2022-01-0113 Published 29 Mar 2022

Routing and Security Mechanisms Design for Automotive TSN/CAN FD Security Gateway

Feng Luo, Zhenyu Yang, Zitong Wang, and Jiajia Wang Tongji University

Citation: Luo, F., Yang, Z., Wang, Z., and Wang, J., “Routing and Security Mechanisms Design for Automotive TSN/CAN FD Security Gateway,” SAE Technical Paper 2022-01-0113, 2022, doi:10.4271/2022-01-0113.

Received: 20 Jan 2022 Revised: 20 Jan 2022 Accepted: 13 Jan 2022

Abstract

With the explosion of in-vehicle data, Time Sensitive Network (TSN) is increasingly becoming the backbone of the in-vehicle network to ensure deterministic real-time communication and Quality of Service (QoS). However, legacy buses such as CAN FD and LIN will not disappear for a long time in the future. Many protocols are deployed in the gateway and it is an important component in the security and functional safety of the communication process. In this paper, the recommended Electrical/Electronic Architecture is first given and the use cases for the TSN/CAN FD gateway are illustrated. Then, a TSN/CAN FD routing mechanism is designed and security mechanisms are deployed. The routing mechanism includes the protocol conversion module, queue cache module, and forwarding scheduling module. The protocol conversion module unpacks or packs the TSN or CAN FD frames according to the routing table. Dynamic space of queue is utilized in the queue cache module to allocate the cached messages appropriately. Time Awareness Shaper and Credit-Based Shaper are used to guarantee the transmission of messages with different priorities. The security mechanism consists of a secure handshake protocol and encrypted secure communication. We negotiate and distribute session secret keys via pre-stored certificates and the RSA algorithm. The confidentiality, integrity, and availability of data are guaranteed via random numbers, MAC, and the AES algorithm. Detailed tests are finally carried out on a physical system and the results show that the designed mechanism in this paper has excellent performance and feasibility.

Introduction

With the increasing introduction of Information Communication Technology (ICT) in vehicles, the traditional signal-oriented Electrical/Electronic Architecture (EEA) is changing to a new Service-Oriented Architecture (SOA). The TSN-based backbone network is becoming a new trend to guarantee a high quality of service (QoS). Time Sensitive Network (TSN) has been proven good scheduling and real-time performance in the industrial control field. Also, increasingly studies are illustrating its feasibility in the automotive domain [1]. In the future, legacy buses such as CAN/CAN FD will exist for a long time. Automotive controllers with the gateway functionality, which are required to undertake the conversion between TSN and CAN FD protocols, should ensure real-time, reliability and security. Strong attention has already been paid to different aspects of the automotive gateway. A reusable and graphical user interface (GUI)-based configurable automotive gateway framework for CAN, FlexRay, and Ethernet is proposed [2]. A CAN-Ethernet gateway, which mainly focuses on the encapsulation and decapsulation principle of different protocols, is designed [3]. Furthermore, the Field-Programmable Gate Array (FPGA) is utilized to improve routing efficiency in the Flexray-Ethernet gateway [4, 5]. The author proposed a synchronization mechanism for AVB and Flexray and implemented it on an embedded gateway [6].

At the same time, the increasing number of external interfaces and complex ethernet communication protocols increase the probability of attacks on vehicles [7]. Once a malicious attacker has penetrated the in-vehicle network, various attacks, such as spoofing, tampering, repudiation, Denial of Service, can be executed on the network [8]. As a security and communication middleware, the gateway connects the internal network and external network of the vehicle. Hence, security mechanisms need to be deployed. The authors analyze the cyberthreats vectors of connected cars and propose a time-based CAN intrusion detection method and a Feistel cipher block method to protect cybersecurity [9]. Encryption-based methods are applied on a Xilinx Zedboard to realize the secure communication of the gateway [4]. The authors compare the performance of AES, DES, and AES-CCM. An automotive gateway firewall is proposed to detect abnormal traffic [10]. A system information entropy-based intrusion detection system and ethernet state packet filter are included in this firewall. An automotive Embedded Firewall for next-generation domain architecture based on software and hardware is designed on an Infineon AURIX TriCore and Altera Cyclone V FPGA [11]. The authors consider the trade-off between software and hardware and verify the reasons is the delay of software after applying the mechanism. The other is because frame 1 happens to fall into the time slot of frame 2 and frame 3. This is the cost of traffic shaping and fixed transmission delay. Secondly, the proposed scheduling mechanism increases the workload of project development. In the early stage of network design, the segmentation of TSN and CAN FD messages should be planned in advance according to the queue priority mapping table in Table 3. In the stage of adjusting the scheduling parameters, the scheduling parameters should be adjusted based on theoretical analysis and actual conditions. This improves the requirements for developers. The scheduling effect may become uncertain once the network communication matrix changes considerably and the scheduling parameters are not adjusted accordingly.

Summary

A possible new in-vehicle network architecture in the future is first given in this paper, and the application scenarios of the design mechanism of this article are clarified. Then we designed a routing mechanism for the TSN-CAN FD gateway. In addition to the basic protocol conversion module, referring to TSN, we design a queue and scheduling module for CAN FD. The mechanism uses priority queues, Time Awareness Shaper, and Credit-Based Shaper. The security mechanism was then designed, including two phases: session establishment and secure communication. This cryptography-based security mechanism includes AES, RSA, and security protocol. Finally, these above mechanisms are implemented on the physical gateway board of our design, and corresponding tests are carried out using CANoe and CAPL to show that these above mechanisms are feasible and effective.

In the future, we have further work to do in two aspects. In one aspect, the security mechanism in this paper cannot detect DOS attacks. As a cyber physical system, a vehicle needs to build an in-depth defense system architecture. The security mechanism based on cryptography is only one part. The intrusion detection and defense systems based on machine learning need to be studied. In another aspect, Field Programmable Gate Array (FPGA) can be utilized to improve the efficiency of routing and security mechanisms.

References

1. Lo Bello, L. and Steiner, W., “A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems,” *Proceedings of the IEEE.* 107, no. 6 (2019): 1094-1120, doi:10.1109/jproc.2019.2905334.
2. Kim, J.H., Seo, S.-H., Hai, N.T., Cheon, B.M. et al., “Gateway Framework for In-Vehicle Networks Based on CAN, FlexRay, and Ethernet,” *IEEE Transactions on Vehicular Technology* 64, no. 10 (2015): 4472-4486, doi:10.1109/tvt.2014.2371470.
3. Postolache, M., Neamtu, G., and Trofin, S.D., “CAN - Ethernet Gateway for Automotive Applications,” in *2013 17th International Conference on System Theory, Control and Computing (ICSTCC)*, doi:10.1109/icstcc.2013.6688995.
4. Lee, T.-Y., Lin, I.A., and Liao, R.-H., “Design of a FlexRay/Ethernet Gateway and Security Mechanism for In-Vehicle Networks,” *Sensors* 20, no. 3 (2020): 641, doi:10.3390/s20030641.
5. Shreejith, S., Mundhenk, P., Ettner, A., Fahmy, S.A. et al., “VEGa: A High Performance Vehicular Ethernet Gateway on Hybrid FPGA,” *IEEE Transactions on Computers.* 66, no. 10 (2017): 1790-1803, doi:10.1109/tc.2017.2700277.
6. Lee, Y.S., Kim, J.H., and Jeon, J.W., “FlexRay and Ethernet AVB Synchronization for High QoS Automotive Gateway,” *IEEE Transactions on Vehicular Technology* 66, no. 7 (2017): 5737-5751, doi:10.1109/tvt.2016.2636867.
7. Kaur, R., Singh, T.P. and Khajuria, V., “Security Issues in Vehicular Ad-Hoc Network(VANET),” in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, doi:10.1109/icoei.2018.8553852.
8. Sommer, F., Dürrwang, J., and Kriesten, R., “Survey and Classification of Automotive Security Attacks,” *Information* 10, no. 4 (2019): 148, doi:10.3390/info10040148.
9. Dadam, S.R., Zhu, D., Kumar, V., Ravi, V. et al., “Onboard Cybersecurity Diagnostic System for Connected Vehicles,” SAE Technical Paper 2021-01-1249 (2021), doi:10.4271/2021-01-1249.
10. Luo, F. and Hou, S., “Security Mechanisms Design of Automotive Gateway Firewall,” SAE Technical Paper 2019-01-0481 (2019), doi:10.4271/2019-01-0481.
11. Pesé, M.D., Schmidt, K., and Zweck, H., “Hardware/Software Co-Design of an Automotive Embedded Firewall,” SAE Technical Paper 2017-01-1659 (2017), doi:10.4271/2017-01-1659.

Contact Information

Zhenyu Yang, Ph.D Candidate
School of Automotive Studies, Tongji University
(+86) 13701936931
1811023@tongji.edu.cn

Acknowledgments

This work was financially supported by prospective study Funding of Nanchang Automotive Institute of Intelligence and New Energy, Tongji University (NO. TPD-TC202110-14).

Definitions/Abbreviations

TSN - Time Sensitive Network

QoS - Quality of Service

CAN FD - Controller Area Network With Flexible Data Rate

AES - Advanced Encryption Standard

MAC - Message Authentication Code

EEA - Electrical/Electronic Architecture

ICT - Information Communication Technology

SOA - Service-Oriented Architecture

DCU - Domain Controller Unit

ADAS - Advanced Driving Assistance System

HSM - Hardware Secure Module
OTA - On The Air
CBS - Credit Based Shaper
TAS - Time Awareness Shaper
TLS - Transport Layer Security
GCL - Gate Control List
CBC - Cipher Block Chaining
MITM - Man-In-The-Middle
DoS - Denial of Service
FPGA - Field Programmable Gate Array
CMAC - Cypher-Based Message Authentication Code
AVB - Audio/Video Bridging.

© 2022 SAE International. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE International.

Positions and opinions advanced in this work are those of the author(s) and not necessarily those of SAE International. Responsibility for the content of the work lies solely with the author(s).

ISSN 0148-7191