Abstract: With the proliferation of automotive electronic devices, electronic control units are increasingly used to share information within in-vehicle networks. This induces a range of security risks, such as information disclosure, spoofing, and tampering. In this paper, we propose a symmetric-key cipher. The method generates pseudo-random numbers using a chaotic and random neural network, and encrypts and decrypts frame messages of in-vehicle networks based on the symmetric key. We also propose a lightweight ID-based key sharing protocol. We evaluated the key sharing, encryption, and decryption in Controller Area Network.

Keywords: In-vehicle network, symmetric key cryptography, ID-based cryptography, network security, network system

Classification: Network system

References

[1] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, “Intra-vehicle networks: A review,” IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 534–545, 2015. DOI:10.1109/TITS.2014.2320605

[2] J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, “Automotive attacks and countermeasures on lin-bus,” Journal of Information Processing, vol. 25, pp. 220–228, 2017. DOI:10.2197/ipsjjip.25.220

[3] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, “A survey of intrusion detection for in-vehicle networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 919–933, 2020. DOI:10.1109/TITS.2019.2908074
[4] A. Van Herreweghe, D. Singelee, and I. Verbauwhede, “Canauth - a simple, backward compatible broadcast authentication protocol for can bus,” ECRYPT Workshop on Lightweight Cryptography, 2011.

[5] S. Bittl, “Attack potential and efficient security enhancement of automotive bus networks using short macs with rapid key change,” Communication Technologies for Vehicles, 2014.

[6] M. Wolf and T. Gendrullis, “Design, implementation, and evaluation of a vehicular hardware security module,” International Conference on Information Security and Cryptology, pp. 302–318, Springer, 2011. https://doi.org/10.1007/978-3-642-31912-9_20

[7] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann, “Car2x communication: securing the last meter-a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography,” 2011 IEEE Vehicular Technology Conference (VTC Fall), pp. 1–5, IEEE, 2011. DOI:10.1109/VETECF.2011.6093081

[8] H. Yoshida, T. Murakami, and Z. Liu, “High-speed and highly secure pseudo-random number generator based on chaos neural network,” New Trends on System Science and Engineering: Proceedings of ICSSE, vol. 276, pp. 224–237, 2015. DOI:10.3233/978-1-61499-522-7-224

[9] H. Yoshida, Y. Akatsuka, and T. Murakami, “Implementation of high-performance pseudo-random number generator by chaos neural networks using fix-point arithmetic with perturbation,” Proceedings of Papers, The 2018 International Symposium on Nonlinear Theory and Its Applications, NOLTA2018, pp. 46–49, 2018.

[10] Z. Liu, T. Murakami, S. Kawamura, and H. Yoshida, “Parallel implementation of chaos neural networks for an embedded gpu,” 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST), pp. 1–6, IEEE, 2019. https://doi.org/10.1109/ICAwST.2019.8923383, DOI:10.1109/ICAwST.2019.8923383

[11] H. Yoshida, H. Fukuchi, and T. Murakami, “Implementation of high-speed pseudo-random-number generator with chaotic and random neural networks,” Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020. DOI:10.24251/HICSS.2020.786

[12] H. Yoshida and T. Murakami, “Non-attractive periodic trajectory formation mechanism on random and chaotic time series,” in Knowledge Innovation Through Intelligent Software Methodologies, Tools and Techniques, pp. 197–208, IOS Press, 2020. DOI:10.3233/FAIA200566

[13] E. Barker, E. Barker, L. Chen, and R. Davis, Recommendation for key-derivation methods in key-establishment schemes, US Department of Commerce, National Institute of Standards and Technology, 2018.
1 Introduction

Vehicles contain an increasing number of Electronic Control Units (ECUs), sometimes in excess of 100, and those ECUs connect to each other and share messages within in-vehicle networks such as Local Interconnect Network (LIN), Controller Area Network (CAN), or FlexRay Network [1].

LIN is a master-slave broadcast serial communication bus offering a data rate of up to 20 kbps, and it is commonly used for controlling vehicle body components, such as windows and doors. CAN is the most widely used multiple-master broadcast serial communication bus. It uses a Carrier Sense Multiple Access/Collision Resolution protocol, providing data rates from 125 kbps to 1 Mbps. FlexRay is a Time Division Multiple Access-based serial communication standard. FlexRay nodes have higher cost but greater speed than CAN nodes, and can operate at a data rate of 10 Mbps.

The message frames are similar in these in-vehicle networks. They all have IDs to identify each frame, and have checksum or cyclic redundancy check fields to verify the data part correctly. Generally, LIN, CAN, and FlexRay are bus topology networks, which lack a security mechanism. Because messages are broadcast on the bus, it is easy to sniff and inject message frames, even to reflash the firmware of ECUs [2][3]. Some methods based on Message Authentication Code (MAC) [4][5] and the Advanced Encryption Standard (AES) [6][7] have been proposed as security mechanisms. However, redundant frames would be sent if part of the payload were used for MAC. As a result, this leads to the occupied rate of the network bus increasing. In addition, the procedure of AES cryptography needs high computation performance, which can have performance implications that disrupt the real-time response of an ECU. Thus, a faster security method is needed for in-vehicle networks.

We have been studying pseudo-random number generation [8][9] for cipher systems. Our method is approximately 49% faster than AES [10]. Recently, we further improved our method and proposed the chaotic and random neural network (CRNN) [11][12], a new high-speed method whose output series involves considerable randomness in addition to the chaotic properties, and it is hard to predict. In this paper, we propose a high-speed cipher based on the CRNN to protect messages on the bus of in-vehicle networks by encrypting them.

Fig. 1. CRNN consists of four neurons in a discrete time system
2 CRNN

To form a pseudo-random number generator, a CRNN is composed of 4 neurons in the discrete-time system (Fig. 1). The CRNN generates chaotic and random time series from neurons that are computed by 32-bit fixed-point arithmetic (Q5.26). An output from the jth neuron at time $t + 1$ is defined as Eq. (1), and the total value of inputs is defined as Eq. (2).

$$x_j(t + 1) = f[u_j(t)],$$

$$u_j(t) = \sum_{i=1}^{n} w_{ij} x_i(t) + I(t),$$

$$I(t) = \begin{cases} I & (t = 0, 2, 4, ...) \\ I + I_d & (t = 1, 3, 5, ...) \end{cases}$$

In Eq. (2), $w_{ij}$ is a synaptic weight, $x_i(t)$ is an input from the $i$th neuron at time $t$, and $I(t)$ is defined as Eq. (3), which is an external input at time $t$. To extend the period of chaotic time series from the CRNN, a perturbation $I_d$ is appended to the external input $I$ when the current time is odd.

As an activation function, $f$ of Eq. (1) is an asymmetric piecewise-linear function (APLF). The activation-function APLF, consisting of linear functions at 5 points, can avoid a periodic window in the chaotic time series. Then, the coordinate values of those points can be used as secret keys in a cipher system [8]. In this paper, $(-31.0001, -31.001), (-7.9811, -8.29999), (0.0001, 0.500012), (7.981101, 8.6901)$ and $(31.0002, 31.00999)$ are set.

The time series output from the CRNN is not only chaotic, but also highly random. The chaotic trajectory is hard to predict, and the period is about $10^{27}$ [12]. The lower 28 bits from the output of the neuron can be extracted as pseudo-random numbers [11]. In this paper, we extract the lower 16 bits from each output of the neurons, and a 64-bit pseudo-random number is applied to the CRNN cipher.

3 CRNN Cipher

We propose a symmetric-key cipher to protect messages on the bus of in-vehicle networks (Fig. 2). First, CRNN generates pseudo-random numbers, then the ECUs use them to encrypt and decrypt messages on the bus.

3.1 ID-based key sharing

Sharing the symmetric key is a vital function in a cipher system. An elliptic curve Diffie–Hellman key exchange (ECDH) and key sharing by public-key cryptography have been recommended by the U.S. National Institute of Standards and Technology [13]. However, these methods are complicated, expensive, and require high computing power, potentially exceeding the capacity of bus networks. Thus, ECDH is not appropriate for ECUs, which prioritize real-time response.
Therefore, we propose a light ID-based key-sharing protocol (Fig. 2a). The details are shown below.

1. Generating a master key
   The master key generator assigns a particular range of frame IDs for key sharing and creates a master key corresponding to the frame ID.

2. Pre-sharing of master keys
   Authorized ECUs share the master keys and key-sharing frame IDs in advance. It is recommended that this information be written to the read-only memory (ROM) of the ECU at the time of factory release.

3. Delivery of the symmetric-key
   As shown in Fig. 2a, the master key is used to encrypt the symmetric key, which is then delivered in a message with the frame ID corresponding to the master key. The receiving ECU decrypts the data using the master key corresponding to the frame ID to obtain the symmetric key.

3.2 Encryption and decryption of messages
The proposed CRNN cipher is shown in Fig. 2b. The symmetric key is shared previously between authorized ECUs. The CRNN uses the symmetric key to generate a stream of pseudo-random bits: $R_1, R_2, R_3, ..., R_i$. This stream is XORed with a stream of bits, $D_1, D_2, D_3, ..., D_i$, that are from the data part in a frame of the in-vehicle network. Then, encrypted data are given by $C_i = D_i \oplus R_i$, which is loaded into a message frame and sent via the bus of the in-vehicle network. The procedure of decryption is almost the same:
after an authorized ECU receives a message frame, the CRNN generates the same stream of pseudo-random bits \( R_i \) and the original data are obtained by \( D_i = C_i \oplus R_i \).

4 Implementation and evaluation

| Table I. Specifications of Evaluation CAN Board |
|-----------------------------------------------|
| CPU               | SAMA5D27C-D1G                |
|                  | ARM Cortex-A5 (492 MHz)      |
| RAM               | DDR2-SDRAM (120 MHz)         |
| CAN Controller    | FPGA IP                      |

We demonstrated the CRNN cipher with two identical CAN boards (see Table I) on a CAN bus, which is the most widely used in-vehicle network. The CRNN was implemented, and the cipher was embedded in each board. The master key was written to ROM and shared in advance, then the evaluation experiments of key sharing and encryption/decryption of CAN messages were executed on the high-speed CAN bus (ISO 11898).

The results show the validity of the procedure for key sharing, transmission of encrypted CAN messages, and decryption of received CAN messages. The encryption or decryption time for one CAN message was approximately 0.75 \( \mu s \). The encryption time was within 1 bit even when the CAN transfer rate was set to 1 Mbps.

5 Conclusions

In this study, we proposed and evaluated a CRNN cipher to secure the frame messages of in-vehicle networks. We also presented an ID-based key-sharing protocol to reduce the data load on the ECUs and bus. According to the evaluation experiment, the CRNN cipher operates at high speed and is compatible with ECUs and in-vehicle networks.

As future work, we will evaluate our method with other types of in-vehicle networks, such as LIN and FlexRay.