An Adaptive Intrusion Detection Algorithm for In-vehicle CAN Bus Based on Periodicity of Message

Wenqi Jiang¹, Zhongwei Li¹*, Kai Tan¹, Yadong Guan² and Weiming Tong¹

¹ School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin, Heilongjiang, 150001, China
² School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang, 150001, China
* Corresponding author’s e-mail: lzw@hit.edu.cn

Abstract. Alongside with the convergence of In-vehicle network (IVN) and wireless communication technology, In-vehicle CAN communication with external networks reinforces the connectivity among systems of a vehicle. Vehicle communication is facing severe challenges. Intrusion detection technology is one of the most widely used technologies to ensure the safety of In-vehicle CAN communication, so an adaptive intrusion detection method for In-vehicle CAN bus based on message periodicity is proposed. Communication load of CAN bus in the vehicle, the unique priority mechanism and transmission waiting mechanism of CAN message cause a certain fluctuation in the message cycle. The influence of this fluctuation on the detection accuracy of intrusion detection algorithm is analysed while rules are determined by establishing and optimizing the detection threshold in order to further improve the accuracy. Experimental results show that the adaptive intrusion detection based on message periodicity can effectively detect injection and interruption attacks.

1. Introduction

The rapid development of automotive industry, especially connected vehicle, has brought great comfort and convenience to users. At the same time, with the improvement of the openness of intra-vehicle communication network, more intra-vehicle communication network attack appear. CAN bus is the mainstream in-car communication choice. Most of the electronic control unit (ECU) in-car communicates through CAN, but the security protection mechanism of CAN bus itself is relatively fragile. Whether the hackers use wired or wireless technology to attack, the ultimate target is CAN bus. Hackers often get control of vehicle-mounted system or ECU, then communicate with CAN bus through vehicle-mounted system to read vehicle information and send malicious messages. Therefore, Researchers need to develop detection algorithms to prevent emerging attacks on vehicles.

Our key contributions are as follows:

- Analysing the cause of the fluctuation of message time cycle and its influence on the detection accuracy of intrusion detection algorithm.
- Optimizing the detection threshold and establishing a determination rule for the detection threshold, thereby further improving the detection accuracy.

A summary of the literature related to security of in-vehicle CAN is provided in section 2. In section 3, we acquire and analyse the characteristics of CAN message period. In section 4, we analyse different attack characteristics and proposes detection strategies. In section 5, we present the detailed
implementation of our scheme for the intrusion detection approach. In section 6, we report the experimental results and discuss the outcomes and conclude the paper in section 7 finally.

2. Related works
In order to ensure the security of CAN communication in vehicle, intrusion detection system (IDS) attracted many scholars’ attention because of its self-adaptive characteristics, which is easy to be applied in vehicle network. The concept and characteristics of on-board intrusion detection are proposed for the first time [1]. Murvay and Groza proposed that under normal circumstances, the sending nodes of each message are relatively fixed [2]. Cho and Shin proposed a clock-based IDS. This detection method takes advantage of the unique clock deviation characteristics of each ECU [3]. The advantage of this method is that there is no need to modify ECUs existing inside the car, but then Sagong et al. proved that hackers can attack by simulating the clock deviation of normal ECU and cannot be detected [4]. Paper [5-6] proposed a CAN bus intrusion algorithm based on neural network, however this method is not really used in actual vehicle network. In paper [7], an intrusion detection method based on hidden Markov model is proposed to detect in-vehicle CAN communication intrusion behaviour. Recent intrusion detection algorithms mainly include machine learning [8], multiple time series [9], and regression learning [10]. Studnia et al. proposed a more formal intrusion detection method based on finite state automata [11], an intrusion detection method based on information entropy was mentioned in paper [12]. Because most of the messages in the vehicle are periodic. Paper [13] detected intrusion by detecting the change of message cycle, but the periodicity of CAN message is not considered, which has a certain impact on the detection accuracy.

3. Acquisition and analysis of normal message cycle characteristics in-vehicle CAN bus
Since most CAN messages in the car are periodic messages, this paper mainly considers attacks and intrusion detection about periodic messages. In order to obtain the periodic characteristics of an ID message, we decide to use the difference between the receiving time of the adjacent message.

As shown in figure 1, the message M sent by node A to node B with the identifier ID, the transmission period of M is T. Ideally, A sends a message M at \( t_{i-1} \), \( t_{i-1} + T \) and \( t_{i+2} + 2T \). Assume that in the actual situation, the transmitting node is occupied by the bus before sending the \( i \) and \( i+1 \) messages, and the bus is idle before the \( i+1 \) is sent, so the \( i-1 \) and \( i \) messages are sent. After the time is delayed, the time for the same node B to receive the \( i \) and \( i+1 \) messages is also delayed, and the time points for receiving B messages are \( t'_{i-1}, t'_{i}, \) and \( t'_{i+1} \).

Since the message transmission time is determined by the timer of the main controller, the transmission time of the \( i \) and \( i+1 \) messages is not affected by the transmission delay of the previous message, but only depends on the bus state at the time of transmission. The transmission delay of the message on bus is ignored, so the message reception time is not affected by the reception delay of the previous message. Therefore, the actual receiving time of the \( i \) and \( i+1 \) messages are \( t'_{i-1} = t_{i-1} + \Delta_{i-1}, \Delta_{i}, t'_{i} = t_{i} + T + \Delta_{i}, \) and \( t'_{i+1} = t_{i+1} + T + \Delta_{i} + \Delta_{i}, \Delta_{i}, \Delta_{i+1} \) is the time delayed transmission due to the occupation of the bus, \( \Delta_{i-1}, \Delta_{i}, \Delta_{i+1} \geq 0 \).

In figure 1, \( \Delta_{i+1} = 0 \), the difference of receiving time between two adjacent messages is \( s_{i-1} = T + \Delta_{i} - \Delta_{i-1} \) and \( s_{j} = T - \Delta_{j} \). The change of \( s_{i-1} \) depends on \( \Delta_{i} - \Delta_{i-1} \), so set \( \Delta_{i}, \Delta_{i-1} \).
indicates the deviation of the reception time interval of the \(i-1\)th and \(i\)th messages from the ideal period \(T\). Due to \(\Delta_{i-1}^{+}, \Delta_{i}^{-}, \Delta_{i}^{+} \geq 0\), when \(\Delta_{i}^{-}=0\) and \(\Delta_{i}^{+}\) take the maximum value \(\Delta_{\text{max}}\) and \(\Psi_{i}^{+}\) takes the maximum value \(\Psi_{\text{max}}^{+}, \Psi_{i}^{-}\) takes the maximum. When \(\Delta_{i}^{-}=0\) and \(\Delta_{i}^{+}\) take the maximum value \(\Delta_{\text{max}}\), \(\Psi_{i}^{-}\) takes the minimum value \(\Psi_{\text{min}}\) and \(s_{i-1}\) takes the minimum.

The scatter plots of the receiving cycles of the three types of messages \(A\), \(B\) and \(C\) collected from the actual car are shown in (a), (b) and (c) of figure 2. The message periods of messages \(A\), \(B\) and \(C\) are all 10ms while the priority are 0, 2 and 5. It can be seen from figure 2 that the lower the priority of periodic messages, the greater the periodic change value.

![Figure 2. Scatter plot of message period over time](image)

4. Analysis and Detection of Attack Characteristics

Forger, DoS, replay and interruption attack can be divided into two types: injection attack and interruption attack. The characteristics and detection methods of injection attack and interruption attack are analysed respectively below.

4.1. Analysis and detection of injection and interruption attack time characteristic

Injection attack can choose to inject CAN diagnostic or standard messages. Since diagnostic messages should not appear when the car is driving, the main consideration is to inject standard messages, it will cause the normal cycle of communication messages on the bus to change.

When the hacker injects the forged message, normal ECU in the car is still sending the forged normal message. Ultimately, the ID message rate on the bus can be increased to more than twice, while in the case of DOS attacks, the rate of sending messages by malicious nodes is usually 20-100 times the original rate. As shown in figure 3, the normal message \(M\) sent from node \(A\) to \(B\) is assumed to be ID_{j}, and the message sending cycle is \(T\). Assume that the bus is idle before \(M\) sends, \(B\) receives the normal message sent by \(A\) at the same time. When a hacker injects a malicious message with ID_{j} identifier into the bus, the message is received by \(B\). Equation (1) can be obtained from figure 3:

\[
\Delta_{e} = t_{e} - t_{i} < T / 2
\]

The receiving period of \(B\) message is reduced to less than half of \(T\), so \(T / 2\) can be used as detection threshold. When the time difference between adjacent messages becomes less than half of normal message cycle, injection attack can be determined.

![Figure 3. Ideal and actual receiving time of message in injection attack](image)

After an interruption attack is performed on a message \(M\), the message may resume normal transmission or permanently interrupt the transmission, which will cause the receiving time of \(M\) to be greatly extended. Taking into account the periodic fluctuations of normal messages, the detection threshold can be adjusted to satisfy the equation (2):
\[ \lambda - T > \Psi_{\text{max}} \]  \hfill (2)

4.2. Analysis and detection of injection and interruption attack time characteristic

4.2.1. Missing report analysis. If the threshold of the detection injection attack is set to \( T/2 \), the report of the abnormal message may occur. Firstly, we analyse the missing report. As shown in figure 4, \( t_i \) is the sending time. If there is no sending delay, B should receive the \( i+1 \) th message at \( t_i + T \), but in this example, \( s_i = t_{i+1}' - t_i' \) takes the maximum value, in other words, when \( \Delta_i \) takes the minimum value of 0 and \( \Delta_{i+1} \) takes the maximum value of \( \Delta_{\text{max}} \), \( t_i \) is equal to \( t_i' \).

Figure 4. Message receiving analysis at the maximum time interval

Since the detection value is set to \( T/2 \) and the time when node B receives \( M' \) is \( t_v \), if \( t_v \) satisfies:
\[
\begin{align*}
  t_i + \Delta_{\text{max}} + T/2 &> t_v > t_i + \Delta_{\text{max}} + T/2 \\
\end{align*}
\]  \hfill (3)

so that we can obtain equation (4):
\[
\begin{align*}
  t_v - t_i' > T/2 \\
  t_{i+1}' - t_v > t_i + T + \Delta_{\text{max}} - t_i - T/2 - \Delta_{\text{max}} = T/2 \\
\end{align*}
\]  \hfill (4)

Equation (4) shows that the time interval between the injected message \( M' \) and its adjacent normal message \( M \) is greater than the detection threshold \( T/2 \). When the receiving time falls in the shadow of figure 4, injection attack can not be detected and a missing report occurs.

4.2.2. False positive analysis. If no false positive occurs when the message interval is the shortest, there will be no false positives in other cases. As shown in figure 5, the transmission time in the case of assuming no \( i \) th and \( i+1 \) th transmission delay, respectively, where \( A \) and \( B \) are the actual transmission times when the \( i \) th and \( i+1 \) th transmissions are respectively, \( s_i = t_{i+1}' - t_i' \). If \( s_i \) takes the minimum value, then \( \Delta_i \) takes the value \( \Delta_{\text{max}} \) and \( \Delta_{i+1} \) takes the minimum value of 0, so it is obtained that \( t_i = t_i' \) and \( t_{i+1}' = t_i + T \). Therefore the necessary and sufficient conditions for the absence of false positives are as follows (5):
\[
  t_i + t_i' + T/2 < t_{i+1}' \Leftrightarrow T > 2\Delta_{\text{max}} \\
\]  \hfill (5)

In summary, if the detection threshold is set to \( T/2 \), there may be missed reports, but no false alarms. If the hacker attacks the \( \Delta_{\text{max}} \) message which is larger the missed detection rate of the algorithm will be greatly improved, so the original algorithm needs to be improved.

5. An adaptive intrusion detection method for in-vehicle CAN bus based on periodicity of message

5.1. Optimizing the original detection threshold
If the minimum value \( \mu_{\text{min}} \) of detection threshold is
\[ (T + \Delta_{\text{max}} - \Delta_{\text{min}}) / 2 = (T + \Psi_{\text{max}}) / 2 \]  

(6)

When \( \mu > \mu_{\text{min}} \), no omission will occur. On the other hand, in order to ensure that there is no false alarm, it is necessary to get \( \mu_{\text{max}} \). If there is no false alarm when the time interval between two messages is the smallest under \( \mu_{\text{max}} \), then there will be no false alarm when \( \mu < \mu_{\text{max}} \) and the time interval between two messages is not the smallest. Therefore, \( \mu \) should be analysed when no false alarm occurs even the time interval between two messages is the smallest.

As it is shown in figure 5, it can be obtained that:

\[ s_i = t_{i+1}' - t_i' = t_i + T - t_i - \Delta_{\text{max}} = T - \Delta_{\text{max}} \]  

(7)

If there is no false positive, it must be satisfied:

\[ T - \Psi_{\text{max}} > \mu \]  

(8)

If the maximum value of \( \mu \) is expressed as \( \mu_{\text{max}} \), and \( \mu_{\text{max}} = T - \Psi_{\text{max}} \). Since the situation of false positives and false negatives is analysed separately, \( \mu_{\text{max}} \) is not necessarily greater than \( \mu_{\text{min}} \).

(1) If \( \mu_{\text{max}} > \mu_{\text{min}} \), equation (9) can be obtained from equation (6):

\[ T - \Psi_{\text{max}} > (T + \Psi_{\text{max}}) / 2 \Rightarrow T > 3\Psi_{\text{max}} \]  

(9)

If \( \mu \) is set to \( \mu_{\text{max}} > \mu > \mu_{\text{min}} \) when equation (9) is satisfied, there will be no false alarm or missed alarm in detection system. Figure 6 shows the false positive rate and false negative rate with detection threshold if \( T > 3\Psi_{\text{max}} \). \( T / 2 < \mu_{\text{min}} \) is known by equation (9), so there will be false negatives when \( \mu = T / 2 \).

(2) If \( \mu_{\text{min}} > \mu_{\text{max}} \), equation (10) can be obtained from equation (6):

\[ T < \Psi_{\text{max}} \]  

(10)

Figure 7 shows the false alarm rate and false negative rate along with the detection threshold when \( T > 3\Psi_{\text{max}} \). \( T / 2 < \mu_{\text{max}} \) can be obtained by equation (5), so there will be a false negative when \( \mu = T / 2 \). If the detection threshold satisfies \( \mu < \mu_{\text{max}} \), there will be no false positives but there may be false negatives; If the detection threshold is \( \mu > \mu_{\text{min}} \), there will be no false negatives but false positive may occur; If the threshold value is \( \mu_{\text{min}} > \mu > \mu_{\text{max}} \), the detection system has both false positives and false negatives.

Considering that the number of malicious messages injected by a hacker under a non-DoS attack is much smaller than the number of normal messages, it is more appropriate to select a detection threshold with no false positives and a small probability of false negatives. Therefore, \( \mu \) can take a value slightly smaller than \( \mu_{\text{max}} \), as shown \( \mu' \) in figure 7.

For ease of understanding, the following analysis compares the false negative rate when the detection threshold is taken as \( \mu_1 = \mu_{\text{max}} \) and \( \mu_2 = T / 2 \) when \( T < 3\Psi_{\text{max}} \).

As shown in figure 8, \( t_i \) is the transmission time when there is no transmission delay when the message is transmitted for the \( i \) th time. \( t_i' \) is the actual transmission time. If there is no transmission delay, \( B \) should receive the \( i + 1 \) th message at \( t_i + T \). For a message, \( s_i = t_i' - t_i ' \) takes the maximum
value, that is, $\Delta_i$ takes the minimum value of 0 and $\Delta_{i+1}$ takes the maximum value of $\Delta_{\text{max}}$.

Figure 8. Analysis of the false negative rate when the detection threshold

When $\mu_i=T+\Psi_{\text{min}}=T-\Delta_{\text{max}}$ and $T<3\Psi_{\text{max}}$, it can be obtained that when the reception time $t_e$ of the injected message satisfy the range of $(t_i+\mu_i,t_i+2\Delta_{\text{max}})$, then

$$t_{i+1}'-t_e > t_e + T + \Delta_{\text{max}} - (t_i + 2\Delta_{\text{max}}) = T - \Delta_{\text{max}} = \mu$$

(11)

And because:

$$t_e - t_i' > t_i + \mu_i - t_i = \mu_i$$

(12)

It can be known from equation (11) and equation (12) that when the reception time $t_e$ of the injected message satisfies the range of $(t_i+\mu_i,t_i+2\Delta_{\text{max}})$, the detection system cannot detect the injection attack, and the detection system has a false report. The time interval for false negative is:

$$t_i + 2\Delta_{\text{max}} - (t_i + \mu_i) = 3\Delta_{\text{max}} - T$$

(13)

When $\mu_i = T/2$, the time interval for false negatives is $\Delta_{\text{max}}$. Currently, the period of periodic messages in the vehicle satisfies $T > 2\Delta_{\text{max}}$, equation (14) can be obtained:

$$3\Delta_{\text{max}} - T < \Delta_{\text{max}}$$

(14)

The rate of false negatives is lower when the periodic detection threshold is set to $\mu_i = T - \Psi_{\text{max}}$.

In summary, the following conclusions are drawn:

If $T > 3\Psi_{\text{max}}$, when the threshold is set to $\mu_{\text{min}} < \mu < \mu_{\text{max}}$, the detection system will not have false positives and no false negatives.

If $T < 3\Psi_{\text{max}}$, no matter what threshold value the detection system takes, there will be false alarm or missed alarm. When the threshold $\mu$ is set to a value $\mu'$ slightly less than $\mu_{\text{max}}$, the detection system will not have false positive, but there is a very low probability of false negative.

5.2. Design of Adaptive Intrusion Detection Algorithm based on periodicity of message

The adaptive intrusion detection algorithm based on periodicity of message includes two parts: (1) adaptive detection threshold calibration algorithm; (2) detection algorithm.

5.2.1. Adaptive detection threshold calibration algorithm. The flow of adaptive detection threshold calibration algorithm is illustrated with figure 9. Firstly, we determine the message which node receiving identifier is $ID_j$ message and record the receiving time stamp of the message, then obtain $n$, the number of receiving cycles $T_i$. $T_{\text{mean}}$ and $T_{\text{max}}$ should be calculated, and $\Psi_{\text{max}}=T_{\text{max}}-T_{\text{mean}}$. The injection attack detection threshold $\mu$ and the interruption attack detection threshold $\lambda$ should be determined. To prevent false positives, a small amount of time margin is required when setting $\mu, \lambda$.

5.2.2. Detection algorithm.

After calibrating the adaptive detection threshold, it can be detected. Similarly taking $ID_j$ message as an example, the flow of detection algorithm is illustrated with figure 10.

First, $i=0$ is initialized to record the receiving time of $i$th message; then judgment is made that if $i+1$th message is not received, it is directly determined that the message is interrupted, and if $i+1$th message is received, the receiving time $t_{i+1}$ of $i+1$th message is recorded; then the time $\Delta_i$ between
The $i$th and $(i+1)$th messages is calculated; If $\Delta_i < \mu$, an injection attack alarm is issued, otherwise it enters interruption detection and after interruption detection. If $\Delta_i > \lambda$, then an interruption alarm is issued, and the next step is to go into the loop and continue to detect until the system shuts down.

![Diagram](image1.png)

**Figure 9.** Adaptive detection threshold calibration algorithm.

![Diagram](image2.png)

**Figure 10.** Flow chart of detection algorithm.

### 6. Implementation and Evaluation

#### 6.1. Experimental Design

To verify the validity of the proposed algorithm, three CAN communication nodes are used to simulate in-car CAN communication. As shown in figure 11, STM32F407ZGT6 is used as the main control chip. The chip uses Cortex M4 core and the main frequency is 168MHz and integrates the CAN controller. The data is sent to the CAN transceiver chip TJ A1050 of the development board through the output pin. The message is then sent to the bus.

![In-vehicle CAN communication platform](image3.png)

**Figure 11.** In-vehicle CAN communication platform.

Because the number of nodes in the simulation platform is small, the bus load is small. In order to simulate the delay of message transmission under high load of CAN bus, random number is added on the basis of the original message transmission cycle of each node. Normally, $A$ sends message $M_1$ to $B$ periodically with $(10 + \Delta)\, \text{ms}$, and message $M_2$ to $B$ periodically with $(10 + 2\Delta)\, \text{ms}$.

#### 6.1.1. Verification of Intrusion Detection Algorithm for Injection Attacks

$C$ is a malicious node, which randomly injects 10,000 forged messages $M'_1$ and $M'_2$, respectively, into the bus. According to the proposed adaptive intrusion detection algorithm based on message cycle characteristics, the injection attack detection threshold $\mu_i$ of message $M_i$ should satisfy equation (15):

$$5.95\, \text{ms} = \frac{10 + 1.9}{2} \, \text{ms} < \mu_i < (10 - 1.9)\, \text{ms} = 8.1\, \text{ms}$$

(15)
Therefore, \( \mu \) is set to 5ms, 5.8ms and 6.5ms respectively. Among them, 5 ms is the detection threshold without considering the change of message cycle. The detection results of injecting \( M_2' \) under different detection thresholds are compared.

### 6.1.2. Verification of Intrusion Detection Algorithm for Interrupt Attacks

Without \( C \) node, only \( A \) and \( B \) are involved in communication, \( M_1 \) and \( M_2 \) are stochastically interrupted to send 10,000 times. The interruption attack detection thresholds of message \( M_1 \) and \( M_2 \) should satisfy equation (16):

\[
\begin{align*}
\lambda_1 > (10 + 1.9) \text{ms} & = 11.9 \text{ms} \\
\lambda_2 > (10 + 3.8) \text{ms} & = 13.8 \text{ms}
\end{align*}
\]

(16)

Therefore, \( \lambda_1 \) is set to 11ms, 12ms and 13ms respectively, and the detection effect of \( M_1 \) interruption attack under different \( \lambda_1 \) is compared. Therefore, \( \lambda_2 \) is set to 13ms, 14ms and 15ms respectively, and the detection effect of interruption attack on \( M_2 \) under different \( \lambda_2 \) is compared.

### 6.2. Experimental results and analysis

As shown in Table 1, for injection attacks, since the period \( T \) of \( M_1 \) satisfies \( T < 3\Delta_{\text{max}} \), there will be no false alarm and false alarm when the threshold is set between 5.95ms and 8.1ms, while 45 false alarms will appear if the threshold is set to 5ms, and 126 normal messages will be false alarmed if the threshold is set to 8.5ms. The period \( T \) of \( M_2 \) satisfies \( T < 3\Delta_{\text{max}} \). When the threshold is less than 6.2ms, there will be no false alarm, but there will be false alarm, and the smaller the threshold, the more false alarms will be missed. If the threshold is set to \( T/2 \) or 5ms, 67 false alarms will be missed and more false alarms will be missed. If the threshold is set to \( T/2 \) or 6.5ms, 15 false alarms will be missed and 3 false alarms will be missed. Therefore, it is proved that the proposed adaptive intrusion detection algorithm based on message cycle characteristics is better than the algorithm which simply sets the threshold as \( T/2 \) to detect injection attacks.

#### Table 1. Detection results of injection attack and interruption attack.

| Attacked type | Attacked message | \( T \)(ms) | \( \Delta_{\text{max}} \)(ms) | Threshold(ms) | False positive | False negative |
|---------------|-------------------|-------------|------------------|---------------|----------------|----------------|
| injection attack | \( M_1 \) | 10          | 1.9              | 5             | 0              | 45             |
| |              | 10          | 1.9              | 6.5            | 0             | 0              |
| |              | 10          | 1.9              | 7              | 0             | 0              |
| |              | 10          | 1.9              | 8.5            | 126           | 0              |
| |              | 10          | 3.8              | 5              | 0             | 67             |
| | \( M_2 \) | 10          | 3.8              | 5.8            | 0             | 21             |
| |              | 10          | 3.8              | 6.5            | 3             | 15             |
| |              | 10          | 1.9              | 11             | 137           | 0              |
| interruption attack | \( M_1 \) | 10          | 1.9              | 12            | 0              | 0              |
| |              | 10          | 1.9              | 13             | 0             | 0              |
| | \( M_2 \) | 10          | 3.8              | 13             | 35            | 0              |
| |              | 10          | 3.8              | 14             | 0             | 0              |
| |              | 10          | 3.8              | 15             | 0             | 0              |

When the interruption detection threshold of \( M_1 \) is set to 11ms, 137 false alarms occur, while when the interruption detection threshold of \( M_1 \) is set to 12ms and 13ms, there is neither false alarm nor false alarm. When \( M_2 \) interruption detection threshold is set to 13ms, 35 false alarms occur, and when \( M_2 \) interruption detection threshold is set to 14ms and 15ms, there is neither false alarm nor false alarm, which verifies the effectiveness of the proposed algorithm for detecting interruption attacks.
7. Conclusion
In this paper, we analysed the characteristics of CAN message cycle and proposed a lightweight intrusion detection algorithm based on message cycle for vehicle network. Certain fluctuation in the message cycle occurs because of communication load and priority mechanism and transmission waiting mechanism of message in CAN bus. The influence of this fluctuation on the detection accuracy of intrusion detection algorithm is analysed. The detection threshold is optimized and the detection threshold is established so that the detection accuracy is proving further. The experimental results show that the algorithm can effectively detect injection and interruption attacks.

Acknowledgement
This research was funded by the “Project for the Development and Application of Safety Testing and Verification Platform for Industrial Robots” of the Ministry of Industry and Information Technology.

References
[1] Hoppe, T., Kiltz, S., (2011) Security threats to automotive CAN networks-Practical examples and selected short-term countermeasures. Reliability Engineering & System Safety., 96: 11-25.
[2] Murvay, P.S., Groza, B. (2014). Source identification using signal characteristics in controller area networks. IEEE Signal Process. Lett., 21: 395-399.
[3] Cho, K.T., Shin, K.G. (2016) Fingerprinting electronic control units for vehicle intrusion detection. Proc. 25th USENIX Secur. Symp. Austin. pp. 911-927.
[4] Ying, X., Sagong, S.U., Clark, A., Bushnell, L., Poovendran, R. (2018) Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks. IEEE Trans. Inf. Forensics Security. IEEE Transactions on Information Forensics and Security., 14: 2300-2314.
[5] Kang M.J., Kang, J.W. (2016) Intrusion detection system using deep neural network for in-vehicle network security. PloS One., 11: 35-41.
[6] Kang M.J., Kang, J.W. (2016) A novel intrusion detection method using deep neural network for in-vehicle network security. IEEE 83rd Veh. Technol. Conf.(VTC Spring). Nanjing. pp. 1-5.
[7] Narayanan, S.N., Mittal, S., Joshi, A. (2016) OBD Secure Alert: An abnormally detection system for vehicles[C]. IEEE Int. Conf. Smart Computer(SMARTCOMP). St louis. pp.1-6.
[8] Daxin T., Yuzhou L., Yunpeng W., Xuting D., Congyu W., Wenyang W. (2017). An intrusion detection system based on machine learning for can-bus. Proc. Int. Conf. Ind. Netw. Intell. Syst. Vietnam. pp. 2017: 285-294
[9] Theissler, A. (2017). Detecting known and unknown faults in automotive systems using ensemble-based anomaly detection. Knowledge-Based Systems., 123: 163-173.
[10] Li H., Zhao L., Juliato M., Ahmed S., Sastry M.R., Yang L.L. (2017) POSTER: Intrusion detection system for in-vehicle networks using sensor correlation and integration. ACM SIGSAC Conf. Comput. Commun. Secur. Dallas. pp. 2531-2533.
[11] Laarouchi, Y., Mohamed, K., Nicomette, V., Studnia, I., Alata, E. (2018). A language-based intrusion detection approach for automotive embedded networks. International Journal of Embedded Systems., 10: 1-12.
[12] Marchetti, M., Stabili, D., Guido, A., Colajanni, M. (2016) Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. Proc. Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI). Bologna. pp. 1-6.
[13] Mutet, M., Groll, A., Freiling, F.C. (2010). A structured approach to anomaly detection for in-vehicle networks. Sixth International Conference on Information Assurance & Security. IEEE. Atlanta. pp. 92-98.