Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2023 SCPE. Volume 24, Issues 4, pp. 743–754, DOI 10.12694/scpe.v24i4.2345

LIGHTWEIGHT INTRUSION DETECTION METHOD OF VEHICLE CAN BUS UNDER COMPUTATIONAL RESOURCE CONSTRAINTS

XIANCHENG MING[*], ZHENYU WANG [†], AND BO XU[‡]

Abstract. In order to improve the security protection performance of the vehicle Controller Area Network (CAN) bus, the research builds an adaptive lightweight intrusion detection algorithm based on the limited computing and storage resources of the on-board ECU environment and the message cycle characteristics to supervise and detect the vehicle CAN bus intrusion. The results showed that the message cycle-based adaptive intrusion detection algorithm had high accuracy and recall rate, and fast computational search efficiency, with a stable detection time of less than 3 seconds. The intrusion detection capability is continuously optimized as the training time increases, and after stabilization, the resource utilization rate reaches over 95% with a throughput of 100Mb/s. The algorithm has strong protection capabilities. The average vehicle CPU usage of the algorithm is only 4.76%, which is 10.17% lower than the intrusion detection algorithm based on support vector machines. It can effectively prevent interference with the normal operation of the vehicle CAN bus. The algorithm has high detection accuracy for interrupt type attacks, and there are no false positives or missed alarms. For injection type attacks, the probability of missed alarms is less than 1%. The intrusion detection of vehicle CAN bus based on the message cycle characteristics provides technical reference for the safety and stability of the vehicle network, and has important practical value for the intelligent and networked development of the automobile industry.

Key words: Vehicle CAN bus; Lightweight; Intrusion detection; Message cycle

1. Introduction.

In recent years, with the continuous development of the automobile industry, the output and ownership of automobiles have been continuously improved, and the requirements for vehicle comfort and technical performance have also been continuously improved [1]. Under the background of the Internet of things, the field of automotive electronic communication is constantly expanding, and intelligent and networked become the key development direction of automobiles. With the continuous innovation of the Internet of things technology, the degree of automobile networking has been continuously improved, which has brought a high degree of experience and comfort to the automobile users, and its openness has also been greatly increased, and the accompanying network attack risk has also been continuously increased [2]. The vehicle CAN bus is one of the key buses in the automotive electronic network system, facing a high risk of invasion. In recent years, the vehicle CAN bus has been frequently attacked by hackers. The relevant safety protection measures of the vehicle CAN bus have received extensive attention from all walks of life [3]. Researchers in the field of automotive network communication security conduct intrusion detection research from the perspective of the electrical characteristics and data fields of the vehicle CAN bus, but they have certain limitations, which are easy to generate detection errors, leading to false alarm or missing alarm [4]. Moreover, the computing and storage conditions of the vehicle Electronic Control Unit (ECU) environment are limited, and the deep learning intrusion detection algorithm requires high computing performance and is difficult to be directly applied in the vehicle environment [5]. Therefore, studying the intrusion risks faced by vehicle CAN buses, considering the actual operating conditions of the vehicle CAN bus, an adaptive intrusion detection algorithm based on the message cycle is proposed under the constraint of computing resources. It is expected to reduce the impact of the detection system on the bus performance while ensuring the detection effect. The innovation of this study lies in the construction of an adaptive lightweight intrusion detection algorithm based on packet cycle characteristics. The main structure of the study is divided into 5 parts. The first part is the introduction; the

[*] Engineering Training and Management Experiment Center, Chongqing University of Technology, Chongqing, 400054, China; *Corresponding Author E-mail: ming$_x$c954@163.com

[†] VChina Coal Science and Industry Group Chongqing Research Institute Co., Ltd., 400042, China

[‡] The 32nd Research Institute of China Electronics Technology Group Corporation, Shanghai, 200233, China

second part is an analysis of the current relevant research status; the third part is the design of a lightweight intrusion detection algorithm for vehicle CAN bus based on message cycle; the fourth part is an analysis of the performance and application effectiveness of the proposed algorithm; the final part is a summary of the entire study.

2. Literature review. In previous studies, a large number of scholars have proposed methods for risk control of vehicle can bus. Jo et al. proposed a mauth can authentication protocol, which can prevent the vehicle from being attacked by camouflage, and proposed a technology to prevent the bus from being attacked by shutdown [6]. Xiang team proposed a global topology constraint network for fine-grained vehicle identification based on vehicle positioning in vehicle can bus intrusion detection. The team also realized vehicle classification using convolutional neural network to achieve more accurate vehicle identification. In combination with vehicle classification and identification and precise positioning technology, the risk of vehicle can bus is investigated and controlled, which greatly reduces the risk of vehicle intrusion [7]. Katragadda steam proposed a sequence mining method to detect the low-rate injection attack of can in view of the problem that networked vehicles are subject to multiple types of network attacks. Through the analysis of four different types of attacks, the effectiveness of the sequence mining method to deal with the four types of attacks is verified. In addition, the sequence mining method of katragadda s group only uses identifiers that can be identified, so this technology can be applied to any type of vehicle and has great value in reducing the probability of vehicle being attacked [8]. In the field of electric vehicles, because the electric vehicles rely more on the in-vehicle communication system, the system will indirectly bear greater risks. Al Saud m et al. Proposed a safe and reliable intelligent framework to prevent hackers from invading vehicles. Al Saud m and others [9] improved and optimized the support vector machine and combined the social spider optimization algorithm to improve the search ability of the intrusion detection algorithm. Finally, the simulation experiment verified that the research method has high reliability and security, and can effectively prevent the electric vehicle from being attacked by denial-of-service hackers.

Intrusion detection is a useful complement to firewalls, helping systems to cope with network attacks and improving the integrity of the information security infrastructure. Ullah M U et al. proposed an intrusion detection system suitable for Apache web servers to make online communication between suppliers and customers more effective and secure [14]. Leevy et al. created datasets such as CSE-IC-IDS2018 to train predictive models for network-based intrusion detection in response to the increase in network attacks [15]. Thakkar et al. addressed the issue of intellectual property expropriation caused by cybercrime by using intrusion detection systems to protect the security of computer systems and users, and studied the performance of the system by developing datasets [16]. Salih A et al. believe that to improve the performance of intrusion detection systems, different classification algorithms must be used to detect different types of attacks, and the results of evaluating different classification algorithms from different aspects are presented to establish intrusion detection systems [23].

To sum up, the network security issue has attracted the attention of many researchers, among which the automobile network risk control supported by the Internet of things technology accounts for a large proportion. A large number of researches have adopted different algorithms to detect different types of attacks. However, it is worth noting that many researchers have not considered the limitation of computing resources in the vehicle ECU environment. Machine learning algorithms require more computing resources and are difficult to be directly applied in the vehicle ECU environment. Therefore, based on this research, aiming at the computing resource constraints of the vehicle ECU environment, an intrusion detection algorithm based on the message cycle characteristics is proposed to improve the efficiency of the intrusion detection of the vehicle network and ensure the safety of the vehicle bus operation.

3. Lightweight Intrusion Detection Method of Vehicle CAN Bus based on Message Cycle.

3.1. Cycle Analysis of Vehicle CAN Message. With the increasing openness of vehicles, the CAN bus of vehicles is exposed to the open network environment, and the vulnerability of its bus is gradually revealed. The filter acceptance mechanism of CAN bus has low security and is easily used by hackers. In addition, the data security cannot be protected, and the data authentication mechanism is not perfect, which provides an opportunity for intrusion attacks. In addition, the vehicle CAN bus strictly follows the priority system, while the vehicle CAN bus lacks the corresponding service rejection protection mechanism. Hackers can take advantage of this defect to preempt the message priority, so that the vehicle CAN bus message sending process is blocked and the system crashes. The vulnerability of the vehicle CAN bus requires the establishment of a more perfect vehicle CAN bus security protection mechanism. While the general on-board ECU is an embedded system, its memory storage performance and calculation performance have an upper limit. If the calculation complexity of the intrusion detection system exceeds the processing capacity of the on-board ECU, it will have a negative impact on the detection effect and the performance of the vehicle bus system [14, 15]. However, the traditional computer network intrusion detection algorithm requires a lot of storage and calculation resources, which is difficult to directly applied in the vehicle ECU environment. Therefore, it is necessary to design the vehicle CAN bus intrusion detection algorithm according to the calculation resource constraints of the vehicle ECU, otherwise it cannot meet the actual application environment [12, 13]. Most of the vehicle CAN messages are periodic. Therefore, considering the limited computing capacity of the on-board ECU, a lightweight bus intrusion detection algorithm based on the message cycle is proposed to adaptively detect the periodic message-oriented intrusion attacks. Instead of repeatedly computing the detection information, the intrusion is detected and identified from the periodic characteristics of the message.

The periodic characteristics of vehicle CAN messages can be obtained by using the sending time difference or receiving time difference of adjacent messages. However, the data field of vehicle CAN messages does not contain the sending time stamp of the message, nor can the sending time information be directly obtained from the receiving node [18, 19]. Therefore, if the periodic characteristics of the message are obtained from the sending time difference of the message, the vehicle ECU needs to be reprogrammed so that the sending node of the message records the sending time so that the system can perform intrusion detection. Reprogramming is too cumbersome, and the operation of the detection system will have an impact on the normal operation of the nodes. Therefore, the research combines the sending and receiving mechanism of the vehicle CAN message, and records the periodic characteristics from the difference of the message receiving time. A recording node is added to the vehicle CAN bus to receive the message and record the message reception time. The new nodes have little impact on the original system, do not interfere with the normal operation of the original functions, and occupy less system computing and storage resources. However, in the actual process, there are certain fluctuations in the cycle of the vehicle CAN message. The priority of the message and the vehicle bus load will affect the periodic characteristics of the message [20, 21]. The priority of the message determines the sending order of the message. The message with lower priority may wait to be sent, and the heavy load of the vehicle bus may also delay the sending and receiving of the message, thus changing the cycle of the message [18-19]. Suppose that the message M is sent from node A to node B, its identifier is ID_j and the sending cycle is T , message acceptance time difference is s ,and message sending sequence is i. Suppose that the sending time of the message is t_i and the actual sending time is t_i. Generally, node A sends the message at time nodes t_i ,$t_i + T$ and $t_i + 2T$. Without considering the bus transmission delay, node B receives the message at time points t_i ,$t_i + T$ and $t_i + 2T$. Assuming that the bus of the sending node is occupied when sending the $i - 1$ message and the i message, resulting in the delay of sending the $i - 1$ message and the i message, and the bus is idle when sending the $i + 1$ message, and the message sending time is normal, the message receiving time points of node Bare t_{i-1},t_i and t_{i+1}. The sending time of vehicle CAN message depends on the timer of the main controller. The sending time of each message will not affect each other, but only affected by the bus load state at the message sending time. Without considering the bus transmission delay, the time point at which node B receives messages $i - 1$,i and $i + 1$ is shown as follows:

$$\begin{cases} t_{i-1} = t_{i-1} + \Delta_{i-1} \\ t_i = t_i + T + \Delta_i \\ t_{i+1} = t_{i+1} + 2T + \Delta_{i+1} \end{cases} \tag{3.1}$$

In equation 3.1, Δ_{i-1}, Δ and Δ_{i+1} are the delay time of message transmission caused by bus occupation, Δ_{i-1} , Δ, Δ_{i+1}. The difference between the receiving time s_{i-1} of the messages in Articles $i - 1$ and i and the receiving time s_1 of the messages in Articles i and $i + 1$ is expressed as follows:

$$\begin{cases} S_{i-1} = t_i - \ t_{i-1} = T + \Delta_i - \Delta_{i-1} \\ S_i = t_{i+1} - \ t_i = T + \Delta_{i+1} - \Delta_{i-1} = T - \Delta_i \end{cases} \tag{3.2}$$

It can be seen from equation 3.2 that the change of reception time difference S_{i-1} is determined by $\Delta_i - \Delta_{i-1}$. Let the difference between the sending cycle error of the $i-1$ message and the i message be ψ_{i-1} and $\psi_{i-1} = .\Delta_i - \Delta_{i-1}$

4. Design of the Proposed Method. According to different attack methods, vehicle bus attacks can be divided into injection attacks and denial of service attacks. Replay attacks, Denial of Service (DoS) attacks and forgery attacks are common injection attacks. Replay attacks involve hackers repeatedly sending normal messages to the vehicle centreline at any time [24, 25]. A DoS attack involves hackers spoofing nodes on the vehicle bus and injecting a large number of high priority messages that should not appear on the vehicle bus, resulting in a large number of vehicle bus resources being occupied by malicious messages, making it difficult for normal and effective messages to be sent normally [26, 27]. The term "forgery attack" refers to the act of hackers sending forged messages to the vehicle bus and interfering with the system's normal communication through faked diagnostic and abnormal messages. This can easily result in system malfunctions and cause vehicle safety accidents. Hackers' injection attacks on the vehicle bus will disrupt the normal message sending cycle.

After the vehicle bus is attacked by interruption, the vehicle ECU cannot receive valid messages, which affects the normal operation of the vehicle. Hackers' interrupt attack on vehicle bus message M is divided into temporary interrupt and permanent interrupt. Temporary interrupt only interrupts the transmission of several messages, and then resumes normal transmission. Permanent interrupt will not resume transmission after interrupting the transmission of messages [28, 29]. If interrupt attack will seriously affect the receiving time of message, combined with the fluctuation of message cycle, the detection threshold conditions of interrupt attack are as follows:

$$\omega - T > \psi_{max} \tag{4.1}$$

Combined with intrusion attack analysis, the minimum detection threshold of injection attack is shown as follows

$$\lambda_{min} = \frac{T + \Delta_{max} - \Delta_{min}}{2} = \frac{T + \psi_{max}}{2} \tag{4.2}$$

When the detection threshold is greater than λ_{min} , missed or false alarms will not occur. In order to avoid false alarm or missing alarm, the detection threshold cannot be too large. It is of great importance to set the maximum value of the detection threshold λ_{max}. When the detection threshold is the maximum value and the time period of the two messages is the smallest, no false alarm or missing alarm will occur; when $\lambda < \lambda_{max}$, and the time interval is not the minimum value, false alarm or missing alarm are bound to occur. Information entropy describes the degree of order in a system that can act on the CAN bus intrusion detection system. It defines the message $F = f_1, f_2, ..., f_n$ that appears in time T of the CAN bus, with a total of different frames. If T takes a sufficiently long time, the calculation of the total number of sending times is shown in formula 4.5.

$$N_T = \sum_{i=1}^{n} \frac{T}{S_i} = T \sum_{i=1}^{n} \frac{1}{s_i} \tag{4.3}$$

In formula 4.5, S_i represents the transmission period. Regardless of the transmission time delay, node B should receive the $i+1$ message at time $t_1 + T$. Take the minimum value of S_i , then take the maximum value of Δ_i , and take the minimum value of Δ_{i+1} as 0. At this time, the reception time difference S_i is shown as follows:

$$S_i = t_{i+1} - t_i = T - \Delta_{max} \tag{4.4}$$

The threshold conditions without false positives are expressed as follows:

$$\lambda < T - \psi \tag{4.5}$$

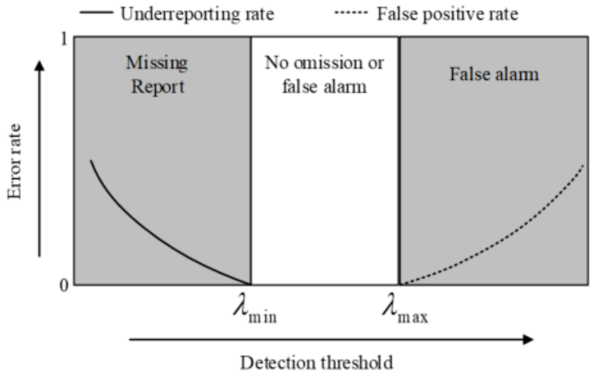

Fig. 4.1: Relationship curve between false positive rate, false negative rate and detection threshold of detection system

The false alarm and missed alarm of the detection system are discussed separately. The false alarm threshold is λ^* and the missed alarm threshold is $\lambda^\#$. The conditions of $\lambda^*_{max} > \lambda^\#_{max}$ and are analyzed separately. When $\lambda^*_{max} > \lambda^\#_{max}$, the message cycle meets the following conditions:

$$T > 3\psi_{max} \tag{4.6}$$

When the condition of equation (9) is met, the threshold meets condition $\lambda^* > \lambda > \lambda^\#_{min}$, no false positives or missing positives will occur. At this time, the relationship curve between the false positives rate and missing positives rate of the detection system and the detection threshold is shown in Figure 4.1.

When $\lambda^*_{max} < \lambda^\#_{min}$, the message cycle meets the following conditions:

$$T < 3\psi_{max} \tag{4.7}$$

As shown in Figure 4.2, when the detection threshold is less than λ^*_{max} or greater than $\lambda^\#_{min}$, the detection system may have false alarm without false alarm. When the detection threshold is within $\lambda^\#_{min} > \lambda > \lambda^*_{max}$, the detection system may have missed and false alarms. At this point, no false alarm is considered a priority condition and the detection threshold is slightly lower than the maximum value. Under the condition of no false alarm, a small probability of false alarm is allowed.

In case $T < 3\psi_{max}$, if the transmission time delay is ignored, node B should receive the $i+1$ message at time $t_i - T$. Take the maximum value of S_i , then take the minimum value of Δ_i as 0, and take the maximum value of Δ_{i+1}. When $\lambda = T + \psi_{max} = T - \Delta_{max}$, the receiving time of the injected message meets the following conditions:

$$t_i + \lambda < t < t_i + 2\Delta_{max} \tag{4.8}$$

Then the detection threshold is expressed as follows:

$$\lambda = T - \Delta_{max} = t_i + T + \Delta_{max} - (t_i + 2\Delta_{max}) < t_{i+1} - t \tag{4.9}$$

At this time, the time interval of missing alarm in the detection system is shown as follows:

$$t_i + 2\Delta_{max} - (t_i + \lambda) = 3\Delta_{max-T} \tag{4.10}$$

You can get:

$$\lambda_{max} > 3\lambda_{max} - T \tag{4.11}$$

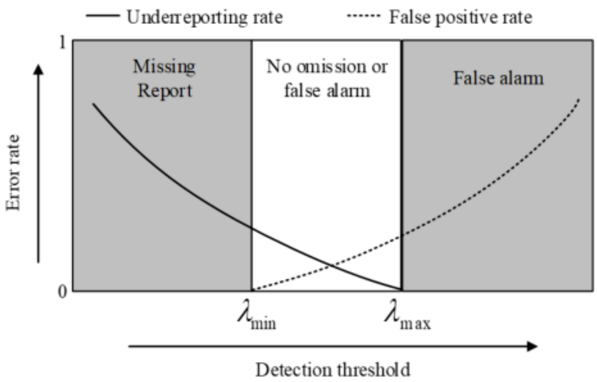

Fig. 4.2: Relationship curve between false positive rate, false negative rate and detection threshold of detection system

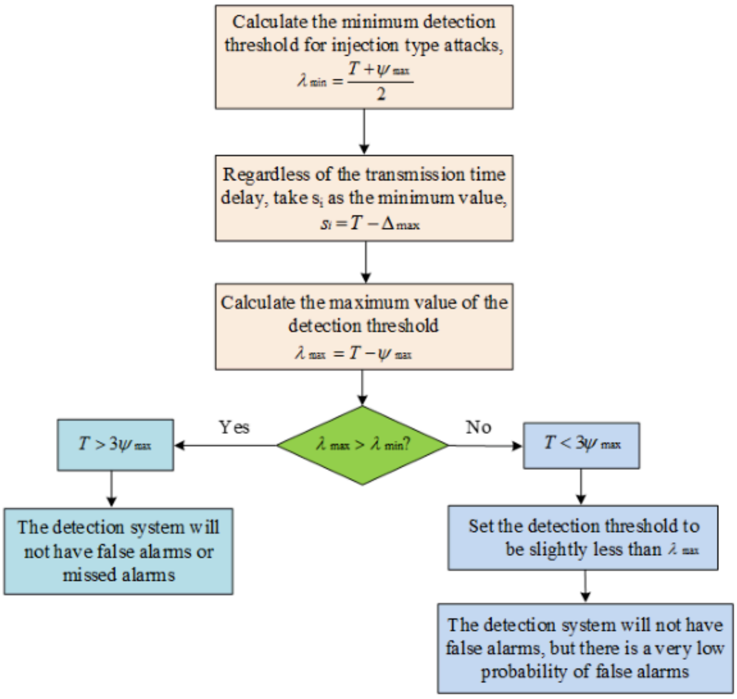
Calculate the minimum detection threshold for injection type attacks, $\lambda_{min} = \frac{T+\psi_{max}}{2}$
Regardless of the transmission time delay, take s_i as the minimum value, $s_i = T - \Delta_{max}$
Calculate the maximum value of the detection threshold $\lambda_{max} = T - \psi_{max}$
$\lambda_{max} > \lambda_{min}$?
Yes
No
$T > 3\psi_{max}$
The detection system will not have false alarms or missed alarms
$T < 3\psi_{max}$
Set the detection threshold to be slightly less than λ_{max}
The detection system will not have false alarms, but there is a very low probability of false alarms

Fig. 4.3: Structured Algorithm for Bus Intrusion Adaptive Detection Based on Message Period Characteristics

To sum up, when the message cycle meets condition , the system detection threshold meets condition , no false alarm or missing alarm will occur. When the message cycle meets condition , set the system detection threshold to slightly less than of the maximum threshold. At this time, no false positives will occur, but there is a minimal probability of false positives. In summary, the structured algorithm for bus intrusion adaptive detection based on packet cycle characteristics is shown in Figure 4.3.

The proposed algorithm is detected after the detection threshold is adaptively determined. Following

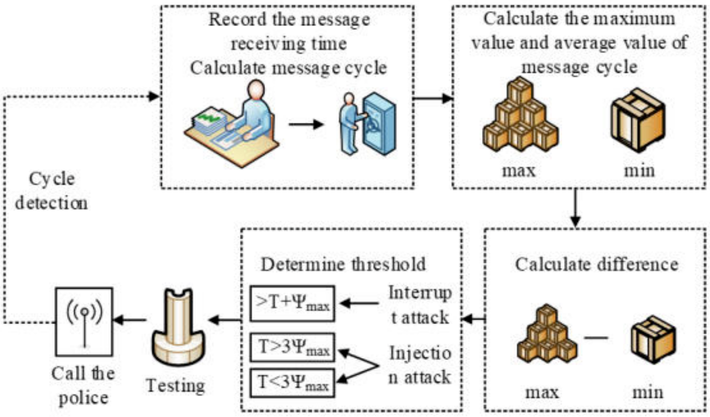

Fig. 4.4: Running flow of bus intrusion adaptive detection algorithm based on message cycle

message receipt, as shown in Figure 4, record the message's receiving time. Next, calculate the message's period. Finally, determine the detection threshold for various bus attacks by comparing the calculated message period's maximum and average values with their values. In order to avoid false positives, a small number of time margin is added to the detection threshold for fine tuning. After determining the detection threshold, the vehicle bus message is detected, the receiving time of the message is recorded and judged after initialization, the time cycle difference is detected and analyzed according to the determined threshold, and the message is judged as an interrupt attack or an injection attack. If no message is received, it is directly judged as an interrupt attack, and the vehicle bus system is circularly detected to intuitively see that the system enters the shutdown state.

5. Experiment And Result Analysis.

5.1. Algorithm Performance Test and Analysis. In order to verify the effectiveness and optimization of the adaptive intrusion detection algorithm based on the message cycle, the algorithm is compared with the sequence mining intrusion detection algorithm to check the accuracy and recall of the two algorithms. The comparison results of the accuracy and recall of the two algorithms are shown in Figure 5.1.

Figure 5.1 compares and analyses the average PR of the message cycle based adaptive intrusion detection algorithm and the sequence mining intrusion detection algorithm. Assuming the same accuracy rate, the recall rate of the message cycle based adaptive intrusion detection algorithm is higher. Given the same recall rate, the accuracy of the message cycle based adaptive intrusion detection algorithm is also higher. Compared with the sequence mining intrusion detection algorithm, the adaptive intrusion detection algorithm based on the message cycle has higher accuracy and recall rate, which proves that the adaptive intrusion detection algorithm based on the message cycle proposed by the research institute is effective and optimized, and its algorithm performance is better than the sequence mining detection algorithm. In order to clarify the detection efficiency of the algorithm in intrusion detection, the detection time of the algorithm is tested and analyzed. The detection running time of the algorithm is shown in Fig. 5.2. It can be seen from Figure 5.2 that the adaptive intrusion detection algorithm based on the packet period is trained and tested three times to observe the change in the detection time of the algorithm. In the first training of the algorithm, the detection time of the algorithm decreases continuously as the number of iterations increases. When the number of iterations reaches 50, the algorithm starts to stabilize and the detection time is stable within 3s. Compared with the first training, in the second and third training, the detection time of the algorithm is significantly reduced, which proves that the adaptive intrusion detection algorithm based on the packet cycle has faster computational search efficiency and will continuously optimize its own intrusion detection capability with the increase of training times.

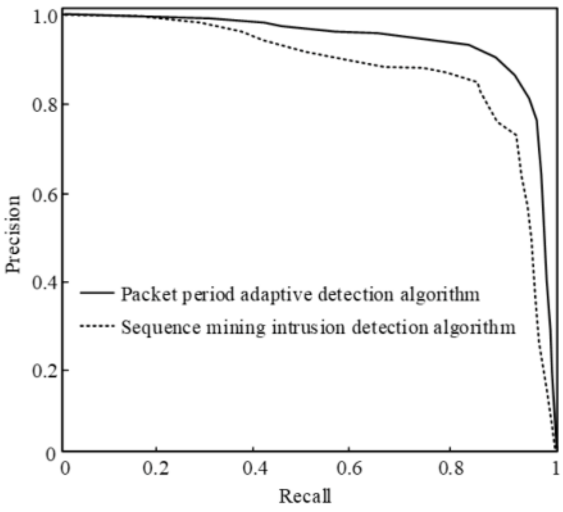

Fig. 5.1: Packet period adaptive detection algorithm PR curve

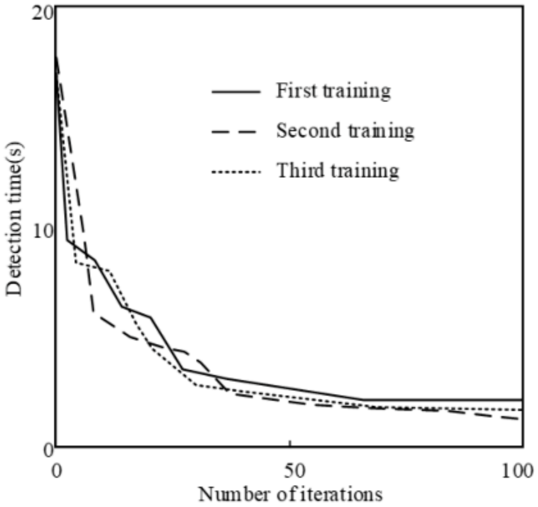

Fig. 5.2: Speed change detected by algorithm

5.2. Application Simulation Experiment Results. The vehicle CAN bus intrusion detection simulation experiment is carried out by using CANoe simulation software to validate the feasibility of the proposed algorithm. The CANoe simulation software is used to simulate the real vehicle CAN bus, to simulate the single channel high-speed vehicle CAN bus system, to add detection nodes to the vehicle bus by using the node programming function in the CANoe simulation software, and to simulate the process of the vehicle CAN bus being attacked by hackers in combination with CANdb++ and Replay Block tools. The CPU memory of the system is 8G, and the main frequency is 3.4GHz. The can main control chip is Cortex M4 core, and the main frequency is 168MHz. The running performance and detection effect of the adaptive detection algorithm based on message cycle are analyzed. The transmission of vehicle CAN bus message in the simulation environment

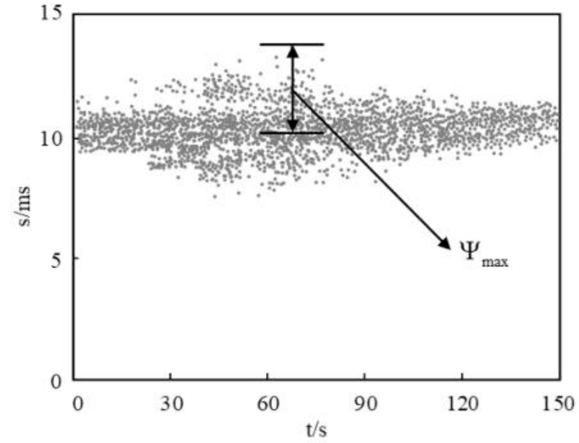

Fig. 5.3: Vehicle CAN bus message sending in simulation environment

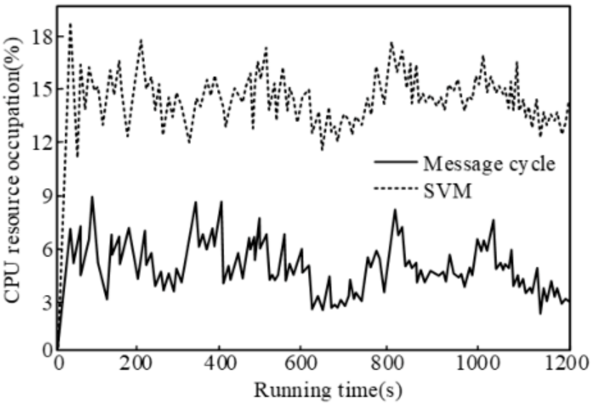

Fig. 5.4: Vehicle CPU resource occupancy detection results under two algorithms

is shown in Figure 5.3.

It can be seen from Figure 5.3 that the average sending period of vehicle CAN bus messages in the simulation environment is 10.3ms, and the CAN bus messages of vehicles have periodic characteristics. The maximum value of the difference between the reception time difference of two adjacent messages and the transmission period in the ideal state is 3.7 Ms. In order to verify the feasibility of the adaptive detection algorithm based on message cycle under the constraint of computing resources, the computing and storage resource conditions of the vehicle CAN bus are considered, and the bus intrusion detection algorithm based on Support Vector Machine (SVM) is compared and analyzed, and the CPU resource occupancy of the two algorithms is compared. The results of the vehicle CPU resource occupancy detection results under the two algorithms are shown in Figure 5.4.

As can be seen from Figure 5.4, the SVM-based detection algorithm is used to detect vehicle CAN bus intrusion. The vehicle CPU occupation is large, and the average vehicle CPU occupation is 14.93%, which seriously compresses the operation space of the original differential CAN bus system and affects the normal transmission of vehicle CAN messages. The average vehicle CPU occupancy of the intrusion adaptive detection algorithm based on message cycle is only 4.76%, which reduces the CPU occupancy by 10.17% when compared

Table 5.1: Threshold and Detection of the Attacked Message

Attack type	Attacked message	Cycle (ms)	Δmax (ms)	Threshold (ms)	False alarm number	Number of missing reports
Injection attack	M1	8 8 8	1.8 1.8 1.8	4.5 6 7.5	0 0 101	19 0 0
Injection attack	M2	8 8 8	3.6 3.6 3.6	3 4 5	0 0 1	32 11 7
Interrupt attack	M1	8 8 8	1.8 1.8 1.8	9 10 11	105 0 0	0 0 0
Interrupt attack	M2	8 8 8	3.6 3.6 3.6	11 12 13	21 0 0	0 0 0

to the SVM-based intrusion detection algorithm. This algorithm fully accounts for the computing resource constraints of the actual on-board ECU environment, occupies fewer computing resources for vehicles, and interferes less with the operation performance of the vehicle CAN bus. It can effectively avoid affecting the normal message sending due to the preemption of computing resources. It is proved that the proposed method can be applied in the actual vehicle environment and has practical feasibility.

To demonstrate the application effect of the proposed algorithm in the actual operation of the vehicle, a malicious node is added to the experimental vehicle CAN bus to simulate injection attack and interrupt attack respectively. The malicious node is used to inject 5000 forged messages into the vehicle CAN bus and conduct 5000 interrupt attacks at random. The thresholds and detection conditions of the attacked messages M1 and M2 when they are subjected to injection attack and interrupt attack respectively are shown in Table 5.1.

It can be seen from table 5.1 that the period of message M1 is 8ms. According to the threshold adaptive determination rule, its injection attack detection threshold should be in the range of [4.9,6.2]. If the threshold is 4.5ms, the detection system has 19 missing messages. If the threshold is 7.5ms, the detection system will have 101 false positives. When the detection threshold is 6ms, there are no false or missing messages. If message M1 is subject to an interrupt attack, its detection threshold must be greater than 9.8ms according to the adaptive detection rule. If the detection threshold is 9ms, there will be 105 false alarms in the detection system. If the detection threshold is 10ms and 11ms, there will be no false or missing alarms.

The time period of message M2 is 8ms. According to the threshold determination rules of the algorithm, the detection threshold of injection attack should be less than 4.4ms. When the threshold is set to 5ms, there are 1 false alarm message and 7 false alarm messages. When it is 4ms and 3MS, there are no false alarm, 11 and 32 false alarm messages, respectively. For interrupt attack on message m2, the detection threshold shall be greater than 11.6ms. When the detection threshold is 11ms, 21 false alarm messages appear in the detection system, and there is no false alarm. When the detection threshold is 12ms and 13ms, there are no false alarm or missing alarm. From the application results of the detection system, it can be seen that the proposed algorithm is effective in determining the detection threshold, and has a good effect on the detection of interrupted attacks, without false positives or missing positives. When the message cycle meets condition , the injection attack detection may have a minimal probability of missing positives.

6. Conclusion. In order to ensure the communication security of the vehicle CAN bus, the research fully considers the computing resource constraints of the on-board ECU environment, and proposes a method of monitoring and detecting the bus attack by adaptively determining the threshold. The bus simulation experiment and vehicle application experiment are carried out with CANoe simulation software. The research results contribute to improving the efficiency of intrusion detection in automotive networks and have some positive implications for communication security in automotive networks. However, the detection accuracy of the algorithm for injection type attacks is lower than that for interrupt type attacks, and there is a possibility of missing reports with a minimum probability. In the future, the injection type attack detection algorithm can be further optimized, and the Generative adversarial network can be used to solve the problem of attack sample data imbalance and improve the detection sensitivity for injection type attacks.

Funding. The research is supported by: the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJQN201801106).

REFERENCES

[1] Tang, C. Ceder, et al. *Vehicle Scheduling Of Single-Line Bus Service Using Operational Strategies.* **20**, 1149-1159 (2019)

[2] Zhang, H., Meng, X., Zhang, X. & Others CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. *Sensors.* **20** pp. 17 (2020)

[3] Jin, H. & Papadimitratos, P. DoS-resilient cooperative beacon verification for vehicular communication systems. *Ad Hoc Networks.* **90**, 1-10177 (2019)

[4] Ning, J., Wang, J., Liu, J. & Others Attacker Identification and Intrusion Detection for In-Vehicle Networks. *IEEE Communications Letters.* **23**, 1927-1930 (2019)

[5] Li, Y., Ni, P., Zhang, S. & Others ProSampler: an ultra-fast and accurate motif finder in large ChIP-seq datasets for combinatory motif discovery. *Bioinformatics.* **35**, 4632-4639 (2019)

[6] Jo, H., Jin, H., Choi, H. & Others MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Networks. *IEEE Transactions On Vehicular Technology.* **69**, 2204-2218 (2019)

[7] Xiang, Y., Fu, Y. & Huang, H. Global Topology Constraint Network for Fine-Grained Vehicle Recognition. *IEEE Transactions On Intelligent Transportation Systems.* **21**, 2918-2929 (2020)

[8] Katragadda, S., Darby, P., Roche, A. & Others Detecting Low-Rate Replay-based Injection Attacks on In-Vehicle Networks. *IEEE Access.* **8**, 54979-54993 (2020)

[9] Al-Saud, M., Eltamaly, A., Mohamed, M. & Others An Intelligent Data-Driven Model to Secure Intravehicle Communications Based on Machine Learning. *IEEE Transactions On Industrial Electronics.* **67**, 5112-5119 (2020)

[10] Ullah, M. Arfa Hassan M A, Farooq M S, et al. *Intelligent Intrusion Detection System For Apache Web Server Empowered With Machine Learning Approaches[J]. International Journal Of Computational And Innovative Sciences.* **1**, 21-27 (2022)

[11] Leevy, J. & And, K. and analysis of intrusion detection models based on cse-cic-ids2018 big data[J]. *Journal Of Big Data.* **7**, 1-19 (2020)

[12] Thakkar, A. & Lohiya, R. review of the advancement in intrusion detection datasets[J]. *Procedia Computer Science.* **167**, 636-645 (2020)

[13] Salih, A. & Abdulazeez, A. Evaluation of classification algorithms for intrusion detection system: A review[J]. *Journal Of Soft Computing And Data Mining.* **2**, 31-40 (2021)

[14] Razmjouei, P., Kavousi-Fard, A., Dabbaghjamanesh, M. & Others Ultra-lightweight Mutual Authentication in the Vehicle Based on Smart Contract Blockchain: Case of MITM Attack. *IEEE Sensors Journal.* **21**, 15839-15848 (2020)

[15] Ye, Z., Ni, H., Xu, Z. & Others Sensor fault estimation of networked vehicle suspension system with deny-of-service attack. *IET Intelligent Transport Systems.* **14**, 455-462 (2020)

[16] Olufowobi, H., Young, C., Zambreno, J. & Others SAIDuCANT: Specification-based Automotive Intrusion Detection using Controller Area Network (CAN) Timing. *IEEE Transactions On Vehicular Technology.* **69**, 1484-1494 (2019)

[17] Ju, Z., Zhang, H. & Tan, Y. Deception Attack Detection and Estimation for a Local Vehicle in Vehicle Platooning Based on a Modified UFIR Estimator[J]. *IEEE Internet Of Things Journal.* **7**, 3693-3705 (2020)

[18] Parham, M. & AA., P. An Effective Privacy-Aware Sybil Attack Detection Scheme for Secure Communication in Vehicular Ad Hoc Network. *Wireless Personal Communications.* **113**, 1149-1182 (2020)

[19] Ayaida, M., Messai, N., Najeh, S. & Others A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs. *Ad Hoc Networks.* **90**, 1-10184 (2019)

[20] Feng, S. & Haykin, S. Cognitive Risk Control for Anti-Jamming V2V Communications in Autonomous Vehicle Networks. *IEEE Transactions On Vehicular Technology.* **68**, 9920-9934 (2019)

[21] Ye, Z., Ni, H., Xu, Z. & Others Sensor fault estimation of networked vehicle suspension system with deny-of-service attack. *IET Intelligent Transport Systems.* **14**, 455-462 (2020)

[22] Su, S., Tian, Z., Liang, S. & Others A Reputation Management Scheme for Efficient Malicious Vehicle Identification over 5G Networks. *IEEE Wireless Communications.* **27**, 46-52 (2020)

[23] Ju, Z., Zhang, H. & Tan, Y. Distributed Deception Attack Detection in Platoon-Based Connected Vehicle Systems. *IEEE Transactions On Vehicular Technology.* **69**, 4609-4620 (2020)

[24] Zhang, Q., Liu, K., Xia, Y. & Others Optimal Stealthy Deception Attack Against Cyber-Physical Systems. *IEEE Transactions On Cybernetics.* **50**, 3963-3972 (2019)

[25] Mousavinejad, E., Yang, F., Han, Q. & Others Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning. *IEEE Transactions On Intelligent Transportation Systems.* **21**, 3821-3834 (2020)

[26] Wu, W. Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Transactions On Intelligent Transportation Systems.* **21**, 919-933 (2019)

[27] Al-Absi, M., Al-Absi, A. & Lee, H. Secure Enhanced Non-Cooperative Cognitive Division Multiple Access for Vehicle-to-Vehicle Communication. *Sensors.* **20** pp. 4 (2020)

[28] Gope, P. & Sikdar, B. An Efficient Privacy-preserving Authentication Scheme for Energy Internet-based Vehicle-to-Grid Communication. *IEEE Transactions On Smart Grid.* **10**, 6607-6618 (2019)

[29] Sanders, C. & Wang, Y. Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications. *IEEE Transactions On Vehicular Technology.* **69**, 15656-15667 (2020)

Edited by: Zhenling Liu
Special issue on: Cloud Computing for Intelligent Traffic Management and Control
Received: June 13, 2023
Accepted: Aug 21, 2023