Research of Automotive Ethernet Security Based on Encryption and Authentication Method

Hua Yang, Meng-Zhuo Liu, Yi-Hu Xu, Yu-Jing Wu, and Yi-Nan Xu

***Abstract*—With the continuous maturity of automotive electronics and automation technologies, cars have provided drivers more driving entertainment by getting connected to smart phones, Bluetooth and the Internet, but it also brings hacker attacks, security vulnerability and other secure issues which cannot be ignored, these issues will seriously affect vehicle drives safety, personal privacy, and even endanger public safety. Automotive Ethernet have feature of high rate, so it can be applied to multimedia systems in cars. However, car bus system and the multimedia system are connected to each other through the Gateway system make the CAN (Controller Area Network), FlexRay and other vehicle bus network systems no longer independent and secure, so the security of the Automotive Ethernet must be guaranteed. In this paper ,we present a vehicle Ethernet network model, and introduces the AES-128 encryption algorithm and HMAC-SHA1 security authentication method and technology into the vehicle Ethernet system, that effectively preventing external intrusion, data hopping, and other possibility, further improved network security performance of automotive Ethernet and car bus networks.**

***Index Terms*—Automotive Ethernet, data encryption, cyber security, video transmission, bus network.**

I. Introduction

With the continuous development of technology, intelligence and networking of automobiles, the number of electronic products in the car is increasing, the electronic control system in the car is becoming more and more complex, and the number of ECUs (Electronic Control Units) is also constantly increasing [1]. At the same time, ADAS (automobile assisted driving system), high-definition car entertainment system, car networking system, cloud service, big data and other emerging technologies are applied to the car, so the requirements for the bandwidth of the car network are getting higher and higher [2]. Automotive Ethernet system can meet satisfying the network broadband needs of smart cars. The car bus network is not only connected to various ECUs in the car, but also connected to the driver's smart phone, Bluetooth, Internet, vehicle to vehicle communication systems, etc., so the car bus network is vulnerable to external hacking intrusion, network vulnerabilities attack, etc., this causes the car to lose its basic function of braking and turning lights [3]. Therefore, it is necessary to ensure the safety and reliability of the vehicle network.

In recent years, more and more cases have shown that the car bus network is not independent and safe. The car bus network can be easily invaded. If not guarded, the intruder can tamper the data on the bus at will [4]. Therefore, it is necessary to adopt network security technologies, such as encryption and authentication to improve the security of the vehicle bus network [5].

At present, the vehicle bus communication protocols LIN, CAN, FlexRay and so on which commonly used in automobiles do not consider network security issues, but the network security technology of the automobile bus network is the basic condition for ensuring the safe operation of automobiles [6]. In recent years, many scholars have reviewed a series studies focus on the network security of car bus networks. In [7], for the weakness of that the on-board diagnostic interface OBD-II is vulnerable to hacking, presented a hardware network architecture consist of the network on chip (NoC) and hardware firewall. The architecture is used between the OBD-II interface and the CAN (Controller Area Network) controller to determine whether the visitor is legal by authenticating the ID information of the visitor in the NoC, once the identity of the visitor is not authenticated, the firewall will blocks the visitor's any access. The experiment simulates multiple attacks can be used by hackers and the architecture can well prevent hacker attacks while the CAN bus system remains stable. In [8], a method for detecting hacker intrusion is proposed for the network security problem of CAN bus. By calculating the information entropy generated during the ECU clock drift process to determine whether there is hacking, once the wrong information entropy result value is detected, it can be judged that a hacker has invaded the vehicle network. Literature [9] comprehensively analyzes the various ways in which hackers attack in-vehicle networks and the threats to cars after they successfully invade the in-vehicle network, so lightweight encryption protocols play an important role in vehicle network security issues. For the problem of lightweight encryption protocol, the literature [10] proposed a Lightweight Authentication for Secure Automotive Networks (LASAN) based on vehicle network security. The protocol improves the algorithm in terms of ECU authentication and data stream authentication. The experimental results show that the authentication protocol shortens the ECU authentication delay and data stream authentication delay compared to classical methods such as TELSA and TLS.

In-vehicle network security technology is one of the important contents to ensure the safety performance of automobiles. Therefore, it is necessary to conduct network failure detection and network security research for the vehicle Ethernet system. In this paper, the advanced security encryption algorithm AES-128 and the key hash authentication algorithm HMAC-SHA1 are combined to

Manuscript received December 10, 2018; revised February 20, 2019. This work was supported by the National Natural Science Foundation of China (61763047).

The authors are with the College of Engineering of Yanbian University, Yanji, 133002, China (e-mail: ynxu@ybu.edu.cn).

DOI: 10.7763/IJCTE.2019.V11.1230

realize a network security architecture system of the vehicle Ethernet. And we used CANoe.Ethernet experimental platform to simulate the encryption authentication and transmission process of video information in the vehicle Ethernet system.

The second chapter of this paper introduces the design process and operation process of AES-128 advanced encryption algorithm. The third chapter introduces the HMAC authentication algorithm and describes the operation steps of the HMAC-SHA1 authentication algorithm. In the fourth chapter, we combine the AES-128 encryption algorithm and the HMAC-SHA1 authentication algorithm, then use them in the vehicle Ethernet system, and carry out the simulation experiment. Finally, the fifth chapter is the conclusion and prospect of our experiment.

II. AES-128 Algorithm

The AES (Advanced Encryption Standard) encryption algorithm is based on the Rijmen algorithm; it has the characteristics of stable and security, fast operation, small memory consumption, and easy implementation, so it can be used in various network environments.

The key length of the AES encryption algorithm allows setting of 128 bits, 192 bits, 256 bits. In this paper, considering the factors of video information transmission capacity and consumption time of AES encryption algorithm in the car Ethernet system, we apply the AES-128 encryption algorithm to the car Ethernet system.

The AES encryption algorithm has five units of measurement which include bits, bytes, words, groups, and states. The word is composed of 4 bytes, so it can be arranged in a matrix by row or column. The AES is grouped into 128 bits, which is represented as a row matrix consisting of 16 row bytes. The state is used to represent the data groups before and after each step of encryption, and can form a 4 × 4 bytes matrix. The encryption and decryption process of the AES-128 algorithm requires ten rounds of operation. The flow chart of the encryption and decryption process is shown in Fig. 1.

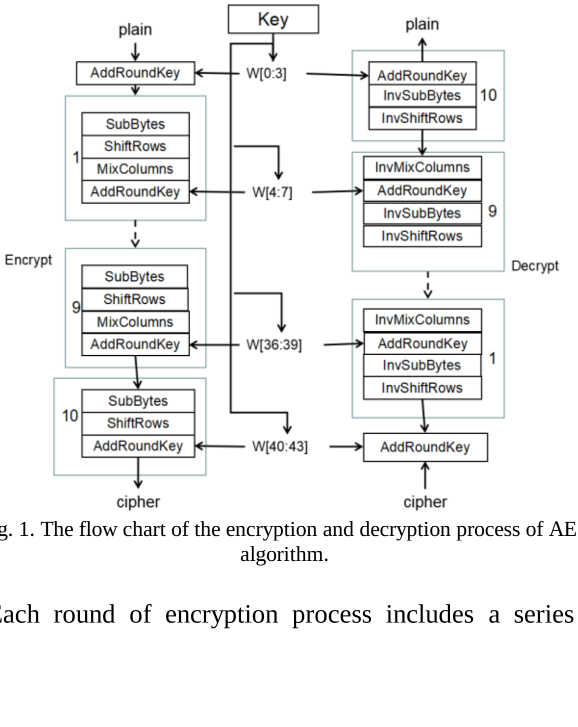

Fig. 1. The flow chart of the encryption and decryption process of AES algorithm.

Each round of encryption process includes a series of substitution and mixture operations. Each round of operations includes four stages: byte substitution (Sub Bytes), column confusion (Mix Columns), line displacement (Shift Rows), and round key addition (Add Round Key).

The sub bytes is a non-linear permutation based on S-box, it can replace each byte of the input or output intermediate state by simply looking up table and transform it into another byte. The S-box is a fixed matrix of 16 rows and 16 columns. When mapping, the upper four bits of the input byte are used as the row value of the S box, and the lower four bits are used as the column values, and then the elements of the corresponding row and column in the S-box are taken as outputs.

The mix columns is to confuse the input state. The method is as shown in formula (1).

$$a'(x) = b(x) \bullet a(x) \bmod (x^4 + 1) \qquad (1)$$

where $a(x)$ and $a'(x)$ respectively indicate the state before the Mix Columns and after it. In the formula (1), $b(x) = \{03\} \bullet x^3 + \{02\} \bullet x^2 + \{01\} \bullet x$ .The number in the brackets is the byte. So,

$$a'(x) = a'_{0,c} + a'_{1,c} \bullet x + a'_{2,c} \bullet x^2 + a'_{3,c} \bullet x^3 \qquad (2)$$

$$a(x) = a_{0,c} + a_{1,c} \bullet x + a_{2,c} \bullet x^2 + a_{3,c} \bullet x^3 \qquad (3)$$

In formula (2) and (3), $a'(x)$ represents the sum of the coefficients of the term with the exponent equal to 0 after multiplication which the index of x $\bmod(x^4 + 1)$. Use the formula $x^i \bmod (x^4 + 1) = x^{i \bmod 4}$ we can get formula (4),

$$\begin{aligned} a'(x) &= \{02\}a_{0,c} + \{03\}a_{1,c} + \{01\}a_{2,c} + \{01\}a_{3,c} \\ &= \begin{bmatrix} 02 & 03 & 01 & 01 \end{bmatrix} \begin{bmatrix} a_{0,c} \\ a_{1,c} \\ a_{2,c} \\ a_{3,c} \end{bmatrix} \end{aligned} \qquad (4)$$

The number in the braces is the byte. The specific process can be represented by a matrix operation (5).

$$\begin{bmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \qquad (5)$$

The Shift Rows is a row-based cyclic shift operation, and Fig. 2 shows the row shifting process. Where a and a' indicate the state before the row displacement and after the row displacement. One state from top to bottom is line 0, line 1, line 2 and line 3. In the Shift Row, the 0th line of a state is unchanged, the 1st line shift to left by one byte, the 2nd line is shift 2 bytes to the left, and the 3rd line is shift to left by 3 bytes.

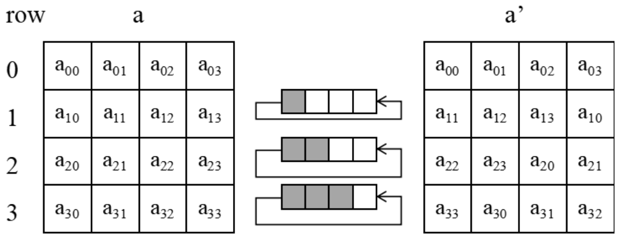

Fig. 2. Shift rows process.

The Add Round Key transformation is a bitwise XOR operation of each column of the input or intermediate state S with a key. Each round of key composed by N_b words, the c-th round key word of the r-th round is expressed as $w_{[r*N_b+c]}$ .The Add Round Key transformation can be expressed as formula (6):

$$\left[S'_{0,c},S'_{1,c},S'_{2,c},S'_{3,c}\right]=\left[S_{0,c},S_{1,c},S_{2,c},S_{3,c}\right]\oplus w_{[r*N_b+c]} \quad (0\le r\le N, 0\le r\le N_b) \qquad (6)$$

The AES decryption process is the inverse of the encryption process and also requires ten rounds of operation. And each round of operations needs to go through four stages of Inverse Sub Bytes, Inverse Shift Rows, Inverse Mix Columns and Add Round Key.

The inverse sub bytes is the inverse of Sub Bytes, and the value of the alternate output is obtained by querying the S-1 box. The S-1 box is also a fixed matrix of 16 rows and 16 columns. When mapping, the upper four bits of the input byte are used as the row value of the S-1 box, and the lower four bits are used as the column values, and then the elements of the corresponding row and column in the S-1 box are taken as outputs.

The inverse shift rows are the opposite of row displacement. The Inverse Shift Rows shifts the last three rows of the 4×4 matrix in opposite directions. That is, the 0th line remains unchanged, the 1st line is cyclically shifted by one byte to the right, the 2nd line is cyclically shifted by 2 bytes to the right, and the 3rd line is cyclically shifted to the right by 3 bytes.

The inverse mix columns have similar processing with Mix Columns, while each column value is multiplied by a fixed polynomial b(x), which is defined by polynomial (7).

$$a'(x)=c(x)\bullet a(x)\bmod(x^4+1) \qquad (7)$$

$c(x)$ is the inverse of $b(x)\bmod(x^4+1)$ in the Mix Columns , so we can get formula (8).

$$b(x)\bullet c(x)=\left(\{03\}\bullet x^3+\{01\}\bullet x^2+\{01\}\bullet x+\{02\}\right)\bullet d(x)\equiv 1\bmod(x^4+1) \qquad (8)$$

Then we get formula (9).

$$c(x)=\{0b\}\bullet x^3+\{0d\}\bullet x^2+\{09\}\bullet x+\{0e\} \qquad (9)$$

For the inverse mix columns process, equation (10) is the matrix representation of the Inverse Mix Columns process.

$$\begin{bmatrix}a_0\\a_1\\a_2\\a_3\end{bmatrix}=\begin{bmatrix}0e & 0b & 0d & 09\\09 & 0e & 0b & 0d\\0d & 09 & 0e & 0b\\0b & 0d & 09 & 0e\end{bmatrix}\begin{bmatrix}a'_0\\a'_1\\a'_2\\a'_3\end{bmatrix} \qquad (10)$$

After the encryption process at the transmitting end and the decryption process step at the receiving end, the receiving end can finally obtain secure information.

III. HAMC-SHA1 Algorithm

A. HMAC Algorithm

HMAC (Hash Operation Message Authentication Code) is a hash-based message authentication code consisting of an internal hash and an external hash. Defining an HMAC requires a hash function and a key K. Assume that data block H is an iterative compression function to encrypt the hash function, ipad is an internal fixed string, opad is an external fixed string, M is the information to be passed, and formula (11) is an expression of the HAMC algorithm.

$$HMAC_K(M)=H\left(\overline{K}\oplus opad\parallel H\left(\overline{K}\oplus opad\parallel M\right)\right) \qquad (11)$$

Fig. 3 shows the flow chart of the HMAC algorithm. First, add 0 to the key K to create a string of length B; then XOR the string with the ipad; next fill the data stream into the result of last step; then generate the data block H through the message digest algorithm. Then the XOR the string of B words with the opad to generate s2; then pad the s2 to the data block H; through the information digest algorithm we finally gets the HMAC result.

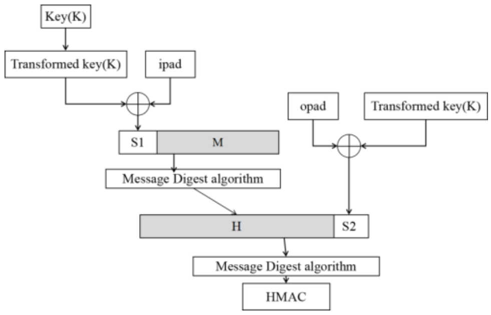

Fig. 3. HMAC processing.

B. HMAC-SHA1 Algorithm

The HMAC-SHA1 algorithm used in this paper is the HMAC algorithm with hash function SHA1. That is, the Message Digest algorithm part in Fig. 3 is the SHA-1 algorithm.

The operation steps of the HMAC-SHA1 algorithm used in this paper are as follows. The secure hash algorithm SHA-1 is a message digest function. The maximum message length allowed is 2^{64} bit, and the resulting message digest is 160 bits. This algorithm needs to preprocess the information before performing the hash calculation. The preprocessing includes three processes of filling, splitting, and setting initial values. The filling process fills the message with a multiple of 512 before calculating the hash; the segmentation process divides the message into packets of length 512 bits before the compression function and each packet can be further divided into 16 sizes of 32. Small grouping of bits; the first round of initial values is a fixed iteration value (five 32-bit small packets), and the next round of initial values is available after the previous iteration of the iteration, so the actual calculation process requires multiple iterations.

The final SHA-1 algorithm produces a 160-bit message digest. Since the information digest generated by the SHA-1 algorithm has the characteristics of irreversible derivation, the sender calculates the information digest and sends it to the receiving end. After receiving the information, the receiving end calculates the message digest calculation about the information, and compared the digest with the information transmitted by the transmitting end.

First, we set N as the synchronization sequence number, and increase N by 1 each time the message digest is calculated. First, at the transmitting end, a new key K0 of the length of the data block B is obtained using the key K, and then the message digest MAC code is calculated using the HMAC-SHA1 algorithm. The transmitted information is then encrypted using the AES-128 encryption algorithm and the SHA-1 message digest algorithm and transmitted to the verification module. In the verification module, the received data is first decrypted, and then the data block B is obtained by using the key K0, and then the message digest is calculated by the HMAC-SHA1 algorithm. Comparing the information digests of the sequence numbers N and N+1, if the information digest values of the sender and the receiver are the same, it indicates that the communication data is accurate. If the inconsistency indicates that the data is changed, the receiver discards the received information and requests the sender to resend data.

IV. Simulation

In this paper, the AES-128 encryption algorithm and HMAC-SHA1 authentication algorithm are performed on the video file, and we carried out the communication experiment based on CANoe.Ethernet vehicle Ethernet experimental platform.

Fig. 4 shows the topology of the car Ethernet network. Among them, HeadUnits is a car video player module, and TV-Reciever is a module for video encryption and authentication functions. The MM is an Ethernet bus with in-vehicle multimedia capabilities.

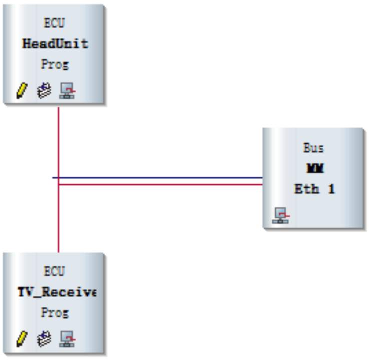

Fig. 4. Topology of the automotive ethernet network.

Fig. 5 is a flow chart for encrypting and authenticating a video file. First, the transmitting end transmits the key K0 of the HMAC and the key K1 of the AES-128 to the receiving end. After the transmitting end receives the video request from the receiving end, the video file is encrypted by using the key K1, and then the information digest is generated by using the key K0, and then the encrypted video and the message digest are sent them together to the receiving end.

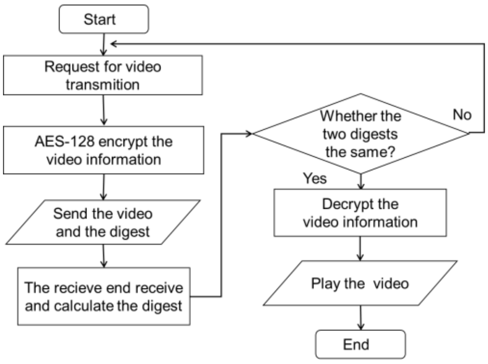
Start
Request for video transmition
AES-128 encrypt the video information
Send the video and the digest
The recieve end receive and calculate the digest
Whether the two digests the same?
No
Yes
Decrypt the video information
Play the video
End

Fig. 5. Flow chart of encrypting and authenticating a video file.

After receiving the video sent by the sending end, the receiving end first calculates the message digest of the decrypted file, and then compares the message digest value calculated by the receiving end with the information digest value of the transmitting end. If the two digests are the same, the receiving end decrypts and plays the video by using the key K1. If not, delete the current file and request the transmitting end to resend.

Fig. 6 shows the playback results of the video after being encrypted and authenticated in the CANoe.Ethernet experimental simulation platform. The simulation results show that there is no stuck and delayed phenomenon in the video transmission and playback process of encryption and authentication processing. It shows that the AES-128 encryption operation and the HMAC-SHA1 authentication operation on the video file improve the security of the video communication information and ensure the normal playback of the video.

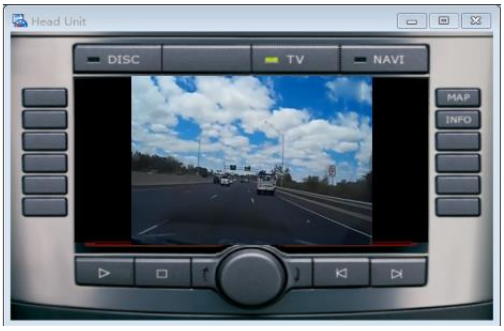

Fig. 6. Video playback simulation results.

V. Conclusion

In this paper, the AES-128 encryption algorithm and HMAC-SHA1 authentication algorithm are combined and applied to video communication for the network security problem of vehicle Ethernet. After the encryption and authentication algorithms are added to the video file, the normal communication is maintained, and the security and reliability of the information of the Ethernet communication network are further improved in the real-time communication environment.

References

[1] A. K. Jadoon, L. C. Wang; T. Li, and M. A. Zia, "Lightweight cryptographic techniques for automotive cybersecurity," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[2] S. S. Karanki and M. S. Khan, "SMMV: Secure multimedia delivery in vehicles using roadside infrastructure," *Vehicular Communications*, vol. 7, pp. 40-42, 2017.

[3] L. Zhou, S. Du, and H. Zhu, "Location privacy in usage-based automotive insurance: Attacks and countermeasures," *Journal of Latex Class Files*, vol. 14, no. 8, pp. 1-3, August 2015.

[4] M. Steger and C. A. Boano, "An efficient and secure automotive wireless software update framework," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2181-2183, 2016.

[5] R. Hussain and H. Oh, "Cooperation-aware VANET clouds: Providing secure cloud services to vehicular Ad Hoc networks," *J. Inf. Process Syst*, vol. 10, no. 1, pp. 103-118, 2014.

[6] S. Woo, H. J. Jo, and I. S. Kim, "A practical security architecture for in-vehicle CAN-FD," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2248-2250, 2016.

[7] G. Kornaros, O. Tomoutzoglou, and M. Coppola, "Hardware-assisted security in electronic control units: Secure automotive communications by utilizing one-time-programmable network on chip and firewalls," *IEEE Micro*, vol. 38, no. 5, pp. 63-65, Sep. 2018.

[8] L. Pike, J. Sharp, and M. Tullsen, "Secure automotive software: The next steps browse," *IEEE Software*, vol. 34, no. 3, pp. 49-55, 2017.

[9] H. Ji, Y. Wang, and H. Qin, "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ECUs," *Digital Object Identifier*, pp. 63-64, Jun 2017.

[10] P. Mundhenk, A. Paverd, and A. Mrowca, "Security in automotive networks: Lightweit authentication and authorization," *ACM Transaction on Design Automation of Electronic Systems*, vol. 22, no. 2, 2017.

Hua Yang was born at Hennan Province of China. He received the bachelor degree in communication engineering from YanBian University, China, in 2017.

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.

Meng-Zhuo Liu was born at JiLin Province of China. He received the bachelor degree in communication engineering from YanBian University, China, in 2017.

He is a currently working toward a master degree in the area of in-vehicle network, which include the design of security architecture of FlexRay.

Yi-Hu Xu was born at Jilin Province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, Korea, in 2014.

He is a lecturer of the Division of Electronic and Communication Engineering of Yanbian University, Yanji, China. His research interests include the automobile electronic control and network.

Yu-Jing Wu was born at 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 are in the area of VLSI implmentation for digital signal processing and communication system, which include the design and in implementation of security protocol for in-vehicle networks.

Yi-Nan Xu was born at 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 network and automobile electronic control.