Research of In-Vehicle Ethernet Information Fault Detection Based on IEEE 802.1Qci

Yue Wang, Yu-Jing Wu, Yi-Hu Xu, and Yi-Nan Xu*

***Abstract*—With features such as the high data transfer rate of 1G/bps and strong compatibility, in-vehicle Ethernet can become the backbone network of next-generation in-vehicle bus network systems. Currently, in-vehicle Ethernet is mainly used in audio and video entertainment systems, to further improve the network security performance of in-vehicle Ethernet, the information security of the data layer and physical layer in the in-vehicle bus network system must be ensured. Based on the characteristics of in-vehicle Ethernet data frame structure, this paper introduces IEEE 802.1 Qci protocol, proposes an information fault detection method through data shifting, detection, and policing, and verifies it by simulation with OMNET++ simulation system. The experimental results show that the accuracy rate of in-vehicle Ethernet data during transmission can reach 99.61%, which further improves the network security performance of in-vehicle Ethernet.**

***Index Terms*—In-vehicle ethernet, information fault detection, IEEE 802.1Qci, OMNET++.**

I. Introduction

Ethernet in the framework of the IEEE standard has been commonly used in industry. With the development of intelligence, the requirement for bus transmission rate is getting higher and higher, and the in-vehicle Ethernet emerges as the times require. As an in-vehicle network system, it has the advantages of high bandwidth, high reliability, and low latency. However, it also increases the complexity of the in-vehicle bus. The development of complexity and connectivity in modern vehicles have led to a significant increase in security risks in in-vehicle networks [1]. In-vehicle Ethernet meets the bandwidth requirements for multimedia applications, autonomous driving, and safety applications, such as Advanced Driver Assistance Systems (ADAS). However, at the same time, it also needs to bring a higher quality of service (QoS) [2]. Time-sensitive networks (TSNs) has attracted much attention because they can meet the time synchronization, high real-time, and high reliability required for quality of service (QOS)in in-vehicle communication systems. The main goal of TSNs is to provide zero congestion loss and limited delay for various time-sensitive data streams, however, the security mechanisms of TSN protocols are rarely discussed [3].

Manuscript received August 18, 2022; revised October 23, 2022; accepted December 21, 2022. This work was supported by the National Natural Science Foundation of China (62161049 and 61763047).

The authors are with the College of Engineering of Yanbian University, Yanji, China.

*Correspondence: (e-mail: ynxu@ybu.edu.cn)

The authors of Reference [3] designed an IEEE 802.1Qci-based ADS(Advanced Drainage Systems) design where a large amount of invalid data intrusion reshapes the data flow and forces it back to the pre-data burst traffic. In [4], they proposed an integrated Time Sensitive Network Defined Software (TSSDN) based on Time Sensitive Network (TSN) and Software Defined Network (SDN) that can establish and investigate trust regions inside the in-vehicle network to reduce the attack surface of connected cars under various attack scenarios. In [5], the authors proposed a security-aware approach for the routing and scheduling of Ethernet control applications. The goal is to maximize the resilience of control applications to malicious interference in these networked control systems while ensuring the stability of all control devices.

In the TSN standard, the IEEE 802.1Qci protocol provides per-flow filtering and supervision of messages arriving at the port [6]. It can control the data flow by limiting the transmission bandwidth to reduce the impact of network attack and traffic overload problems. When a large amount of abnormal data intrudes, normal frames and abnormal frames will be filtered first, and then IEEE802.1Qci will reduce the transmission of abnormal frames by flow restriction or blocking [7]. Therefore, processing the messages arriving at the port first and reducing the possibility of abnormal frames entering the link will significantly improve the security and stability of the link.

The rest of this paper is organized as follows: Section 2 introduces the IEEE 802.1Q frame structure and describes the IEEE 802.1Qci protocol. Section 3 proposes an information fault detection method based on IEEE802.1Qci for the structural characteristics of IEEE 802.1Q frames. Section 4 uses OMNET++ to simulate and analyze the fault detection system. Finally, we conclude this work in Section 5.

II. Analysis of IEEE 802.1Q Frame Structure and IEEE 802.1Qci Protocol

A. IEEE 802.1Q Frame Structure

Frame tagging refers to assigning a unique tag to a necessary frame to identify the VLAN(A virtual local area network) information of this frame. The IEEE802.1Q protocol stipulates that after the destination MAC address (DA) and source MAC address (SA) fields of the data frame and before the protocol type field, a 4-byte VLAN tag is added to indicate that the data frame belongs to VLAN [8]. The position of the VLAN tag in the VLAN data frame is shown in Fig. 1.

doi: 10.18178/ijfcc.2023.12.1.595

The VLAN tag contains two fields: Tag Protocol Identifier (TPID), specified by the IEEE802.1Q protocol to take the value 0x8100; and Tag Control Information (TCI), which includes the priority, standard format indicator bits and VLAN ID.

Priority (PRI), the value range is 0~7. The larger the value, the higher the priority. Canonical Format Indicator (CFI), a CFI of 0 indicates that the MAC address is encapsulated in the standard format, and a CFI of 1 indicates that it is encapsulated in a non-standard format. In in-vehicle Ethernet, the value of CFI is 0. The VLAN ID (VID) is the number of the VLAN to which the data frame belongs, and the range of the VLAN ID is 0 ~ 4095. Since 0 and 4095 are reserved for the protocol, the valid value range of VLAN ID is 1~4094.

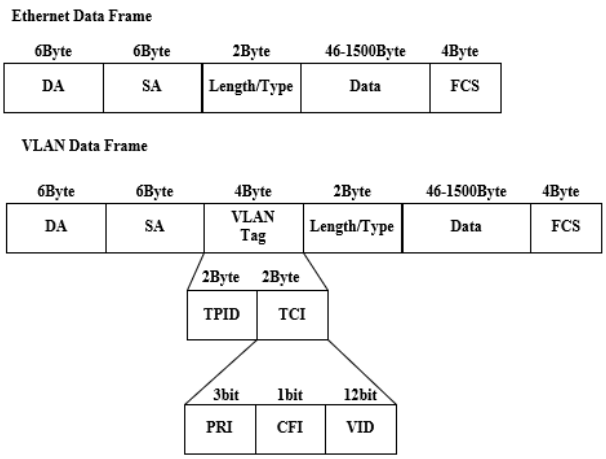

Fig. 1. VLAN data frame format for IEEE 802.1Q encapsulation.

B. IEEE 802.1Qci (Per-stream filtering and policing, PFSP)

The IEEE 802.1Qci Per-stream Filtering and policing (PSFP) standard [9] defines per-stream control and enforces rules for all incoming traffic. Fig.2 shows how the traffic is filtered and policed at the ingress.

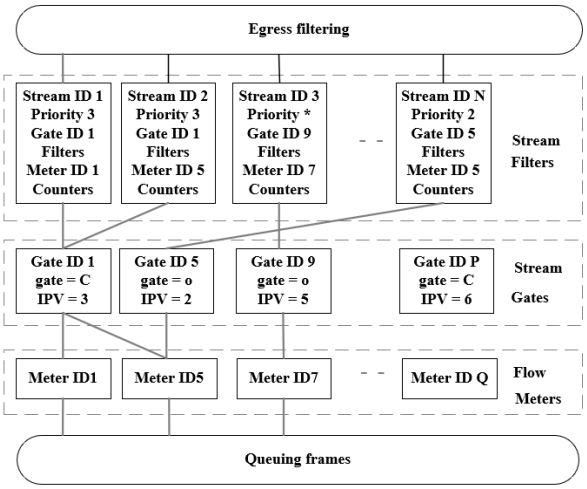

Fig. 2. IEEE 802.1Qci Per-stream filtering and policing process （PSFP）

Frames must go through three stages of monitoring and identification before they are queued. In the first stage, specific streams are filtered and policed in the Stream Filter, including Gate ID and Meter ID. They are mapped to the corresponding Stream Gates and Meters. In the second phase, Stream Gates are responsible for receiving incoming frames, and the status of the Stream Gates can be either closed or open, with the status of the gates being controlled by the Gate Control List. If a gate is "closed," the incoming frames are discarded. If it is "open," the frame is measured by a flow meter in the third stage. The flow meter applies an algorithm to determine whether to allow the frame to pass. For example, the flow meter can limit the bandwidth or burst size and flag or discard frames when they exceed the bandwidth or burst allowance [10].

III. Information Fault Detection Method

According to the format specified in the IEEE 802.1Q frame above, as shown in Fig.3 (a). When adding VLAN tags to untagged frames, different priorities are assigned depending on the type of data frame. For example, the highest priority of 7 should be used for critical network traffic. Priority 6 and 5 are mainly used for latency-sensitive applications. Priority 4 through 1 are used for controlled load applications, and priority 0 is automatically enabled if no other priority value is set. At the same time, different VIDs are assigned depending on the switch port information.

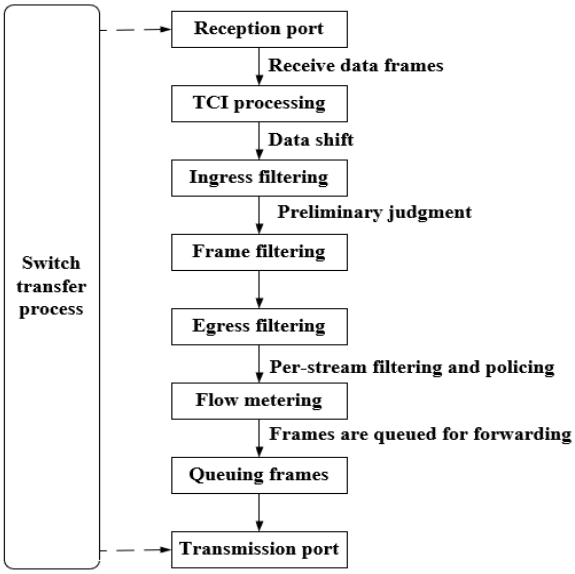

Fig. 3. Data frame forwarding process.

In the TCI data processing part, the value of TCI is related to whether the incoming ports of the switch can recognize it and whether the priority of the filtered ports can determine it. Therefore, we improve the tag control information. The 16-bit marker control information AX is divided into high eight-bits (AH) and low eight-bits (AL), and the buffer variable BX is set to interchange the data of AH and AL positions.

The rules for swapping marker control information data during transmission are as follows:

As shown in Eq. (1-3), the low value AL in the original data AX is saved in the buffer variable BX, the high value of the original data AX is assigned to the low bit, and the high value is now 0, and then the low value in the buffer variable BX is assigned to the high bit.

$$BX = AX|0xF \tag{1}$$

$$AX = AX \gg 8 \tag{2}$$

$$AX = AX|(BX \ll 0xF) \tag{3}$$

When the receiver port of the switch receives a data frame, the VLAN information and port information in the data frame are judged by ingress filtering. Therefore, before ingress filtering, we perform another shift process on the tag control information (TCI) to restore it to the original data state. The data frame forwarding process is shown in Fig.3.

After the tagged data frame arrives at the switch receive port, the normal frame will be restored to its original state by shift processing, while the abnormal frame will be processed to generate a new priority and VID.

Suppose the switch has only one VLAN port. When performing ingress filtering, it first determines whether the incoming port is a member port of the tagged VLAN. If not, the data frame will be discarded. If it is a member port, the switch will further determine whether the destination port is a member port of the tagged VLAN. If not, the data frame will be discarded. Otherwise, the packet will be forwarded to the destination port.

After the judgment is correct, it passes through frame and egress filtering and enters the IEEE 802.1Qci per-stream filtering and policing module. Most abnormal frames can be discarded by judging the mark control information (TCI), relieving the pressure on the per-stream filtering and policing module.

IV. Simulation and Analysis

A. Simulation Model

Simulations were performed using the OMNET++ simulation environment with the INET and CoRE4INET frameworks. coRE4INET supports in-vehicle network simulation and simulates most protocol frameworks, including the IEEE802.1Q model [11].

The topology is shown in Fig.4 and configured in detail.

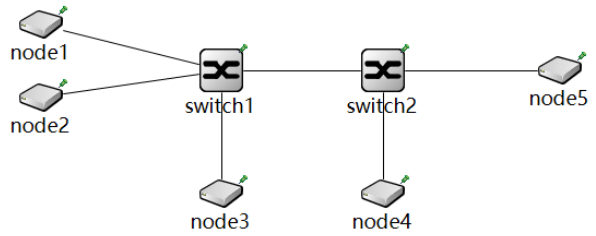

Fig. 4. Link topology.

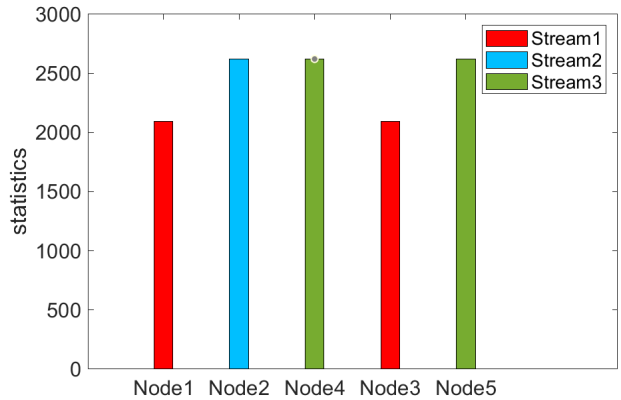

Fig. 5. Results of data flow transmitted by each node showing.

All links are configured with a bandwidth of 100Mbit/s. Node 1 and node 2 transmit the same size data with destination node 3. Node 1 sends the original data, and node 2 sends the data after being shifted and processed. Node 4 sends normal data to node 5. For easy differentiation, the data transmitted by node 1 is set as Stream1, and the sending interval is 500us. The data transmitted by node 2 is set as Stream2, and the sending interval is 400us. The data transmitted by node 4 is set as Stream3, and the sending interval is 400us. The experimental results are shown in Fig. 5.

B. Data Analysis

We counted the total number of data frames transmitted in 1 second. The results show that during the data transmission, when node 1, node 2, and node 4 respectively send Stream1, Stream2, and Stream3, node 3 only receives Stream1 from node 1 and does not receive the abnormal frame Stream2, and receives node 5 receives Stream3 from node 4 normally.

All data occurrences were counted, and according to the characteristics of IEEE 802.1Q frames, a total of 28672 cases were counted, of which the number of abnormal data shifted, and equal to the original data was 112. The correct rate is 99.61%.

V. Conclusion

In this paper, according to the structural characteristics of IEEE 802.1Q frames, its VLAN Tag is improved and combined with IEEE802.1Qci protocol, a message fault detection method is designed by the method of shifting, detection, and policing, which can discard abnormal frames just entering the switch. Its performance is evaluated by using OMNET++ simulation tool. The experimental results show that the method can achieve 99.61% accuracy in transmitting in-board Ethernet data during the simulation after simulating all simulation scenarios for simulation purposes. In future work, the performance of this information fault detection method will be further evaluated based on the simulation design method and model.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Yue Wang and Yu-Jing Wu: Methodology and writing of original draft; Yi-Hu Xu: Software and formal analysis; Yi-Nan Xu: Conceptualization and supervision.

Funding

This research was supported by National Natural Science Foundation of China (62161049 and 61763047).

References

[1] R. W. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919-933, 2020.

[2] K. Narayan and S. Rakesh, and N. S. Yeob, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, vol. 10, no. 2, pp. 1-33, 2021.

[3] F. Luo, B. Wang. Z. H. Fang, Z. Y. Yang, and Y. Jiang, "Security analysis of the TSN backbone architecture and anomaly detection system design based on IEEE 802.1Qci," *Security and Communication Networks*, vol. 2021, pp. 1-17, 2021.

[4] T. Häckel, P. Meyer, F. Korf, and T. C. Schmidt, "Secure time-sensitive software-defined networking in vehicles," Hamburg land, Germany, January1-14, 2022.

[5] R. Mahfouzi, A. Aminifar, S. Samii, P. Eles, and Z. Peng, "Security-aware routing and scheduling for control applications on Ethernet TSN

networks, " *ACM Transactions on Design Automation of Electronic Systems*, vol. 25, no. 1, pp. 1-26, 2019.

[6] P. Meyer, T. Häckel, S. Reider, F. Korf, and T. C. Schmidt, "Network anomaly detection in cars: A case for time-sensitive stream filtering and policing," Hamburg land, Germany, 2021.

[7] S. Samii and H. Zinner, "Level 5 by layer 2: Time-sensitive networking for autonomous vehicles," *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 62-68, 2018.

[8] D. A. J. A. Khaffaf, "Improving LAN performance based on IEEE802. 1Q VLAN switching techniques," *Journal of University of Babylon for Engineering Sciences*, vol. 26, no.1, pp. 286-297, 2018.

[9] IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks, Amendment 28: Per-Stream Filtering and Policing, *IEEE*, Piscataway, NJ. USA, September1–65, 2017.

[10] P. Meyer, T. Häckel, S. Reider, F. Korf, and T.C. Schmidt, "Network anomaly detection in cars based on time-sensitive ingress control," in *Proc. 2020 IEEE 92nd Vehicular Technology Conference*, 2020.

[11] P. Meyer, T. Häckel, S. Reider, F. Korf, and T. C. Schmidt, "Simulation of mixed critical in-vehicular networks," *Recent Advances in Network Simulation*, Hamburg land, Germany, May317-345, 2019

Yue Wang was born at Shandong Province of China. She received the bachelor degree in communication engineering from Yanbian University, China, in 2021.She is a currently working toward a master degree in the area of In-vehicle network, which include the design of security architecture of automotive Ethernet.

Yu-Jing Wu was born at Jilin Province of China. She received her M.S. and Ph.D in electronic and information engineering from Chonbuk National University, South Korea, in 2013 and 2016, respectively.

She is a lecturer of the division of electronic and communication engineering of Yanbian University, China. Her research interests include the In-vehicle communication networks.

Yi-Hu Xu was born at Jilin Province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, South Korea, in 2014.

He is a associate professor of the division of electronic and communication engineering of Yanbian University, Yanji, China. His research interests include the automobile electronic control and network.

Yi-Nan Xu was born at Jilin Province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, South Korea, in 2009.

He is a professor of the division of electronics and communication engineering of Yanbian University, Yanji, China. His research interests include the In-vehicle network and automobile electronic control.