International Journal of Networked and Distributed Computing, Vol. 3, No. 3 (August 2015), 159-166

Secure in-vehicle Systems using Authentication

Masaya Yoshikawa
Department of Information Engineering, Meijo University
Nagoya, Aichi, Japan

Kyota Sugioka, Yusuke Nozaki and Kensaku Asahi
Department of Information Engineering, Meijo University
Nagoya, Aichi, Japan

Abstract

Recently, driving support technologies have been practically used. However, a problem has been pointed out that when a vehicle is connected with an external network, the safety of the vehicle is threatened. Ensuring the security of in-vehicle systems becomes an important priority. The present study proposes a CAN communications method that uses a lightweight block cipher to realize secure in-vehicle systems. Experiments using both FPGA and a radio-controlled car verify the proposed method.

Keywords: Security; Embedded system; Lightweight block cipher; CAN communication; Authentication;

1. Introduction

The basic functions of vehicles — "run," "turn," and "stop" — are currently realized using electronic control units (ECUs) in almost all commercially available vehicles. More than a dozen ECUs are mounted in a vehicle. Between these ECUs, data are exchanged using a communications protocol for an in-vehicle network, the controller area network (CAN)[1]. The CAN handles data on the velocity of the vehicle and the state of the brake. Since information for controlling the vehicle is involved, these data are important from a safety viewpoint.

Since the development of this communications network infrastructure, vehicles have been connected to the Internet. Methods of using information possessed by vehicles and using vehicle-related services through smartphones have been examined and put to practical use.

Similar to how to achieve conventional vehicle safety, how to ensure vehicle information security has grown in importance as the use of information processing technologies has advanced. E-safety Vehicle Intrusion Protected Applications (EVITA)[2] and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE)[3] are examples of European vehicle safety projects in which multiple countries and companies participate. In Japan, the Information-technology Promotion Agency (IPA)[4] and the Japan Automotive Software Platform and Architecture (JASPAR)[5] standardization effort have examined the safety of vehicles, focusing on the in-vehicle local area network (LAN).

In previous studies[6–8] on vehicle information security, the On-Board Diagnostics II, the second generation of on-board self-diagnostic equipment, was installed in a vehicle. When in-vehicle systems were attacked from a parallel running vehicle, the brake and the windshield wiper could not be controlled correctly.

An experiment revealed that CAN communications in the vehicle under attack could be intercepted and that the intercepted data could be analyzed. Since the ECU currently has no authentication capability and no source address, it is easy to perform "spoofing" by sending improper control data from a spoof ECU, instead of a genuine ECU, as shown in Fig. 1. To ensure the safety of vehicles in the future from an information security viewpoint, measures to prevent illegal attacks against CAN communications are critical.

Published by Atlantis Press

The present study proposes a secure CAN communications method using a cipher. In the proposed method, an authentication code is incorporated into the cipher in order to protect against both spoofing attacks and replay attacks (providing tamper resistance). To verify the proposed method, the present study develops a CAN communications evaluation system. In this evaluation system, data can be exchanged using multiple field-programmable gate array (FPGA) boards that comply with CAN communications standards, and data can be observed at an arbitrary point. By verifying tamper resistance using this evaluation system, the enhanced safety of in-vehicle systems is realized.

2. Preliminaries

2.1. *CAN communications*

CAN is communication protocol proposed by BOSCH. CAN is standardized as ISO11898, ISO11519. CAN signal consists of both CAN-High and CAN-Low. Logical value of CAN signal is determined by potential difference between CAN-High and CAN-Low, as shown in Fig. 2. When potential difference is high, CAN state is called by 'Dominant'. In Dominant, the logical value is '0'. By contrast, when potential difference is low, CAN state is called by 'Recessive'. In Recessive, the logical value is '1'.

CAN communicates in frame such as data frame, remote frame, error frame and overload frame. When CAN communicates between the ECU, CAN uses data frame. As shown in Fig. 3, data frame consists of ID field, Data field and Cyclic Redundancy Check (CRC). Constitution of data frame is as follows.

(1) Star of Frame (SOF) : Date length is 1bit. SOF represents start of the frame.
(2) Arbitration field : Data length is 12bit. Arbitration field represents priority of the frame.
(3) Control field : Data length is 6bit. Control field represents byte length of the data.
(4) Data field : Data length is from 0 to 64bit. Data field incorporate CAN data which communicate between the ECU.
(5) CRC : Data length is 2bit. CRC checks the frame.
(6) Acknowledgement (ACK) : Data length is 2bit. ACK notices normal reception of the frame.
(7) End of Frame (EOF) : Data length is 7bit. EOF represents end of the frame.

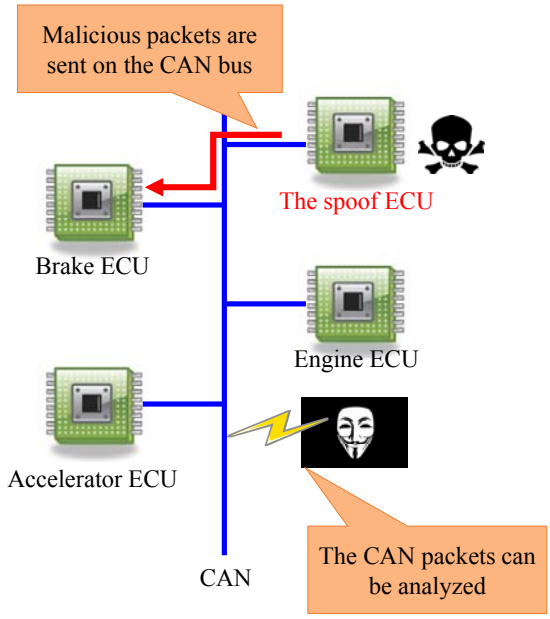

Fig. 1. Example of a spoofing attack on CAN

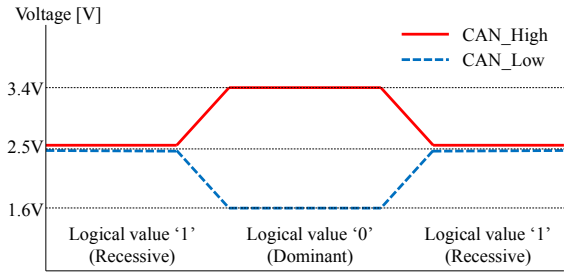

Fig. 2. CAN signal

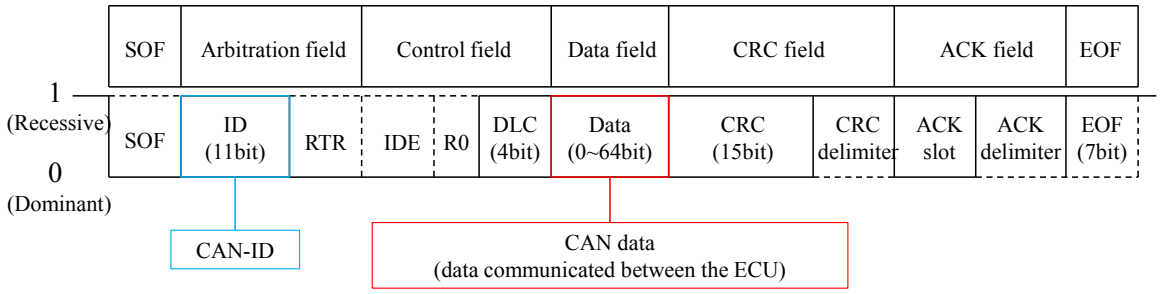

Fig. 3. The structure of data frame

2.2. *PRESENT lightweight block cipher*

Since there is a risk of information leakage from embedded devices, the data they handle must be enciphered. A lightweight block cipher algorithm[9–16] must be used in these devices, due to their resource constraints. PRESENT[9] is such an algorithm that has attracted much attention.

The PRESENT algorithm uses a substitution-permutation network structure with 31 rounds. The block length of PRESENT is 64 bits, and its key length is either 80 or 128 bits. In the encryption processing of PRESENT, a round composed of key addition (addRoundKey), S-box layer (sBoxLayer), and bit-replacement layer (pLayer) is repeated 31 times, as shown in Fig. 4. The sBoxLayer that performs the final addRoundKey is composed of 16 parallel 4-bit S-boxes with 4-bit input and 4-bit output. The pLayer rearranges output bits of sBoxLayer and replaces bit positions following Table 1.

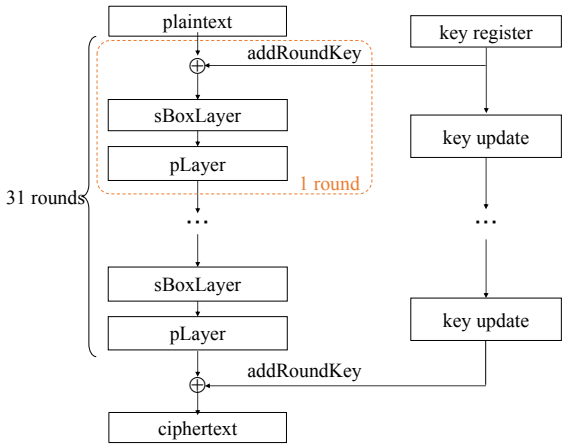

Fig. 4. Encryption processing of PRESENT

Table 1. The sBoxLayer and pLayer

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	8	9	0	A	D	3	E	F	8	4	7	1	2

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p[i]$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$p[i]$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$p[i]$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$p[i]$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

2.3. *Trends in vehicle security*

The EVITA project, performed in Europe during 2008–2011, examined the security of in-vehicle LANs. The project defined three hardware security levels — "EVITA light," "EVITA medium," and "EVITA full" — in order to cover a broad range of applications for in-vehicle LANs. The PRESERVE project succeeded the EVITA project.

In Japan, organizations in the automotive industry, such as the IPA, the Society of Automotive Engineers of Japan, and intelligent transport systems (ITS) Japan, have promoted information security efforts. In particular, the IPA published the Approaches for Vehicle Information Security guide on its website in 2013. In this guide, problems with information security are examined from the planning stage to the disposal stage of vehicles, and in-vehicle equipment is summarized.

3. Encryption Method into which Authentication Feature is Incorporated

Since the payload of CAN communications is 64 bits, neither the advanced encryption standard (AES)[17] nor the data encryption standard (DES)[18], both widely used for smart cards, can be used. The present study uses a lightweight block cipher algorithm based on the PRESENT algorithm, whose block length is 64 bits and which has been standardized by the International Organization for Standardization. In encryption, it is important to protect against replay attacks. Replay attacks are means to invade software. Such attacks intercept passwords and cipher keys, and then use them to pretend to be the user.

In the proposed method, a counter is incorporated into an ECU at the sending side and an ECU at the receiving side. Authentication is performed by inserting the counter value into 8 bits from the least significant bit (LSB) of the 64-bit CAN communications data. The counter value uses only 8 bits, so the values (from 0 to 255) are possible. The counter value counts up (0, 1, 2, ...). After reaching 255, the counter value returns to 0. Subsequently, the counter value counts up from 0 again. The encryption method into which this authentication feature is incorporated is depicted in Fig. 5.

Step 1: As shown in Fig. 5 (1), the counter value is inserted into the last 8 bits of CAN data to be sent by an ECU at the sending side.

Step 2: As shown in Fig. 5 (2), the CAN data, into which the counter value has already been inserted, is encrypted, and the encrypted CAN data are sent to an ECU at the receiving side.

Step 3: As shown in Fig. 5 (3), 1 is added (+ 1) to the counter value by the ECU at the sending side.

Step 4: As shown in Fig. 5 (4), the received CAN data are decrypted by the ECU at the receiving side, and authentication is performed.

Step 5: As shown in Fig. 5 (5), the last 8 bits of the received CAN data are compared with the counter value.

Step 6: As shown in Fig. 5 (6), if the last 8 bits agree with the counter value, the received CAN data are sent to a radio-controlled car. If they disagree, the received CAN data are deleted.

Step 7: As shown in Fig. 5 (7), only if the last 8 bits of

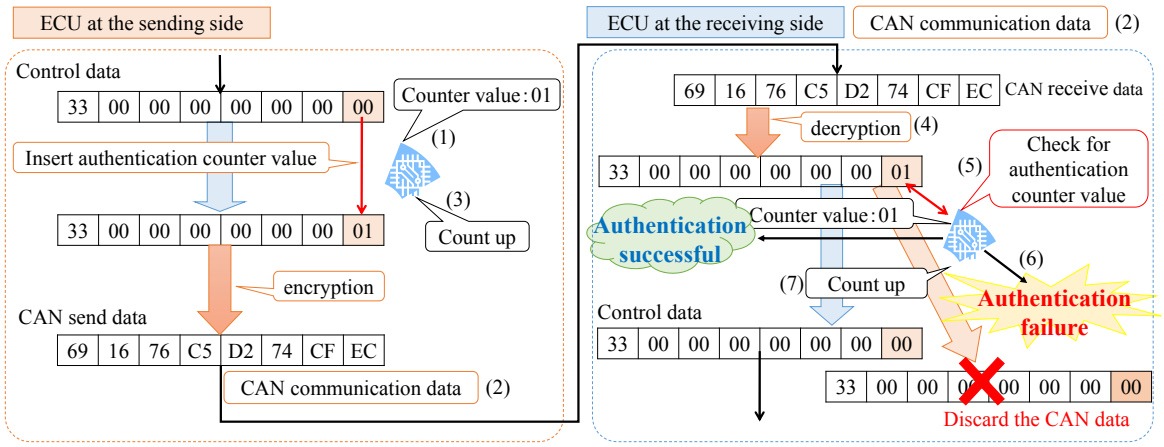

Fig. 5. Proposed authentication method

the received CAN data agree with the counter value, 1 is added (+ 1) to the counter value by the ECU at the receiving side.

4. Evaluation Experiments

4.1. *Experimental environment*

To verify the proposed method, an evaluation system, shown in Fig. 6, was developed. In this evaluation system, an analog voltage value and a switch ON/OFF signal from a controller are received by the ECU at the sending side. The received data are converted into control data and state data in the ECU at the sending side.

Next, the converted data are packed into a CAN message, and the message is sent to the ECU at the receiving side through CAN communications. The ECU at the receiving side unpacks the received CAN message, and converts it into control data.

Finally, pulse width modulation is performed for the voltage value and port control is performed for the switch ON/OFF signal in order to control various devices in the radio-controlled car. A spoof ECU has already intercepted CAN communications data in the ECU at the receiving side, so it sends the wrong control data to the ECU at the receiving side.

4.2. *Evaluation Results*

First, we conducted an experiment to examine whether general CAN communications were performed properly. In the experiment, a radio-controlled car was operated without mounting the proposed method. Figure 7 shows the observed CAN communications data. As shown in this figure, the data consisted of 64 bits, with a payload that contained control data to be sent for the accelerator, brake, steering, headlight, and blinker.

Next, we performed spoofing attacks against general, unencrypted, CAN communications. Specifically, malicious packets were sent on the CAN bus from the spoof ECU. Figure 8 shows the observed data. In this figure, improper control data sent from the spoof ECU are surrounded by a red frame. In the case of general CAN communications, spoofing attacks can be easily performed and cause the radio-controlled car to malfunction, as shown in the figure.

We then used the proposed method between the ECUs at the sending and receiving sides. Figure 9 shows the observed CAN communications data. In the proposed method, CAN communications are encrypted and a counter is incorporated by an ECU at the sending side and an ECU at the receiving side. Therefore, data analysis is more difficult to perform in the proposed

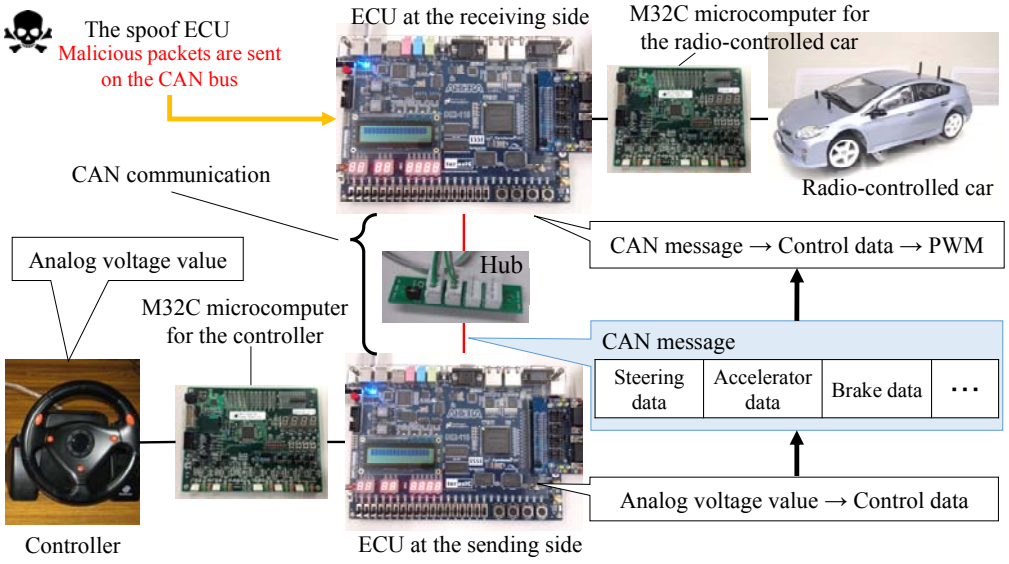

Fig. 6. Developed evaluation system for CAN communications

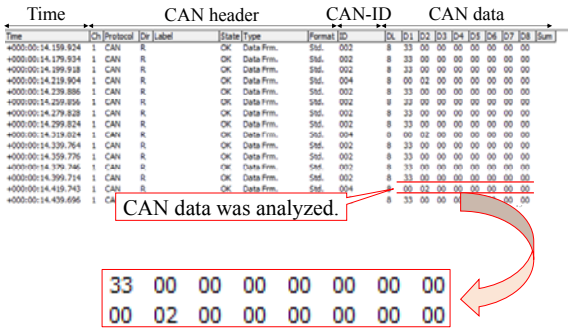

Fig. 7. Observed data (Normal CAN communications)

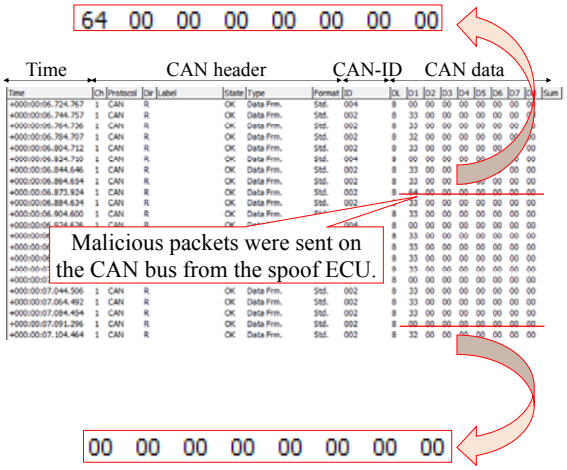

Fig. 8. Observed data (CAN communications with malicious packets)

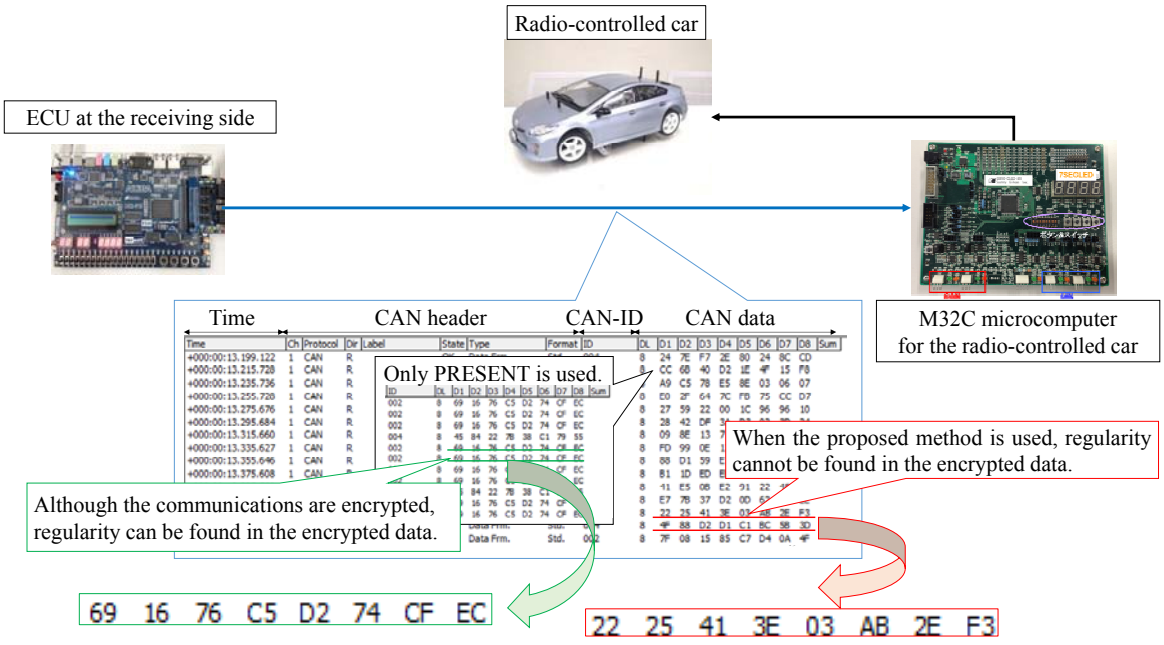

Fig. 9. Observed data (Proposed CAN communications without attacks)

method than in general CAN communications. In the case where only PRESENT is used, although the communications are encrypted, regularity can be found in the encrypted data. When the proposed method is used, regularity cannot be found in the encrypted data, as shown in the figure.

Finally, we performed spoofing attacks against the proposed method. Figure 10 shows the observed CAN communications data.

When the proposed method was used, improper data could not be sent from the spoof ECU. We also performed replay attacks against the proposed method. Data observed in CAN communications, which had been encrypted by PRESENT, were directly sent on the bus by the spoof ECU as a malicious packet. As shown in this figure, the same packet was not repeatedly sent, so that replay attacks are prevented.

5. Conclusion

The present study first examined the foreign and domestic trends of in-vehicle systems, and pointed out the vulnerability of CAN communications. To realize secure communications, the present study then proposed a method using the lightweight block cipher PRESENT. In the proposed method, CAN communications packets were encrypted, and encryption processing that incorporated an authentication feature using a counter was introduced. By using this approach, vehicle systems were protected from both spoofing attacks and replay attacks. Using an FPGA board and a radio-controlled car, an evaluation system compatible with CAN communications standards was developed. Using this evaluation system, the proposed method was verified.

References

1. ISO, ISO 11898-1:2003 – Road vehicles – Controller area network (CAN), International Organization for Standardization, (2003)
2. EVITA, http://www.evita-project.org/
3. PRESERVE, http://www.preserve-project.eu/
4. IPA, http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf (2013)
5. JASPER, https://www.jaspar.jp/index.html
6. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy (SP 2010), (2010), pp.447–462

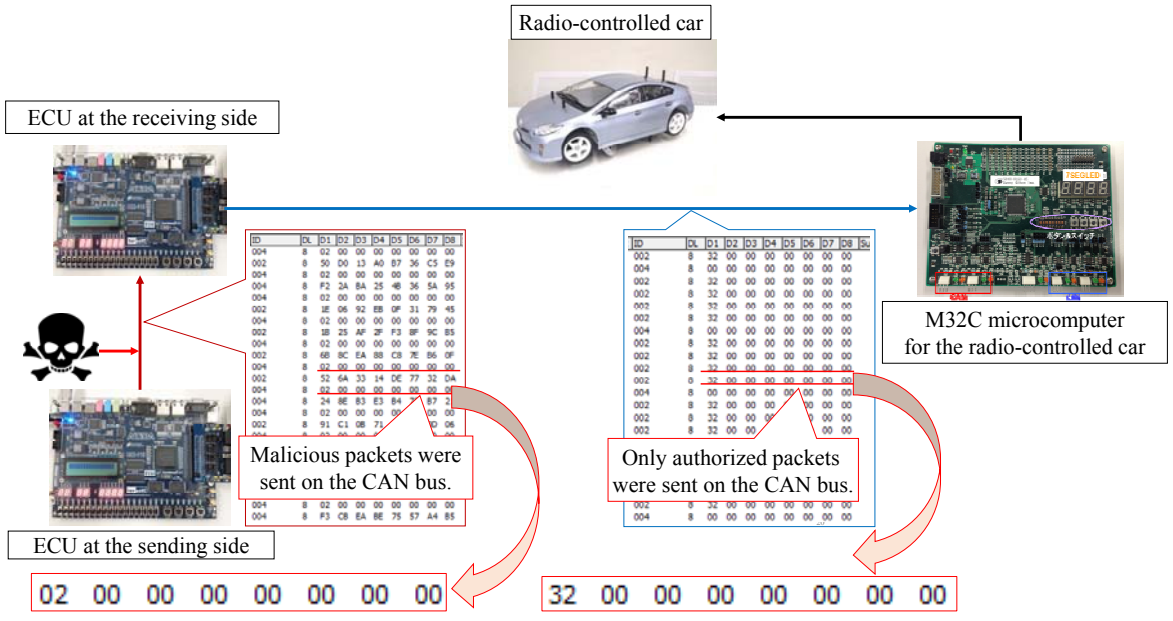

Fig. 10. Observed data (Proposed CAN communications with attacks)

7. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, Comprehensive Experimental Analysis of Automotive Attack Surfaces, Proc. of the 20th USENIX conference of Security, (2011)
8. T. Hoppe, S. Kiltz and J. Dittmann, Security Threats to Automotive CAN Networks — Practical Examples and Selected Short-Term Countermeasures, Proc. of the 27th international conference of Computer Safety, Reliability, and Security (SAFECOMP '08), (Springer-Verlag, 2008), LNCS vol.5219, pp.235–248
9. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, Proc. of Cryptographic Hardware and Embedded Systems (CHES 2007), (Springer-Verlag, 2007), LNCS vol.4727, pp.450–466
10. C. D. Cannière, O. Dunkelman and M. Knežević, KATAN and KTANTAN — A Family of Small and Effcient Hardware-Oriented Block Ciphers, Proc. of Cryptographic Hardware and Embedded Systems (CHES 2009), LNCS vol.5747, (2009), pp.272–288
11. W. Wu, L. Zhang, LBlock: A Lightweight Block Cipher, Proc. of the 9th international conference of Applied Cryptography and Network Security (ACNS 2011), (2011), LNCS vol.6715, pp.327–344
12. J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavum, M. Knežević, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen and T. Yalçin, PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications, Proc. of ASIACRYPT 2012, (Springer-Verlag, 2012), LNCS vol.7658, pp.208–225
13. T. Suzaki, K. Minematsu, S. Morioka and E. Kobayashi, TWINE: A Lightweight, Versatile Blockcipher, Proc. of ECRYPT Workshop on Lightweight Cryptography (LC11), (2011), pp.146–149
14. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita and T. Shirai, Piccolo: An Ultra-Lightweight Blockcipher, Proc. of Cryptographic Hardware and Embedded Systems (CHES 2011), (Springer-Verlag, 2011), LNCS vol.6917, pp.342–357
15. J. Guo, T. Peyrin, A. Poschmann and M. Robshaw, The LED Block Cipher, Proc. of Cryptographic Hardware and Embedded Systems (CHES 2011), (2011), LNCS, vol.6917, pp.326–341
16. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers, The SIMON and SPECK Families of Lightweight Block Ciphers, Cryptography ePrint Archive, Report 2013/404, (2013), http://eprint.iacr.org/
17. National Institute of Standards and Technology (NIST), Announcing the ADVANCED ENCRYPTIOHN STANDARD (AES), Federal Information Processing Standards Publication 197 (2001), http://csrc.nist.gov/publications/fips/index.html/
18. National Institute of Standards and Technology (NIST), DATA ENCRYPTIOHN STANDARD (DES), Federal Information Processing Standards Publication 46-3 (1999)