A Security Framework for In-Vehicle FlexRay Bus Network

Jin-Hui Piao, Yu-Jing Wu, and Yi-Nan Xu

***Abstract*—With the continuous development of automotive electronic technology and the maturity of system integration technology, the real-time performance and security have attracted more and more attention in automotive industries. However, identically with other in-vehicle bus protocol (e.g. CAN, LIN and MOST), their security are not considered in the origin of design. Therefore, security of FlexRay bus is directly related to human's privacy and life. In this paper, we proposed a security framework for FlexRay network. Considering the limitation of computing resources and the real-time performance of in-vehicle ECUs, we optimize the original MAC(Message Authentication) algorithm. To strength the security level and robutness of the system, we recommend to use ECC (Elliptic Curves Cryptography) encryption algorithm and dual channel model for our security framework. By using our proposed model, the bandwidth can be reduced 25% and the computational time can decrease evidently.**

***Index Terms*—In-vehicle network security, FlexRay, encryption, message authentication.**

I. Introduction

Modern vehicles are no longer simple mechanical devices. The connection between the in-vehicle network and the outside world has expanded the security vulnerabilities. Hackers can use these vulnerabilities to invade the vehicle, and even cause serious traffic accidents [1]. Therefore, the technology of in-vehicle information security has attracted great attention of researchers. Controller Area Network (CAN), LIN, FlexRay and automotive Ethernet are popular protocols for in-vehicle network (IVN), which will continuous apply in the automobile industry for many years. However, these protocols are not designed with security in mind. They have several loopholes, such as lack of message authentication and encryption mechanisms [2]. In July 2015, Miller C and valasek C invaded the Uconnect automotive system produced by Chrysler and sent instructions to the system remotely through software to implement various operations on the vehicle [3]. In addition, megamoscrypto protection systems of Volkswagen brands such as Audi, Porsche, Bentley and Lamborghini have also been broken. Attackers use these security vulnerabilities to implement complex attacks, which may lead to casualties and property losses. Therefore, how to deal with vehicle security vulnerabilities has become a key issue that must be solved in the development of modern vehicles.

Experts mainly use encryption mechanisms, message authentication mechanisms and intrusion detection systems to defense against the cyber security threats of in-vehicle networks. Literature [4] explored the identity-based authentication key protocol and several group extensions based on the Diffie-Hellman key exchange protocol in CAN-FD & FlexRay in a comparative way. Groza B et al. discuss the traditional signature and identity signature methods, and obtain the advantages from bilinear pairing. By turning to the non-pairing-friendly curve, the calculation requirement is reduced by five to ten times. All required calculations are affordable on the basis that identity-based message verification is feasible, which further provides greater flexibility and brings constructive advantages. Wu et al. proposed a data compression algorithm to decrease the data field of the in-vehicle network, which can provide space for us to attach encryption and message authentication code in the message [5]. Compared with the proposed ECANDC algorithm, it has better compression effect and can better reduce unnecessary resource consumption. However, the compression model of XOR mode have lots of security risks need to be adequately resolved. In reference [6], the encryption key is efficiently managed and distributed by using the reverse hash chain in FlexRay bus and the authentication label is split on two physically independent channels which ensure the system has a higher degree of fault tolerance and security. Unfortunately, there are still many questions to be considered, since the limitation of computing resources in hardware conditions.

The FlexRay bus is a new communication standard designed for vehicle intranets, which is jointly developed by Daimler Chrysler, BMW, Motorola and Philips in 2000. FlexRay supports the time trigger mechanism in the static segment and event trigger mechanism in dynamic segment. It has the characteristics of high bandwidth, good fault tolerance, etc. It has advantages in real-time performance, reliability and flexibility [7]. With the increasing of the number of electronic equipment in modern vehicle, bus overload occurs during the communication process. The real-time performance of the additional security functions in the in-vehicle networks put forward higher requirements.

In this paper, we focus on the security issues of FlexRay bus and propose a security framework for the FlexRay. Our proposed method considers the real-time performance of in-vehicle ECUs. The proceeds are as follow. In Chapter 2, a brief description of FlexRay protocol is given. In Chapter 3, we introduce our proposed security framework for FlexRay network. Chapter 5 discusses several security mechanisms in FlexRay bus network and shows experimental results for

Manuscript received December 13, 2021; revised March 23, 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: 997284369@qq.com, yjwu@ybu.edu.cn, *ynxu@ybu.edu.cn).

DOI: 10.7763/IJMO.2022.V12.807

verifying the proposed model by using CANoe simulation platform. Finally, Chapter 6 briefly summarizes the full text.

II. FlexRay Protocol

FlexRay is a hybrid communication protocol tailored to meet the requirements of the automotive field. At the end of 2006, the BMW X5 series used FlexRay in the electronically controlled damping system for the first time. In 2008, the BMW 7 series began to fully adopt the FlexRay bus in vehicles. In addition, the FlexRay bus system has gradually been widely used in Audi, Mercedes-Benz, Rolls-Royce and other vehicles. The static segment of FlexRay is a time trigger mechanism in accordance with the principle of TDMA (Time Division Multiple Access). Therefore, the time slot will be allocated to certain messages in the time control area. The specified time period will be assigned to a specific message. The time slot repeats in a fixed period, which means that the time of the message on the bus can be predicted to ensure its certainty. This means that the control signal is transmitted according to a predefined time schedule. No matter what happens outside the system, unplanned events will not be generated.

The maximum communication rate of FlexRay in dual channel mode can reach 20MB/s. In dual channel mode, even if the data transmission in one channel is incorrected, the other channel can transmit normally, which greatly improves the fault-tolerant performance. The FlexRay specification defines the physical layer and data link layer in the OSI reference model. Each node is composed of Host, CC (Communication Controller), BG (Bus Guardian), and BD (Bus Driver), shown in Fig. 1.

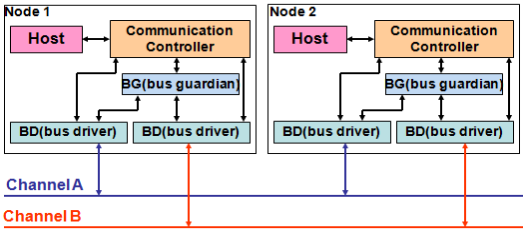

Fig. 1. FlexRay node structure.

1) Host: Control the user software in the communication process.
2) CC: Implement the protocol of the FlexRay.
3) BG: Against faulty media access.
4) BD: Transmitter and receiver.

The host processor is used to provide and generate messages. It notifies the BG of the time slot allocated by the FlexRay bus controller and activate the BD at the same time. The bus guardian allocates the communication cycles and time slots for the FlexRay bus controller for data transmission. They are connected to the bus through a FlexRay controller and two bus drivers.

The FlexRay communication cycle is composed of four parts: (SS) static segment, (DS) dynamic segment, (SW) symbol window and (NIT) network idle time [7]. The length of the communication cycle is fixed after installation of the systems, as shown in Fig. 2. Among them, the static segment adopts TDMA (Time Division Multiple Access) mechanism, which composes of fixed and unchangeable time slots. The dynamic segment adopts FTDMA (Flexibile Division Multiple Access) mechanism. The mini-slots in the DS can be flexibly changed according to communication requirements. The symbol window is used to transmit characteristic symbols.

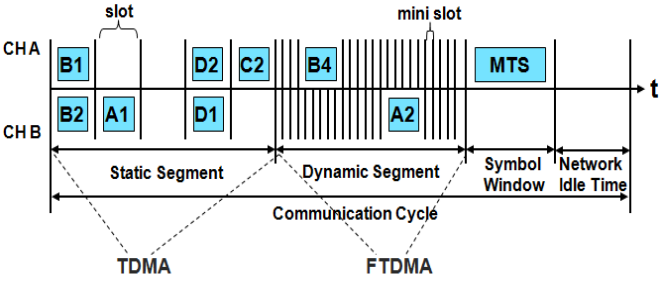

Fig. 2. FlexRay communication cycle.

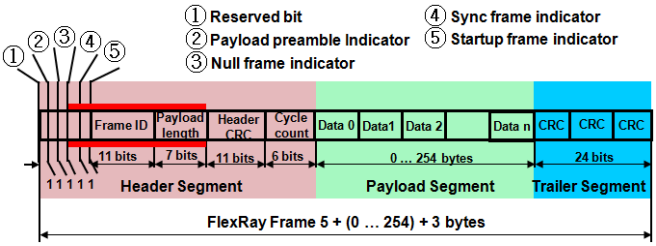

Fig. 3. FlexRay frame structure.

The FlexRay communication cycle is composed of four parts: (SS) static segment, (DS) dynamic segment, (SW) symbol window and (NIT) network idle time [7]. The length of the communication cycle is fixed after installation of the systems, as shown in Fig. 2. Among them, the static segment adopts TDMA (Time Division Multiple Access) mechanism, which composes of fixed and unchangeable time slots. The dynamic segment adopts FTDMA (Flexibile Division Multiple Access) mechanism. The mini-slots in the DS can be flexibly changed according to communication requirements. The symbol window is used to transmit characteristic symbols.

The FlexRay data frame is divided into three parts: the start segment, the payload segment and the end segment, as shown in Fig. 3. The initial segment includes 40 bits (FID) frame indicators, payload length, CRC and communication cycle count. Frame ID determines the order in which data is sent in the time window and each data frame has an independent ID. Payload length indicates the length of the payload in the frame. The length of each frame is the same in the static segment. However, the length is different in the dynamic segment. Header CRC is used to check the redundancy of the initial segment and errors in transmission. The payload segment contains the control information . The end segment consists of a three-byte CRC check code.

III. Security Architecture

In the FlexRay bus environment, the proposed security architecture in this paper contains three parts. In the first part, we introduces ECC encryption algorithm to encrypt data. In the second part, we introduces the proposed session key establishment method. In the third part, we introduces the proposed grouped MAC algorithm for message authentication.

A. FlexRay Data Encryption using ECC Algorithm

Elliptic encryption algorithm is a public key encryption system, which was first proposed by Koblitz and Miller in 1985. Its mathematical foundation is to use the rational points on the elliptic curve to calculate the discrete logarithm of the ellipse on the Abelga group. Public key cryptosystems are generally divided into three categories: large prime decomposition problem, discrete logarithm problem and elliptic curve problem. Sometimes the elliptic curve is also classified as discrete logarithm. The main advantage of ECC is that it can provide an equivalent or higher level of security even if it uses a smaller key than other methods (such as RSA encryption algorithm). Another advantage of ECC is that it can define bilinear mapping between groups based on Weil pairs or Tate pairs. Bilinear mapping has found a lot of applications in cryptography, such as identity based encryption. However, one disadvantage is that the implementation time of encryption and decryption operations is longer than other mechanisms. ECC is widely regarded as the most powerful asymmetric algorithm for a given key length. Therefore, it is effective in connections with completely strict bandwidth requirements. An elliptic curve satisfies formula (1), in which all elements satisfy in the finite field GF(P) (P is a large prime):

$$\begin{cases} y^2 = (x^3 + ax + b) \ (\text{Mod P}) \\ (4a^3 + 27b^2) \ (\text{Mod P}) \\ a, b \in GF(P) \end{cases} \quad (1)$$

The limiting condition of $(4a^3 + 27b^2)$ (Mod P)$\neq 0$ is to ensure the curve does not contain singularity (in mathematics, it means that there is a tangent at any point on the curve) [8]. It is easy to find point P when b and point R are known. However it is difficult to find b when point R and point P are known. ECC algorithm uses this classic discrete logarithm problem function for encryption. Point P is the public key, b is the private key and point R is the base point. The biggest practical difference between ECC and RSA is the key length

ECC Algorithm Encryption Process

Input: An elliptic curve Ep(1, j), base point R on Ep(1, j), a large number b as private key

1. Public key P=bR
2. User⟵Ep(1, j), P, R
3. Encodes the plaintext⟶M on Ep(1, j)
4. Generates a random r
5. Public key encryption: C={rR, M+rP}
6. Private key decryption M + rP-k(rR)=M
7. Decode the point M⟶plaintext

Fig. 4. ECC encryption process.

$T = (p, l, j, n, x, y)$ is used to describe an elliptic curve on F_P. (p, l, j) used to determine an elliptic curve. Among that, p is the number of points in the prime field, and l and j are the two large numbers in it. x and$y$ (two large numbers) are the coordinate of the base point R, and n is the order of the base point R. The above six parameters can describe an elliptic curve. Sometimes we also use the integer part of the number of points on the elliptic curve divided by p and n [9]. The encryption and decryption processes of ECC algorithm are shown in Fig. 4. Firstly, select an elliptic curve $Ep(1, j)$ based on infinite field Fp, convert the original data into a single large integer point m, and then map m to the elliptic curve. Take the point on a group of curves$Ep(l, j)$ as the base point R, select a large integer B as the private key for FlexRay bus data, and calculate P = bR as the public key. When the transmitter wants to transmit the message M in FlexRay bus, it will select a random number r and calculate two points $C1 = rR$ and $C2 = M + rP$. Then send a pair of points $Cm = \{rR, M + rP\}$ as ciphertext to the receiving node. The receiver receives the ciphertext $Cm = \{rR, M + rP\}$ from the transmitter. The formula for the receiver to obtain the original data M is: $M + rP - b(rR) = M + r(bR) - b(rR) = M$.

B. Establishment of Session Key

The first part is to establish a session key $K_{Sa,b}$ between a transmitting ECU_a and a receiving ECU_b by using the ECC asymmetric encryption algorithm. The second part is the message authentication part, which uses the SHA256 algorithm and the generated key to transmit the message and the authentication part to the receiving node. The whole security architecture of this article is shown in Fig. 5, where Cps is the cipher text after using the ECC encryption algorithm, and AUT=1 is the successful authentication of the session key of the receiving node.

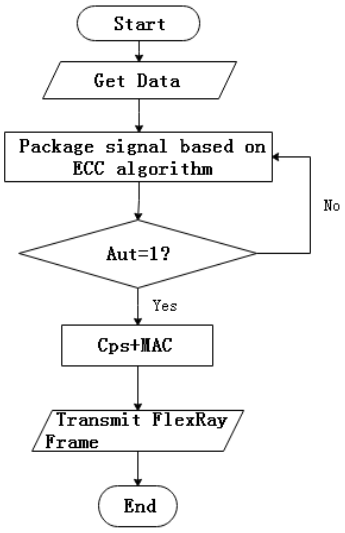

Fig. 5. Network security architecture.

Firstly, select an elliptic curve $Ep(l, j)$ and a point R in the finite field F_p as the base point. In the FlexRay network environment, we must install a set of public key and private key (P_a, b_a) for each ECU_a, where $P_a = b_a \times R$ is the multiply operation in the finite field F_p, in which the public key P_a is installed in all ECUs. After setting various parameters and public key keys on elliptic curve $Ep(l, j)$, we will establish a set of session keys $K_{Sa,b}$ between ECU_a and ECU_b to ensure the completion of communication. The process in Fig. 6 is as follows:

1. The following calculations are performed in ECU_a:
   a) Select $q_a \in F_p$, calculate $U_a = q_a \times P_a$ and

$\mathrm{AUT_a} = H(ID_a||U_a||b_a||P_b)$.

b) Send $C_a = (ID_a||U_a||AUT_a)$ to ECU_b.

2. ECU_a after receiving the message($\mathrm{ID_a||U_a||AUT_a}$)

a) Select $q_a \in F_p$ calculate $U_a = q_a \times P_a$ and $\mathrm{AUT_a} = \mathrm{H(ID_a||U_a||b_a \times P_b)}$.

b) ECU_b compares whether $\mathrm{AUT_a}$ and $\mathrm{AUT_a'}$ are equal, and if they are equal, a conversation can be conducted between ECU_a and ECU_b.

c) ECU_b select $q_b \in F_p$, then calculate $D_b = q_b \times b_b \times U_b = q_a \times q_b \times b_a \times R$

3. After authentication between ECU_a and ECU_b:

a) Calculate and $AUT_b = H(ID_b||U_b||b_b \times P_b)$.

b) Calculate $U_b = q_b \times P_b$ and generate the session key $K_{S_{a,b}} = H(ID_a||ID_b||U_a||U_b||AUT_a||AUT_b||D_b)$

4. If ECU_a receiving the message:

a) Calculate $AUT_{b'} = H(ID_b||U_b||b_a \times P_b)$

b) If $\mathrm{AUT_b}$ is equal to $\mathrm{AUT_{b'}}$, the authentication, the authentication between ECU_b and ECU_a is successful.

c) Calculate, $D_a = q_a \times b_a \times U_b = q_a \times q_a \times b_a \times b_b \times R$ and generate the session key: $K_{S_{a,b}} = H(ID_a||ID_b||U_a||U_b||AUT_a||AUT_b||D_a)$

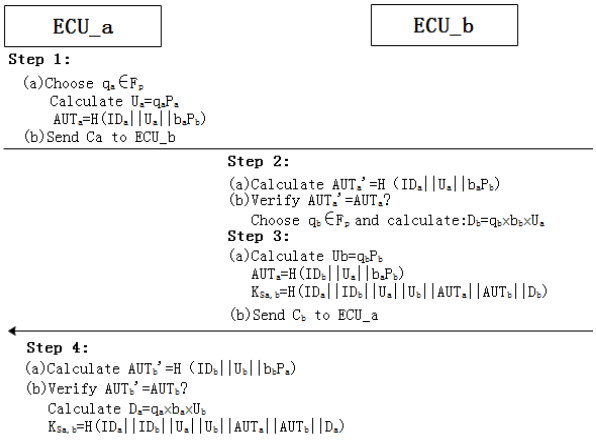

Fig. 6. Key distribution process.

C. Grouped MAC

In order to reduce unnecessary waste of resources, we adopt an allocation method where a group of time slots share one MAC. In the FlexRay dual channel mode, even if one channel is damaged, the other channel can exchange data. Considering the fault tolerance of the system, this paper selects the dual channel mode to effectively transmit MACs. The two channels can transmit different data or the second channel can repeatedly transmit the data of the first channel to improve reliability. As shown in Fig. 7, *ma* is the data to be transmitted, and r is a random value. We divide the data ma into two equal length parts *ma1* and *ma2*, where w is the bit length of ma, $\mathrm{MA1 = MA\{w, w/2\}}$, $\mathrm{MA2 = MA\{w/2, 0\}}$. The sender sends (*ma*, *ma1*) on the first channel and (*ma*,*ma2*) on the second channel, so the receiver can receive the ma through two channels. Finally, the original MAC can be reconstructed by concatenating MA1 and MA2 (for example, $ma = \mathrm{MA1||MA2}$). When the receiver verifies *ma*, there are three results: a) If the MAC of the message *ma* authenticated successfully, the receiver will receive the message *ma*; b) If the MAC of one channel can be successfully verified, and the other channel is attacked by hackers, it can at least guarantee the security of a complete channel and receive information; c) If the MAC of the message *ma* was failed in both two channel, the system will be terminated.

In order to reduce unnecessary waste of bandwidth and computational resources, FlexRay filtering mechanism is used to determine whether these messages are allowed to be received. If it was determined as allowed to be received, attach MAC into the message. Otherwise, refuse service.

When the transmitting node ECU_a, wants to transmit data Mh (ID: h) in the FlexRay bus, its steps are as follows:

1) Searching the ID from the list shown in Table I, if it does not matching the rules in the list the system will be terminated. Otherwise, it will go to next step.
2) Calculate interval T_i.
3) Each receiver whose ID is $j_{h,k}$ calculates a MAC: $C_{h,k}=MACK_{Sa,jh,k}(Mh||Ti)$
4) Transmit $M_h||T_i||C_{h,1}||C_{h,2}||\ldots||C_{h,k}$ to the receiving node The steps to be checked when the receiving node ECU_b wants to receive the message

Mh sent from ECU_a, are as follows:

1) Receive $M_h||T_i||C_{h,1}||C_{h,2}||\ldots||C_{h,k}$.
2) Obtain the transmission time interval $\mathrm{T_i}$ and the current time $\mathrm{T_n}$.
3) Calculate, If $C = C_{h,k}$ and the time interval between $\mathrm{T_i}$ and $\mathrm{T_n}$ meets the FlexRay protocol, ECU_b will receive the message.

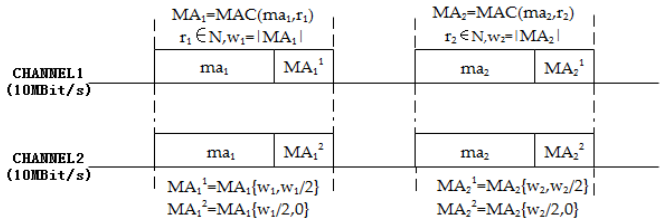

Fig. 7. MAC allocation under dual channels.

TABLE I: SEND RECEIVE NODE ID

IDs	Sender's ID	List of Receiver's IDs
h	I_h	$J_{h,1}, j_{h,2}, \ldots j_{h,nh}$
k	I_k	$J_{k,1}, j_{k,2}, \ldots j_{k,nk}$
f	I_f	$J_{f,1}, j_{f,2}, \ldots j_{h,nf}$

IV. EXPERIMENTAL RESULTS

A. Analysis of the FlexRay Security Framework

As shown in Fig. 8, network deployment, message authentication, intrusion detection system(IDS) and data encryption mechanisms are used to ensure the security of the

in-vehicle bus networks[10]. Since illegal frames generated during eavesdropping of messages can be invalidated in network deployment, effective network deployment can reduce the risk of eavesdropping during data transmission. Message authentication is that MAC verifies the information transmitted between the two sides of the shared key. It can avoid message tampering and forgery, and ensure the integrity of data. Intrusion detection is to prevent eavesdropping and various attacks to ensure security by detecting abnormal data.

In Table II, Kishikawa *et al.* [11] proposed an intrusion detection and prevention system to reduce message eavesdropping. However, the attack prevention coverage of this scheme is very limited and its robustness is low. The prevention of replay attacks and injection attacks is also critical, and the detection range needs to be further improved to ensure security. Mousa *et al.* [12] proposed a lightweight authentication protocol based on FlexRay bus to ensure the security of message transmission. The protocol is highly scalable, but the algorithm is too simple, and it needs further consideration to improve its security. This paper proposes an elliptic encryption scheme and adds grouped MAC after the ciphertext to ensure the integrity of the message and improve the security of the system.

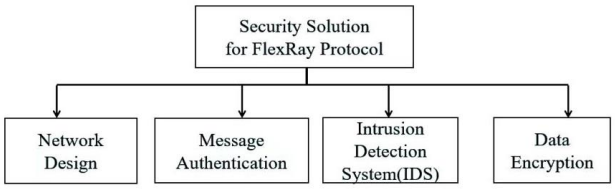

Fig. 8. Safety solution of FlexRay bus.

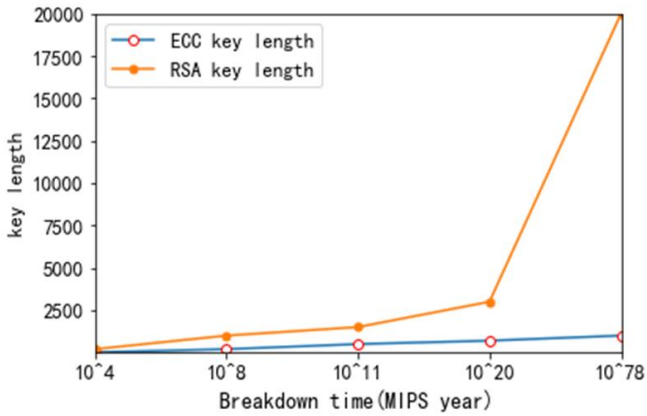

Fig. 9. Security performance analysis of ECC encryption algorithm.

TABLE II: COMPARISON OF FLEXRAY BUS SAFETY MECHANISMS

Reference	Security Mechanisms	Security	Algorithm Complexity	Detection Coverage
D Püllen et al.[6]	Message authentication	Medium	Medium	N.A
Kishikawa et al.[11]	IDPS	Low	N.A	Spoofing attack
Mousa et al.[12]	Message authentication	Low	Low	N.A
Han at al.[13]	Message authentication	N.A	Medium	N.A
Gu Z et Al.[14]	Message authentication	N.A	Medium	N.A
Our solution	Encrypion &MAC	High	Medium	N.A

B. Simulation Results

As shown in Fig. 9, compared with the RSA asymmetric encryption algorithm the ECC algorithm selected in this paper has improved security. Under the condition of providing the same security performance (the time of cracking is the same, about 10 ^ 4mips years), the length of RSA key is 512 bits and the length of ECC key is 106 bits. When improve the security performance, the length of RSA key will increase exponentially, while the length of ECC key will only increase linearly. For example, when provide a 128 bits security encryption requires a 3072 bits for RSA key and 256 bit for ECC key. When provide a 256 bits security encryption requires a 15360 bits RSA key and 512 bits ECC key. The ECC encryption and decryption times for different length of bytes are shown in Table III.

TABLE III: ECC ALGORITHM ENCRYPTION AND DECRYPTION TIME CONSUMPTION

Data size(bytes)	Encryption time(ms)	Decryption time(ms)
200	360	222
400	691	377
600	875	465
800	1011	527
1000	1341	729

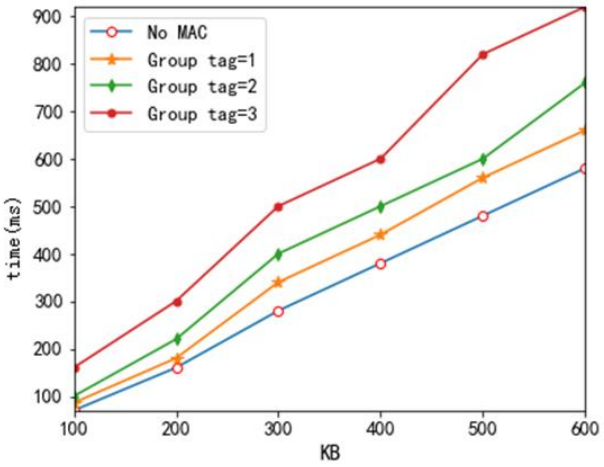

Fig. 10. Network overhead.

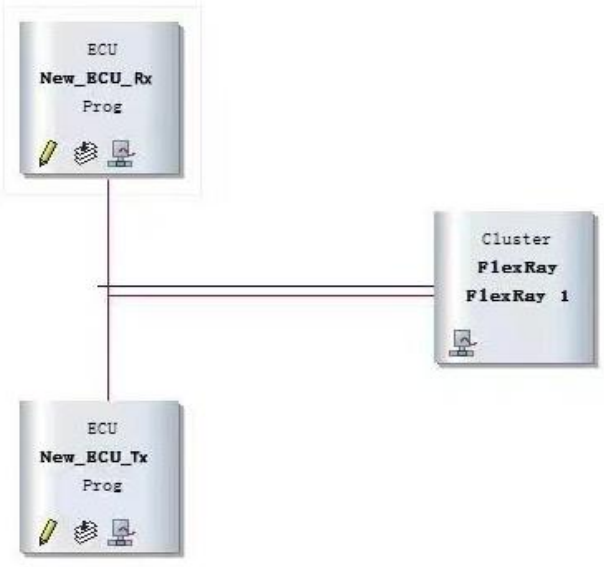

Fig. 11. Establishment of transceiver node in CANoe.

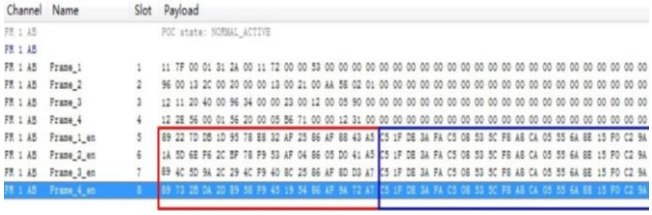

Fig. 12. CANoe simulation results.

It is not feasible to add MAC directly in each frame to ensure the authenticity of the message, because of the length limitation of the data segment for in-vehicle bus protocol and the constraint of hardware resources. As shown in Fig.10, Group tag = x indicates that a group with the number of x time slots share a MAC [15]. The related measurement value of the network overhead caused by the transmission of the MAC is an average value of more than 200 operations. In the dual channel mode, the MAC length is halved and transmitted through two channels respectively. Compared with single channel mode, the bit rate is reduced. If the MAC is transmitted with group tag = 1, the bit rate is about 50% of the original code. Group tag = 2 reduces the bandwidth by approximately 33%, while group tag = 3 reduces the bandwidth to 25%. However, sharing multiple time slots for message authentication will cause the delay of data authentication, because of the computational resources of the hardware (as shown in Fig. 10). Therefore, we choose three time slots to share a MAC.

In order to verify the feasibility of our algorithm, we use Network Designer soft-ware to establish the database of FlexRay Network. Then, we use CANoe software designed by Vector company to simulate and verify the proposed security scheme. Using the C-like language CAPL (Communication Access Programming Language) in CANoe can simulate the behavior of real bus during the driving. CAPL contains a wealth of library functions, which can help users realize the simulation and testing of vehicle networking communication and diagnosis function. We use node simulation function of CAPL to realize the encryption processing of the data transmission process through the FlexRay bus. By associating ECU nodes in Simulation Setup window, ECU node simulation and vehicle network system simulation can be realized. As shown in Fig. 11, a data frame transmitted through the FlexRay bus environment is established in CANoe, where New_ECU_Tx is used to transmit data, and New_ECU_Rx is used to receive data. As shown in Fig. 12, in the Trace window of CANoe, the transmission status data of some messages are recorded in real time. Frame_1~Frame_4 are unencrypted messages for dual-channel transmission, and Frame_1_en~Frame_4_en are encrypted messages for dual-channel transmission (with message authentication code attached), the red box is the encrypted message, and the blue box is the additional message authentication code. The simulation results of CANoe show that our solution can encrypt data and verify the security of messages in the FlexRay bus environment.

V. Conclusions

In this paper, we propose a in-vehicle FlexRay network security framework, which cotains data encryption technic and message authentication technic. ECC encryption algorithm is used to encrypt the data and grouped MAC is used to further ensure the authenticity of the message. Then we suggest using dual channel communication model in FlexRay network to provide the redundancy and strength the robustness of the system. Compared with RSA and other encryption algorithms, ECC algorithm can not only shorter the length of key, but also achieve faster encryption and decryption speed, which can greatly reduces unnecessary waste of resources. As for message authentication, the grouped MAC can decrease the unnecessary time delays caused by original MAC algorithm. Finally, we use CANoe to simulate the actual in-vehicle network, the simulation results show that computational time satisfy the system requirement. It means that, it is feasible to use ECC algorithm and grouped MAC algorithm in FlexRay network at the same time. Compared with original method, our propose security scheme can reduces the bandwidth up to 25%, which can reduces time-consuming and unnecessary waste of resources.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Jin-hui Piao: 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] J. Zhang, F. Li, H. Zhang *et al*., "Intrusion detection system using deep learning for in-vehicle security," *Ad hoc Networks*, 2019.

[2] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-Vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, 2021, vol. 10, no. 8.

[3] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat, Las Vegas, USA, 2015.

[4] B. Groza and P. S. Murvay, "Identity-based key exchange on in-vehicle networks: CAN-FD & FlexRay," *Sensors*, 2019, vol. 19, no. 22.

[5] Y. J. Wu and J. G. Chung, "An improved controller area network data-reduction algorithm for in-vehicle networks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 2, 2017, pp. 346-352.

[6] D Püllen, N. A. Anagnostopoulos, and T Arul *et al*., "Securing flexray-based in-vehicle networks," *Microprocessors and Microsystems*, 2020, vol. 77, p.103144.

[7] F. Sagstetter, M. Lukasiewycz, and S. Chakraborty, "Generalized asynchronous time-triggered scheduling for flexray," in *Prof. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 2, pp. 214-226, Feb. 2017.

[8] C. Guo and B. Gong, "Efficient scalar multiplication of ECC using SMBR and fast septuple formula for IoT," *EURASIP Journal on Wireless Communications and Networking*, 2021.

[9] J. R. Shaikh, M. Nenova, G. Iliev, and Z. Valkova-Jarvis, "Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications," in *Proc. 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems*, 2017, pp. 1-4.

[10] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, 2021, vol. 10, no. 8, p. 893.

[11] T. Kishikawa, R. Hirano, Y. Ujiie, T. Haga, H. Matsushima, K. Fujimura, and J. Anzai, "Intrusion detection and prevention system for flexray against spoofed frame injection," in *Proc. the 17th Escar Europe: Embedded Security in Cars Conference*, Detroit, MI, USA, 2019, pp. 59-73.

[12] "Lightweight authentication protocol deployment over FlexRay," in *Proc. the 10th International Conference on Predictive Models in Software Engineering*, Turin, Italy, 17 September 2014.
[13] G. Han, H. Zeng, Y. Li, and W. Dou, "SAFE: Security-aware flexray scheduling engine," in *Proc. the 2014 Design, Automation& Test in Europe Conference & Exhibition (DATE)*, Dresden, Germany, 2014.
[14] Z. Gu, H. H. Gang, and H. Zeng *et al*., "Security-aware mapping and scheduling with hardware co-processors for flexray-Based distributed embedded systems," I*EEE Transactions on Parallel & Distributed Systems*, 2016, vol. 27, no. 10, pp. 3044-3057.
[15] S. K. Khare, "Fast-track message authentication protocol for DSRC using HMAC and group keys," *Applied Acoustics*, vol. 165.
[16] S. Y. 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.

Jin-Hui Piao received the bachelor degree in communication engineering from Yanbian University, China, in 2020. She is a currently working toward a master degree in the area of in-vehicle network, which include communication algorithm and security of in-vehicle network.

Yu-Jing Wu 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 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.