Intrusion Detection System for In-Vehicle Networks

Yoshihiro HAMADA*, Masayuki INOUE, Naoki ADACHI, Hiroshi UEDA,
Yukihiro MIYASHITA, and Yoichi HATA

In light of the security incident of the Jeep Cherokee in 2015, where a vehicle was illegally controlled remotely using spoofing messages inserted via a public mobile network, security measures have become one of the most crucial issues in the realization of autonomous driving and connected cars. Taking security measures for each unknown cyberattack requires quick detection of attacks that happen throughout the life cycle of the vehicles. This paper introduces an intrusion detection system (IDS) to detect spoofing messages at the central gateway. Additionally, we report on the detection performance of the system using messages from an actual in-vehicle network.

Keywords: intrusion detection system, in-vehicle network, unknown cyberattack, central gateway, security

1. Introduction

Modern vehicles have 70 to 100 embedded controllers known as electronic control units (ECUs) connected via in-vehicle networks. These ECUs achieve safety driving and convenience by sharing control data with external services via networks in and outside of the vehicle. Meanwhile, the possibility of cyberattacks has been pointed out, in which the vehicle's communications with the aforementioned external services are abused for unauthorized remote control over the vehicle. Countering cyberattacks has become an urgent issue.[1] In order to take suitable security measures to protect vehicles from cyberattacks, it is necessary to detect attacks on the vehicles. An intrusion detection system (IDS) is known as a means to serve for this purpose. The product life of a general vehicle model is more than 10 years. This implies that the vehicle would be subject to cyberattacks that are unknown at the time of development. Consequently, it is critical for an in-vehicle IDS to detect unknown cyberattacks. To detect unknown cyberattacks, an anomaly-based IDS is effective, detecting attacks based on the degree of deviation from the normal state of the monitored subject. However, research on conventional anomaly-based IDSs has revealed that they do not do well in identifying spoofing messages that cyber attackers send and insert in in-vehicle networks. By identifying inserted spoofing messages, it becomes possible to reduce the time taken before implementing concrete countermeasures and to delimit the scope of the countermeasures. Therefore, this paper proposes an anomaly-based detection system with a high detection capability for monitoring control data contained in the payload. In addition, the detection performance of this detection system is also reported, being evaluated with traffic data under the Controller Area Network (CAN) protocol commonly used by in-vehicle networks.

2. CAN Protocol and Security Threats

2-1 Features of CAN

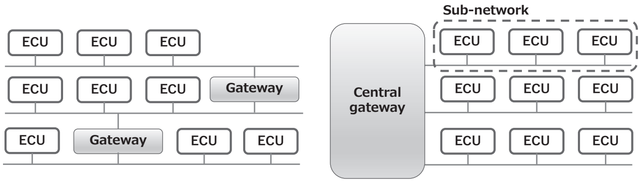
The CAN protocol and the CAN with Flexible Data Rate (CAN FD) protocol exist. The CAN protocol was standardized by ISO 11898-1 (2003).[2] The CAN FD protocol was standardized by ISO 11898-1 (2015)[3] as a revision to ISO 11898-1 (2003). These protocols use a bus topology with multiple nodes (ECUs). Of these nodes, one that has obtained the transmission right through bus arbitration broadcasts a payload comprised of up to 8 bytes (CAN) or 64 bytes (CAN FD) to communicate low-latency messages for control systems.

2-2 Communication characteristics

Over CAN, messages are sent in the CAN frame format provided with a CAN-ID, which is a unique identifier over an in-vehicle network, in two patterns. One is a transmission pattern used to send CAN frames cyclically for the notification of key control information, such as the vehicle speed, engine speed, and accelerator position. The other is a transmission pattern intended for noncyclic messages for the notification of events, such as unlocking and locking of the doors.

2-3 Network configuration

The CAN protocols use a bus topology. The maximum number of connected ECUs per bus is limited. For this reason, systems that use many ECUs make up a network by incorporating gateways to relay from one bus to another, as shown in Fig. 1 (a). With these systems, the presence of multiple gateways between buses results in an increasing communication delay. Figure 1 (b) illustrates a network that incorporates a central gateway, in which the network consists of sub-networks assigned to different functional lines. Connecting these sub-networks with a single gateway reduces communication delay.



a) Connection via gateways b) Connection via a central gateway

Fig. 1. Network configuration

2-4 Security threats

Koscher et al. pointed out the following three vulnerabilities of the CAN protocols[4]: (1) control information on a network can be easily analyzed; (2) spoofing messages can be easily inserted into the network; and (3) the CAN protocols are vulnerable to denial-of-service (DoS) attacks. In this regard, spoofing messages are inserted or DoS attacks are made via an attacker ECU connected to the CAN bus, as represented in Fig. 2. The attacker ECU is a normal ECU until its firmware is tampered with or an unauthorized ECU connected to the network.

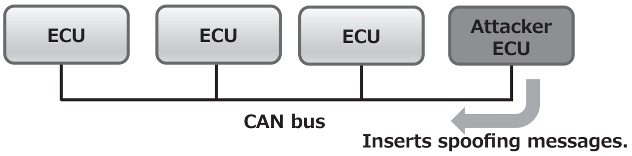


Fig. 2. Spoofing messages inserted by an attacker ECU

3. In-Vehicle Network Security Measures

3-1 Conventional technology

Studies on security measures for in-vehicle networks are divided into the following two classes. Vehicles with a long product life require an IDS to ensure continued security measures even when its secure communications are nullified by an unknown cyberattack.

(A) Secure communications
Security measures at the level of network protocol

(B) IDS
Designed to operate at a higher level than the network protocol to detect dubious operations of applications or networks

3-2 IDS

Two types of IDSs exist: signature-based and anomaly-based. These systems detect an intrusion by detecting dubious behaviors of the monitored subject. The signature-based system defines examples of anomalous usage of the monitored subject and detects operations that coincide with the definition of dubious. The anomaly-based system defines normal operations of the monitored subject and detects those that depart from the definition of dubious. Unknown cyberattacks can only be detected by the anomaly-based detection system.

4. In-Vehicle IDS

4-1 Newly developed system

Sumitomo Electric Industries, Ltd. is developing an anomaly-based in-vehicle IDS, which has three monitoring levels distinguished according to the constituent elements of the in-vehicle network, as shown in Fig. 3. At higher monitoring levels, the system monitors splintered subjects, facilitating the identification of the attacked subject. As a result, it becomes easier to develop specific measures to counter the attack. However, this requires the system to monitor an increasing overall number of subjects. Consequently, in an on-board environment, which is subject to memory capacity and CPU speed limitations, it is difficult for a high-level monitoring system to monitor the entire in-vehicle network if no other monitoring system is used. Sumitomo Electric's system combines the above-mentioned three monitoring levels to apply a low-level system to monitor the entire in-vehicle network and a high-level system to monitor specific critical subjects in the vehicle.

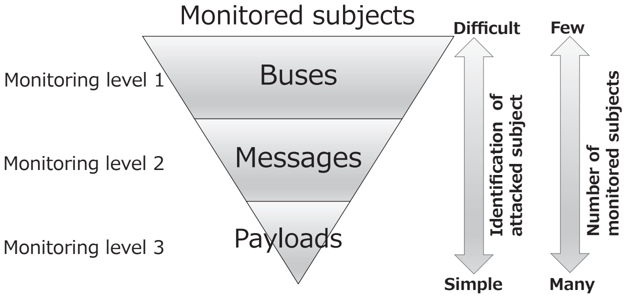


Fig. 3. Anomaly-based in-vehicle IDS

4-2 Shortcomings of conventional in-vehicle IDSs

One challenge facing conventional in-vehicle IDSs is their low capability to detect spoofing messages. Of conventional systems, those which monitor message communication characteristics[5] are unlikely to detect and distinguish spoofing messages from normal messages when a cyberattack occurs. Detection systems that monitor sensor-based control data,[6] in which the value contained in the payload shifts smoothly, fail to detect spoofing messages if the monitored control data is slightly and repeatedly tampered with.

5. Proposed System

5-1 CDEC

As a solution to the low performance of conventional in-vehicle IDSs to detect spoofing messages, this paper proposes Control Data Estimation for anomaly detection with Correlation data (CDEC),[7] which monitors sensor-based control data contained in the message payload, as discussed in Section 5-2 "Application model." To monitor control data, CDEC uses a group of control data correlated with the monitored control data. As such, if many sets of correlated control data are obtained within the vehicle, CDEC exhibits improved performance to detect spoofing messages. For this reason, for this proposed system, it is desirable to monitor control data at a location suitable for accessing many sub-networks of the in-vehicle network, such as in the central gateway.

5-2 Application model

The proposed system consists of three functions, as shown in Fig. 4. The divider, when a message that contains control data correlated with the monitored control data is received, memorizes the correlated control data contained in the payload. The estimator, when a message that contains the monitored control data is received, calculates an estimate of the monitored control data based on the groups of correlated control data stored in memory, via the vehicle data model described in Section 5-3. When the estimate of the monitored control data has been calculated, the evaluator compares, with a threshold, the difference between the current value of the monitored control data and the estimate. If the difference is below the threshold, the evaluator determines the monitored control data to be normal. If the threshold is exceeded, the evaluator determines the monitored control data to be anomalous.

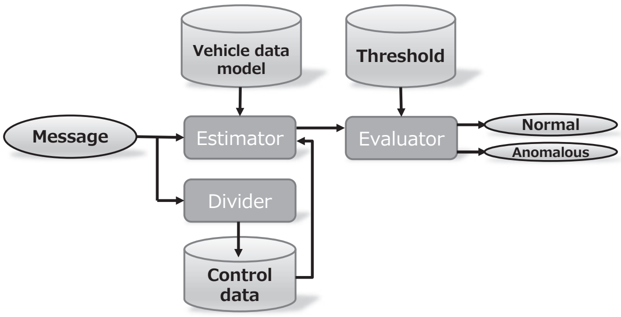


Fig. 4. CDEC application model

5-3 Vehicle data model

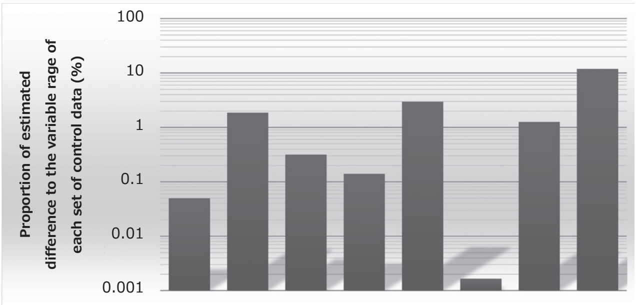
A vehicle data model is used to calculate estimates of the monitored control data based on groups of correlated control data. Learning for the vehicle data model proceeds in two stages. The first stage is correlation analysis,*[1] which extracts groups of control data correlated with the monitored control data from the traffic data on the in-vehicle network. In the second stage, learning for the vehicle data model takes place, determining vehicle data model parameters by using the monitored control data and the groups of correlated control data. The proposed system uses a regression model*[2] as the vehicle data model. For the regression model, references (8) and (9) provide detailed explanations.

6. Evaluation

6-1 Learning for vehicle data model and estimation accuracy

Eight types of sensor-based control data that indicate vehicle driving characteristics were used to evaluate learning feasibility for the vehicle data model required for the proposed system and the model's estimation accuracy. The traffic data of the in-vehicle network was used to learn each set of control data for the vehicle data model, as described in Section 5-3 "Vehicle data model." The proportion of the root mean square (RMS) of the estimated difference to the variable range of each set of control data was used as an evaluation index of estimation accuracy.

Figure 5 represents the evaluation results. First, it was confirmed that learning for the vehicle data model was possible using the traffic data of the in-vehicle network for all of the eight types of sensor-based control data that indicated the driving characteristics of the test vehicle. Estimation accuracy for the B-torque was 11.9%. For the other seven types, the estimation accuracy was below 3%.



	Vehicle Speed	Engine Speed	Steering angle	AP	E-Torque	Acceleration	Y-rate	B-torque
Variable range	0-180 [km/h]	0-4000 [rpm]	±612 [deg]	0-100 [%]	0-140 [Nm]	±3 [m/s^2]	±30 [deg/s]	±210 [Nm]
RMS of estimated difference	0.18	74.9	3.87	0.14	4.16	1e-4	0.76	50.0

Note: Variable ranges are estimates based on traffic data.

Fig. 5. Estimation accuracy

6-2 Detection performance

The proposed system was evaluated as to its spoofing message detection performance along with two types of conventional systems. Of these two types, one monitored message reception intervals, while the other monitored time-series variation of the monitored control data. The latter conventional system used the previously received normal data to estimate the current value of the monitored control data and if the difference between the current value and the estimate exceeded the allowable range, determined the received message to be a spoofing message.

The evaluation indices used were sensitivity and true negative rate*[3] expressed by Eqs. 1 and 2, respectively. The sensitivity value of 1 indicates that every inserted spoofing message was detected. The true negative rate of 1 implies that the system recognized every normal message correctly and made no error detecting it as a spoofing message. True positive and false positive in these equations represent the number of correctly identified spoofing messages and the number of erroneously identified spoofing messages, respectively. Likewise, true negative and false negative represent the number of correctly identified normal messages and the number of erroneously identified normal messages, respectively.

$$Sensitivity = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{Eq. 1}$$

$$True\ Negative\ Rate = \frac{True\ Negative}{True\ Negative + False\ Positive} \quad \cdots \text{Eq. 2}$$

The test used the attack model illustrated in Fig. 6. While vehicle speed data (approx. 60 km/h) was sent repeatedly, the attacker ECU sent spoofing messages repeatedly by two attack methods to tamper with the vehicle speed to 81 km/h. One attack method was a straight attack. The tampered speed of 81 km/h was repeatedly sent, as shown in Fig. 7 (a). The other attack method was a jab attack. The attacker ECU sent tampered data 14 times, each time raising the speed gradually from the normal data of 60 km/h to the target tampered speed of 81 km/h at 1.5 km/h intervals, followed by repeated transmission of tampered data of 81 km/h. Figure 8 represents all the speed data used for the jab attack, with the samples thinned for visibility. Figure 8 (A) indicates the duration in which the jab attack took place. The early part of this duration is enlarged in Fig. 7 (b). All the speed data subjected to the straight attack was similar to the jab attack except for the tampered data used at the beginning of the attack.

Figure 9 gives the evaluation results. The conventional system monitoring the message reception cycles exhibited a sensitivity value of 1 for both the straight and jab attacks. However, its true negative rate was low at 0.7. When receiving normal and spoofing messages within the allowable range of message reception intervals, this conventional system failed to distinguish between these messages and determined both normal and spoofing messages to be spoofing messages. In the test, the true negative rate of this conventional system was low in the duration indicated by Fig. 8 (A) in which normal messages were received among spoofing messages.

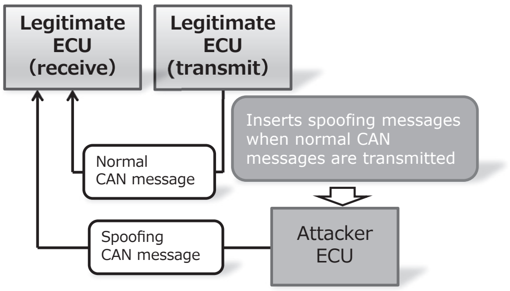
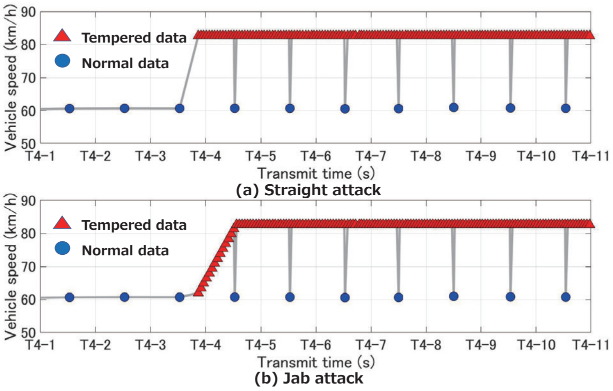
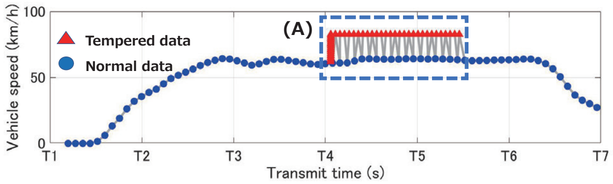

Legitimate ECU (receive)
Legitimate ECU (transmit)
Inserts spoofing messages when normal CAN messages are transmitted
Normal CAN message
Spoofing CAN message
Attacker ECU

Fig. 6. Attack model



Note: The label on the horizontal axis from “T4-1” to “T4-11” in above two charts indicates a transmit time of a vehicle speed between T4 (s) and T5 (s) in Fig.8.

Fig. 7. Types of attacks



Note: The label on the horizontal axis from “T1” to “T7” indicates a transmit time of a vehicle speed instead of an actual value.

Fig. 8. All speed data subjected to jab attack

When subjected to straight attacks, the conventional system that monitored the time-series variation of the monitored control data exhibited a sensitivity and true negative rate of 1. However, its detection performance was substantially low against jab attacks, with its sensitivity and true negative rate decreasing to 0 and 0.5, respectively. When the jab attack commenced, which tampered with the normal data repeatedly and raised the speed gradually from approximately 60 km/h to the target tampered speed of 81 km/h at 1.5 km/h intervals, estimation of the current speed based on the speed data previously determined to be normal resulted in a difference between the estimate and the tampered data falling in the allowable range. Therefore, received spoofing messages were all erroneously determined to be normal. Moreover, once the tampered speed data reached 81 km/h, estimation of the current speed based on the tampered data previously determined to be normal resulted in a difference between the estimate and the normal data of approximately 60 km/h, exceeding the allowable range. Consequently, all normal messages were erroneously determined to be spoofing messages. These are the causes of the low detection performance.

The proposed system exhibited higher detection performance than the conventional systems in both types of attacks. Subjected to straight attacks, its sensitivity and true negative rate were both 1. Against jab attacks, the proposed system exhibited a sensitivity and true negative rate of 0.99. The miniscule erroneous determination under jab attacks occurred once, immediately after the commencement of the attack. The reason for this was that the value of the tampered data inserted as a spoofing message was below the difference estimated by the vehicle data model. Nonetheless, the value of tampered data inserted as a spoofing message increased gradually at 1.5 km/h intervals up to 81 km/h. In the test, the tampered data of the second

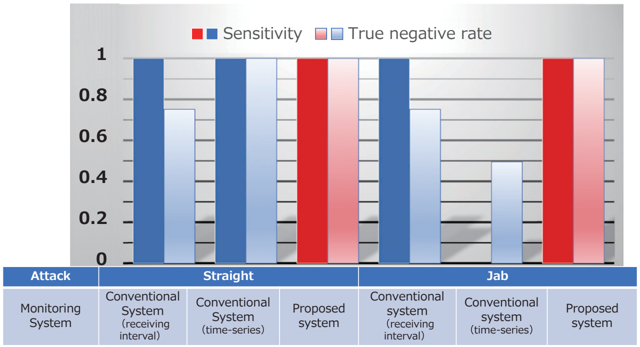


Fig. 9. Detection performance

and following spoofing messages exceeded the difference estimated by the vehicle data model. Consequently, these were all detected as spoofing messages. The proposed system monitors the target control data indirectly, based on groups of correlated control data via a vehicle data model. Therefore, in the test, it proved itself to be capable of detecting even jab attacks as well as straight attacks.

7. Conclusion

An anomaly-based IDS CDEC for in-vehicle networks was proposed. The proposed system monitors sensor-based control data by comparison of estimates produced via a vehicle data model based on groups of correlated control data.

In a test, the proposed system was applied to eight types of sensor-based control data that represented the vehicle's driving characteristics. It proved itself to be capable of learning traffic data in every aspect for the vehicle data model. Accuracy estimates of the vehicle data model were below 3% for seven types of data. Furthermore, the proposed system was compared with two types of conventional systems as to their capability of detecting spoofing messages. The results showed that the detection performance of the proposed system was the highest and the proposed system detected inserted spoofing messages, distinguishing them from normal messages.

Using the proposed system, it is possible to identify spoofing messages inserted in an in-vehicle network by a cyber attacker. Consequently, the proposed system facilitates identification of the attacked subject, thereby reducing the time taken before implementing concrete countermeasures and delimiting the scope of the countermeasures. Using the proposed system and the conventional systems used in the comparison, the IDS being developed by Sumitomo Electric configures three monitoring levels for in-vehicle networks to detect unknown cyberattacks on long-product-life vehicles in an on-board environment.

Technical Terms

*1 Correlation analysis: The correlation between two variables (x, y) is determined by the formula of Pearson's product-moment correlation coefficient expressed by Eq. 3. In this equation, γ is a cross-correlation coefficient, x is the value of monitored control data, y is the value of other control data; μx and μy are mean values of the monitored control data and the other data, respectively, and n is the sample size. The cross-correlation coefficient varies within a range between 0 and ±1.0. The correlation between two variables is stronger when their values are closer to 1.0 or −1.0. There is a cross-correlation between two variables when the values are either 0.4 or greater or −0.4 or smaller.

$$r = \frac{\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y)}{\sqrt{\sum_{i=1}^{n}(x_i-\mu_x)^2}\sqrt{\sum_{i=1}^{n}(y_i-\mu_y)^2}} \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{Eq. 3}$$

*2 Regression model: A relational expression between a target variable and explanatory variable calculated by a statistical method. In this report, the monitored control data is the target variable and other control data correlated with the monitored control data is the explanatory variable.

*3 True negative rate: An evaluation index for detection performance. The true negative rate indicates how much normal messages have been correctly identified. The ideal value for the true negative rate is 1.

References

(1) Miller, C., and Valasek, C., "Remote Exploitation of an Unaltered Passenger Vehicle," presented at DEF CON 23, August 2015.

(2) International Organization for Standardization, "Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling," ISO11898-1, Rev. 2003.

(3) International Organization for Standardization, "Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling," ISO11898-1, Rev. 2015.

(4) Koscher, K., Czeskis, A., Roesner, F., Patel, S. et al., "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, 2010.

(5) Hamada, Y., Inoue, M, Ueda, H., Miyashita, Y, et. al., "Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks," SAE International Journal of Transportation Cybersecurity and Privacy, Vol1, 2018.

(6) Müter, M., and Asaj, N., "Entropy-Based Anomaly Detection for In-Vehicle Networks," 2011 IEEE Intelligent Vehicle Symposium (IV), 2011.

(7) Hamada, Y., Inoue, M., Tateishi, H., Adachi, N., et. al., "Virtual Sensing Anomaly Detection for In-Vehicle Network," 2018 Symposium on Cryptography and Information Security, January, 2018.

(8) Tibshirani, R., "Regression shrinkage and selection via the lasso," Journal of the Royal Statistical Society. Series B (Methodological), pp. 267–288, 1996.

(9) Breiman, L., Friedman, J., Stone, C.J., and Olshen, R.A., "Classification and Regression Trees," Boca Raton: Chapman and Hall/CRC, Monterey, CA, 1984.

Contributors The lead author is indicated by an asterisk (*).

Y. HAMADA*

- Assistant General Manager, Cyber-security R&D Office

M. INOUE

- Assistant Senior Manager, AutoNetworks Technologies, Ltd.

N. ADACHI

- AutoNetworks Technologies, Ltd.

H. UEDA

- Manager, AutoNetworks Technologies, Ltd.

Y. MIYASHITA

- Senior Manager, AutoNetworks Technologies, Ltd.

Y. HATA

- General Manager, Cyber-security R&D Office