High-Efficiency Encryption and Authentication Network Security for Automotive Ethernet

Jia-Ming Li, Shuo-Fu, Yu-Jing Wu, and Yi-Nan Xu

***Abstract*—Automotive ethernet has the advantages of high bandwidth, low latency, and strong compatibility, which meets the needs of new energy vehicles for the development of network integration. Automotive ethernet can not only solve the problem of increased wiring harness and complicated wiring in the intelligentization of automotive electronics, but also can improve the comfort, reliability and multiple safety of the car. Although the car is connected to the smart phone, Bluetooth, Internet and other network systems to improve the driving pleasure for the driver, but it brings hacker attacks, security loopholes and other car network security problems that cannot be ignored, which seriously affects the safe driving of the car, personal privacy, and even endanger public safety. In this paper, we focus on the need for the network security of automotive ethernet, and analyses problem in encryption authentication algorithm. An improved AES-128 encryption algorithm and an improved MD5 authentication algorithm are proposed innovatively. Through the experimental simulation of CANoe.Ethernet, the improved AES-128 encryption algorithm proposed in this paper is 15% more efficient than the traditional encryption algorithm, and the improved MD5 authentication algorithm is 4 times faster than the traditional authentication algorithm. Thus, the active network security performance of automotive ethernet is further improved.**

***Index Terms*—Automotive ethernet, network intrusion, data encryption, data authentication, active network security.**

I. Introduction

The concept of automotive ethernet was investigated quite intensively in recent years. Vehicle-mounted bus network technology involves the integration of cross-field technologies such as electronics, communications, computers and automation technology [1]. As the process of automotive electronics and automation continues to accelerate, and technology continues to mature, most vehicles are currently equipped with advanced driver assistance systems (ADAS), entertainment systems, and on-board diagnostic systems (OBD). New energy vehicles such as pure electric vehicles, driverless vehicles, and connected vehicles based on mechatronics and X-by-wire technology have gradually become the development direction of next-generation vehicles [2].

Automotive ethernet is a latecomer in the part representation In-Vehicle bus network. Automotive ethernet is an indispensable network tool in new energy vehicles. Automotive ethernet has the advantages of high bandwidth up to 1G/bps, high reliability, strong anti-interference ability, low latency, and high synchronization. It can replace traditional In-vehicle bus network systems such as LIN, CAN, FlexRay, etc., have become the backbone network of the next generation In-vehicle bus network system. Automotive ethernet can not only solve the problem of increased wiring harness and complicated wiring in the intelligentization of automotive electronics, but also can improve the comfort, reliability and multiple safety of the car. Due to the harsh environment of the car, various electronic products such as the electronic control processing unit, sensor system and cable of the automotive Ethernet are affected by external electromagnetic field interference, vibration, temperature, etc., and the life of the electronic product itself. At the same time, when the automobile electronic control system is connected to external network systems such as WiFi, Bluetooth, OBD II network tester, cellular network, etc., it is easy for hackers to steal In-vehicle bus network information, and invade the automotive ethernet system through remote control to tamper with the important control information of the engine, throttle, brake, steering wheel and other controllers [3]. Therefore, when the vehicle-mounted ethernet system transmits data, it is easy to cause various network failures such as data jumps, data packet loss, node and network link disconnection, resulting in the loss of control systems such as braking systems, steering systems, and advanced driver assistance systems.

Thanks to the integration of multiple networks, connected cars have more abundant in-vehicle information functions and applications. These information functions and applications increase the internal and external access interfaces of the car. At the same time, these interfaces will also become the access points for malicious attacks, and the car information security risk index is also increasing [4]. Therefore, it is necessary to improve the security of the vehicle bus network through network security technology, encryption and authentication algorithms [5]. Automotive ethernet is an important part that directly affects the active safety of automobiles, so the real-time, reliability and safety of automotive ethernet must be guaranteed. So the main emphasis is placed on the problem of on-board bus security.

Since the vehicle bus network is an independent local area network system, computer network security technologies such as firewalls and network keys with a relatively largeamount of calculation are difficult to apply to the vehicle electronic control unit. Literature [6] carried out a remote attack vehicle test and proposed a safety mechanism based on the characteristics of the CAN bus. The test results show that the mechanism has low communication delay and strong load capacity. There have been many attempt to Automotive

Manuscript received September 13, 2021; revised January 13, 2022. This research was supported by National Natural Science Foundation of China (61763047, 62161049).

The authors are with the Division of Electronics and Communication Engineering of Yanbian University, Yanji, China (corresponding author: Yi-Nan Xu*; e-mail: 515894529@qq.com, 1391509814@qq.com, yjwu@ybu.edu.cn, ynxu@ybu.edu.cn).

DOI: 10.7763/IJMO.2022.V12.797

network security experiment. Literature [7] is based on CAN (Controller area network+), uses 15 bytes of the 16 bytes of the data field for message verification, and calculates the signature verification of the data frame through the hash encryption function to achieve communication security authentication. However, since only 1 byte can be used for data transmission, the bus load rate will increase. Literature [8] proposed a lightweight authentication protocol LASAN (Lightweight Authentication for Secure Automotive Networks) based on vehicle network security. The protocol improves the algorithm in terms of ECU authentication and data flow authentication. The experimental results show that the authentication protocol shortens the ECU authentication delay and data stream authentication delay compared with classic methods such as TELSA and TLS. Literature [9] proposed a signal packing method based on the Next Decrease of Fit (NFD) algorithm. Then use the Frame ID (FID) multiplexing method to minimize the number of FIDs. This model can quickly obtain the message schedule of each node, effectively control the message payload size, make the FlexRay static segment message improves the transmission efficiency. Although a lot of effort is being spent on improving these weakness, the efficient and effective method has yet to be developed. So a major thrust of the paper is to discuss approaches and strategies for structuring encryption methods.

In this paper, aiming at the network security of the automotive ethernet, through the analysis of the security requirements of vehicle network communication, the AES-128 encryption algorithm and the MD5 authentication algorithm have been comprehensively improved. The combination of improved AES-128 encryption algorithm and MD5 authentication algorithm can greatly improve security. Detail on improve AES-128 encryption algorithm and MD5 authentication algorithm are discussed in later sections. This paper proceeds as follows. In the second chapter, the basic principles of traditional AES encryption algorithm and MD5 authentication algorithm are introduced. In Section 3, the improved AES-128 encryption algorithm and MD5 authentication algorithm are proposed successively. Section 4 show experimental studies for verifying the proposed model. And uses CANoe. Ethernet dedicated automotive ethernet network design platform to build vehicle bus network architecture and experimental platform, and analyze the results of simulation experiments. Section 5 contains some conclusions plus some ideas for further work.

II. Car Bus Network Security

A. AES Encryption Method

Advanced Encryption Standard (AES) Rijndael created a cryptographic algorithm in 2001. As the highest security standard at present, AES has been widely used in the field of information security [10]. AES uses a block iterative encryption algorithm called Rijndael. Its main features are short key establishment time, good sensitivity, and low memory requirements [11]. The AES algorithm groups the plaintexts. The length of each group of plaintexts is 128 bits. There are three key lengths of 128, 192, and 265 bits, and the corresponding iteration rounds are 10, 12, and 14 respectively.

Each iteration of AES consists of four stages: byte replacement, row shift, column confusion, and round key addition (Fig. 1).

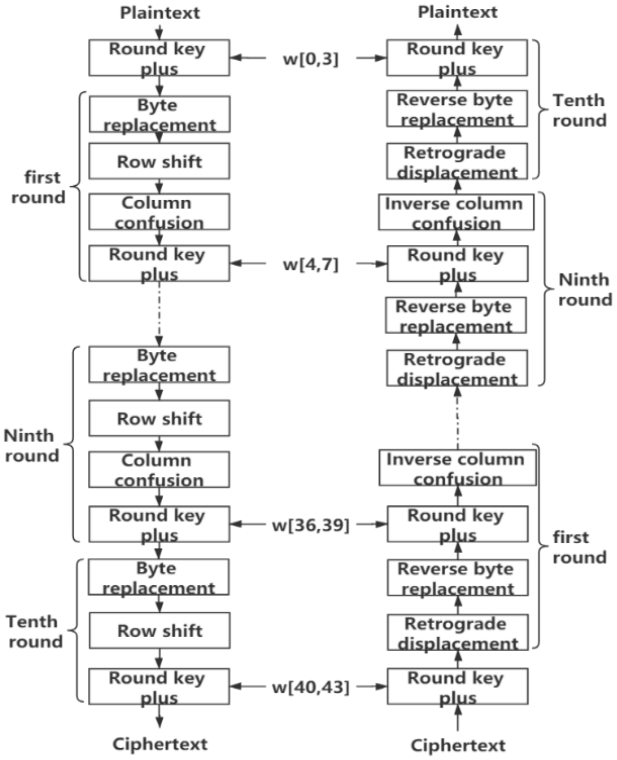

Fig. 1. AES algorithm encryption and decryption flowchart.

Byte replacement uses the S box to map the byte in the state matrix to another byte through a table lookup operation; row shift is a left cyclic shift operation; column confusion is a replacement using arithmetic characteristics in the field GF (2^8); The round key addition is a bitwise XOR operation between the round key and the current group. After the plaintext is grouped, it is XOR with the initial key and then enters n rounds of transformation. The first n-1 round of transformation process is the same. The difference of the nth round of transformation is that the column confusion transformation is no longer performed. The decryption process is the inverse operation of the encryption process. The difference between the algorithm using different key lengths is that the number of iterations n is different.

B. MD5 Authentication Method

MD5 stands for Message-Digest Algorithm 5, which was developed by MIT Laboratory for Computer Science (IT Computer Science Laboratory) and RSA Data Security Inc (RSA Data Security Company). It has gradually developed through MD2, MD3, and MD4. It is a kind of the irreparable conversion assembles data of any length into a 128-bit hash value length, which is a continuous processing system [12]. MD5 algorithm can input variable length information and output fixed length 128-bits. It consists of four 32-bit packets, and cascading these four 32-bit packets will generate a 128-bit hash value.

The MD5 authentication algorithm is classified by three steps: filling, initializing variables, and processing packet data (Fig. 2).

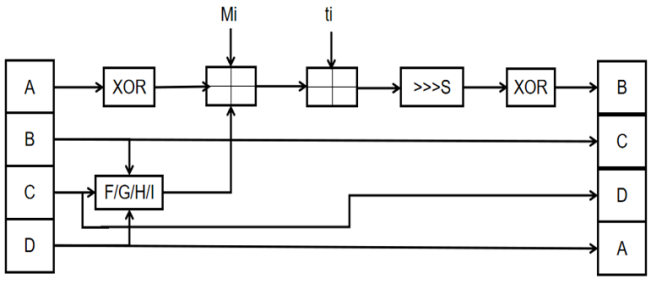

Fig. 2. MD5 authentication algorithm flow.

In the filling module, the input information needs to be filled first, so that the result of the remainder of the bit length of 512 is equal to 448, and the bit length of the information will be expanded to N*512+448. N is a non-negative integer, and N can be zero [13]; In the initialization variable module, the initial 128-bit value is the initial test link variable. These parameters are used in the first round of calculation. The values of variables A, B, C, and D in the program are: A=0x01234567, B= 0x89ABCDEF, C=0xFEDCBA98, D=0x76543210; In the processing packet data module, the MD5 algorithm operation consists of similar 64 cycles, divided into 4 groups of 16 times. The first grouping needs to copy the four link variables of A, B, C, and D into the other four variables, namely, A to a, B to b, C to c, and D to d. The variables starting from the second grouping are the results of the previous grouping, namely A = a, B = b, C = c, D = d. The main loop has four rounds, and each round is very similar. In the first round, 16 operations are performed. Each operation performs a nonlinear function operation on three of a, b, c, and d, and then adds the result to the fourth variable, a subgroup of the text and a constant. Then move the result to the left by an indefinite number, and add one of a, b, c, or d. Finally, replace one of a, b, c, or d with the result. Among them, F is a non-linear function, and a function is operated once. Mi represents a 32-bit input data. ti represents a 32 bits constant, which is used to complete different calculations each time.

Formula (1) is the four nonlinear functions used in each operation.

$$\begin{aligned} F(X,Y,Z) &= (X \wedge Y) \vee (X \wedge Z) \\ G(X,Y,Z) &= (X \wedge Z) \vee (Y \wedge \bar{Z}) \\ H(X,Y,Z) &= (X \oplus Y \oplus Z) >>> 1 \\ I(X,Y,Z) &= X \vee Z \oplus Y) \end{aligned} \tag{1}$$

If the corresponding bits of X, Y, and Z are independent and uniform, then each bit of the result is also independent and uniform. F is a function of bitwise operation. That is, if X, then Y, otherwise Z. Function H is a bit-wise parity operator.

Let Mk denote the k-th subgroup of the message (from 0 to 15) ，<<S means to rotate the left S bit.

Then the four operations can be described as formula (2).

$$\begin{aligned} &FF(a,b,c,d,Mi,s,ti) \to a = b + ((a + F(b,c,d) + Mi + ti << s) \\ &GG(a,b,c,d,Mi,s,ti) \to a = b + ((a + G(b,c,d) + Mi + ti << s) \\ &HH(a,b,c,d,Mi,s,ti) \to a = b + ((a + H(b,c,d) + Mi + ti << s) \\ &II(a,b,c,d,Mi,s,ti) \to a = b + ((a + I(b,c,d) + Mi + ti << s) \end{aligned} \tag{2}$$

Fig. 3 is the cyclic process of the MD5 algorithm. After the loop operation is over, add A, B, C, and D to a, b, c, and d respectively, that is, a = a + A, b = b + B, c = c + C, d = d + D. The next packet data continues to run the above algorithm. Finally, a 128-bit hash value is obtained.

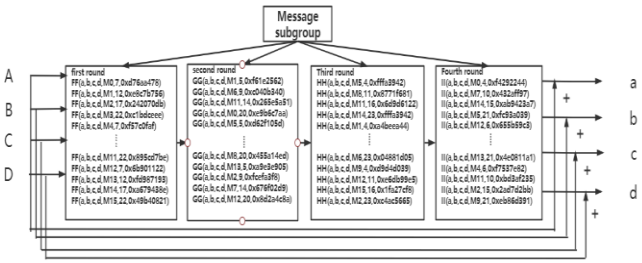

Fig. 3. MD5 algorithm cycle process.

III. Improved Encryption and Authentication Methods

A. Improved AES-128 Encryption Algorithm

Except for the last round of the AES algorithm, the remaining nine rounds have undergone four complete transformations (byte replacement, row displacement transformation, column confusion transformation, and round key addition). This article optimizes the first nine rounds of the same transformation, combining row shift transformation and column confusion transformation into row-column transformation, which will improve the efficiency of the encryption process in the AES algorithm.

The state matrix after byte replacement transformation is formula (3):

$$S = \begin{pmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{pmatrix} \tag{3}$$

The state matrix after row displacement transformation and column confusion transformation is formula (4):

$$S' = \begin{pmatrix} S_{00}' & S_{01}' & S_{02}' & S_{03}' \\ S_{10}' & S_{11}' & S_{12}' & S_{13}' \\ S_{20}' & S_{21}' & S_{22}' & S_{23}' \\ S_{30}' & S_{31}' & S_{32}' & S_{33}' \end{pmatrix} \tag{4}$$

Thus, the relation matrix formula (5) is obtained.

$$S' = \begin{pmatrix} S_{00}' & S_{01}' & S_{02}' & S_{03}' \\ S_{10}' & S_{11}' & S_{12}' & S_{13}' \\ S_{20}' & S_{21}' & S_{22}' & S_{23}' \\ S_{30}' & S_{31}' & S_{32}' & S_{33}' \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{pmatrix} \tag{5}$$

Among them, the element operation is described by formula (6):

$$
\begin{aligned}
&S_{00}'=2S_{00}+1S_{11}+3S_{22}+1S_{33}, S_{01}'=2S_{01}+1S_{12}+3S_{23}+1S_{30},\\
&S_{02}'=2S_{02}+1S_{13}+3S_{20}+1S_{31}, S_{03}'=2S_{03}+1S_{10}+3S_{21}+1S_{32},\\
&S_{10}'=1S_{00}+2S_{11}+1S_{22}+3S_{33}, S_{11}'=1S_{01}+2S_{12}+2S_{23}+1S_{30},\\
&S_{12}'=1S_{00}+2S_{13}+1S_{20}+3S_{31}, S_{21}'=3S_{01}+1S_{12}+2S_{23}+1S_{30},\\
&S_{20}'=3S_{00}+1S_{11}+2S_{22}+1S_{33}, S_{23}'=3S_{03}+1S_{10}+2S_{21}+1S_{32},\\
&S_{22}'=3S_{02}+1S_{13}+2S_{20}+1S_{31}, S_{31}'=1S_{01}+3S_{12}+1S_{23}+2S_{30},\\
&S_{30}'=1S_{00}+3S_{11}+1S_{22}+2S_{33}, S_{33}'=1S_{03}+3S_{10}+1S_{21}+2S_{32},\\
&S_{32}'=1S_{02}+3S_{13}+1S_{20}+2S_{31},
\end{aligned}
\tag{6}
$$

Thus the vector transformation matrix formula (7) is obtained:

$$
\begin{pmatrix} S_{00}' \\ S_{01}' \\ S_{02}' \\ S_{03}' \\ S_{10}' \\ S_{11}' \\ S_{12}' \\ S_{13}' \\ S_{20}' \\ S_{21}' \\ S_{22}' \\ S_{23}' \\ S_{30}' \\ S_{31}' \\ S_{32}' \\ S_{33}' \end{pmatrix} = \begin{pmatrix} 2&0&0&0&0&1&0&0&0&0&3&0&0&0&0&1 \\ 0&2&0&0&0&0&1&0&0&0&0&3&1&0&0&0 \\ 0&0&2&0&0&0&0&1&3&0&0&0&0&1&0&0 \\ 0&0&0&2&1&0&0&0&0&3&0&0&0&0&1&0 \\ 1&0&0&0&0&2&0&0&0&0&1&0&0&0&0&3 \\ 0&1&0&0&0&0&2&0&0&0&0&1&3&0&0&0 \\ 0&0&1&0&0&0&0&2&1&0&0&0&0&3&0&0 \\ 0&0&0&1&2&0&0&0&0&1&0&0&0&0&3&0 \\ 3&0&0&0&0&1&0&0&0&0&2&0&0&0&0&1 \\ 0&3&0&0&0&0&1&0&0&0&0&2&1&0&0&0 \\ 0&0&3&0&0&0&0&1&2&0&0&0&0&1&0&0 \\ 0&0&0&3&1&0&0&0&0&2&0&0&0&0&1&0 \\ 1&0&0&0&0&3&0&0&0&0&1&0&0&0&0&2 \\ 0&1&0&0&0&0&3&0&0&0&0&1&2&0&0&0 \\ 0&0&1&0&0&0&0&3&1&0&0&0&0&2&0&0 \\ 0&0&0&1&3&0&0&0&0&1&0&0&0&0&2&0 \end{pmatrix}
\tag{7}
$$

The row displacement transformation and column confusion transformation of the AES algorithm are combined into row and column transformation. Suppose$16*16$, the vector transformation matrix is R,Then the rank transformation can be expressed as $S'=R\otimes S$ .The encryption flow chart after optimizing the AES algorithm is shown in Fig. 4.

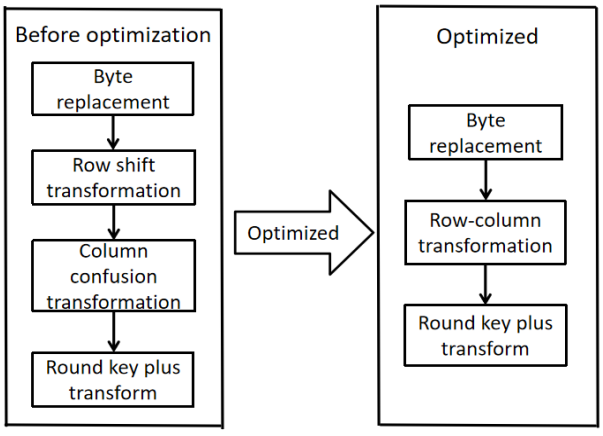

Fig. 4. Flowchart before and after round transformation optimization.

Aiming at the AES-128 encryption algorithm, this paper compares the functions of the AES encryption algorithm before and after optimization. Table I is a time-consuming comparison table before and after optimization. Figure 5 is a performance comparison chart before and after optimization. The optimized AES encryption algorithm is 15% more efficient than the traditional algorithm.

TABLE I: TIME-CONSUMING COMPARISON TABLE BEFORE AND AFTER OPTIMIZATION

Times	TraditionalAES-128	Improved AES-128
100	212ms	182ms
200	220ms	190ms
300	207ms	181ms
400	215ms	177ms
500	209ms	180ms

Fig. 5. Performance comparison chart before and after optimization.

B. Improved MD5 Authentication Algorithm

Combined with the characteristics of the vehicle bus network, this article improves the MD5 authentication algorithm. Since the output of the MD5 authentication algorithm is a hash value with a fixed number of 128 bits, the length of the output value does not change and the flexibility of the tutor becomes worse. This paper changes from a fixed 128-bit to a variable-length combination of 32-bit and 64-bit.The cycle rule is based on the MD5 authentication algorithm flow, and the output value is changed from a fixed 128-bit to a variable-length 32-bit, 64-bit, and 128-bit.Fill any input message value into groups and divide them into 512-bit groups. After 64 rounds, the final output length can be changed with the user's message digest. So as to meet the periodicity, cyclicality and real-time performance requirements of the vehicle bus network.

The improved MD5 authentication algorithm proposed in this paper is divided into the following four steps:

1) In the filling module part, the steps are the same as the original MD5 algorithm.
2) Initialize the variable part, at the beginning of the hash calculation, first set the initial value of the A, B, C, and D registers, the initial value is the square root of the smallest 4 prime numbers（$\sqrt{2}$、$\sqrt{3}$、$\sqrt{5}$、$\sqrt{7}$） The decimal part of the binary representation is composed of the first 64 bits.
3) In the calculation of the message digest part. The algorithm generates a total of 64 words. First, the 512-bit message is decomposed into 16 32-bit words, denoted as w[0], …, w[15], and the remaining 48 words are obtained by iterative formula (8).

$$Ti=\sigma_1(T_{i-2})+T_{i-7}+\sigma_0(T_{i-15})+T_{i-16} \tag{8}$$

In the processing of packet data, the main loop has a total of 4 rounds, each with 16 operations. In each operation, first assign the 4 link variables A, B, C, and D to the variables a, b, c, and d. Then perform a nonlinear function operation of formula (9) on the assigned variables (a, b, c, d) and the constants Mj, ti (ti=2^64* |sin(i)|) and variable s, and Replace a, b, c, and d with the result of the calculation.

The following are the four nonlinear functions used in each operation (one for each round).

$$\begin{aligned} F(X,Y,Z) &= (X \wedge Y) \vee (X \wedge Z) \\ G(X,Y,Z) &= (X \wedge Z) \vee (Y \wedge \bar{Z}) \\ H(X,Y,Z) &= (X \oplus Y \oplus Z) >>> 1 \\ I(X,Y,Z) &= X \vee Z \oplus Y) \end{aligned} \tag{9}$$

In formula (9), we improved the nonlinear functions H and I. The change of H shifts the output of the XOR one bit to the right, which plays a role of pre-diffusion and improves the speed of the avalanche effect. Changing G from $(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$ to $(X \wedge Y) \vee (Y \wedge \bar{Z})$ can reduce the symmetry of the second-cycle nonlinear function. The non-linear function $I(X,Y,Z) = X \vee \bar{Z} \oplus Y$ is improved to$I(X,Y,Z) = X \vee Z \oplus Y$ reduce the symmetry of the fourth loop of the non-linear function and further increase the running speed.

Let Mk denote the *k-th* subgroup of the message (from 0 to 15). <<S represents the left S position of the cycle, then there are four operation is formula (10):

$$Z` \tag{10}$$

In order to make the output length of the MD5 authentication algorithm variable, this paper proposes the following scheme:

1) Level 1: The length of the output hash value is 32 bits. but,$T = A \oplus B \oplus C \oplus D$. Among them, A, B, C, and D are the values in the registers after 64 iterations.
2) Level 2: When the length of the output hash value is 64bit, the message is divided into two groups. When the first group of messages is completed, it is marked as T1, and when the second group of messages is completed, it is marked as T2,$T1 = A \oplus B \oplus C \oplus D$,$T2 = A \oplus B \oplus C \oplus D$. The output result T is the sequential splicing of T1 and T2.
3) Level 3: When the length of the output hash value is 128bit, the message is divided into four groups, and the message output results are respectively marked as T1, T2, T3, and T4.$T1 = A \oplus B \oplus C \oplus D$,$T2 = A \oplus B \oplus C \oplus D$, $T3 = A \oplus B \oplus C \oplus D$, $T4 = A \oplus B \oplus C \oplus D$. The output result T is the sequential splicing of T1, T2, T3, and T4.

The authentication speed of level 1 is four times that of the traditional MD5 algorithm, and the authentication speed of level 2 is twice that of the traditional MD5 algorithm. The authentication speed of Level 3 is the same as that of the traditional MD5 algorithm. Compared with the traditional MD5 algorithm, the optimized MD5 algorithm further improves the authentication efficiency and security performance.

This paper has done 100 avalanche effect experiments on the optimized MD5 and traditional MD5 authentication algorithms. The experimental results are shown in Figs. 6 and 7.

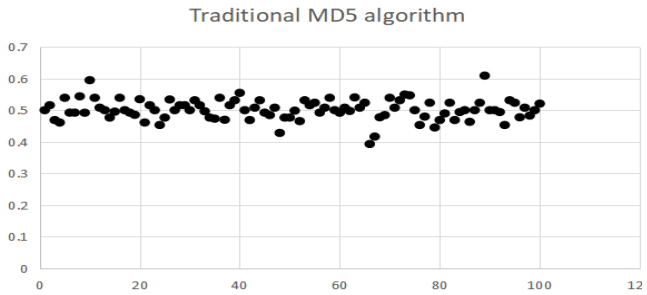

Fig. 6. The experimental results of the traditional MD5 avalanche effect.

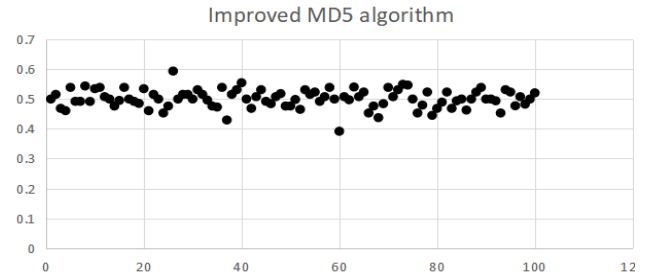

Fig. 7. The improved MD5 avalanche effect experimental results.

The point in the figure refers to the proportion of the same position in the result of a pair of plaintexts with different digits in the total digits. According to the description of the avalanche effect, the closer to 50%, the better the avalanche effect. Then we stipulate that the percentage is greater than 55% and the points smaller than 45% are dead pixels. We think that such a point affects the security of the algorithm. Through statistics, it is found that the probability of bad pixels of the traditional MD5 authentication algorithm is 5%, and the probability of bad pixels of the improved MD5 authentication algorithm proposed in this paper is 3%.

IV. Simulation Experiment

This paper uses the improved AES-128 encryption algorithm and the improved MD5 authentication algorithm for the video files of the automotive ethernet to give a network security flowchart as shown in Fig. 8.

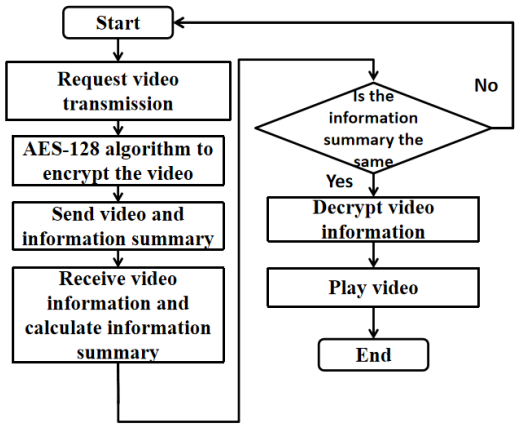

Fig. 8. Network security flowchart.

Before transmitting the video, the Sender and the receiver share the MD5 key K0 and the AES-128 key K1. When the sender receives the video request from the receiver, it uses the key K1 to encrypt the video file, then uses the key K0 to generate an information digest, and then sends the encrypted video and the information digest to the receiver.

After receiving the video sent by the sending end, the receiving end first uses the key K0 to calculate the information digest of the received file, and then compares the information digest value calculated by the receiving end with the information digest value of the sending end. If the two are the same, the receiving end uses the key K1 to decrypt and play the video. If they are inconsistent, the current file is deleted and the sending end is requested to resend.

This text carries on the hardware simulation to the improved AES-128 encryption algorithm and the improved MD5 authentication algorithm through CANoe.Ethernet automotive ethernet design platform. Figure 9 shows the network topology of the automotive ethernet. Among them, HU is a vehicle-mounted video player module, CAMF is a video encryption and authentication function module, and ethernet is an ethernet bus with vehicle-mounted multimedia functions.

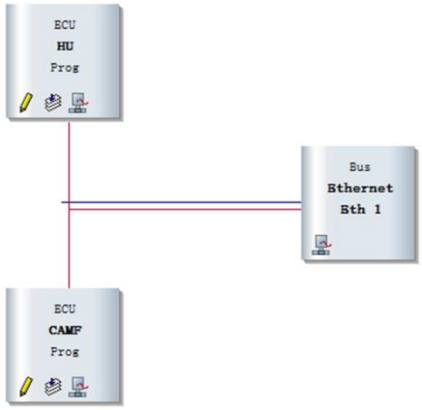

Fig. 9. Network topology.

Fig. 10 shows the result of playing a video with a size of 2.8M after being encrypted and authenticated.

Fig. 10. Video playback simulation results.

Experiments show that after the video has passed the AES-128 encryption algorithm and MD5 authentication algorithm, there is no freeze or delay. Therefore, on the premise that the video can be played normally, it is ensured that the video transmission is not tampered with and attacked, which greatly improves the security of the video transmission.

V. Conclusion

Automotive ethernet is an important part that directly affects the active safety of automobiles, It is also an important direction for the development of human science and technology. so the real-time, reliability and safety of automotive ethernet must be guaranteed. On-board bus security is a difficult problem, yet to be adequately resolved Much work has been studied recently in this field. This paper proposes an improved AES encryption algorithm and MD5 authentication algorithm for the network security of automotive Ethernet. And use CANoe.Ethernet automotive ethernet design platform to verify the performance of the improved AES encryption algorithm and MD5 authentication algorithm. On the basis that there is no stutter or delay in the video, the improved AES encryption algorithm proposed in this paper increases the efficiency by 15%, and the speed of the improved MD5 authentication algorithm is increased by 4 times. It further improves the real-time, security and reliability performance of the automotive ethernet.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Jia-Ming Li and Shuo Fu: Methodology and writing of original draft; Yu-Jing Wu: Software and formal analysis; Yi-Nan Xu: Conceptualization and supervision.

Acknowledgment

This research was supported by National Natural Science Foundation of China (61763047, 62161049).

References

[1] R. Zalman and A. Mayer, "A secure but still safe and low cost automotive communication technique," in *Proc. 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp .1-5, Germany, 2014.

[2] S. S. Karanki and M. S. Khan, "SMMV: Secure multimedia delivery in vehicles using rode side infrastructure," *Vehicular Communications*, pp. 40-44, USA, 2016.

[3] L. Zhou, S. G. Du, and H. J. Zhu, "Location privacy in usage-based automotive insurance: Attacks and countermeasure," *Journal of Latex Class Files*, vol. 14, no. 8, pp. 1-3, 2016.

[4] S. Mortazavi, D. Schleicher, and F. Gerfers, "Modeling and verification of automotive multi-gig ethernet communication up to 2.5 gbps and the corresponding EMC analysis," in *Proc. 2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI & PI)*, pp. 329-334, USA, 2018.

[5] H. Yang, M. Z. Liu, Y. H. Xu, Y. J. Wu, and Y. N. Xu, "Research of automotive ethernet security based on encryption and authentication method," *International Journal of Computer Theory and Engineering*, vol. 11, no. 1, pp. 1-5, 2019.

[6] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-14, Korea, 2014.

[7] A. V. Herrewege and D. S. VerbauwhedeI, "CANAuth-A simple, backward compatible broadcast authentication protocol for CAN bus," *ECRYPT Workshop on Lightweight Cryptography*, pp. 20-26, Belgium, 2011.

[8] P. Mundhenk and A. Paverd, "Security in automotive networks: Lightweight authentication and authorization," *ACM Transaction on Design Automation of Electronic Systems*, vol. 22, no. 25, pp. 1-27, 2017.

[9] S. Jin, M. Z. Liu, Y. J. Wu, Y. H. Xu, J. N. Jiang, and Y. N. Xu, "Research of message scheduling for in-vehicle FLEXRAY network static segment based on next fit decreasing (NFD) algorithm," *Applied Science*, vol. 8, no. 2071, pp. 1-13, 2018.

[10] K. D. B. Utama, Q. M. R. Al-Ghazali, L. I. B. Mahendra, and G. F. Shidik, "Digital signature using MAC address based AES-128 and SHA-2 256-bit," in *Proc. 2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*, pp. 72-78, Indonesia, 2017.
[11] R. Andriani, S. E. Wijayanti, and F. W. Wibowo, "Comparison of AES 128, 192 and 256 bit algorithm for encryption and description file," in *Proc. 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, pp. 120-124, Indonesia, 2018.
[12] S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," in *Proc. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 856-860, India, 2017.
[13] K. Quist-Aphetsi and M. C. Xenya, "Node to node secure data communication for IoT devices using diffie-hellman, AES, and MD5 cryptographic schemes," in *Proc. 2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, pp. 88-92, Ghana, 2019.

Jia-Ming Li was born in Heilongjiang province of China.

He received the bachelor degree in communication engineering from YanBian University, China, in 2019. He is a currently working toward a master degree in the area of In-vehicle network, which include the design of security architecture of automotive Ethernet.

Shuo Fu was born in Shandong province of China.

He is a currently working toward a bachelor degree in the communication engineering of Yanbian University, Yanji, China. His research include the in-vehicle network.

Yu-Jing Wu was born in Jilin province of China. She received her M.S. and Ph.D in electronic and information engineering from Chonbuk National University, South Korea, in 2013 and 2016, respectively.

She is a lecturer of the division of electronic and communication engineering of Yanbian University, China. Her research interests include the In-vehicle communication networks.

Yi-Nan Xu was born in Jilin province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, Korea, in 2009.

He is a professor of the Division of Electronics and Communication Engineering of Yanbian University, Yanji, China.

His research interests include the in-vehicle communication network and automobile electronic control.