vehicles will eventually realize automatic driving and the interconnection between vehicles and everything. As the "five senses" of the automobile, the Internet

978-1-6654-2711-1/21/$31.00 ©2021 IEEE
DOI 10.1109/CCNS53852.2021.00016

of vehicles can more effectively understand the external environment and internal operation status of the car. As the "brain" of the automobile, artificial intelligence can make decisions according to the comprehensive judgment of information [2]. The Internet of vehicles is the premise of automatic driving, The application of Internet of vehicles will be more fully developed in the era of automatic driving, for example, satellite navigation will use high-precision map to improve the accuracy, and automatic driving will liberate the driver's attention so as to use more abundant vehicle entertainment.

B. information security threats faced by intelligent connected vehicles

1) background server threat

Server is a kind of computer. It runs faster, has higher load and is more expensive than ordinary computer. The server provides computing or application services for mobile app and vehicle terminal in the network. Servers are usually faced with threats such as data vulnerability, account hijacking, apt virus, permanent data loss, potential crisis caused by sharing [3].

2) mobile app security threats

Mobile app security threat refers to that hackers use these remote control apps to obtain personal information and vehicle control rights through root user's mobile terminal or luring users to download and install malicious programs [4].

3) Tbox system security threats

The full name of Tbox is telematics box, which means on-board network connection terminal. In short, it is equivalent to the host control system on the car. It can be connected through the network and various terminals to control the internal electronic equipment of the car. The main functions of Tbox system are remote control, inquiry and security service.

4) can bus security threats

Automotive electronic components are connected through can network, and the communication between electronic components is through can package. The CAN bus security threat obtains its communication matrix through reverse engineering, fuzzy test and other methods, and breaks the application layer bus protocol of the automobile, so as to realize the automatic control function of the automobile without adding the automobile actuator. In other words, as long as the CAN bus is grasped, We can control the car by grasping the nerve of the car.

II. COMMON ATTACK METHODS IN THE CAR NETWORK

A. CAN bus attack

1) CAN data frame flooding attack

The CAN bus network communication protocol stipulates that the priority of data frames transmitted between ECU is determined by the ID of CAN data frames, and the smaller the ID, the higher the priority of data frames [6]. Therefore, if an intruder sends a high priority CAN data frame on a CAN bus at a high frequency, it will probably block the sending of other data frames, thus realizing DoS attack.

2) CAN ID forgery

Because the CAN bus network communication is broadcast communication, intruders CAN easily obtain all the data frames sent on one CAN bus. Generally, CAN data frames are transmitted in plaintext. intruders can analyze the format and content of data frames by guessing, traversing or other means, and reverse crack the key control signals of vehicles. Further, illegal data frames are sent on the CAN bus in the name of these IDs, thus interfering with or blocking the normal communication between ECU's, and even actually controlling one or more ECU's of key systems (such as power system).

3) CAN data frame replay attack

Because the CAN bus network communication is broadcast communication, intruders CAN easily capture all the data frames of a specific CAN ID in time sequence, and then re-inject these data frames into the CAN bus network, so as to interfere with and illegally control one or more ECU.

B. in-car Ethernet attack

1) ICMP flooding attack

A simple denial of service attack, also known as ping flooding attack, in which the attacker floods the victim with ICMP "ping" packets [9].

2) UDP flooding attack

A denial of service attack using UDP, a session-free, connectionless transport layer protocol.

3) Teardrop attack

In the header of IP packet, there is a field called fragment offset, which indicates the starting position or offset of the fragmented packet in the original unfragmented packet.

Teardrop attack refers to using IP packets which maliciously modify the IP fragment offset value to attack, which makes the attacked person unable to reassemble the IP packets normally, and even leads to system crash.

4) IP spoofing attack

IP address spoofing refers to the attacker sending packets by impersonating the IP address of a legitimate host, so as to gain the trust of the attacker or hide the attacker's real IP address.

5) ICMP Smurf attack

This attack method combines IP spoofing attack and ICMP flooding attack. The attacker forged the source address of internet control message protocol and set the destination address of the packet as the broadcast address of the network [11]. If the network device does not filter this traffic, the internet control message protocol will be broadcast to all computers in the network. However, all computers in the network will send response request packets to the forged source address, which will flood the computer with forged source address, and may congest the whole network and reduce the availability rate. This attack is named after the malicious program "Smurf" which originally launched this attack.

III. Introduction of Common Encryption Algorithms

A. AES algorithm

Advanced Encryption Standard (AES) in cryptography, also known as Rijndael encryption method, is a block encryption standard adopted by American federal government.

This standard is used to replace the original DES (Data Encryption Standard), which has been analyzed by many parties and widely used all over the world. After a five-year selection process, the Advanced Encryption Standard was published in FIPS PUB 197 by NIST on November 26, 2001, and became an effective standard on May 26, 2002. In 2006, Advanced encryption standard has become one of the most popular algorithms in symmetric key encryption [12].

In cryptography, block cipher operation mode is an algorithm that uses block cipher to provide information services such as confidentiality or authenticity. Block-based symmetric cryptographic algorithms such as DES/AES only describe how to encrypt a fixed length (block) of data according to the secret key. For longer data, The working mode of block cipher describes how to repeatedly apply an algorithm to encrypt packets to safely convert data larger than blocks.

To put it simply, AES algorithm describes how to encrypt a data block, and the working mode of block cipher determines that multiple data blocks are long if repeated encryption is performed.

There are five working systems of block cipher: 1. Electronic Codebook (ECB); 2. Cipher Block Chaining (CBC); 3. Cipher feedback mode (CFB); Output feedback mode (OFB).

1) ECB

ECB mode is the simplest encryption mode, in which plaintext messages are divided into fixed-size blocks (packets), and each block is encrypted separately.

Encryption and decryption of each block are independent, and the same method is used for encryption, so parallel calculation can be performed. However, once a block is cracked, all plaintext data can be decrypted by using the same method, and the security is relatively poor.

It is suitable for the case of less data, and it is necessary to fill the plaintext data to an integral multiple of the block size before encryption.

2) CBC

In CBC mode, each packet should be XOR-XOR with the encrypted data of the previous packet, and then encrypted.

In this way, each ciphertext block depends on all plaintext blocks before the block. In order to keep each message unique, the first data block needs exclusive OR operation with initialization vector IV before encryption.

CBC mode is one of the most commonly used encryption modes. Its main disadvantage is that encryption is continuous and cannot be processed in parallel. Like ECB, message blocks must be filled to whole multiples of block size.

3) CFB

CFB mode is similar to CBC mode. The ciphertext of the previous packet is encrypted and XOR with the plaintext of the current packet to generate the ciphertext of the current packet. Decryption of CFB mode and encryption of CBC mode are very similar in flow.

4) OFB

OFB mode converts block cipher into synchronous stream cipher, which means that stream cipher with corresponding length can be generated independently according to plaintext length. It can be seen from the flow chart that OFB is very similar to CFB. CFB is the encrypted ciphertext of the previous packet and XOR the plaintext of the current packet. OFB is the stream cipher XOR the plaintext of the current packet before the previous packet and the previous plaintext block. Because of the symmetry of XOR operation, the decryption and encryption of OFB mode are exactly the same.

Based on the above four block encryption modes, it is considered that OFB mode is safer and more reliable, and it is a safer measure in the future. This paper chooses OFB mode.

B. Sha256

An N-bit hash function is a mapping from an arbitrarily long message to an N-bit hash value, and an N-bit encrypted hash function is a one-way and collision-free N-bit hash function. Such a function is an extremely important means in digital signature and password protection at present.

At present, the popular hash functions mainly include 128-bit MD4 and MD5 and 160-bit SHA-1. The SHA-2 family introduced today has more output hash values, which is more difficult to crack and can improve higher security.

SHA-2, whose name comes from the abbreviation of Secure Hash Algorithm 2 (English), is a cryptographic hash function algorithm standard developed by the National Security Agency of the United States and released by the National Institute of Standards and Technology (NIST) in 2001. It belongs to one of SHA algorithms and is the successor of SHA-1. It can be further divided into six different algorithm standards, including SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256. The HASH value calculation process is shown in Figure 1 below.

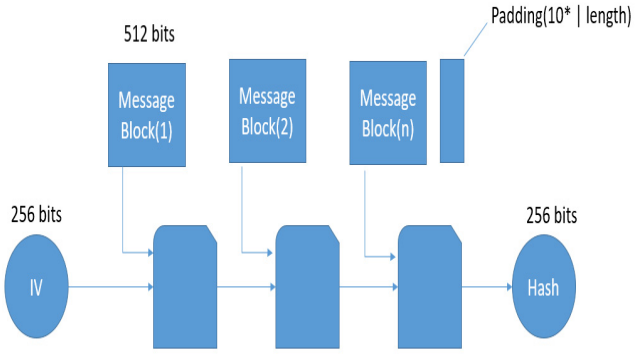

Figure 1. Hash value calculation process

C. *Hmac_ sha256*

Hmac is a method to construct message authentication code by using one-way Hash function, in which H in Hmac means hash.

The one-way hash function used in Hmac is not limited to one type. Any high-strength one-way hash function can be used in Hmac, and if a new one-way hash function is designed in the future, it can also be used.

Hmac constructed using Sha-256 is called Hmac_ sha256, and its calculation process is shown in Figure 2 below.

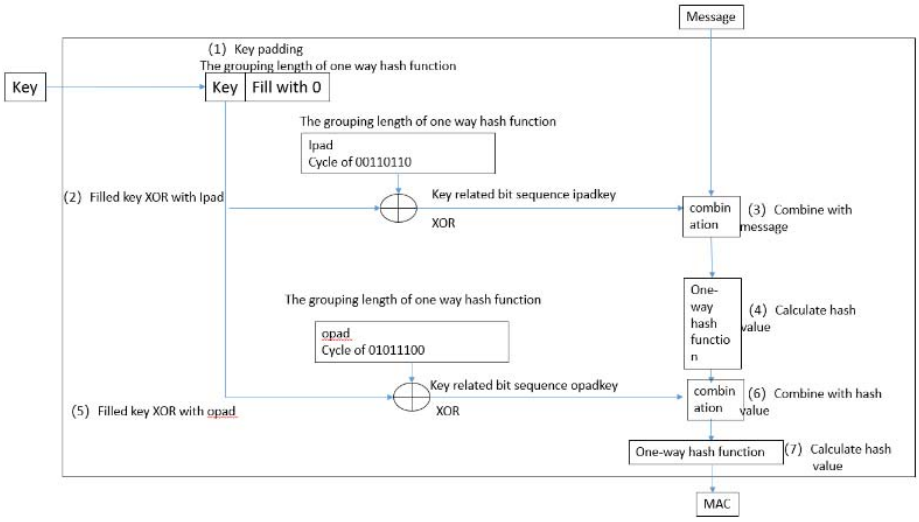

Figure 2. Calculation steps of Hmac_ sha256

IV. ANALYSIS OF THE INFLUENCE OF ENCRYPTION AND DECRYPTION ON THE REAL-TIME PERFORMANCE OF CAN MESSAGES

A. *Space occupancy rate of different algorithms*

For a vehicle-mounted microcontroller, its memory size (RAM and FLASH) is an important index to measure its performance. Insufficient or overflowing memory will cause the vehicle controller to crash. Therefore, it is necessary to know the memory space occupied by various algorithms before applying encryption and decryption algorithms on CAN bus [13].

The ROM space changes before and after calling the algorithm are calculated respectively, so as to determine the space occupied by each algorithm.

1) *Space occupied by AES algorithm*

The memory changes before and after calling OFB mode of AES algorithm are as follows:

(1) before calling OFB mode of AES algorithm

Before calling OFB mode of AES algorithm, the occupied ROM space is 0x4d1c (sixteen mechanisms).

(2) after calling AES algorithm

After calling OFB mode of AES algorithm, it shows that the occupied ROM space is 0x88c2 (sixteen mechanisms).

It is calculated that after calling AES algorithm, 14.9K ROM memory space is used more.

2) *Space occupied by Sha256 algorithm*

The memory changes before and after calling Sha256 algorithm are as follows:

(1) before calling Sha256 algorithm

Before calling Sha256 algorithm, it shows that the occupied ROM space is 0x4d1c (sixteen mechanisms).

(2) after calling Sha256 algorithm

After calling Sha256 algorithm, it shows that the occupied ROM space is 0x5308 (sixteen mechanisms).

According to the calculation, after calling Sha256 algorithm, 1.48K ROM memory space is used more.

3) *Space occupied by HMAC_SHA256algorithm*

The memory changes before and after calling Hmac_sha256 algorithm are as follows:

(1) before calling Hmac_sha256 algorithm

Before calling Hmac_sha256 algorithm, it shows that the occupied ROM space is 0x4d1c (sixteen mechanisms).

(2) after calling Hmac_sha256 algorithm

After calling Hmac_sha256 algorithm, the occupied ROM space is 0x558c (sixteen mechanisms).

According to the calculation, after calling Hmac_sha256 algorithm, 2.11K ROM memory space is used more.

It can be seen from the above that different encryption algorithms occupy space ranging from 2K to 15K, and most microcontrollers will spare this memory at present.

B. Encryption and decryption efficiency of different algorithms

1) calculation steps and principles of encryption and decryption time

1. Test environment

The efficiency of encryption and decryption algorithm is related to chip processing and other hardware environments. this paper calculates the encryption and decryption time of AES algorithm (OFB mode), Sha256 and Hmac_ Sha256 for Infineon chip TC299. Chip TC299 information is shown in Table 1.

TABLE I. PERFORMANCE PARAMETERS OF CHIP TC299

brand name	model	Basic frequency
Infineon	TC299	200MHz

2. Calculation steps

The steps of calculating encryption and decryption time are as follows:

(1) before calling the encryption function, pull up the output voltage; After calling the encryption function, pull down the output voltage;

(2) Check the external logic analyzer and check the encryption time;

(3) before calling the decryption function, pull up the output voltage; After calling the decryption function, pull down the output voltage;

(4) Check the external logic analyzer and check the decryption time;

3. View the results

In the picture below①②③④They represent encryption start time, encryption end time, decryption start time and decryption end time respectively. The logic analyzer can directly calculate the encryption and decryption time.

Figure 3. Schematic diagram of encryption and decryption time

2) Encryption and decryption time analysis

1. OFB mode of AES algorithm

AES algorithm (OFB mode) encrypts and decrypts 8 bytes, 64 bytes and 128 bytes, and the time taken is shown in Figure 4 below.

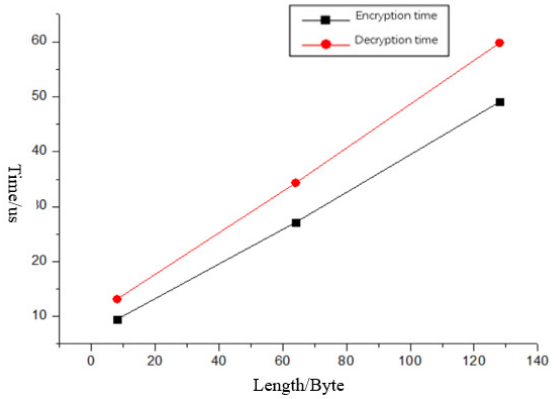

Figure 4. The time taken by AES algorithm (OFB mode) to encrypt and decrypt data of different lengths

It can be seen from the above figure that the encryption time of data with different lengths is different; With the increase of length, the longer it takes to encrypt and decrypt;

For encryption, the encryption length is from 8 bytes to 64 bytes, the encryption time is increased from 9.5µs to 27.12µs, and the encryption time is increased by 185%. The encryption length is from 8 bytes to 128 bytes, the encryption time is increased from 9.5µs to 49.062µs, and the encryption time is increased by 322%. For decryption, the decryption length is from 8 bytes to 64 bytes, the encryption time is increased from 13.19µs to 34.31µs, and the encryption time is increased by 160%. The encryption length is from 8 bytes to 128 bytes, the encryption time is increased from 13.19µs to 59.81µs, and the encryption time is increased by 353%.

2. Sha256

Sha256 encrypts and decrypts 16 bytes, 64 bytes and 128 bytes, and the time taken is shown in Figure 5 below.

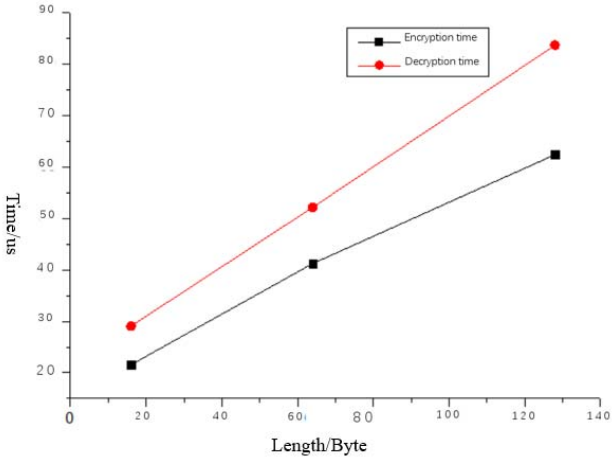

Figure 5. The time taken by sha256 to encrypt and decrypt data of different lengths

It can be seen from the above figure that the encryption time of data with different lengths is different; With the increase of length, the longer it takes to encrypt and decrypt;

For encryption, the encryption length is from 16 bytes to 64 bytes, the encryption time is increased from 21.56μs to 41.25μs, and the encryption time is increased by 91.3%. The encryption length is from 16 bytes to 128 bytes, the encryption time is increased from 21.56μs to 62.44μs, and the encryption time is increased by 190%. For decryption, the decryption length is from 16 bytes to 64 bytes, the encryption time is increased from 29.06μs to 52.19μs, and the encryption time is increased by 79.6%. The encryption length is from 16 bytes to 128 bytes, the encryption time is increased from 29.06μs to 83.72μs, and the encryption time is increased by 188%.

3. Hmac_sha256

Hmac_sha256 encrypts and decrypts 16 bytes, 64 bytes and 128 bytes, and the time taken is shown in Figure X below.

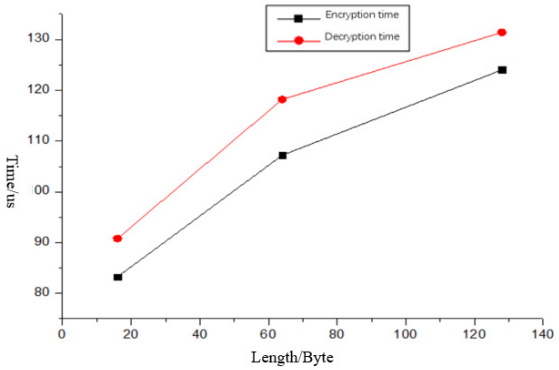

Figure 6. The time taken by Hmac_sha256 to encrypt and decrypt data of different lengths

It can be seen from the above figure that the encryption time of data with different lengths is different; With the increase of length, the longer it takes to encrypt and decrypt;

For encryption, the encryption length is from 16 bytes to 64 bytes, the encryption time is increased from 83.25μs to 107.2μs, and the encryption time is increased by 28.8%. The encryption length is from 16 bytes to 128 bytes, the encryption time is increased from 83.25μs to 124μs, and the encryption time is increased by 48.9%. For decryption, the decryption length is from 16 bytes to 64 bytes, the encryption time is increased from 90.81μs to 118.2μs, and the encryption time is increased by 30.1%. The encryption length is from 16 bytes to 128 bytes, the encryption time is increased from 90.81μs to 131.4μs, and the encryption time is increased by 44.7%.

4. Encryption and decryption time analysis of different algorithms

The time for encrypting and decrypting 8 bytes, 16 bytes, 64 bytes and 128 bytes by AES algorithm, Hmac_sha256 algorithm and sha algorithm, respectively, is shown in Figure 7 and Figure 8 below.

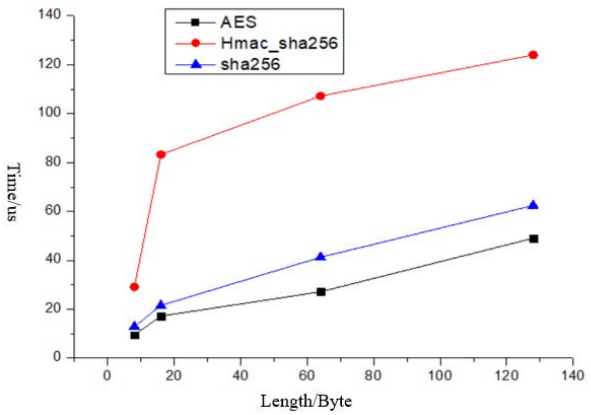

Figure 7. The time taken by different algorithms to encrypt different lengths

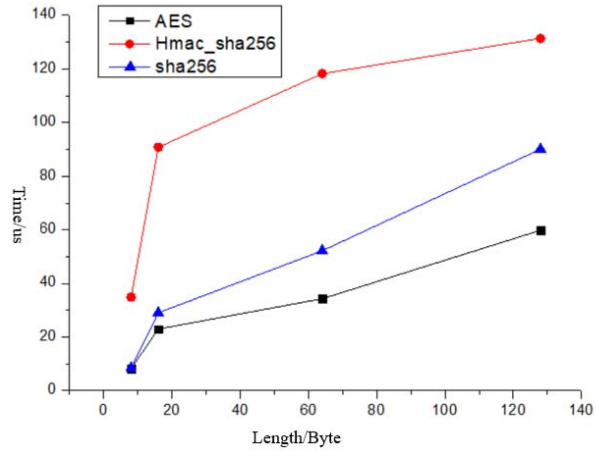

Figure 8. The time taken by different algorithms to decrypt different lengths

It can be seen that the encryption and decryption time of Hmac_sha256 algorithm is obviously longer than that of AES algorithm and sha256 algorithm. The algorithm with the shortest encryption and decryption time is AES algorithm, which is the reason why AES algorithm is widely used at present.

3) Summary

1. symmetric encryption takes far less time than asymmetric encryption;

2. As the length of data to be encrypted and decrypted increases, the required encryption and decryption time also increases;

3. The efficiency of different encryption and decryption algorithms is obviously different, and AES algorithm takes the least time;

4. For the common 8-byte message in the market at present, the set CAN reading period is about 5 ms. The time consumed to encrypt and decrypt it is us level, which will not cause obvious influence on the real-time performance of the bus.

REFERENCES

[1] white paper on China's intelligent networked automobile market and user insight.2018

[2] Intelligent Networked Automotive Architecture and Key Technologies [J]. Wang Jianqiang, Wang Xin. Journal of Chang 'an University (Social Science Edition) .2017 (06)

[3] Analysis of Efficient Optimization Design of Cloud Server [J]. Wang Hang. Enterprise Technology and Development .2018 (12)

[4] Research on Personal Information Protection of Mobile Intelligent Terminal APP Consumers [D]. Feng Ankang. Southwest University of Political Science and Law, 2017

[5] Adaptive CAN Bus Security Mechanism in Vehicle [J]. Chen Ying, Zhong Cheng, Li Xinghua, Jiang Qi, Zhang Huilin, Jing Yuwen. Information Security Research .2019 (12)

[6] Traffic anomaly detection method for flooding attack in Internet of Vehicles [J]. Ethan, Xie Yizhen, Wang Yongjian, Jiang Hong, journal of nanjing university of science and technology.2020 (04)

[7] An Overview of Attacks and Defences on Intelligent Connected Vehicles. [J]. Mahdi Dibaei, Xi Zheng, Kun Jiang,Sasa Maric,Robert Abbas, Shigang Liu, Yuexin Zhang, Yao Deng, Sheng Wen, Jun Zhang, Yang Xiang 0001,Shui Yu. CoRR. 2019

[8] Intelligent Networked Vehicle Security Threat Analysis and Remote Intrusion Research in Complex Network Environment [D]. Yansong Li xidian university 2019

[9] Research on Interest Packet Flooding Attack in Content Center Network [D]. Zhu Hongmei. Chongqing University of Posts and Telecommunications, 2019

[10] TCP/IP network principle and technology [M]. Tsinghua University Publishing House, Zhou Tomorrow, edited by Wang Wenyong, 1993

[11] network performance analysis based on ICMP [J]. Hu Yanping, Wang Lianjie, Liu Wu, Liu Qiming. computer engineering and design .2003 (04)

[12] Efficient protocols for secure broadcast in controller area networks. Groza B,Murvay S. IEEE Transactions on Industrial Informatics . 2013

[13] VeCure:A practical security framework to protect the CAN bus of vehicles. Wang Q,Sawhney S. 2014 International Conference on the Internet of Things . 2014