Adaptive Controller Area Network Intrusion Detection System Considering Temperature Variations

Woojin Jeong, Eunmin Choi, Hoseung Song, Minji Cho, and Ji-Woong Choi, *Senior Member, IEEE*

***Abstract*— Security threats increase as connectivity among vehicles increases. In particular, a lack of authentication, integrity, and confidentiality makes the controller area network (CAN) protocol, which is used in critical domains such as vehicle body and powertrain, vulnerable to threats. In this paper, we propose methods for CAN security enhancement that use a support vector machine (SVM) and the autocorrelation of the received signal to detect a malicious node. Robustness to temperature variation is also considered because autocorrelation is affected by temperature variation. There are two methods based on the degree of uniformity of the temperature distribution. If the temperature is uniformly distributed over the vehicle and the temperature sensor is embedded in the secure node, the first scheme (temperature measurement system) trains data in each segmented temperature range more precisely using multiple classifiers. If not (i.e., a nonuniform temperature distribution or an absence of a temperature sensor), the alternative scheme (all-temperature training system) trains data in all temperature ranges with a single classifier. The performances of the proposed systems are evaluated on a testbed. The proposed method can operate without modifying the CAN protocol because it is based on the characteristics of the physical layer. In addition, security can be enhanced redundantly by the system running independently without authentication protocols.**

***Index Terms*— Controller area network (CAN), intrusion detection system (IDS), transmitter identification, temperature, physical-layer security.**

I. Introduction

ELECTRONIC control units (ECUs) have become increasingly common as automotive technology has advanced to meet the demands of autonomous and connected vehicles. An earlier study [1] estimated that the automotive ECU market would reach $3.29 billion by 2025 with a compound annual growth rate of 4.4 %. In addition, the number of embedded ECUs in a high-performance vehicle is approaching one hundred. To allow these ECUs to communicate, there are many in-vehicle network (IVN) standards, such as the controller area network (CAN), the CAN with flexible data rates (CAN-FD), the local interconnected network (LIN), FlexRay, media-oriented system transport (MOST), and automotive Ethernet [2], [3].

In 1985, Bosch developed the CAN, which was used in a variety of cyber-physical systems (CPSs), including robots, cars, and trains. In terms of cost, reliability, and distributed control, the CAN offers many benefits. The line is typically composed of a single twisted pair to resist electromagnetic interference (EMI) and noise [4]. As a bus network, the CAN operates as a multi-master and its frames are physically shared by all nodes on the line. These benefits of CAN have led to widespread deployment in critical areas such as the powertrain, chassis, and body control domains. However, because the CAN protocol does not include any authentication procedures, it is vulnerable to security threats. An attacker can easily manipulate and inject CAN frames using various external access protocols, such as vehicle-to-everything (V2X) connectivity, Bluetooth, and the universal serial bus (USB) protocol [5].

Many studies of authentication protocols have been proposed for the CAN, particularly group key allocation-based authentication techniques [6], [7], [8]. Because these authentication techniques require changing the CAN protocol, there are drawbacks, such as the necessity to update the firmware of ECUs already installed in vehicles and the communication overhead of the authentication protocol.

Physical-characteristic-based security for CAN has been proposed to supplement the drawbacks of authentication-based methods. Earlier research [9] proposed a method for identifying transmitters based on a transmission delay. The transmission delay of each transmitter varies depending on its location. In two studies [10] and [11], transmitter identification approaches were proposed using the clock offset of the nodes, which is an intrinsic feature of the node, and the time interval of each CAN signal. These approaches, however, have limitations. Additional connections are required at both ends of the CAN bus in [9]. The other two papers [10] and [11] only operate on periodic CAN signals because they use the periodicity of the CAN signal.

Manuscript received 25 March 2022; revised 26 August 2022; accepted 15 October 2022. Date of publication 26 October 2022; date of current version 30 November 2022. This work was supported in part by the Institute for Information and communications Technology Planning and evaluation (IITP) funded by the Korean Government (Ministry of Science and ICT (MSIT)) under Grant 2021-0-01277 and in part by the National Research Foundation of Korea (NRF) funded by the Korean Government (MSIT) under Grant NRF-2021R1A2C2008415. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stefano Tomasin. *(Woojin Jeong and Eunmin Choi are co-first authors.) (Corresponding author: Ji-Woong Choi.)*

Woojin Jeong, Eunmin Choi, Minji Cho, and Ji-Woong Choi are with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu 42988, South Korea (e-mail: kwdnwls@dgist.ac.kr; eunminchoi@dgist.ac.kr; pminjiq@dgist.ac.kr; jwchoi@dgist.ac.kr).

Hoseung Song is with the Department of Technical Strategy, Autocrypt Company Ltd., Seoul 07241, South Korea (e-mail: hssong@autocrypt.io).

Digital Object Identifier 10.1109/TIFS.2022.3217389

1556-6021 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

Recently, temperature-based security systems that consider the vehicle's environment were also proposed. In [12], a method for identifying transmitters based on signal characteristics was proposed. This method identifies the transmitter of each CAN signal by extracting statistical features of the dominant bit as well as the falling edge and rising edge of a signal. When the model trained at 25 °C was evaluated on data at 32 °C and 36 °C, the accuracy of identifying transmitters was 99.99 %. Another study [13] also proposed transmitter identification considering temperature variations using bit time characteristics. After training data at various temperatures, the average transmitter detection accuracy was 99.5 % at temperatures ranging from 17 °C to 41 °C. Other researchers [14] proposed a clock skew method based on a linear relationship with temperature. The average accuracy was 97.2 % within temperatures ranging from 20 °C to 80 °C. However, there are drawbacks, such that the evaluated temperature ranges used in two studies [12] and [13] were relatively narrow compared to the ECU operating range from −40 °C to 125 °C, and the aforementioned method only works with periodic CAN signals [14].

In this paper, we propose an adaptive CAN intrusion detection system (IDS) that considers temperature variations to enable detection over a broad temperature range regardless of the periodicity of the signal. The proposed CAN IDS uses the autocorrelation of the received signal as a physical feature to reflect intrinsic channel characteristics and classifies the transmitter using a support vector machine (SVM). In addition, we provide two methods to consider temperature variations that affect channel characteristics and thus degrade detection performance. The first method, called a temperature measurement system, can be applied under the assumption that temperature information can be obtained by embedding a thermometer in the secure node and the temperature variation is relatively small (e.g., within a 30 °C range). This system trains the data by partitioning the temperature range into increments of 30 °C and generates multiple classifiers for each partitioned temperature range. The second method is an all-temperature training system that trains data over the entire operating temperature range of the vehicle to create a single classifier to identify the transmitter. The performance of the system under temperature variations is also evaluated on a testbed.

II. Background

A. Controller Area Network (CAN)

Before introducing the proposed system, this subsection describes the CAN configuration, signal, channel characteristics, and frame structure. Fig. 1 shows a CAN configuration in which M nodes called ECUs are connected to a bus line. The CAN bus line consists of a twisted pair of CAN_H and CAN_L. CAN transmits a differential signal that is resistant to noise and EMI. Signals are encoded by a non-return-to-zero (NRZ) scheme. To transmit a CAN frame, the transmitter generates a differential signal between lines CAN_H and CAN_L. Bit '1' of the *recessive* state is sent by generating CAN_H and CAN_L with the same 2.5 V voltage level, resulting in a 0 V differential voltage level. For bit '1' of the *dominant* state, the transmitter generates a 2 V differential voltage level between CAN_H and CAN_L at 3.5 V and 1.5 V, respectively. When the *recessive* bit is sent simultaneously with the *dominant* bit, the *dominant* bit overrides the *recessive* bit. Collisions between CAN frames are arbitrated by this property.

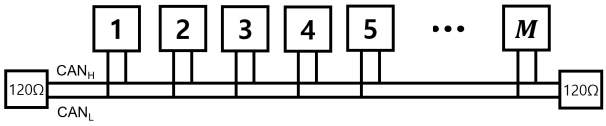


Fig. 1. CAN configuration model.

The channel is determined by the cable characteristics and is primarily affected by the impedance mismatch. Because the CAN channel is configured by a bus topology, the primary points of impedance mismatch are the injunction points: between the node and connected stub line, and between the primary line and stub line. Therefore, the channel gain varies depending on the location of the node and the length of the line and can be used to identify the transmitter's location. According to transmission line theory, channel gain can be modeled using the resistance, inductance, capacitance, and conductance (RLCG) parameters of the cable [15]. Because the RLCG parameters are affected by temperature, the channel gain also varies with temperature. Considering this temperature-related variation in the channel gain, we propose a temperature variation-resistant IDS.

The arbitration field of the CAN data frame contains an 11-bit identifier (ID), and the nature of the *dominant* and *recessive* bits mentioned above determines the priority of the message. IDs are determined based on message content, such as speed and engine temperature, and each node has its own ID set based on the functionality of the node. Thus, each ID is matched to a single transmitter based on the functionality of the transmitter in use [16]. However, the receiver does not check the transmitter with the ID of the received data frame but determines only whether the data is necessary based on the ID to process that frame. In addition, the CAN data frame does not include transmitter and receiver addresses. Therefore, if a malicious node transmits data by substituting the ID of the normal node, the receiver cannot distinguish between normal or attack signals by the received frame because there is no transmitter and receiver addresses. Therefore, it is vulnerable to malicious attacks because the bus topology can send and receive data at all nodes and the frame does not contain the information of the transmitter and receiver. Attack scenarios include bus off, tampering, masquerade, suspend, denial of service (DoS), and data modification [10], [11], [17], [18]. The proposed IDS can detect an attack signal pretending to be a normal signal, such as manipulation, DoS, and masquerade attacks. The proposed IDS can also detect compromised nodes that cause failures by transmitting data with abnormal ID on the bus.

B. Support Vector Machine (SVM)

Many classification methods, including the SVM, k-nearest neighbor (k-NN), and deep neural network algorithms, exist.

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

To achieve high performance, it is important to consider the characteristics and environment of the classification data and to apply an appropriate classifier. The proposed system identifies the transmitter using the autocorrelation of the transition parts of the received CAN signal, meaning that the size of input data (autocorrelation of transition parts) and the number of classes (number of nodes) are relatively small compared to those in certain applications, such as image classification. To prevent receiving a malicious signal and resulting malfunction, it is also important to detect the attack signal prior to finishing the signal reception. Considering these characteristics, it is critical to select an appropriate classification algorithm.

The SVM trains decision boundaries to maximize the distance between classes [19]. After training, the SVM requires a trained decision boundary model for inference. In the k-NN case, the class of the input data is derived based on the class of the k nearest samples. Inference requires relatively more memory and time due to the need for all training data to identify the class of the input data [20]. A deep neural network can also be considered. Adjusting the hyperparameters, which are controllable and performance-affecting values, can result in improved performance. The deep neural network uses a trained model that is similar to an SVM for inference. However, because more hyperparameters are required to optimize the classifier, complexity increases [21]. Constructing a deep network can also lead to an overfitting issue and increase the complexity [21]. Considering the properties of each classifier and the properties of the input data, we use the SVM, which takes less time to infer and has low complexity.

III. Proposed Adaptive Controller Area Network Intrusion Detection System (IDS)

A. Temperature-Dependent Channel Gain

We consider an electric vehicle (EV) environment in this study because the market share of EVs is expected to exceed that of internal combustion engine (ICE) vehicles by 2040 [22]. In [23], the temperature of the EV is affected by the ambient temperature, and the temperature variation across the entire vehicle is relatively small (approximately 6.3 °C). However, EVs may operate in extreme environments as well, including −36 °C and 120 °C [24], [25], where the deviation of temperature distribution may be large if the temperature management system is activated (e.g., battery temperature management to maintain optimum battery performance and heating ventilating and air conditioning for driver convenience [26], [27]). As a result, we propose systems based on possible scenarios for temperature distribution. One system operates with the presumption that the temperature is distributed uniformly, while the other does not. In this study, the uniform distribution means that a variation is less than a specific range, and this specific range is the segmented interval of the temperature measurement system; the segmented interval is 30 °C in this paper.

The configuration of the CAN bus used for the performance evaluation is shown in Fig. 2. We assume that there are nine nodes (i.e., $M = 9$). Node 9 is the receiver acting as the secure node and the others are the transmitters. The measured

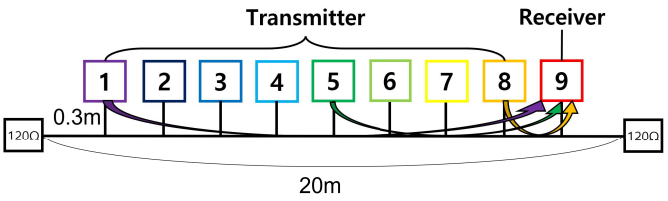


Fig. 2. CAN bus configuration for performance evaluation.

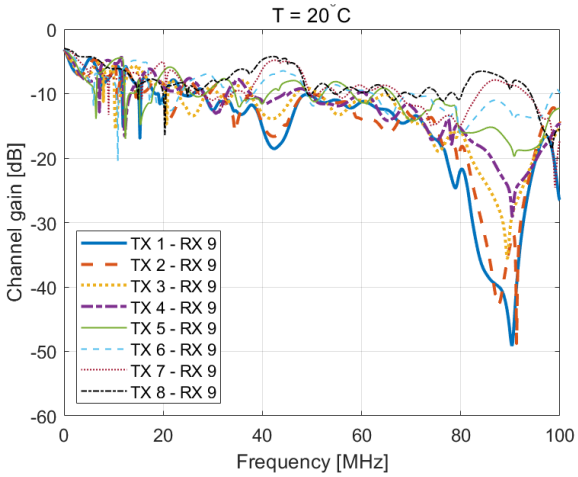


Fig. 3. Measurement of CAN bus channel at room temperature (20 °C).

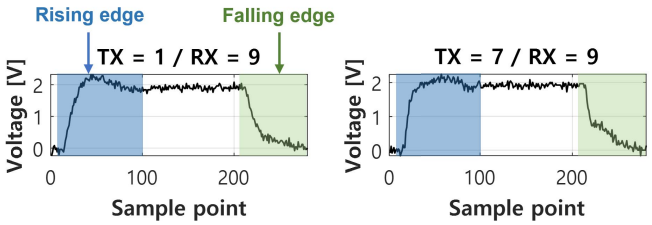
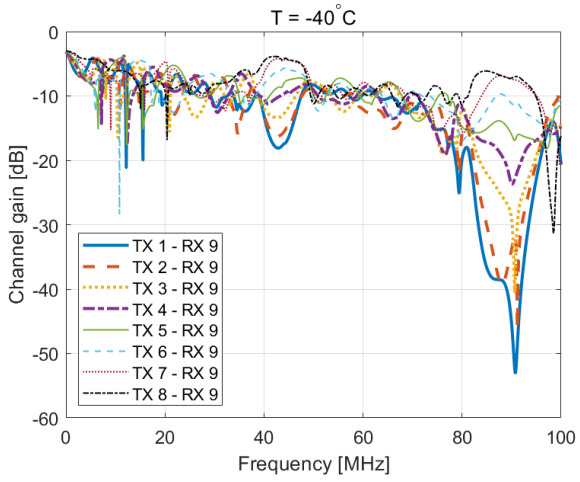


Fig. 4. Received CAN signal at node 9 transmitted by node 1 and 7.

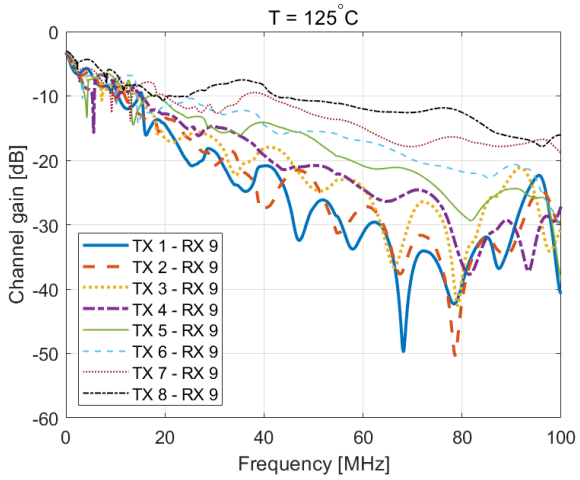
channel gain for each transmitter (nodes 1∼8) and receiver (node 9) pair at room temperature (20 °C) is shown in Fig. 3. Because the channel gain of each pair exhibits a marked difference in high frequency bands, the secure node requires a high sampling rate to take advantage of this distinguishable property. Fig. 4 shows the received signal of one CAN bit transmitted by nodes 1 and 7 and received by node 9, where the sample point on the x-axis represents the digital sample index of the analog-to-digital converter output of node 9 with a high sampling rate of 100 MHz. The transition part of the CAN signal, where the bit level is changed depends on the channel (i.e., transmitter location), which occurs because the transition part contains a high-frequency component, and the channel gain of each transmitter differs in the high-frequency bands. Therefore, to train high-frequency components in the time domain intensively, we extracted the transition part of the received CAN signal.

As mentioned earlier, the vehicle is in an environment with high-temperature fluctuations with an operating temperature

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.



(a)



(b)

Fig. 5. (a) Channel gain measurement when T = −40 °C. (b) Channel gain measurement when T = 125 °C.

ranging from −40 °C to 125 °C. The channel characteristics change with the temperature because temperature affects the cable's resistance, inductance, capacitance, and conductance. Fig. 5a and Fig. 5b show the measured channel gain at −40 °C and 125 °C, respectively. These figures show that the channel gain changes with temperature and that the distortion is more severe at a higher temperature. Because the proposed system identifies the transmitter based on the channel characteristics, it is necessary to consider these characteristics according to temperature variations.

B. Proposed Temperature Variation-Resistant CAN IDS

To use the distinguishable features of the channel gain of each transmitter, we used the autocorrelation value of the received signal:

$$y[k] = x[k] * h[k] + w[k], \tag{1}$$

where k is the sampling point; $x[k]$ is the transmitted signal; $h[k]$ is a channel impulse response; $w[k]$ is the noise; and $*$ denotes convolution. Autocorrelation refers to the correlation between a signal and its own time-shifted delayed signal [28]. Fig. 6 shows an example of obtaining the autocorrelation value between samples. The autocorrelation value of the received signal is calculated as follows:

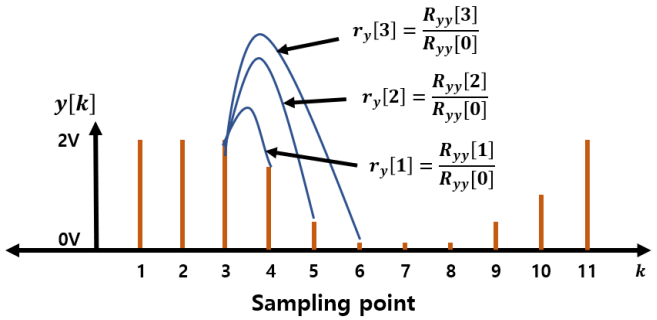


Fig. 6. Examples of autocorrelation value between samples of CAN signal.

$$\begin{aligned} r_y[n] &= \frac{R_{yy}[n]}{R_{yy}[0]} = \frac{E[y[k]y[k+n]]}{E[y[k]^2]} \\ &= \frac{R_{hh}[n] * R_{xx}[n] + R_{ww}[n]}{R_{hh}[0] * R_{xx}[0] + R_{ww}[0]}, n = 1, 2, \ldots, N, \end{aligned} \tag{2}$$

where n is the time-shift value, $n = 1, 2, \ldots, N$ and $R[n]$ is the autocorrelation function. The autocorrelation value of the received signal reflects the autocorrelation of the channel impulse response as $R_{hh}[n]$ in (2). Representing the channel impulse response, $R_{hh}[n]$ can be rewritten as:

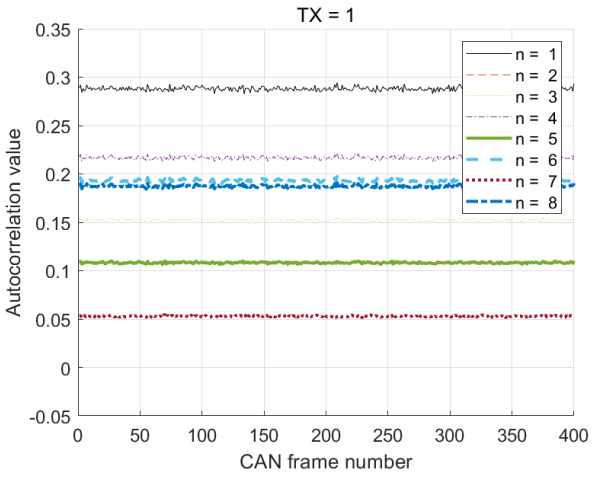
$$R_{hh}[n] = E[h[k]h[k+n]], n = 1, 2, \ldots, N, \tag{3}$$

which represents the correlation between the channel impulse response and the corresponding n-th delayed response. If the channel attenuation is more severe, the delay of the channel impulse response is more widely dispersed, which indicates that the channel impulse response is correlated even at a high n. Therefore, we calculated the autocorrelation value of the received signal according to n, which implies a distinguishable channel impulse response according to the transmitter, and trained it to identify the transmitter using the SVM.

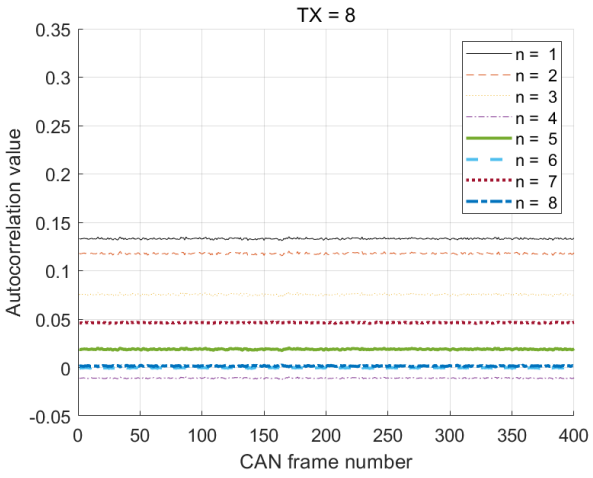
Fig. 7a and Fig. 7b show the calculated autocorrelation values of the CAN signals of nodes 1 and 8, as received by node 9 in Fig. 2, where n ranges from 1 to 8. The x-axis represents the index of 400 different received CAN signals, and the y-axis is the autocorrelation value. Node 1 shows higher autocorrelation values according to n than node 8 because node 1 is further from receiver node 9 than node 8. The more attenuated channel gain causes the channel impulse response to be more spread, which raises the autocorrelation values at a high n.

Fig. 8 shows the adaptive intrusion detection system based on autocorrelation. There are two proposed methods according to how the temperature variation is reflected, and the preprocessed method is identical. The received signal was preprocessed as follows. After the start of frame (SOF) at the beginning of the CAN data frame, the received signal is sampled at a high sampling rate of 100 MHz. The system concurrently extracts the transition part from the sampled signal and the ID from the data frame. To classify the transmitter,

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.



(a)

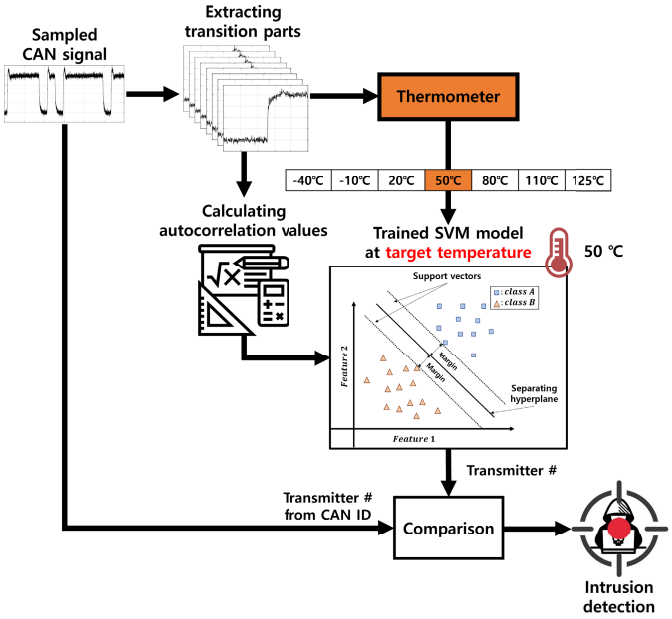


(b)

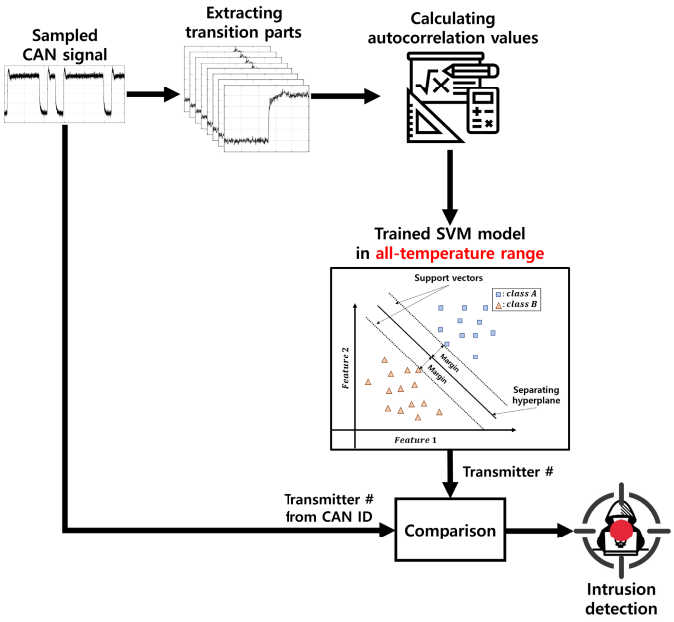
Fig. 7. (a) Autocorrelation values of node 1. (b) Autocorrelation values of node 8.

the SVM uses the autocorrelation values calculated from the transition parts as input.

As mentioned earlier, the vehicle is an environment in which the temperature changes; thus, the autocorrelation values also change. We propose two training methods based on the uniformity of the temperature distribution over the vehicle to reflect the effect of temperature change. When the temperature distribution of the vehicle is relatively uniform within 30 °C and the secure node has an integrated temperature sensor, the first method, called the temperature measurement system, uses the temperature information as an input and generates multiple classifiers based on the temperature (Fig. 8a). The second method, called the all-temperature training system, classifies the transmitter by training the autocorrelation values at all temperatures when the temperature is unknown or nonuniformly distributed (Fig. 8b). Specifically, in the first method, the training temperature is divided into regular intervals in the operating temperature range. The SVM generates multiple classifiers based on the temperature interval by training each temperature segmented by the interval. The first method is more accurate than the all-temperature training system but uses



(a)



(b)

Fig. 8. (a) Autocorrelation-based adaptive intrusion detection system with temperature measurement. (b) Autocorrelation-based adaptive intrusion detection system with all-temperature training.

more memory because the system requires multiple trained classifiers according to the temperature. In the comparison block, an intrusion is determined based on whether the transmitter identified by the SVM matches the transmitter identified by the ID of the signal.

IV. Performance Evaluation of Proposed System

We consider the transmitter identification accuracy and the attack detection accuracy as performance evaluation metrics. The transmitter identification accuracy is the probability of

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

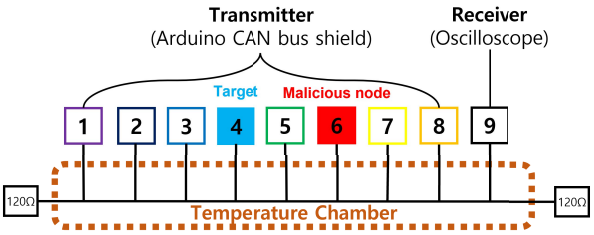


Fig. 9. Testbed configuration.

TABLE I
CAN ID OF EACH NODE FOR THE EXPERIMENT

Transmitter node	1	2	3	4	5	6	7	8
CAN ID	0A0	153	260	164	316	18F	43F	690

TABLE II
PARAMETERS FOR PERFORMANCE EVALUATION

Parameter	Value
CAN symbol rate (= bit rate)	500 kbps
Sampling rate	100 MHz
# of transmitters	8
Attack node number	6
Training dataset	2400
Test dataset	800
Attack dataset	400
# of transition part samples	70
Temperature range [°C]	[-40, 125]
Temperature interval [°C]	30
# of time-shift value of autocorrelation (N)	10, 20, 30, 40

correctly identifying the transmitter in the test dataset and is evaluated in the absence of an attack signal. The attack detection accuracy is the probability of correctly detecting attack signals in the test dataset when attack signals are present. The attack signal is generated by modifying its ID to that of another node so that the ID of the received CAN signal differs from the classification result of the SVM. As described in Section III, the all-temperature training system trains data in all temperature ranges, and the performance of this system is evaluated without prior knowledge of the temperature. Using the signals measured in the testbed, we performed simulations in MATLAB to evaluate the performance of the proposed systems.

Fig. 9 shows the configuration of the testbed. We assumed that node 4 is a victim node, and that node 6 is a malicious node that is sending attack signals using the CAN ID of node 4. To evaluate the performance at various temperatures, we placed the channel (i.e., bus cable) in a temperature chamber. The experiment with the testbed is shown in Fig. 10. Arduino CAN bus shields served as transmitters, while an oscilloscope (Tektronix DPO7254C) served as the receiver. Each CAN bus shield transmitted a CAN signal with a unique ID (see Table I) and a randomly generated data field. Table II shows the parameters for the performance evaluation. The temperature interval of the dataset is set to 30 °C. There are 10 to 40 time-shift values of autocorrelation N for the two experimental trials of the performance evaluation according to each method.

To compare the results, the performance outcomes of training at room temperature, training in all-temperature ranges, and training at each temperature interval are evaluated. When N is set to 10, the accuracy of transmitter identification and attack detection is shown in Fig. 11 and Fig. 12, respectively.

Fig. 11a and Fig. 11b show the transmitter identification accuracy at each temperature interval and the average transmitter identification accuracy over the operating temperature range, respectively. Training only at room temperature decreases the accuracy at other temperatures, and the average accuracy is 74.11 % in the operating temperature range. The all-temperature training system has comparable performance across all temperature ranges, with less accuracy at room temperature and better accuracy at other temperatures than training at room temperature. The average accuracy of the all-temperature training is 9.21 % higher than the result of training at room temperature. The temperature measurement system offers the highest accuracy across all temperature ranges because it contains a precisely trained model of each temperature interval. The average accuracy of the temperature measurement system is 16.37 % higher than the result of training at room temperature.

Fig. 12a and Fig. 12b show the attack detection accuracy at each temperature interval and the average attack detection accuracy over the operating temperature range, respectively. The results for attack detection accuracy show a similar tendency to those for transmitter identification accuracy. The average accuracy of the all-temperature training system is 8.15 % higher than the result of training at room temperature. The temperature measurement system shows the best performance and has 14.36 % higher average accuracy than the result of training at room temperature.

Because the autocorrelation value is related to the channel impulse response, the channel impulse response is reflected more as the number of time-shift values N used for the autocorrelation value increases, making it easier to distinguish for each transmitter. As a result, the performance of the proposed system improves as N increases. Fig. 13 shows the average transmitter identification accuracy as a function of N used for the autocorrelation values. As mentioned previously, the accuracy of the proposed systems increases as N increases. When N is 40, the average transmitter identification accuracy rates of the all-temperature training system and temperature measurement system are 97.60 % and 99.43 %, respectively. Increasing N causes longer inference times because the system must wait until all of the autocorrelation values have been collected.

Table III compares the conventional temperature-related IDS schemes with the proposed scheme. The table represents the IDS scheme, the validated temperature range, and the accuracy. The proposed scheme shows similar accuracy to conventional schemes (e.g., 99.43 % accuracy for a temperature measurement scheme with $N = 40$) but provides the

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

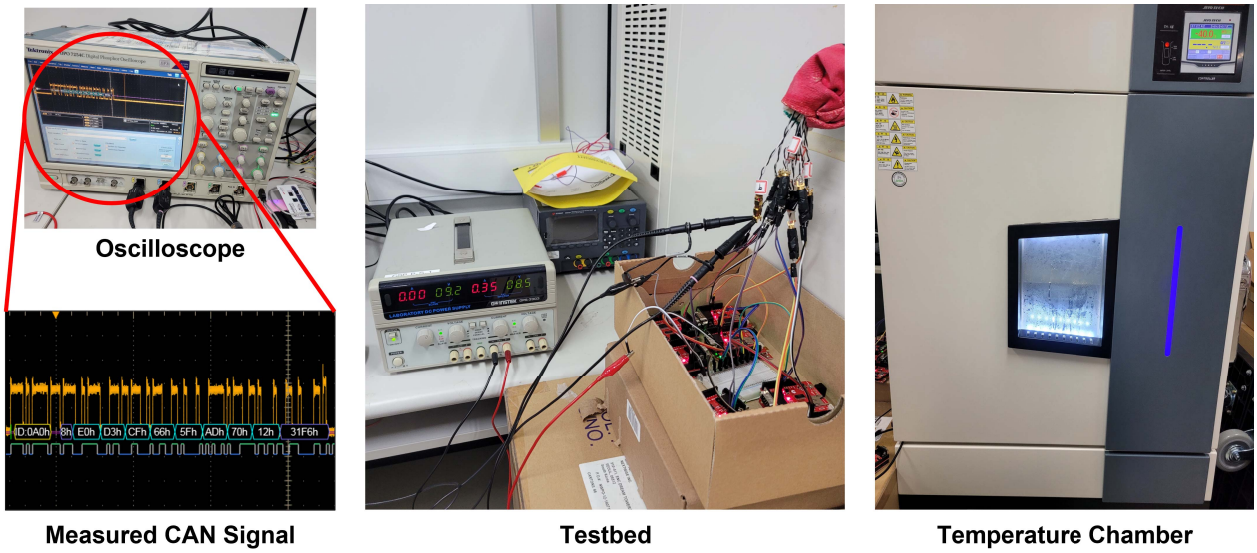


Fig. 10. Testbed experiment.

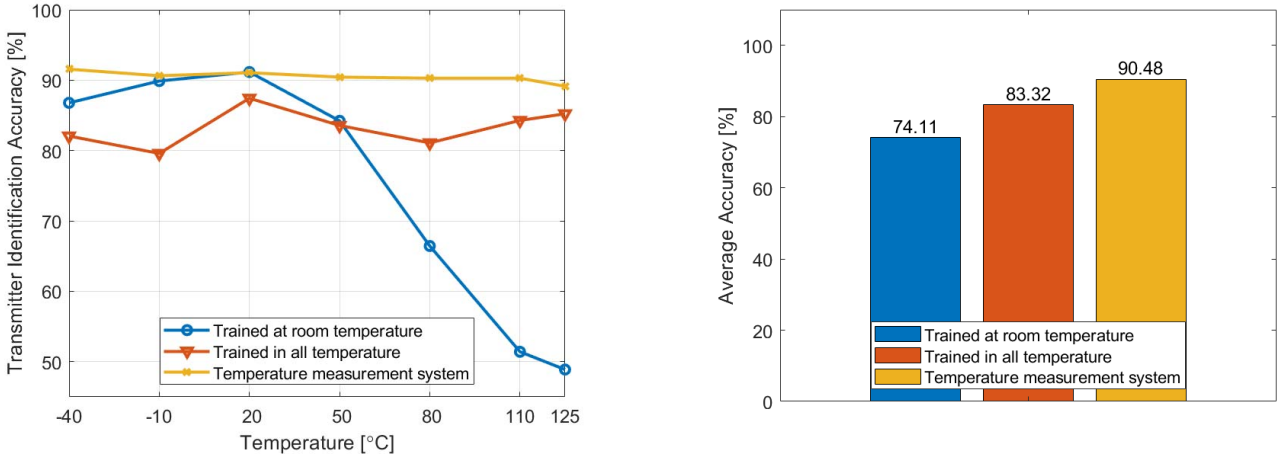


Fig. 11. (a) Transmitter identification accuracy at each temperature interval ($N = 10$). (b) Average transmitter identification accuracy ($N = 10$).

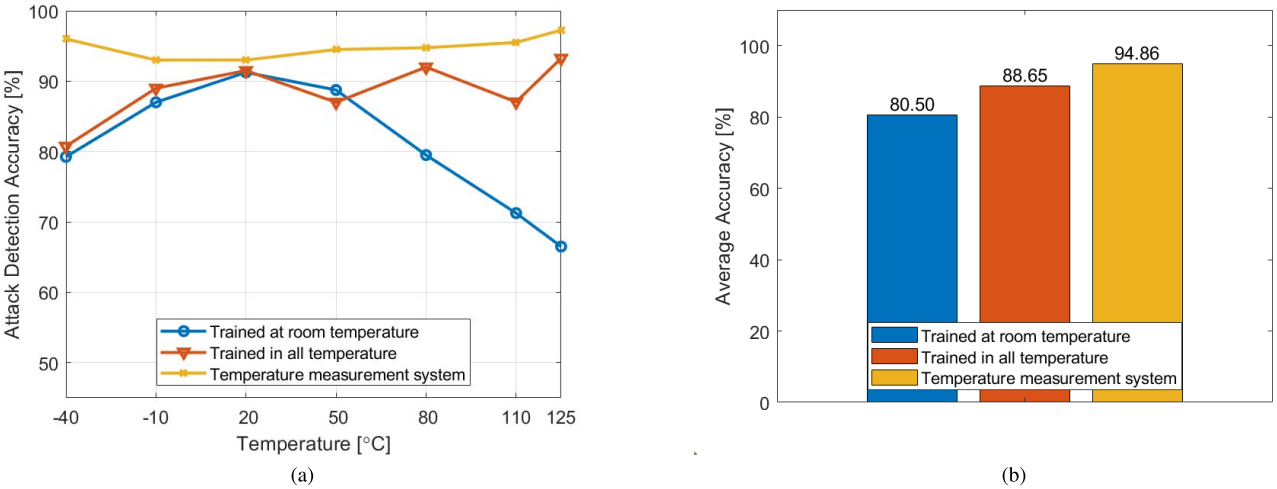


Fig. 12. (a) Attack detection accuracy at each temperature interval ($N = 10$). (b) Average attack detection accuracy ($N = 10$).

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

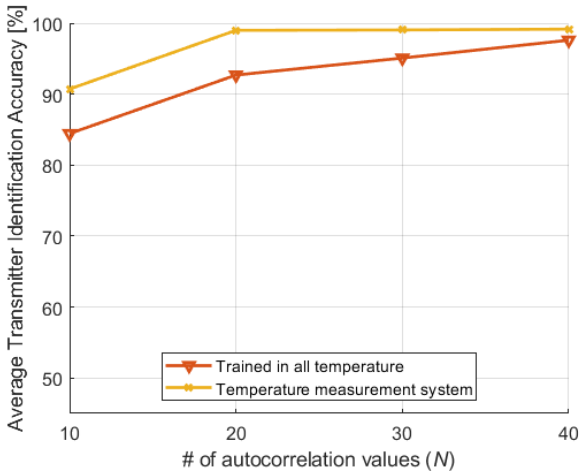


Fig. 13. Average transmitter identification accuracy according to the number of autocorrelation values.

TABLE III
COMPARISON

Paper	Year	Scheme	Temperature range	Accuracy
[12]	2018	Statistical features of signal	32∼36 °C	99.99 %
[13]	2019	Bit time characteristics	17∼41 °C	99.50 %
[14]	2020	Clock offset	20∼80 °C	97.20 %
Proposed	2022	Channel characteristics	-40∼125 °C	99.43 % (temperature measurement) 97.60 % (all-temperature training)

widest temperature range, validating the highest robustness to temperature variations.

V. CONCLUSION

In this paper, we propose two adaptive CAN intrusion detection systems that use autocorrelation values considering temperature variation. The proposed systems use the fact that each transmitter on the CAN bus has distinct channel characteristics. The systems compare the classification result using the autocorrelation values of the received CAN signal and the identified result using the received CAN ID to identify the transmitter and detect an intrusion. The operating temperature of the vehicle ranges from −40 °C to 125 °C. Temperature variations in this range affect the physical features of the CAN system, such as the channel characteristics. To consider temperature variations, a temperature measurement system and an all-temperature training system are proposed. The temperature measurement system identifies the transmitter as a trained system at the measured temperature, assuming that the temperature is uniformly distributed over the vehicle and using the temperature information from the secure node's thermometer. The all-temperature training system is trained using all data in the operating temperature range. During training, the system identifies the transmitter even for data without prior knowledge of the temperature or uniformity of the temperature variation. Results show that the temperature measurement system achieves a higher accuracy than the all-temperature training system but requires more memory, computing power, and cost.

The performance of the proposed systems is evaluated on a testbed. Compared to the result of training at room temperature, the proposed systems achieve higher accuracies. The performance of the proposed systems can be improved because it describes channel characteristics more accurately by increasing the number of autocorrelation values used for classification. Conversely, the inference time lengthens because the system has to wait until it has sufficient autocorrelation values.

REFERENCES

[1] Grand View Research. (2019). *Automotive Electronic Control Unit Market Size, Share, & Trends Analysis Report by Application, by Propulsion Type, by Capacity, by Vehicle Type, by Region, and Segment Forecasts*. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/automotive-ecu-market

[2] W. Zeng, M. A. S. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1552–1571, 3rd Quart., 2016.

[3] D. Paret, *Multiplexed Networks for Embedded Systems: CAN, LIN, FlexRay, Safe-by-Wire*. New York, NY, USA: Wiley, 2007.

[4] *CAN Specification, Version 2.0, Robert Bosch GmbH*, Robert Bosch, Gerlingen, Germany, 1991.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Sec. Symp.*, 2011, pp. 1–6.

[6] S. Jain and J. Guajardo, "Physical layer group key agreement for automotive controller area networks," in *Proc. Conf. Cryp. Hard. Embed*, May 2016, pp. 85–105.

[7] B. Groza, S. Murvay, A. V. Herrewege, and I. Verbauwhede, "LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks," in *Proc. Conf. Cryp. Net. Sec*, Dec. 2012, pp. 185–200.

[8] J. Hur and Y. Lee, "A reliable group key management scheme for broadcast encryption," *J. Commun. Netw.*, vol. 18, no. 2, pp. 246–260, Apr. 2016.

[9] P.-S. Murvay and B. Groza, "TIDAL-CAN: Differential timing based intrusion detection and localization for controller area network," *IEEE Access*, vol. 8, pp. 68895–68912, 2020.

[10] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. USENIX Sec. Symp.*, May 2016, pp. 911–927.

[11] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2016, pp. 63–68.

[12] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 787–800.

[13] J. Zhou, P. Joshi, H. Zeng, and R. Li, "Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network," *ACM Trans. Embedded Comput. Syst.*, vol. 18, no. 6, pp. 1–23, Jan. 2020.

[14] M. Tian, R. Jiang, H. Qu, Q. Lu, and X. Zhou, "Advanced temperature-varied ECU fingerprints for source identification and intrusion detection in controller area networks," *Secur. Commun. Netw.*, vol. 2020, Sep. 2020, Art. no. 8834845.

[15] P. Golden, H. Dedieu, and K. S. Jacobsen, *Fundamentals of DSL Technology*. Boca Raton, FL, USA: CRC Press, 2005.

[16] J. Yajima, T. Hasebe, and T. Okubo, "Data relation analysis focusing on plural data transition for detecting attacks on vehicular network," in *Proc. Conf. Net. Info. Sys.*, 2019, pp. 270–280.

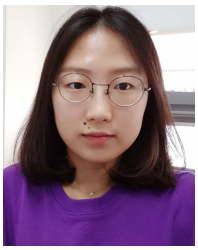
[17] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1044–1055.

[18] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. Conf. Det. Intru. Mal. Vul. Assess.*, Aug. 2017, pp. 185–206.

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.

[19] V. Kecman, "Support vector machine—An introduction," in *Support Vector Machines: Theory and Applications*, L. Wang, Ed. Berlin, Germany: Springer, 2005, pp. 1–47.
[20] P. Cunningham and S. J. Delany, "K-nearest neighbour classifiers—A tutorial," *ACM Comput. Surv.*, vol. 54, no. 6, pp. 1–25, Jul. 2022.
[21] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, Apr. 2017.
[22] C. McKerracher, A. O'Donovan, N. Albanese, N. Soulopoulos, and D. Doherty. (2021). *Electric Vehicle Outlook 2021*. BloombergNEF. [Online]. Available: https://about.bnef.com/electric-vehicle-outlook/
[23] D. Svorc, T. Tichy, and M. Ruzicka, "Detection of the electric vehicle using thermal characteristics," in *Proc. Smart City Symp. Prague (SCSP)*, Jun. 2020, pp. 1–5.
[24] C. Johnna. *Teslas & Other EVs in Extreme Cold (-36° C), CleanTechnica*. Accessed: Jan. 21, 2020. [Online]. Available: https://cleantechnica.com/2020/01/21/teslas-other-evs-in-extreme-cold-36c/
[25] E. D. Staff. *Electric Car Range in Extreme Heat, Electric Driver*. Accessed: Jul. 16, 2021. [Online]. Available: https://electricdriver.co/articles/electric-car-range-in-extreme-heat/
[26] C. Zhou, Y. Guo, W. Huang, H. Jiang, and L. Wu, "Research on heat dissipation of electric vehicle based on safety architecture optimization," *J. Phys., Conf.*, vol. 916, Oct. 2017, Art. no. 012036.
[27] Brianp. *Proper Auto A/C Vent Temperature: How Cold or Hot Should be it Blow? Drivezone*. Accessed: Aug. 12, 2021. [Online]. Available: https://drivrzone.com/proper-auto-ac-vent-temperature/
[28] P. F. Dunn and M. P. Davis, *Measurement and Data Analysis for Engineering and Science*, 4th ed. Boca Raton, FL, USA: CRC Press, 2017.

Woojin Jeong received the B.S. degree from the School of Undergraduate Studies, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2019, and the M.S. degree from the Department of Electrical and Engineering and Compute Science (EECS), Daegu Gyeongbuk Institute of Science and Technology (DGIST), in 2022. His research interests include in-vehicle networks and vehicular security.



Eunmin Choi received the B.S. degree from the Department of Electronics Engineering, Kyungpook National University, Daegu, South Korea, in 2014, and the M.S. degree from the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, in 2017, where she is currently pursuing the Ph.D. degree. Since 2015, she has been with the Department of Electrical Engineering and Computer Science, DGIST. Her research interests include in-vehicle networks, vehicular security, and high-speed link.

Hoseung Song received the B.S. and M.S. degrees from the Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2019 and 2022, respectively. He is currently with AUTOCRYPT, Seoul, South Korea. His research interests include in-vehicle networks, such as in-vehicle SerDes and Automotive Ethernet.

Minji Cho received the B.S. degree from the Department of Electronics Engineering, Incheon National University, Incheon, South Korea, in 2017. She is currently pursuing the M.S. degree with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea. Since 2021, she has been with the Department of Electrical Engineering and Computer Science, DGIST. Her research interests include in-vehicle networks.

Ji-Woong Choi (Senior Member, IEEE) received the Ph.D. degree from Seoul National University, Seoul, South Korea, in 2004. From 2005 to 2007, he was a Post-Doctoral Researcher with Stanford University, Stanford, CA, USA. From 2007 to 2010, he was at Marvell Semiconductor, Santa Clara, CA, USA. Since 2010, he has been with the Department of Electrical Engineering and Computer Science (EECS), Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, as a Professor. His research interests include communication theory, vehicular communications, and brain–computer interface.

Authorized licensed use limited to: Concordia University Library. Downloaded on March 17,2024 at 12:58:39 UTC from IEEE Xplore. Restrictions apply.