



Message Transmission Reliability Evaluation of CAN Based on DSPN

Shujun Yong¹, Lerong Qi², Yunhong Ma²(✉), and Yifei Zhao²

¹ Huayin Ordnance Test Center, Weilan 710142, China

² Northwestern Polytechnical University, Xi'an 710072, China
mayunhong@nwpu.edu.cn

Abstract. The message transmission reliability is an important performance of CAN communication. The message transmission reliability of the CAN refers to the ability of the message to be successfully transmitted within its deadline. In order to assess the message transmission reliability of CAN, a four-node CAN communication model is set up based on the deterministic and stochastic Petri net in this paper, which is used to simulate the arbitration mechanism and error handling mechanism of CAN. The model is used to demonstrate the operation of the CAN bus in an interference environment with transient bursts which is used to simulate the external electromagnetic interference. Message transmission failure probability under the interference is used as the indicator of the message transmission reliability of CAN, and a solution method for proposed model based on the queuing theory is given to acquire the stationary value of the message transmission failure probability. The simulation gives the analysis of reliability of message transmission under different interference arrival intervals, different message priorities, different message periods and different number of nodes, which verifies the validity and feasibility of the proposed model.

Keywords: Controller area network · Reliability evaluation · Petri nets

1 Introduction

CAN-bus has the characteristics of good real-time performance because of short message frame, such as strong anti-interference ability and high cost performance. It is widely used in bus data communication between automobiles and various industrial sites. As a real-time information transmission system, CAN message failure will have a strong impact on system performance, so message transmission reliability [1] is an important indicator of CAN. The CAN message is considered to be successfully transmitted when its response time is less than its deadline. In this paper, the successful transmission probability of the CAN message is used as the indicator for evaluating the reliability of the message transmission of CAN.

There are many factors that affect the reliability of CAN data transmission, including design factors and environmental factors. With the development of electronic technology, the data communication in the industrial field is becoming more and more complex, and

the electromagnetic interference intensity is getting larger and larger. Electromagnetic interference can cause transmission errors, and trigger CAN error handling mechanism. With this mechanism the error message is generated and the message with error is retransmitted. The error handling mechanism effectively guarantees the successful transmission of the message. But too many errors will increase the bus utilization and delay the message response time. In severe cases, the message may miss its deadline and so the message transmission fails.

The analysis of message transmission reliability mainly evaluates whether the message response time exceeds the deadline of the message. For the response time analysis, the worst-case response time (WCRT) indicator of a message is a commonly used indicator. Tindell et al. [2] proposed a scheduling method based on fixed-priority preemption scheduling for single-processor systems in 1994. They gave a WCRT analysis method based on recursion, and concluded that the message is schedulable if the WCRT is less than the deadline. Punnekkat et al. [3] proposed a more general fault model and applied it to the WCRT analysis of CAN. Nolte et al. [4] proposed a worst-case probability response time analysis method based on the number of bits in CAN as a random variable, which reduces the conservativeness of WCRT analysis. Mubeen et al. [5] gave the WCRT analysis based on several different queues such as priority queue and FIFO queue, etc.

In addition to WCRT analysis, many researches focus on the response time distribution. As early as 1994, Muppala et al. [6] calculated the response time distribution of fixed-length periodic messages based on the stochastic reward network (SRN), but the limitation was large, which caused a big difference with the actual CAN bus. Nilsson et al. [7] considered random message lengths but did not consider bit stuffing and fault models, so the results are still too optimistic. Navet et al. [8] proposed the Worst-Case Deadline Failure Probability (WCDFP) in 2000. They believed that because of the random interference, the event that the message response time exceeded the deadline became a random event. Then give the probability algorithm of WCDFP. Portugal [9] proposed a determination of stochastic Petri nets (DSPN) model to analysis the reliability of CAN, while the model is complex and the index chosen was unable to get the required result. Kumar et al. [10] analyzed the response time distribution of CAN messages and gave an analysis model based on the (DSPN). Chen et al. [11] gave an analysis of average response time of CAN based on the queuing theory, which could only analysis the average value instead of the distribution of response time. Sun et al. [12] improved the model and compared the results obtained with the results of the simulation based on colored Petri nets (CPN) to verify the validity of the model, but the above two did not consider the fault impact.

Deterministic and Stochastic Petri Nets (DSPN) is one of the effective tools for discrete event modeling. Based on DSPN, this paper proposes a CAN communication model which simulates the arbitration mechanism and error handling process, and evaluates the reliability of CAN message transmission.

2 Working Mechanism of CAN

2.1 Bit-by-Bit Arbitration

The CAN adopts a bus topology, and all nodes are equally connected to the bus with a multi-master transmission mechanism. Since the CAN bus can only transmit one message at a time, there is a preemption of the bus when multiple messages are ready to be transmitted at the same time. The CAN bus stipulates that each message has a unique ID. Non-destructive bit-by-bit arbitration is carried out according to ID between messages. The message winning the arbitration with high priority uses the bus and transmits the message. The message that lost the arbitration waits for the next arbitration. This causes the message losing the arbitration unable to be sent immediately after the message is generated, and the message response time increases which also increases the probability of message transmission failure.

2.2 Error Handling

The CAN has a strong error detection capability. The probability of an error message being missed by the CAN bus [13] is less than 4.7×10^{-11} . Any node that detects an error will perform error signaling and recovering, which guarantee the accurate transmission of the message.

Error signaling is the process by which a node signals an error by transmitting an error flag. According to the fault confinement mechanism of CAN, the CAN node has three statuses: error active, error passive and bus-off. The error flag of the error active node is 6 dominant bits. These 6 bits will cause a bit stuffing error to abort the transmission of the message and signal the error; the error flag of the error passive node is 6 recessive bits, which can not affect the bus level; the node in the bus-off status is not allowed any interaction with the bus.

The error flag of the error active node will be superimposed. As shown in Fig. 1, if both the error bit and the previous correct bit are dominant, then for the receiving node, after monitoring the fourth dominant bit of the sending node's error flag, together with the previous two dominant bits there have already been six dominant bits monitored. Then the receiving node detects a bit stuffing error and transmits six dominant bits to signal the error, which causes the error flag on the bus to be superimposed into 10 dominant bits. Obviously, if the error bit is a recessive bit, then the two error flags will be superimposed with 12 bits, which is the maximum length of the error flag overlay. After the error flag is superimposed, 8 recessive bits are added to the error delimiter, and the transmission of the error frame is completed. In a word, in the error active status, the error signal will be an error message with length within 17 bits to 23 bits adding the 3 bits of interframe space. This error message will cause the occupation of bus and generate delay.

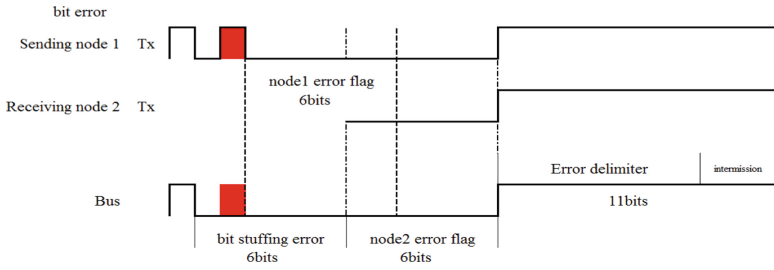


Fig. 1. Superposition of the active frame

The error recovering mechanism allows previously erroneous messages to be automatically retransmitted after the error frame is transmitted, but note that messages from other nodes are also allowed to preempt the bus. If a higher priority message is ready to be transmitted, the retransmission of the erroneous message is delayed and the probability of transmission failure increases.

3 Model Framework and Solution Method

3.1 DSPN Features

Petri nets are often used to simulate discrete events. DSPN is an improvement of the Stochastic Petri net (SPN): the forbidden arc is added to the DSPN to implement the prohibition of the transition when the place contains the number of tokens greater than or equal to the arc weight; the DSPN increases the immediate transition and can assign priorities to several conflicting immediate transitions; DSPN adds deterministic transitions to describe events that occur at a fixed time. These features of DSPN can be used to simulate the CAN communication model.

3.2 Model Framework

This paper makes the following assumptions for the model: each node transmits a periodic message, and the normal transmission times of all the messages are the same which is the maximum value; the message period is the deadline for the message. When the deadline arrives, the new message will overwrite the old message and cause the old message to fail; all nodes are in the error active status because the probability of the node being in the error passive status is very low [8]; the interference on the CAN bus is the electrical fast transient burst, which is the standard test signal of electromagnetic compatibility; the Portugal [9] founded that the change of the interference duration does not cause an order of magnitude change in the probability of message failure when other parameters are unchanged. Therefore, it is assumed that the burst signal has the same width with the bit time and affects only one bit; the interference during the error frame transmission is ignored. The error frame transmission length is the maximum length of the active error frame plus the interframe space total 23 bits.

Based on the above assumptions, a single-node CAN communication model is established as shown in Fig. 2.

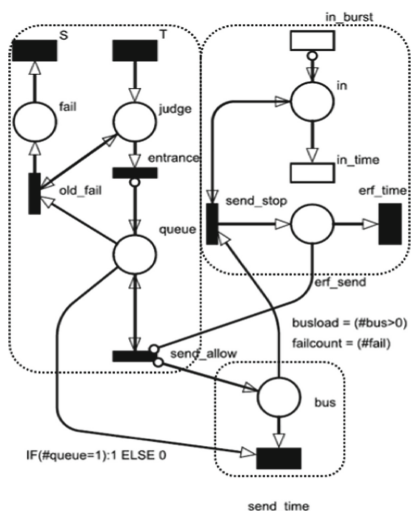


Fig. 2. Single-node model of CAN based on DSPN

The model includes the node model (the part in the dotted line on the left), the interference and error handling model (the part in the dotted line on the right), and the bus channel model (the part in the lower dotted line box).

The node model is responsible for message generating, message transmitting and message failure counting. The deterministic transition T represents the generation of periodic messages. The place $queue$ represents the message queue. The intermediate transition $Entrance$ indicates that the generated message enters the message queue $queue$, and the intermediate transition old_fail indicates that the old message is overwritten by the new message and so exits the message queue $queue$. Whether the two transitions mentioned before are enabled or not is determined by whether there is a token in $queue$. The token entering $queue$ waits until $send_allow$ is enabled, while the place $fail$ and the deterministic transition S form a simple queuing system to count the number of failed messages.

The place bus and the deterministic transition $send_time$ form a bus channel model. No token in bus indicates that the bus is idle. At this time, the intermediate transition $send_allow$ will be enabled. After $send_allow$ fired, a token is placed in bus to indicate that the bus is transmitting a message now. The deterministic transition $send_time$ represents the message transmission time. After $send_time$ fired, the token in $queue$ and bus are deleted at the same time, indicating that the message in the node's message queue is already transmitted and the bus becomes idle. Note that the arc weight of $queue$ to $send_time$ is a logical expression, which promises that only the token in the highest priority node's queue will be deleted when $send_time$ fires.

The interference and error handling model only considers the operation of the bus within the transient interference group burst interval. It is assumed that the transient interference group burst is periodic, and the conditional probability is used to extend the results of the model to the entire time domain. The exponential transition in_burst represents the interference of the arrival interval obeying the exponential distribution during

the group burst. The place *in* with a token indicates that the bus is facing interference at this time, and the inhibiting arc with *in* pointing to *in_burst* ensures that only one interference at the same time. The exponential transition *in_time* describes the interference duration obeying the exponential distribution.

When *bus* and *in* are marked at the same time, the intermediate transition *send_stop* fires indicating that there is interference when the message is being transmitted at this time, so the token in *bus* is deleted, and a token is placed in *erf_send* to represent the error frame transmission. The inhibit arc of *erf_send* pointing to *send_allow* indicates that normal message transmission is prohibited during error frame transmission. The deterministic transition *erf_time* describes the transmission time of the error frame.

3.3 Solution Method

The simulation tool used in this paper is TimeNET4.4, which supports graphical modeling and multiple simulation solutions. Stationary simulation is a common analysis method provided in TimeNET. It can obtain the stationary value of the model when the time tends to infinity. Therefore, it is often used for probability measurement. Stationary simulation is to obtain a certain frequency value through a large number of samples. Since the number of samples is large, according to Bernoulli's law of large numbers, the frequency is infinitely close to the probability required.

In this paper, the message failure probability is obtained by solving the stationary value of the number of message failures per unit time. This value is divided by the total number of messages generated per unit time to obtain the message failure probability, and the message transmission reliability of CAN is evaluated by the message failure probability.

After experimental comparison, the Multi-trajectory stationary analysis method provided in TimeNET has higher efficiency in solving the model. Therefore, Multi-trajectory stationary analysis method is used to carry out all the simulations in the paper.

The way to solve the TimeNET model is to build a measure expression and then run the simulation to get the result of the measure expression. TimeNET gives the syntax of the measure expression, and the user can create the expression of the desired measure. The measure established in the model built in this paper is (#fail), which means the average number of tokens contained in the place *fails*. The purpose is to get the number of failed messages per unit time.

The little formula is a basic conclusion in queuing theory that describes the relationship between the average arrival rate of customers, the average number of customers in the system, and the average length of time the customer spends in the system in a stable queuing system. For this model, the place *fail* and the deterministic transition *S* can be considered as a queuing system. The token is regarded as the customer, the average arrival rate of the customer is the number of message failures per unit time which is defined as λ , and the average number of customers n in the system is the average number of tokens in the steady state, the average stay time of the customer in the system s is the delay of the transition *S*, which is determined by the little formula:

$$\lambda = n/s = E_f/delay_T \quad (1)$$

Where E_f is the average number of tokens in *fail*, that is, the stationary result of the measure: (#fail), and $delay_T$ is the firing delay of the deterministic transition T . The failure probability P_{fail} of a message with a generation period of T_g is:

$$P_{fail} = \lambda / (1/T_g) = \lambda \cdot delay_{msg} \tag{2}$$

Where $delay_{msg}$ is the delay of T of the message. Bringing the formula (1) into the formula (2):

$$P_{fail} = E_f \cdot delay_{msg} / delay_T \tag{3}$$

The message failure probability P_{fail} during the transient interference burst is obtained above and it can be extended to the entire time domain. Let the transient interference period be t_a , the duration be t_c , the probability of message failure in the entire time domain be P_a , and the probability of transient interference bursting be P_{in} , then the conditional probability is:

$$P_a = P_{fail} \cdot P_{in} \tag{4}$$

The probability of transient interference burst P_{in} is:

$$P_{in} = t_a / (t_a + t_c) \tag{5}$$

Bring Eqs. (3) and (5) into Eq. (4) to get the probability of message failure in the entire time domain P_a :

$$P_a = E_f \cdot delay_{msg} \cdot t_a / [delay_T \cdot (t_a + t_c)] \tag{6}$$

4 Simulation Analysis

4.1 Simulation Model and Parameter

A four-node model is extended by following the working mechanism of the single node model. The simulation verification of CAN message transmission reliability is carried out with the four-node model. The four-node DSPN model is shown in Fig. 3.

In the model shown in Fig. 3, there are four nodes 1, 2, 3, and 4 from left to right named queue1, queue2, queue3 and queue4 separately. The priorities of them are sequentially lowered. We have established three measurements for node 2, node 3, and node 4 to assess the probability of message transmission failure. Node 1 has the highest priority, and there is no delay caused by arbitration failure, which lead the probability of message failure to a very low level. Besides, in TimeNET, the time spent on simulation of low probability events is huge which reduces the simulation efficiency. So the node 1 is out of consideration.

The simulation was performed in the TimeNET 4.4 environment, setting a 95% confidence interval for all simulations with a relative error of 10%. Set the CAN bus communication bit rate to 125 kb/s. All nodes send data frame messages with a data field length of 8. The average frame transmission time is approximately equal to 1

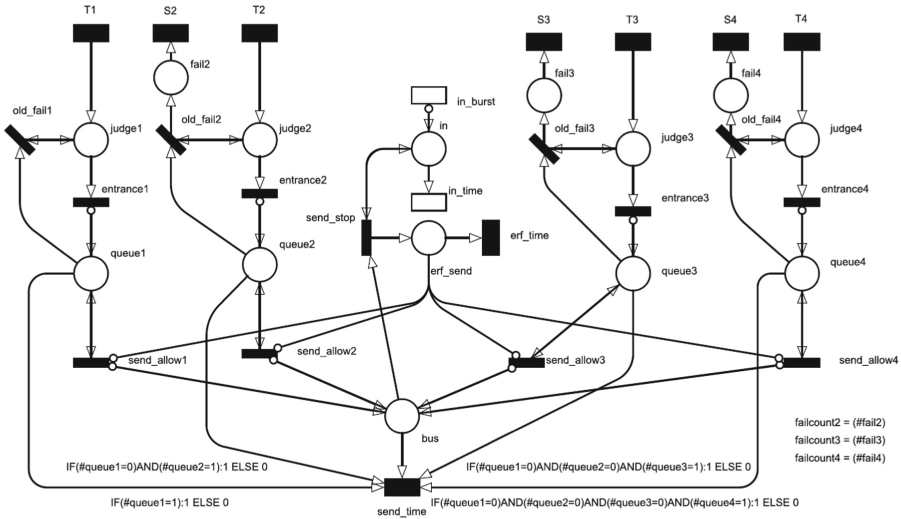


Fig. 3. Extended four-nodes model of CAN based on DSPN

ms. If an error occurs, the error frame length is 23 bits and the transmission time is approximately equal to 0.18 ms. In the simulation, the interference is assumed to be transient interference, the occurrence period is 450 ms, and the interference duration is 50 ms.

Based on the CAN model of DSPN established in this paper, the total probability P_a is simulated and counted.

4.2 Interference Arrival Interval

In order to analyze the relationship between the interference arrival interval and the message failure probability, the average interval of transient interference is set to 2 ms, 4 ms, 6 ms, 8 ms, 10 ms and then simulate separately. Other all simulation parameters are listed in the Table 1.

Table 1. Simulation parameters

Transition	Firing delay/ms
T1	6
T2	7.5
T3	7.5
T4	7.5
S2	10
S3	10
S4	10
In_time	0.008
Erf_time	0.18
Send_time	1

Note that the T2, T3, and T4 are set to the same value, which can simulate the effect of priority on failure probability when other parameters are unchanged. However, at this time, T2, T3 and T4 will fire at the same time, which will increase the probability that the three messages preempt the bus. For this reason, the delay modules are added after the transitions T3 and T4, which can effectively reduce the probability of the preemption of the bus. The message of node 3 is delayed by 2.5 ms and the message of node 4 is delayed by 5 ms, and the comparison of the failure probability of the message before and after adding the delay is analyzed. The simulation results are shown in Fig. 4.

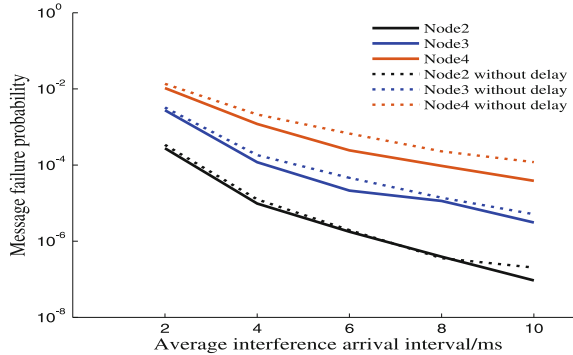


Fig. 4. The simulation results of the interference arrival interval

In Fig. 4, the vertical axis is the logarithmic axis which indicates the message failure probability, and the horizontal axis is the interference arrival interval. For all messages, as the interval of interference arrival increases, the message failure probability decreases exponentially. For the same node, the message failure probability with delay is almost always less than the value without delay, because the message generation is more uniform with delay and then the blocking and preemption phenomenon is reduced. In the case where the interference arrival interval is unchanged, the higher the priority of the node, the smaller the message failure probability, because higher priority means less waiting time, so the message is more likely to be successfully transmitted before the deadline.

4.3 Message Period

The simulation of the message period still sets the delay for node 3 and node 4. The interference arrival interval is fixed to 2 ms and the other parameters are kept unchanged. Firstly, the simulation of changing only one message period is implemented to observe the effect on all three messages failure probability. In this section, message period of node 3 is selected and changed from 7.5 ms to 15 ms with a 2.5 ms step size. The simulation results are shown in Fig. 5.

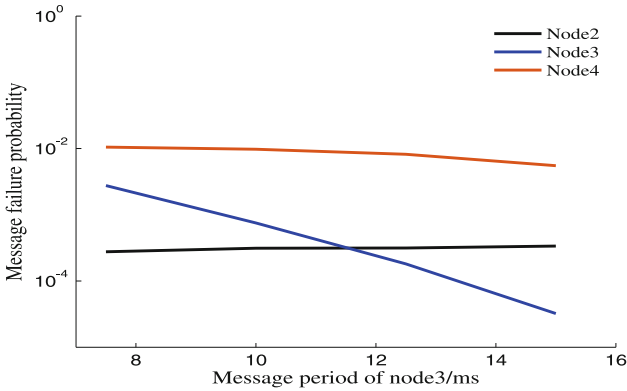


Fig. 5. The simulation results of the message period of node 3

As seen from Fig. 5, the message failure probability of node 3 decreases as the node 3 message period increases, while the failure probability of the other two messages is almost unchanged.

Secondly, all the three messages periods are changed from 7.5 ms to 15 ms with a 2.5 ms step size. The simulation results are shown in Fig. 6.

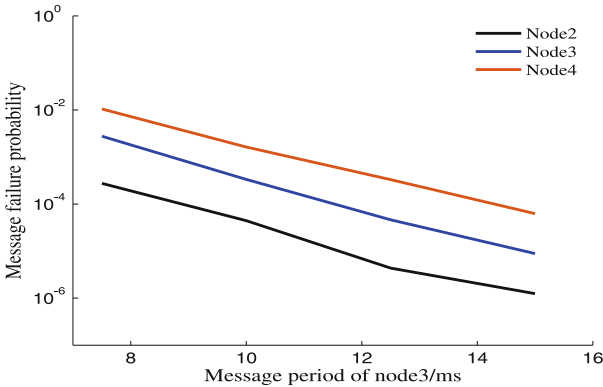


Fig. 6. The simulation results of all the three message period

It can be seen from Fig. 6 that after three message periods are changed, the failure probability of each message decreases as the message period increases, and the high priority message failure probability is always less than the low priority. From Figs. 5 and 6, we can draw a conclusion that in the case of other parameters unchanged, the message failure probability is only related to the message itself period, and the change of the message period has little effect on the failure probability of other messages.

4.4 Number of Nodes

In order to show the influence of the number of nodes on the simulation results, we performed two sets of simulations. The first group of simulations deleted the node 1 (the highest priority node) and compared the message failure probability before and after deletion while the second group deleted the node 4 (the lowest priority node) and do the same thing. The simulation parameters are the same as the Sects. 4.1 and 4.2. The simulation results are shown in the Figs. 7 and 8.

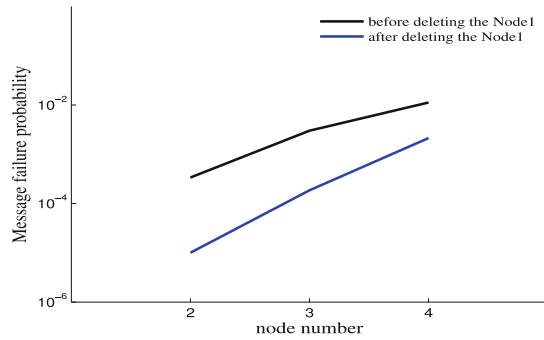


Fig. 7. The simulation results of deleting the Node1

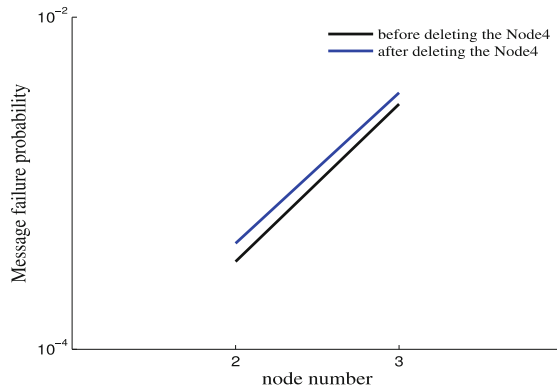


Fig. 8. The simulation results of deleting the Node4

It can be clearly seen from Figs. 7 and 8 that the message failure probability of the node 2 to node 4 is reduced after the node 1 is deleted while the message failure probability of the node 2 and node 3 do not change much after the node 4 is deleted. The results are reasonable because the node 1 as the highest priority node will hinder the transmission of node 2 to node 4. After it is deleted, other nodes send faster so the message failure probability is significantly reduced. But the node 4 has the lowest priority, so it has little influence on the transmission of other messages.

5 Conclusions

This paper establishes a CAN communication model based on DSPN, and it is used to simulate the arbitration mechanism and error handling mechanism of CAN. Based on the model, the reliability of message transmission of CAN under interference environment is evaluated. By adding transient impulse interference to the model, the influence of interference interval, message priority, message period and the number of nodes on CAN message transmission failure probability under interference environment is analyzed. The simulation example shows that the model has a good effect in evaluating the reliability of CAN message transmission in the presence of interference.

References

1. Hansson, H., Norstrom, C., Punnekkat, S.: Integrating reliability and timing analysis of CAN-based systems. *IEEE Trans. Industr. Electron.* **49**(6), 1240–1250 (2002)
2. Tindell, K., Burns, A., Wellings, A.J.: Calculating controller area network (CAN) message response times. *Control Eng. Pract.* **3**(8), 1163–1169 (1995)
3. Punnekkat, S., Hansson, H., Norstrom, C.: Response time analysis under errors for CAN. In: *Proceedings of the 6th IEEE Real-Time Technology and Applications Symposium (RTAS 2000)*, pp. 258–265 (2000)
4. Nolte, T., Hansson, H., Norstrom, C.: Probabilistic worstcase response-time analysis for the controller area network. In: *Proceedings of the 9th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2003)*, pp. 200–207 (2003)
5. Mubeen, S., Maki-Turja, J., Sjodin, M.: Extending worst case response-time analysis for mixed messages in controller area network with priority and FIFO queues. *IEEE Access* **2**(1 Suppl.), 365–380 (2014)
6. Muppala, J.K., Trivedi, K.S., Mainkar, V., et al.: Numerical computation of response time distributions using stochastic reward nets. *Ann. Oper. Res.* **48**(2), 155–184 (1994)
7. Nilsson, J., Bernhardsson, B., Wittenmark, B.: Stochastic analysis and control of real-time systems with random time delays. *Automatica* **34**(1), 57–64 (1998)
8. Navet, N., Song, Y.Q., Simonot, F.: Worst-case deadline failure probability in real-time applications distributed over controller area network. *J. Syst. Architect.* **46**(7), 607–617 (2000)
9. Portugal, P.: A model based on a stochastic Petri Net approach for dependability evaluation of controller area net. In: *Fieldbus Systems & Their Applications*, vol. 38, no. 2, pp. 150–157 (2005)
10. Kumar, M., Verma, A.K., Srividya, A.: Response-time modeling of controller area network (CAN). In: Garg, V., Wattenhofer, R., Kothapalli, K. (eds.) *ICDCN 2009*. LNCS, vol. 5408, pp. 163–174. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-92295-7_20
11. Chen, X., Liu, L., Lu, W.: Modeling and analysis of response time of CAN bus based on queueing theory. *J. Tianjin Univ.* **45**(3), 228–235 (2012)
12. Sun, W., Zhang, H., Pan, C.: Analysis on real-time performance of CAN bus with improved non-preemptive M/G/1 model. *J. China Railway Soc.* **35**(12), 57–63 (2013)
13. ISO 11898: Road Vehicles—Interchange of Digital Information—Controller Area Network (CAN) for High-Speed Communication. International Standards Organization (1993)