Hindawi
Security and Communication Networks
Volume 2021, Article ID 6902138, 17 pages
https://doi.org/10.1155/2021/6902138

Research Article

Security Analysis of the TSN Backbone Architecture and Anomaly Detection System Design Based on IEEE 802.1Qci

Feng Luo, Bowen Wang, Zihao Fang, Zhenyu Yang, and Yifan Jiang

School of Automotive Studies, Tongji University, Shanghai 201804, China

Correspondence should be addressed to Bowen Wang; bowen@tongji.edu.cn

Received 18 July 2021; Revised 30 August 2021; Accepted 10 September 2021; Published 25 September 2021

Academic Editor: Konstantinos Demertzis

With the development of intelligent and connected vehicles, onboard Ethernet will play an important role in the next generation of vehicle network architectures. It is well established that accurate timing and guaranteed data delivery are critical in the automotive environment. The time-sensitive network (TSN) protocol can precisely guarantee the time certainty of the key signals of automotive Ethernet. With the time-sensitive network based on automotive Ethernet being standardized by the TSN working group, the TSN has already entered the vision of the automotive network. However, the security mechanism of the TSN protocol is rarely discussed. First, the security of the TSN automotive Ethernet as a backbone E/E (electrical/electronic) architecture is analyzed in this paper through the Microsoft STRIDE threat model, and possible countermeasures for the security of automotive TSNs are listed, including the security protocol defined in the TSN, so that the TSN security protocol and the traditional protection technology can form a complete automotive Ethernet protection system. Then, the security mechanism per-stream filtering and policing (PSFP) defined in IEEE 802.1Qci is analyzed in detail, and an anomaly detection system based on PSFP is proposed in this paper. Finally, OMNeT++ is used to simulate a real TSN topology to evaluate the performance of the proposed anomaly detection system (ADS). As a result, the protection strategy based on 802.1Qci not only ensures the real-time performance of the TSN but can also isolate individuals with abnormal behavior and block DoS (denial of service) attacks, thus attaining the security protection of the TSN vehicle-based network.

1. Introduction

Autonomous vehicles are driving rapid advances in technologies, including next-generation vehicle communications, V2X (vehicle to everything), and advanced driver-assistance systems. The environment around the vehicle can provide key information to the intelligent driving vehicle, and these technologies need the support of advanced sensors with high bandwidth, such as cameras and radar. In addition, long-term evolution (LTE) and 5G communication technologies also provide external communication means for intelligent driving. In the context of large bandwidth requirements, the network architecture of modern vehicles should be a new link combined with traditional buses, for example, controller area network (CAN), local interconnect network (LIN), and new buses, for example, CAN FD (CAN with a flexible data rate) and Ethernet technologies [1]. In these networks, the same Ethernet infrastructure is shared by various domains and distinct requirements on timing. In the future, the E/E architecture of intelligent vehicles has been developed with the centralization of communication [2]. In the meantime, the automotive Ethernet applying the time-sensitive network (TSN) technology will exist as the backbone network of the in-vehicle network.

After the TSN standard is introduced, the automotive Ethernet can meet the functions necessary for the quality of service (QoS) of the communication system in the vehicle, including time synchronization, high real-time performance, and high reliability. The TSN began as an extension of audio-video bridging (AVB) and has since expanded to include many new consumer segments. Its main goals are to provide zero loss from congestion and

bounded latency for a variety of time-sensitive data streams coexisting on a network that also support best-effort traffic [3]. While TSN brings benefits to the automotive Ethernet, vehicles are also facing new challenges.

Vehicles used to be disconnected from the outside world, so there is only a tiny chance of hackers attacking and operating a vehicle. However now, vehicles are exposed to an open network environment due to the V2X technology, which increases the attack surface of vehicles. For example, most modern cars have an onboard diagnostic (OBD-II) interface under the dashboard that hackers can use to gain direct access to in-vehicle networks. Hackers may also target vehicular ad hoc networks (VANETs) to disrupt vehicle operations. Furthermore, in-vehicle Ethernet can use more complicated communication protocols in addition to TSN, the flaws of which will raise vehicle security risks. There are some studies on the security of diagnostic communication over Internet protocol (DoIP), scalable service-oriented middleware over IP (SOME/IP), and AVB [4–6], but there are only a few studies on TSN security.

TSN is a combination of series standards. One of the TSN standards is IEEE 802.1Qci, which defines per-stream filtering and policing before queue frames to protect time-sensitive flow. This is a significant security enhancement to TSN because it protects against unnecessary bandwidth consumption, burst sizes, and malicious or improperly configured endpoints. IEEE 802.1Qci may also be used to restrict faults to particular regions of the network, reducing their effects on other areas of the network. Although IEEE 802.1Qci is a published standard, there has been little progress in connecting the standard to current Ethernet security systems and architectures. Furthermore, nothing has been done to investigate how IEEE 802.1Qci policies could be implemented on network devices and integrated with established automotive security policies.

The motivations of this work are as follows.

First, to study the security of TSN and the application scope of IEEE 802.1Qci, the E/E architecture of TSN as the vehicle backbone network is studied. At the same time, threats under the network architecture should be analyzed to determine the vulnerable points of the TSN as the backbone network. To study the performance of IEEE 802.1Qci defense policies, a model or simulation platform should be established to evaluate the network functions of TSN and IEEE 802.1Qci defense policies and what countermeasures can be achieved based on PSFP should be discussed in detail. The performance of countermeasures should be analyzed using the simulation. In addition, how IEEE 802.1Qci influences the TAS (time-aware shaper) defined in IEEE 802.1Qbv and guard band in automotive Ethernet should be discussed.

Based on the above considerations, an integrated defense and protection policy for TSN automotive Ethernet is proposed in this paper. The contributions of this paper can be summarized as follows:

(i) The vulnerability and threats of automotive Ethernet with TSN as the backbone network are analyzed through the STRIDE threat model developed by Microsoft

(ii) The blocking and detection mechanisms of PSFP are discussed and analyzed in detail

(iii) A novel anomaly detection system is proposed, and stream filters, stream gates, and flow meters in PSFP are innovatively used to effectively solve the problem caused by DoS attacks and abnormal traffic behavior

(iv) The open-source simulation tool OMNeT++ was used to develop a precursory ADS model, including the MSDU (maximum service data unit) size filter, gate control filter, and token bucket meter

(v) The performance of ADS is evaluated, and the experimental results show that the ADS not only does not affect the normal traffic performance but can also detect the abnormal behavior of traffic and DoS attacks

The rest of this paper is organized as follows: Section 2 introduces the background and related work of this paper. Section 3 analyzes the threat of automotive E/E architecture with TSN as the backbone based on the STRIDE threat method. Section 4 discusses the defense and detection policies of PSFP and proposes the anomaly detection system based on IEEE 802.1Qci. Section 5 simulates and analyses the performance of ADS based on a TSN advanced driver-assistance systems (ADASs) sensor fusion zone using the OMNeT++ simulation tool. Section 6 summarizes this paper.

2. Background and Related Work

2.1. TSN Standard Overview. Standard TSN is an extension of the standard AVB. The emergence of TSN is to ensure the required QoS requirements for critical data transmission, especially to achieve deterministic, low-latency, and fault-tolerant data transport. Table 1 shows the TSN standard overview. Table 1 lists some projects that the TSN task group has completed and is completing regarding automobiles.

2.2. Threat and Attack Vector of the In-Vehicle Ethernet Network. The increasing number of application scenarios in vehicles requires the involvement of Ethernet, such as diagnostics, deterministic transmission with a high rate, and service-oriented architectures. With this comes a diverse range of vulnerability points. Once the attackers have penetrated the system through the vulnerability, they can launch an attack on the in-vehicle Ethernet network with the following three attack vectors:

2.2.1. Active Manipulation or Eavesdropping of the Message. This type of attack is an attacker who wants to manipulate the vehicle's feature set or even exploit the original equipment manufacturer's (OEM) back-end servers through the vehicle's parts. In addition, eavesdropping on the information in the car is related to analysis. By collecting the messages in the car for a long time, the attacker can obtain

Table 1: TSN standard overview.

Standard	Status	Purpose	Application scenario
IEEE 802.1AS-2020 [7]	Proposed	Timing and synchronization	As the time-base for every node connected in the TSN, fault-tolerant time synchronization with the backup grandmaster.
IEEE 802.1Qbv-2015 [8]	Proposed	Time-aware traffic shaping	Periodic critical sensors; closed-loop control (e.g., steering and braking)
IEEE 802.1Qbu-2016 [9]	Proposed	Frame pre-emption	Strongly critical data (e.g., steering and braking actuation), usually be used in cooperating with IEEE 802.1Qbv
IEEE 802.1Qci-2017 [10]	Proposed	Filtering and policing	Network protection, intrusion detection for malicious attacks, or DoS attacks
IEEE 802.1Qch-2017 [11]	Proposed	Cyclic traffic shaping	Periodic sensors
IEEE 802.1Qcr-2020 [12]	Proposed	Asynchronous traffic shaping	Aperiodic traffic
IEEE 802.1CB-2017 [13]	Proposed	Redundant communication	Fail-operational applications tolerating nodes or wire faults
P802.1DG [14]	Draft	TSN profile for automotive in-vehicle Ethernet communications	Profiles for secure, highly reliable, deterministic latency, automotive in-vehicle bridged IEEE 802.3 Ethernet networks based on IEEE 802.1 TSN standards and IEEE 802.1 security standards

the details of the encryption method and key used by the network in the car.

2.2.2. Masquerading Attacks. Attackers are generally unauthorized devices. The attackers use a false identity to communicate with the original network, and if the authorization process of the communication system is not adequately protected, it is easy to attack.

2.2.3. DoS Attacks. A denial of service attack is similar to a flood attack in which it is intended to bring down the target network. DoS attacks use a large amount of available bandwidth to prevent the original message from working correctly.

2.3. Related Work. In terms of international standards, to promote the construction of automotive network security, SAE international published Cybersecurity Guidebook for Cyber-Physical Vehicle System (J3061) in June 2016 [15]. J3061 provides a framework and guidance for cybersecurity processes for automotive. In February 2020, draft Road Vehicles–Cybersecurity Engineering (ISO/SAE 21434) was published by the SAE international and ISO [16]. In addition, the United Nations Economic Commission for Europe (UNECE) WP.29 Working Party on Automated and Connected Vehicles (GRVA) adopted a draft UN Regulation on Cyber Security and Cyber Security Management System in March 2020, which will be the first regulation governing information security in vehicles [17].

In terms of academic research, Sommer et al. [18] have a detailed classification of automotive attacks, including 23 different categories, according to the description of the attack, a violation of the security attribute or the exploit of a vulnerability, and so on. Carnevale et al. [19] provided a hardware accelerator architecture for key derivation and encryption required by IEEE 802.1X-2010 in automotive applications, and for further research, IEEE 802.1AE was also implemented by Carnevale [20, 21]. The three researchers are all hardware support for automotive Ethernet security. Choi et al. [22] proposed a new MACsec (media access control security) extension over the SDN (software defined network) for in-vehicle secure communication based on IEEE 802.1X authentication mechanism. Nasrallah et al. [23] surveyed the existing research studies toward achieving ultralow latency (ULL) in the context of the TSN standards and mentioned that IEEE 802.1Qcp is used to support IEEE 802.1AX and IEEE 802.1X. Bello et al. [24] gave an overview of TSN in industrial communication and automation systems and clarified how to configure IEEE 802.1Qci to achieve a concrete effect is largely missing. Ergenç et al. [25] discussed more than 30 potential security issues and threats of IEEE 802.1TSN protocols.

There are also some studies on abnormal detection systems; Grimm et al. [26] provided an extension of a hybrid anomaly detection system using specifications and machine learning methods. Herold et al. [5] studied anomaly detection for SOME/IP using a method called complex event processing. Table 2 lists the contributions and disadvantages of some researches.

There are some researches on TSN as well. Farzaneh et al. [27] developed a modeling approach based on logic programming (LP) to support a more efficient configuration and verification process focusing on in-vehicle TSNs. A prototypical experimental setup was also designed and developed by Farzaneh deploying a time-aware shaper defined in IEEE 802.1Qbv [28]. Brunner et al. [29] presented a future evolution for automotive E/E architectures, which is centralized with the communication of TSN. Mahfouzi et al. [30] proposed a security-aware methodology for routing and scheduling for control applications in Ethernet networks to maximize the resilience of control applications.

It can be seen that the information security of the vehicle is imperative, but the security of the TSN protocol with

Table 2: Research for the security aspect of automotive Ethernet.

Researcher	Contributions	Disadvantages
Sommer et al. [18]	Detailed classification of automotive attacks	Lack of the detailed analysis for vulnerability and threats of the automotive TSN
Carnevale et al. [19]	Hardware solution for IEEE 802.1X-2010 and EEE 802.1AE in automotive applications	Hardware needs to be specially designed, and the universality is low
Choi et al. [22]	MACsec extension over the SDN	The proposed mechanism needs to operate in the context of SDN, and the universality is low
Grimm et al. [26]	Hybrid anomaly detection system using specifications and machine learning methods	Lack of features relevant to the TSN
Herold et al. [5]	Anomaly detection for SOME/IP using complex event processing	Only focus on the upper layer some/IP protocol and no consideration given to TSN
Ergenç et al. [25]	Discussed more than 30 potential security issues and threats of IEEE 802.1TSN protocols	Lack of countermeasures and attack mitigation techniques

many advantages is rarely discussed. TSN is primarily based on the data link layer. However, only the encryption and authentication introduced by MACsec and IEEE 802.1X cannot completely override TSN security.

3. Security Analysis of the TSN Backbone Network

3.1. TSN Backbone E/E Architecture. Over the last few years, features such as automated driving, networking, and cybersecurity have become increasingly important. The importance of these functionalities will increase as these advanced technologies develop and consumer adoption increases. In-vehicle communication networks, power networks, connectivity, safety, and security require a paradigm shift in E/E architectures to implement these functionalities in mainstream vehicles [31].

Today, the E/E architecture of intelligent connected vehicles is facing these four challenges: security, real-time performance, bandwidth bottlenecks, and computing power black hole. However, there is no common E/E architecture among the car manufacturers, and each car manufacturer uses its own architecture. According to the Ethernet as the core network in the centralized vehicle E/E architecture proposed by Volvo [32], this paper adds the concept of TSN into the E/E architecture. The main goal of TSN functions in E/E architecture is intended to ensure the compliance of various application domain requirements within the network in real time and to reduce the interference of real-time traffic from nonreal-time traffic in the network. Figure 1 shows the E/E architecture, and Table 3 lists the function of each unit.

tIn this architecture, the core network consists of four VIUs and one VCU. VCU can be the computational unit. One or more high-performance controllers (HPCs) in the VCU will provide vehicle-level behavior, such as behavior decision or motion planning for driverless. Furthermore, VCU also receives a large amount of data from sensors such as cameras or radars. This leads to the demand for high bandwidth and high transmission speed between the VCU and other nodes, and Ethernet as a backbone network becomes necessary. VIU can be a zone gateway in which frames from the edge nodes are forwarded or routed. Connected to a VIU is an edge node, which can be a sensor, an actuator, or a controller. The communication between VIU and edge nodes can be CAN or LIN. TSN is added because the traffic of different priority levels share the same link resource, and TSN can ensure that they are not affected by each other.

3.2. STRIDE Threat Model. Microsoft's STRIDE threat model is used to identify system security threats [33]. The STRIDE model establishes a mapping relationship with security threats and security properties. As shown in Figure 2, the data flow of TSN Ethernet as core network E/E architecture is analyzed through threat modeling tool (TMT), and only Ethernet was considered.

The architecture of Figure 2 is basically the same as that of Figure 1. The difference is that some real sensors, actuators, and controllers are placed in Figure 2, and the firmware update server outside the car is connected to the inside of the car through the OBD port. In addition, the communication between any nodes is Ethernet. The report is generated through TMT, and the attack methods are mainly counted and analyzed.

As shown in Figure 3, the threats are always divided into six types according to different threats of attacks and targets: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

In the absence of any security technology, the most common type of attack is the denial of service because there will be the denial of service threat on every data link. The second most is information disclosure. Information disclosure happens when the information can be read by an unauthorized party. Elevation of privileges is all related to ECUs, either gain complete control of actuators, or exploit the standard ECU, or manipulate sensor fusion data. Tampering and spoofing are related to sensors' data and cameras' data. Repudiation is from the external interactor. Through the analysis of the STRIDE model, the general threats can be obtained. However, in the TSN system, there should be other factors, such as bandwidth and configuration. Bandwidth should be of consideration because secure encryption can change the bandwidth requirements. The configuration of TSN streams should also be security relevant.

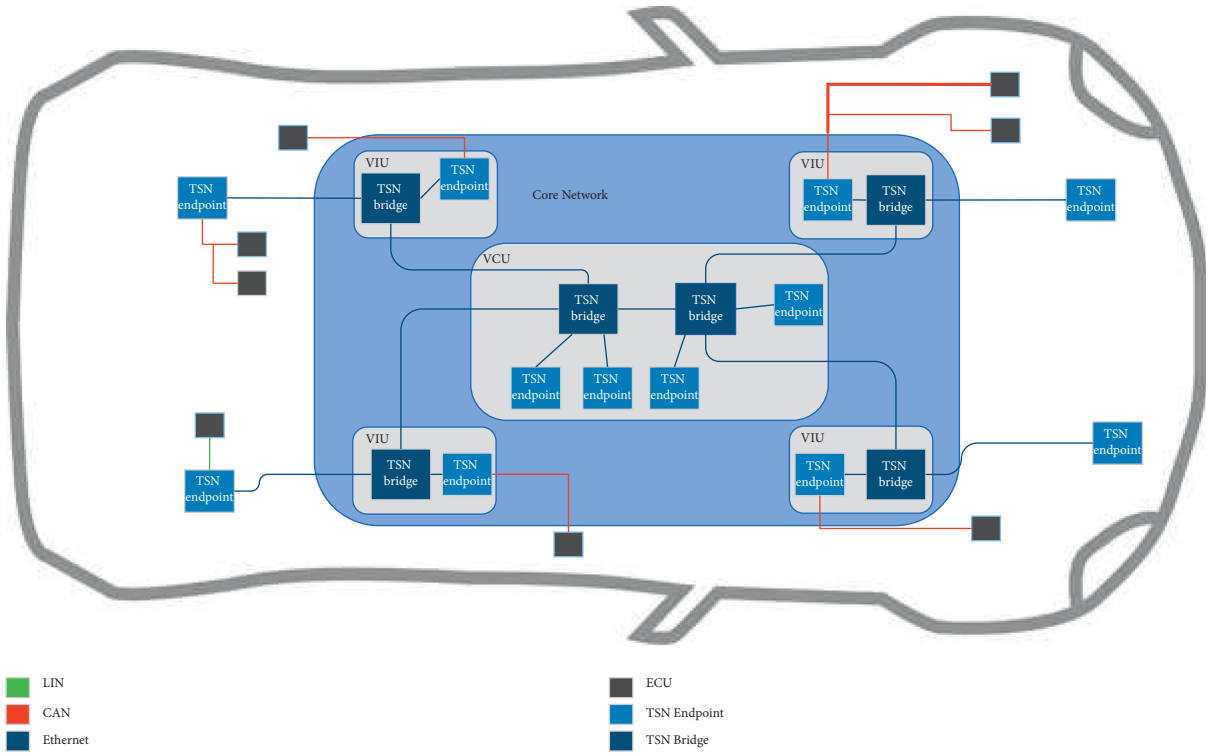

Figure 1: TSN Ethernet as the core network in the centralized vehicle E/E architecture.

Table 3: Functions of VIU, ECU, VCU, TSN endpoint, and TSN bridge.

Unit	Function
Vehicle interface unit (VIU)	VIU as a zone gateway to provide a translation from the specific network interfaces of the nodes to the core network
ECU	ECU is highly specialized for controlling its specific device
Vehicle computation unit (VCU)	The VCU coordinates fundamental capabilities to provide vehicle-level behavior
TSN endpoint	The TSN endpoint usually as ECU or processor in the core network can also translate traffic from CAN/LIN bus to Ethernet
TSN bridge	The TSN bridge is in the VIU or VCU connected with a controller

3.3. Supported Countermeasures. Here is the list of security countermeasures that can be used in the TSN, mainly including firewall, IDPS system, cryptographic, and access control.

3.3.1. Firewall. Firewalls are part of access control. Over the past few decades, different types of firewall systems have been built for traditional Ethernet, as shown in Table 4. Firewalls can be applied according to different categories and different technologies. Firewalls are set up to avoid DoS Attacks and limit the number and throughput of simultaneous connections to the network. The firewall of traditional Ethernet is based on the OSI layer 3 and layer 4. However, the second layer needs to be protected in the car Ethernet, so per-stream filtering and policing are considered, depending on how the different detection parameters are used, such as Port No., IP, VLAN ID, Frame Length, and so on.

3.3.2. Intrusion or Anomaly Detection System. An intrusion detection system (IDS) is a passive detection system that detects an attack or abnormal issues as a warning. The IDS generally provides high accuracy but has the disadvantage that it can only detect known attacks. For unknown attacks, a new signature needs to be developed. An abnormal detection system detects specific behavior. For layers 5, 6, and 7, we use deep packet inspection (DPI) to detect abnormal network behavior. This technology adds application protocol identification, packet content inspection, and deep decoding of application layer data to the traditional IP packet inspection techniques.

3.3.3. Cryptography. IEEE 802.1AE MAC security (MACsec) provides specifications for authenticating the content of message payloads in fixed networks and specifies how to encrypt the content of message payloads to provide confidentiality in addition to message authentication [34]. In

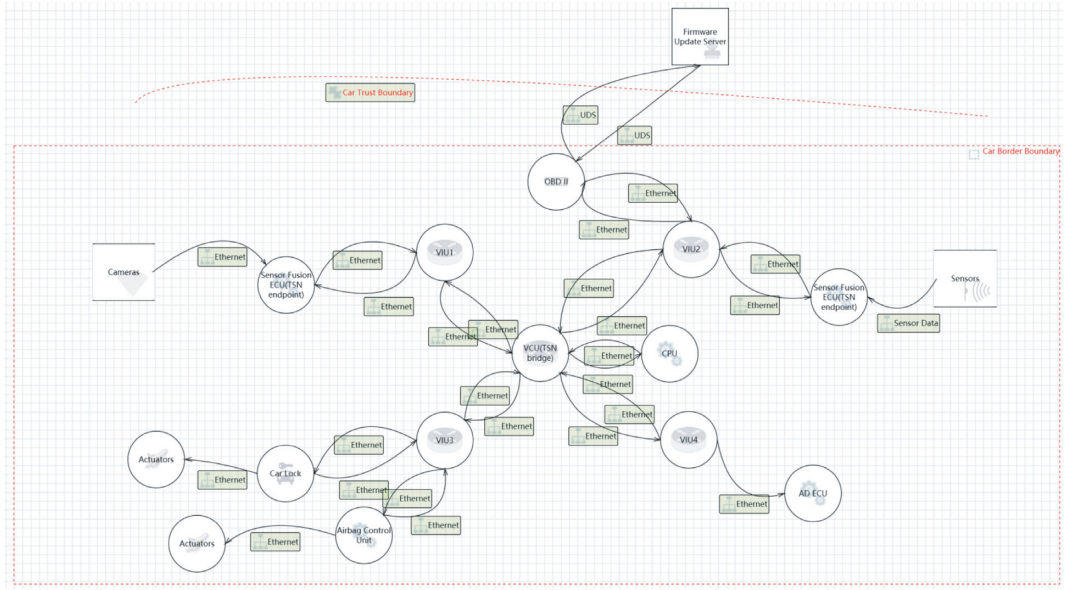

Figure 2: Data flow of TSN Ethernet as the core network topology.

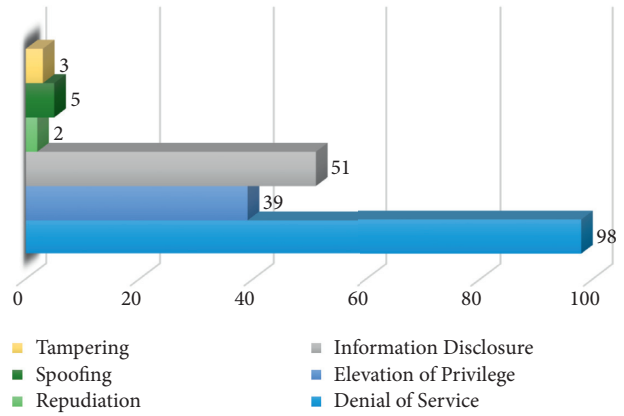

Figure 3: Threat list through the TMT analysis view without security technologies.

addition to the traditional Ethernet security protocols that can be utilized in the upper layer, such as secure sockets layer (SSL), transport layer security (TLS), and datagram transport layer security (DTLS), the AUTOSAR (automotive open system architecture) organization has specifically standardized the definition of security onboard communication (SecOC) for automotive Ethernet.

3.3.4. Access Control. IEEE 802.1X specifies port-based network access control [35] and provides a means of authenticating and authorizing devices attached to local area network (LAN) and includes the MACsec key agreement protocol (MKA) necessary to use IEEE Std 802.1AE. IEEE 802.1X provides effective protection against masquerading attacks.

There are several other technologies. Figure 4 classifies them according to the OSI model and divides security technologies into isolation and filtration, detection and defense, and authentication and encryption. Through countermeasures on each layer, the automotive Ethernet is perfectly protected.

4. ADS Design Based on IEEE 802.1Qci

4.1. Problem Formulation. As shown in Figure 5, an example of PSFP applied to DoS attacks or sensor failure defense is presented. Figure 5(a) shows the traffic transmission plan of sensor A and sensor B in the scheduling plan. The two traffic streams belong to the same traffic type, and the scheduling table allocates 45 Mbps bandwidth for this traffic type. However, when the node of sensor A encounters DoS attacks or node failure, its transmission flow becomes abnormal, which surges from the panned 15 Mbps to 60 Mbps. If there is no protection mechanism, as shown in Figure 5(b), the data of sensor B will be affected by the fault data of sensor A, resulting in the data of sensor B cannot be transmitted normally, which is unacceptable for functions such as automatic driving. If PSFP is applied to the switch connected to sensor A and sensor B, as shown in Figure 5(c). The sudden increase of the traffic

Table 4: Firewall types with the OSI layer, protocols, and techniques.

Firewall type	OSI layer	Protocols	Filter techniques
Link level	2	TSN	PSFP
Packet filter	3, 4	TCP/IP, UDP/IP	Stateful, White/Black lists
Proxy	4	TCP/UDP	Content-based
Application level	7	HTTP, FTP, SMTP	DPI, IDS

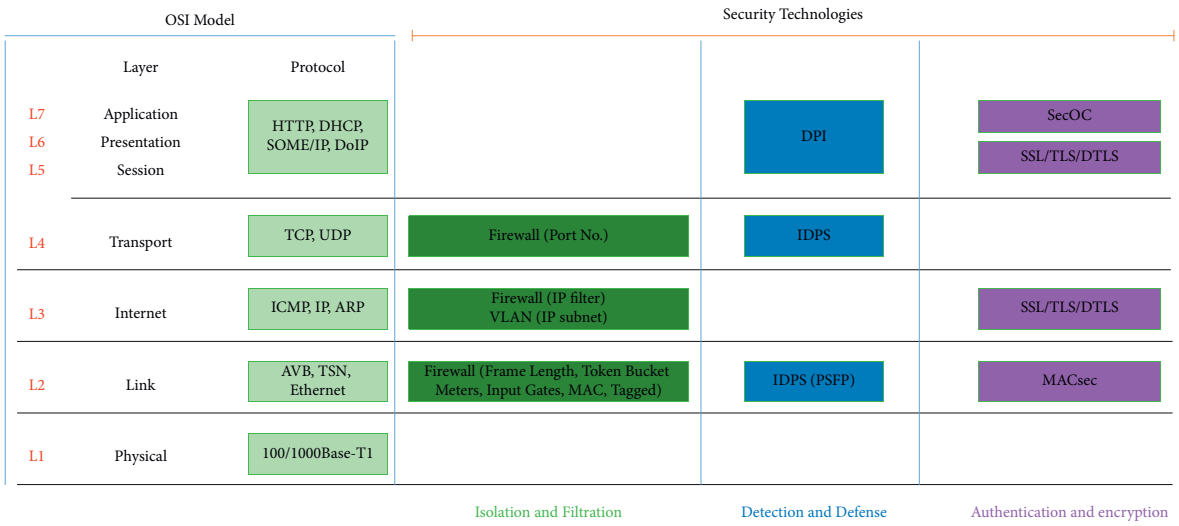

Figure 4: OSI models and security technologies.

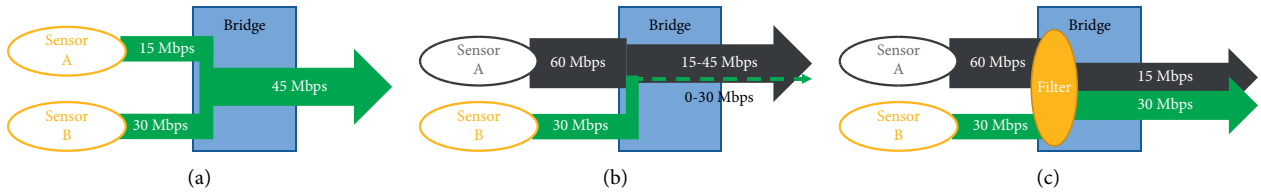

Figure 5: Sensor failure or DoS attack scenario.

generated by sensor A may squeeze the bandwidth of the other data stream. PSFP will reshape the data stream and force it back to the state before the data outbreak. Thus, the data of sensor B, which is working correctly, will not be affected by the other stream, and the rest of the system will not be affected either.

4.2. Per-Stream Filtering and Policing. The PSFP is defined in IEEE 802.1Qci. As shown in Figure 6, PSFP consists of three parts: stream filter, stream gate, and flow meter. Stream filters define the filtering and policing actions on a specific stream, including gate ID and meter ID, and the filters are related to the priority and stream handle defined in IEEE 802.1CB. As the entrance of PSFP, stream filters determine which stream gate and which flow meter a specific stream will enter. Stream gate defines the gate state and internal priority value (IPV), the gate state can be "OPEN" or "CLOSED". The gate states are all controlled by a gate control list, and the IPV replaces stream priority in a sense, which determines the frame's traffic class. The flow meter defines the color mode and committed information rate and excess information rate which reflect the bandwidth of a specific stream. The color of the stream can be "GREEN," "YELLOW," or "RED."

4.3. System Model. As mentioned above, each of the three sections, namely stream filters, stream gates, and flow meter in IEEE 802.1Qci, has parameters that can be set for filtering and policing. Therefore, these parameters defined in IEEE 802.1Qci are introduced into the design of ADS. As shown in Figure 7, the parameters are defined in ADS that can be filtered and monitored for each part. In addition to defining which specific gate ID and meter ID the traffic enters, the stream filter can set a value of the maximum SDU size, and messages exceeding this value can be blocked. In stream gates, the state of the gate is set according to the gate control list, and messages can be blocked if the gate state is CLOSED. In addition, depending on the value of OctetsExceeded, OctetsExceeded specifies the maximum number of MSDU octets permitted to pass the gate during the specified gate timer interval. Flow meters decide the bandwidth of the

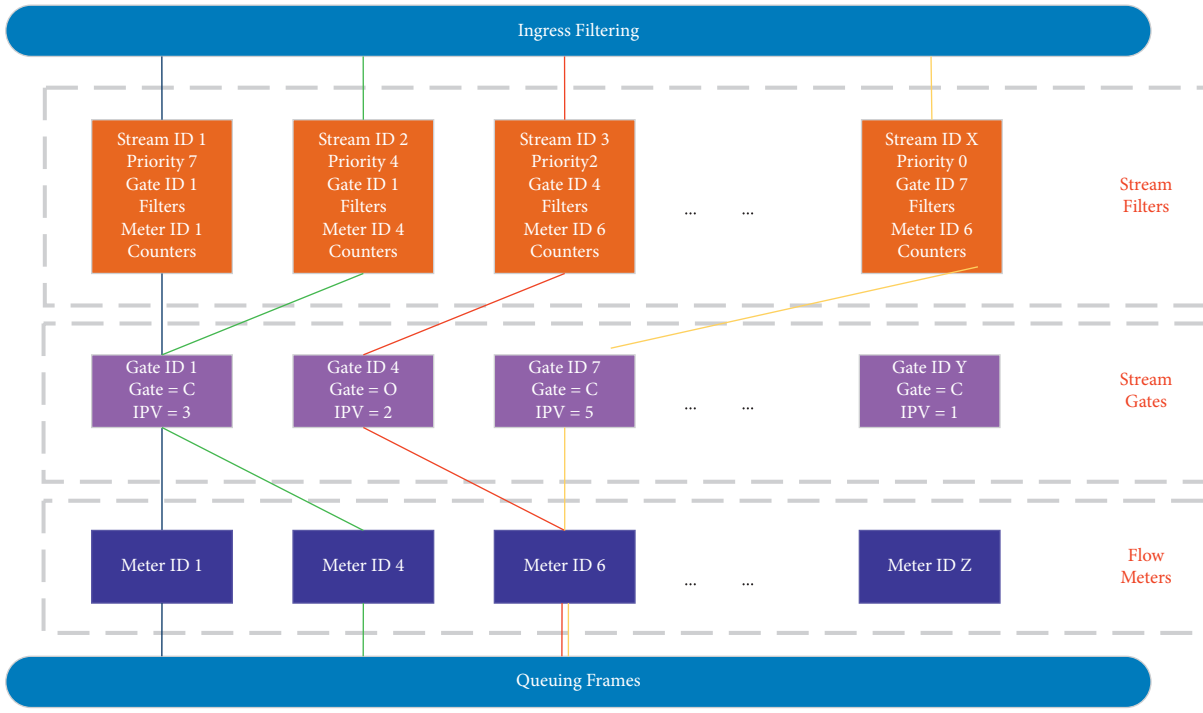

Figure 6: Per-stream filtering and policing.

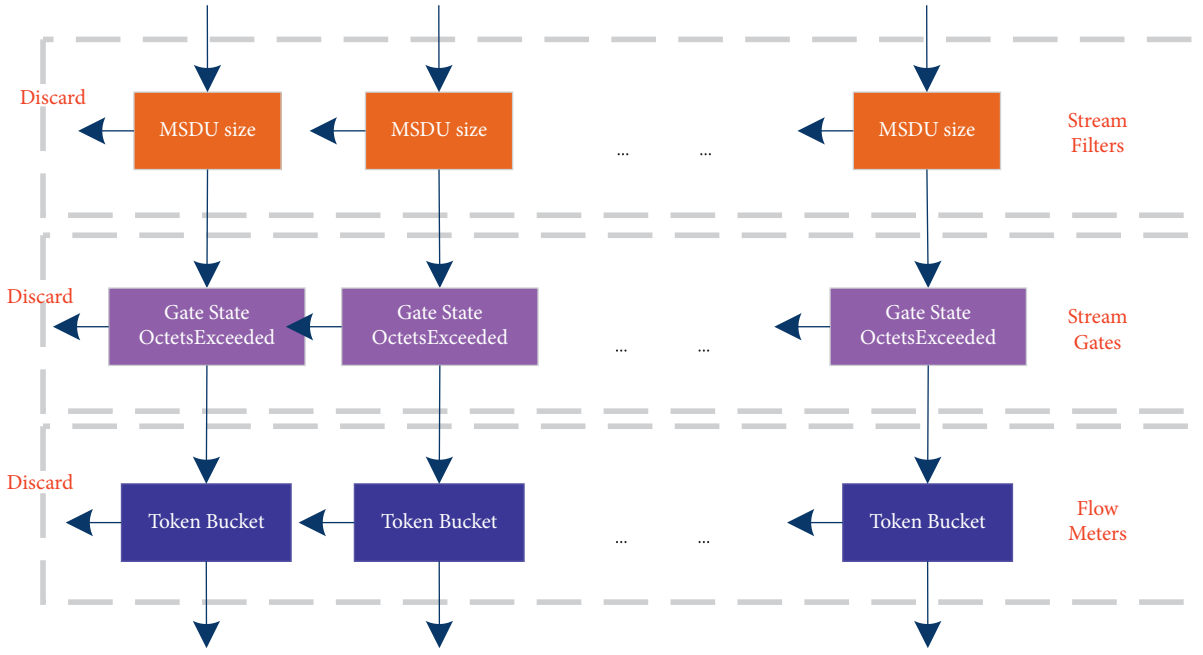

Figure 7: Detection parameters.

stream in a way that is called token bucket meter. The "Yellow" stream and "RED" stream can be blocked.

During ADS operation, the Stream Filters detect and discard the packets whose SDU size exceeds a maximum threshold value, whereas the Stream Gates detect and discard the traffic received in a wrong time window. Flow meters detect and discard the abnormal traffic exceeding a fixed bandwidth determined by the token bucket.

As shown in Figure 8, two levels can be set when detection through the meter. When the color mode (CM) is turned on as Colour Aware, the warning level is when the YELLOW stream was detected, while the dropping level is when the RED stream was once detected.

In equation (1), $B_C^i(t_j)$ represents the number of tokens in the committed buckets for meter i at time t_j. CIR (committed information rate) is expressed as bits per

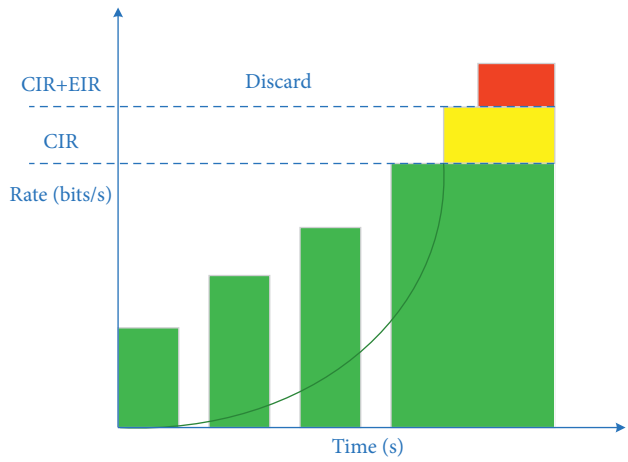

Figure 8: Detection level.

second. The CIR limits the average rate of policing frames which will be declared GREEN. The committed burst size (CBS) is expressed as bytes. The CBS indicates the maximum number of bytes to be sent in the meter queue, which will be declared GREEN. In equation (2), $O_C^i(t_{j-1}, t_j)$ represents the number of tokens that overflow the committed buckets at meter i between time t_{j-1} and t_j. The coupling flag (CF) has only two possible values, 0 or 1. When the CF is 1, the overflow tokens not used for the GREEN stream can be used as YELLOW tokens. In equation (3), $B_E^i(t_j)$ represents the number of tokens in the excess token buckets for meter i at time t_j. The excess information rate (EIR) is expressed as bits per second. The EIR limits the average rate of policing frames which will be declared YELLOW. The excess burst size (EBS) is expressed as bytes. The EBS indicates the maximum number of bytes to be sent at the meter queue, which will be declared YELLOW.

$$B_C^i(t_j) = \min\left\{B_c^i(t_{j-1}) + \frac{\mathrm{CIR}^i}{8} \times (t_j - t_{j-1}), \mathrm{CBS}^i\right\}, \tag{1}$$

$$O_C^i(t_{j-1}, t_j) = \max\left\{B_c^i(t_{j-1}) + \frac{\mathrm{CIR}^i}{8} \times (t_j - t_{j-1}) - \mathrm{CBS}^i, 0\right\}, \tag{2}$$

$$B_E^i(t_j) = \min\left\{B_E^i(t_{j-1}) + \frac{\mathrm{EIR}^i}{8} \times (t_j - t_{j-1}) + \mathrm{CF}^i \times O_C^i(t_{j-1}, t_j), \mathrm{EBS}^i\right\}. \tag{3}$$

Figure 9 shows the flowchart of the token bucket meter when there is a frame of length l_j arrives at time t_j, for meter i. If there are enough GREEN tokens, then the GREEN tokens minus the packet length of GREEN tokens and mark the frame GREEN. Otherwise, if there are enough YELLOW tokens, YELLOW tokens minus the packet length of YELLOW tokens and mark the message YELLOW. If neither is satisfied, mark the message as RED.

At the beginning of the design of the in-vehicle network, the security-related traffic should be determined, including the traffic type, the characteristics of the traffic, scheduling rules, and the worst-case analysis and time details. Thus, the configuration of the parameters in PSFP is deterministic at the beginning, including the stream filters, stream gates, and flow meter. Strictly speaking, the traffic passing through PSFP will not be discarded if the network traffic is not abnormal. In other words, if the traffic is discarded by the accurately configured PSFP, there must be abnormal traffic in the network. The PSFP can be regarded as an anomaly detector, and the use of strict configuration can force the expected behavior of the network. As shown in Figure 10, the three operating modes of the switch are shown. When the PSFP is not turned on, the DoS attack traffic will directly enter the queue frames of the switch. Under the working mode of the firewall, PSFP will directly discard the messages that do not meet the configuration, and under the working mode of ADS, the controller should sound a warning.

In the design of PSFP, the switch will count the frames through the filters, gates, and meter. In addition to recording the messages of normal behavior, it also counts the discarded messages with an exception, thus generating exception prompts. If the PSFP is configured correctly, these exception hints will not result in false positives, as shown in Figure 11.

Finally, the whole structure of the ADS and the detection process is shown in Figure 12.

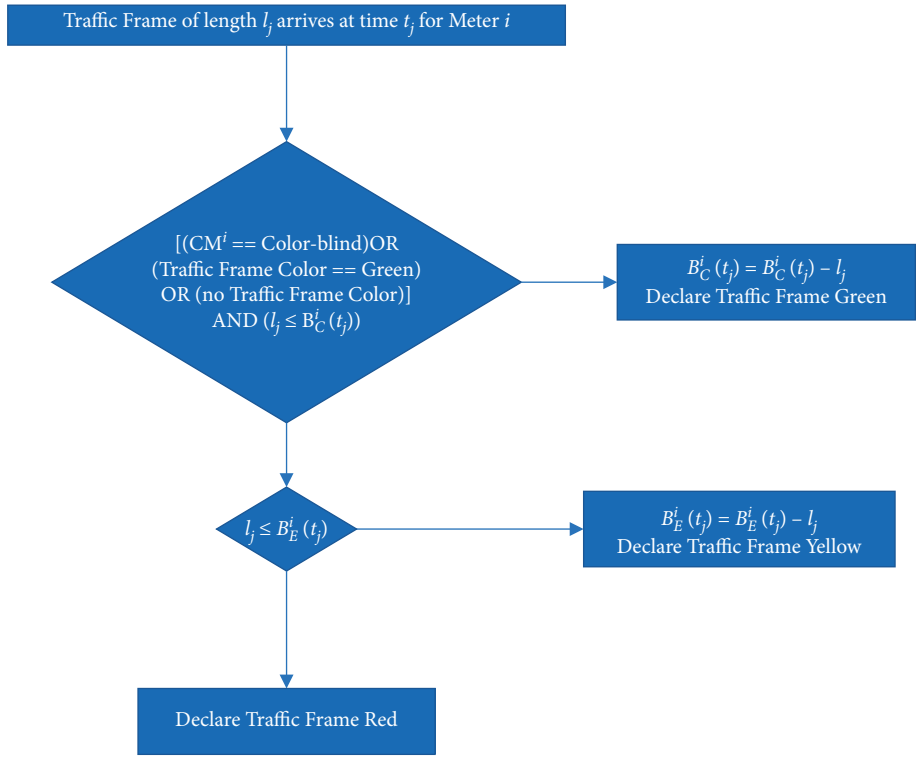

Figure 9: Token bucket meter.

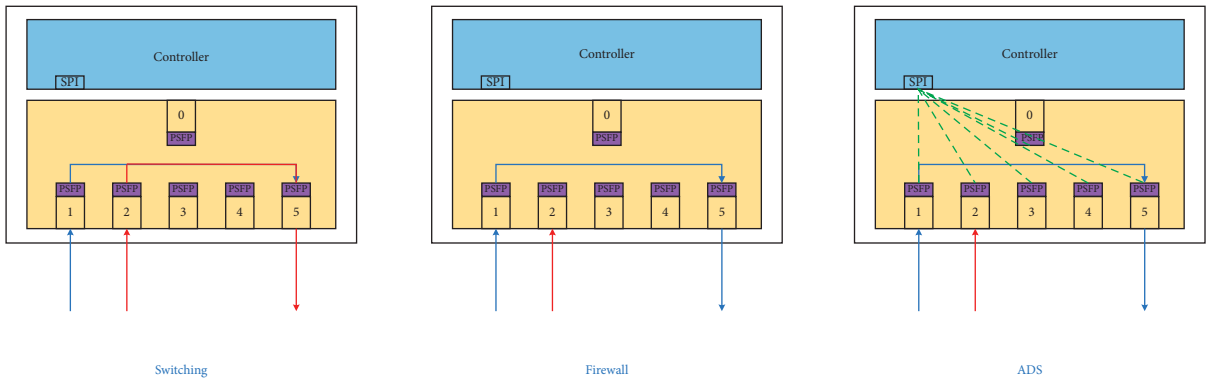

Figure 10: Three modes of Qci configuration.

5. Simulation and Results

The simulation environment used in the experiment is OMNeT++, which is an open-source simulation tool. The experiment uses a case study to evaluate the performance of ADS based on IEEE 802.1Qci. The case study is a TSN ADAS sensor fusion zone network in which PSFP is supported on every port of every switch, and TAS defined in IEEE 802.1Qbv is also applied. Switch nodes are corresponding to TSN bridges, and controller nodes are corresponding to TSN endpoints of the TSN backbone E/E architecture.

5.1. Topology. The network adopts the star network architecture, as shown in Figure 13. The network consists of two switch nodes and five ECU nodes. The CentralHost with switch2 makes up the module VCU, while ZonalHost with switch1 make up the module VIU. The sensor nodes consist of AV1, AV2 and Radar. The speed of each link is 100 Mbps automotive Ethernet, and the message format is based on Ethernet II with IEEE 802.1Q VLAN (virtual local area network) tag.

The simulation time of the scenario is 150 ms, and the switch buffer capacity is set to a maximum of 30 packets. The relevant parameters of various traffic flow in the network are shown in Table 5.

The TAS scheduling table of two switches has the same design. The scheduling rules are as follows:

(1) The scheduling cycle is set to 500 us

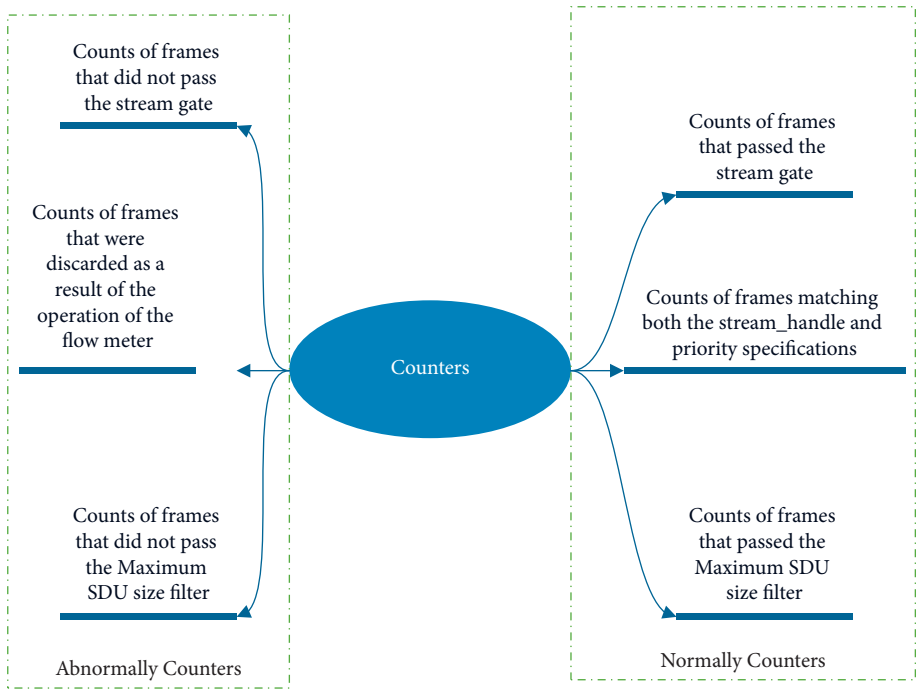

Figure 11: Normal and abnormal counters.

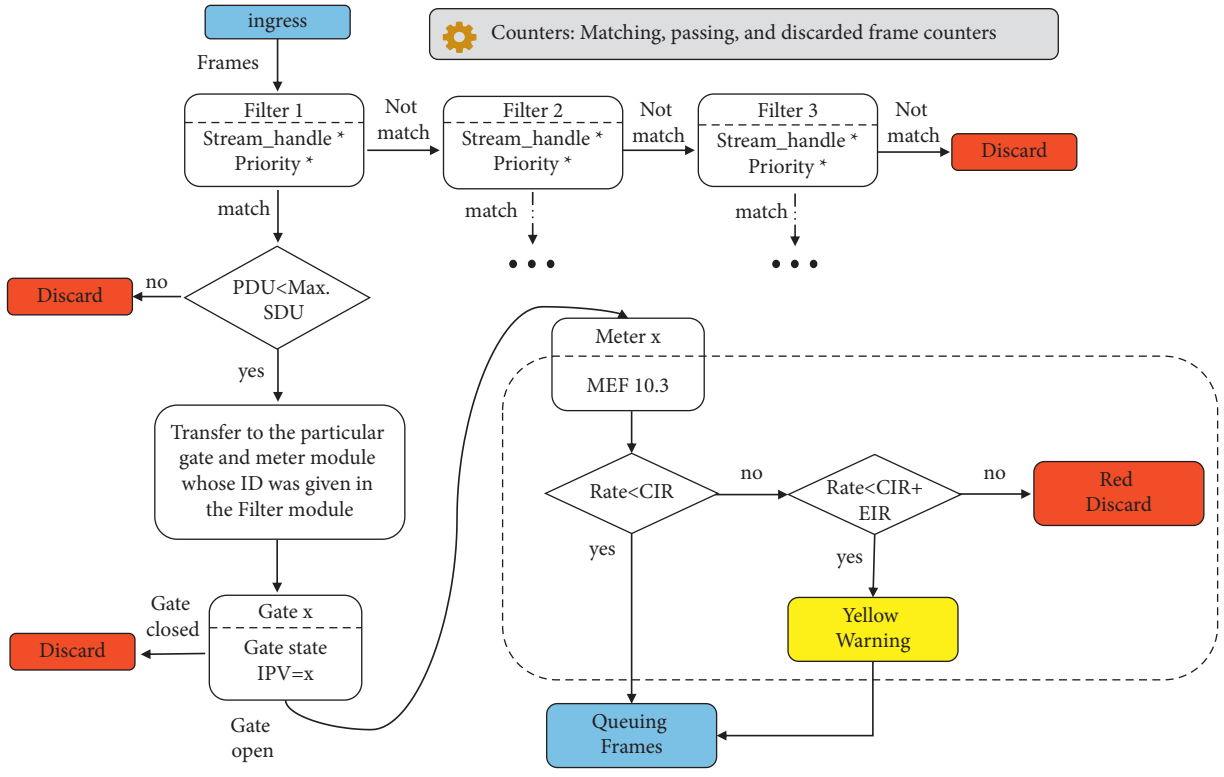

Figure 12: The structure of the ADS.

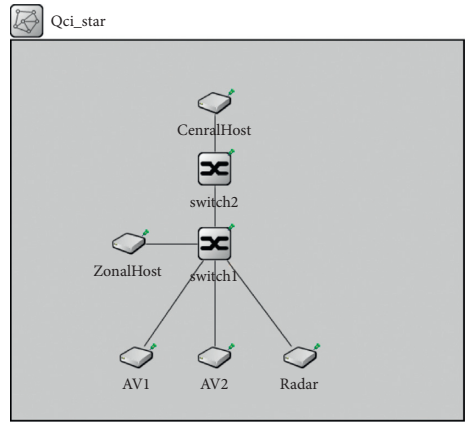

Figure 13: ADAS fusion zone system with the star-topology TSN.

Table 5: Traffic characteristics of the star-topology TSN.

Stream info	Priority	Source	Destination	Cycle time (us)	Quantity	Start time (us)	Interval (us)	Frame length (bytes)
Forward camera	4	AV1	CentralHost	500	3	100	90	400–500
Forward camera	4	AV2	CentralHost	500	3	145	90	400–500
Radar data	4	Radar	CentralHost	500	1	100	500	64
Control data	7	ZonalHost	CentralHost	500	1	0	500	20

(2) The priority code point (PCP) of control messages is 7 (the highest priority)

(3) The PCP of the Forward Camera message is 4 (the medium priority)

(4) The PCP of the Radar message is 4 (the medium priority)

(5) The switching processing delay is set at 8 us, which is the same as the NXP SJA1105Q

(6) The design of gate control lists (GCLs) is shown in Table 6

The ADS strategies are applied only in the switch1, and the parameter configurations are given in Table 7.

The Stream Filter 2 of all ports is used to detect and drop the undefined frames.

5.2. Detection. To analyze the performance of the ADS system, the abnormal traffic is added to the normal traffic. The characteristics of abnormal traffic are shown in Table 8, including the abnormal type and quantity. The addition of abnormal traffic can significantly change the real-time performance of the original traffic, as shown in Figure 14. Figure 14(a) shows the end-to-end delay of each traffic without abnormal traffic, and the end-to-end delay of each traffic type is very stable. Figure 14(b) shows the end-to-end delay for each traffic with added bandwidth traffic. Figure 14(c) shows the end-to-end delay for each traffic with all abnormal traffic.

In addition, the behavior of abnormal traffic is mainly divided into the following four kinds.

5.2.1. MSDU. The messages transmitted by the sensor network are generally within a known range. Messages exceeding MSDU are regarded as abnormal traffic.

5.2.2. Timing. The cycle of messages transmitted by the sensor network is also known. In the network design stage, the time that each message should be transmitted is also determined. Therefore, messages received at an abnormal time are regarded as abnormal traffic.

5.2.3. Undefined. After the network topology and traffic are determined, the type of network traffic is known. If an unknown traffic type is received, it will be considered abnormal traffic.

5.2.4. Bandwidth. For ADAS traffic in the sensor, the bandwidth is also statically configured, and abnormal bandwidth behavior is treated as an exception.

Comparatively speaking, MSDU and undefined can be classified as tempering attacks, as mentioned in Section 2. Timing and bandwidth are usually caused by node corruption. The performance of ADS is closely related to the configuration of PSFP. Figures 14 and 15 show the effects of ADS on four different kinds of abnormal traffic. The system starts abnormal traffic from 50 ms, and abnormal traffic is detected and discarded from the 50 ms after passing through the ADS system.

There is no difference between Figures 14(a) and 14(d), Figures 14(b) and 14(e) are also the same. In the absence of abnormal traffic, ADS will not cause any impact on the TSN system. Figure 14(c) shows the worst impact caused by abnormal traffic, in which control packets with high priority are affected because the abnormal control packets are added to the normal control message flow, and the length of the abnormal control packets is larger than MSDU. Therefore, the increase in end-to-end delay of normal control packets is due to the influence of abnormal control packets. At the

Table 6: GCL design of the star-topology TSN.

Scheduling interval (us)	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
0–125	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Open
125–450	Open	Open	Open	Open	Open	Open	Open	Closed
450–500	Closed	Closed	Closed	Closed	Closed	Closed	Closed	Closed

Table 7: Detection parameter configuration.

Switch1 Connection		Port0 Zonal host	Port1 AV1	Port2 AV2	Port3 Radar
Stream filter 1	Priority	7	—[1]	—	4
	VID	1	—	—	—
	DestMAC	—	0A-00-00-00-01-01[2]	0A-00-00-00-01-01	0A-00-00-00-01-01
	Gate ID	0	0	0	0
	Meter ID	0	0	0	0
	MSDU size	100 bytes	530 bytes	530 bytes	100 bytes
Stream filter 2	Priority	—	—	—	—
	VID	—	—	—	—
	DestMAC	—	—	—	—
	Gate ID	1	1	1	1
	Meter ID	0	0	0	0
	MSDU size	100 bytes	530 bytes	530 bytes	100 bytes
Gate ID0	Gate status	O[3]: 0 us; C[4]: 125 us	C: 0 us; O: 125 us	C: 0 us; O: 125 us	O: 0 us
Gate ID1	Gate status	C: 0 us	C: 0 us	C: 0 us	C: 0 us
Meter ID0	CIR	—	22 Mbit/s	22 Mbit/s	1 Mbit/s
	CBS	—	5004 bytes	5004 bytes	1002 bytes
	EIR	—	4 Mbit/s	4 Mbit/s	1 Mbit/s
	EBS	—	1000 bytes	1000 bytes	100 bytes

1: means the parameter is not related to the corresponding port. 2 The MAC address of the CentralHost node. [3]o: open state of the gate (the gate state period is 500us). [4]C: closed state of the gate.

Table 8: Abnormal traffic characteristics.

Stream info	Priority	Source	Destination	Cycle time (us)	Type	Quantity	Start time (us)	Frame length (bytes)
Forward camera	4	AV1	CentralHost	500	Wrong timing	1	50	400–500
Forward camera	4	AV2	CentralHost	500	DoS attacks	10	0	400–500
Radar data	5	Radar	CentralHost	500	Undefined	1	100	64
Control data	7	ZonalHost	CentralHost	500	Exceed MSDU	1	0	1000–1500

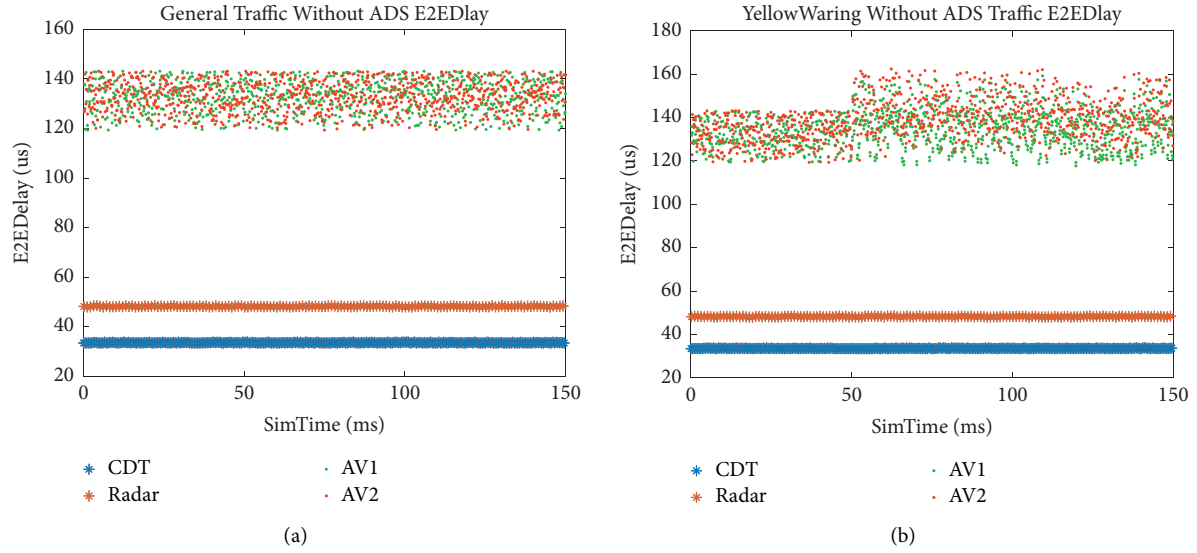

Figure 14: Continued.

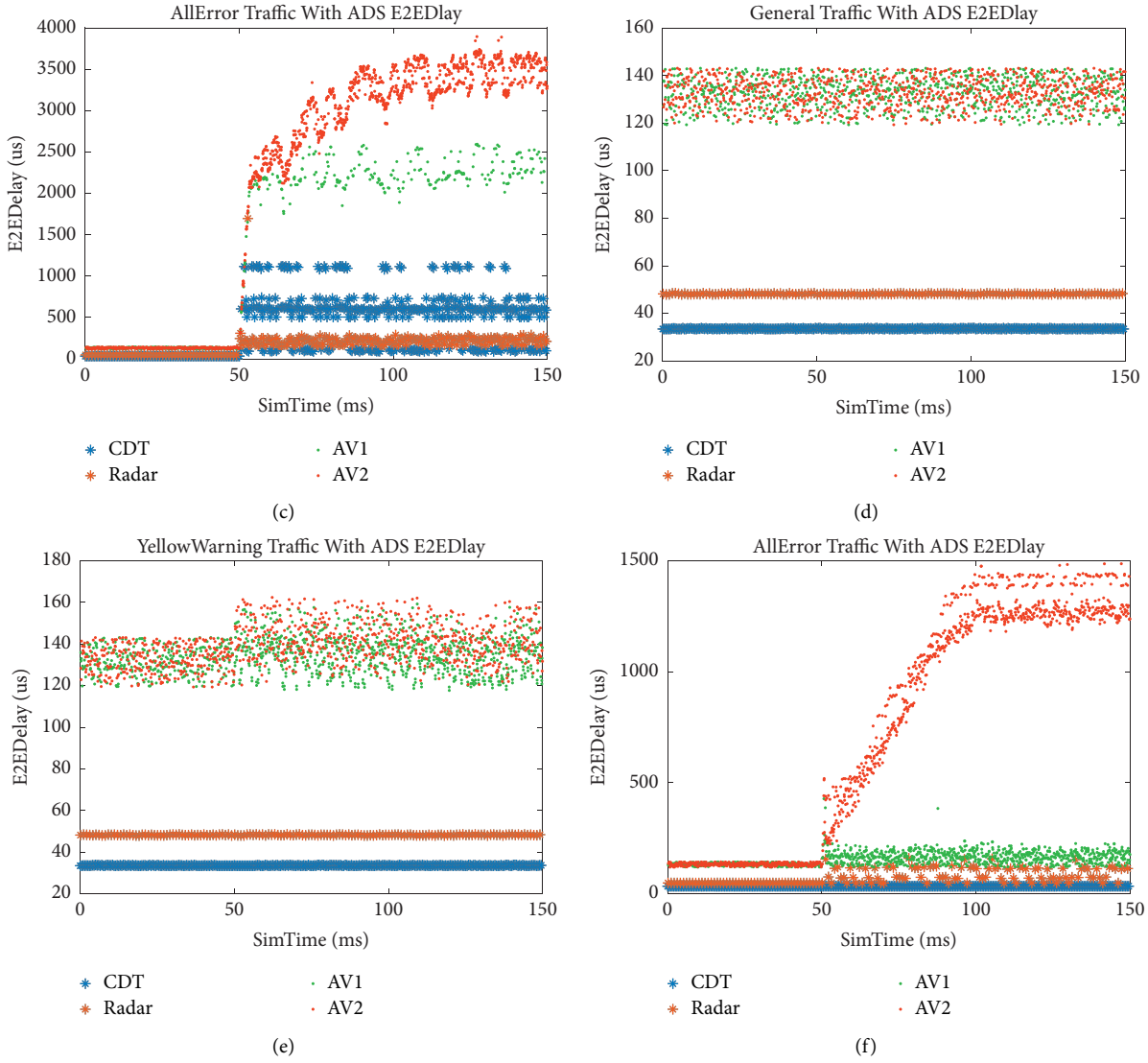

Figure 14: (a) End-to-end delay of each traffic without abnormal traffic. (b) End-to-end delay for each traffic with added bandwidth traffic. (c) End-to-end delay for each traffic with all abnormal traffic. (d) End-to-end delay of each traffic without abnormal traffic when ADS is applied. (e) End-to-end delay for each traffic with added bandwidth traffic when ADS is applied. (f) End-to-end delay for each traffic with all abnormal traffic when ADS is applied.

same time, the end-to-end delay itself includes both normal and abnormal end-to-end delays. Similarly, the other three types of messages are affected by abnormal traffic. As shown in Figure 14(f), for the system after applying ADS, the average end-to-end delay of each traffic has been greatly improved.

As a bonus, Figure 16 shows the behavior of the warning level. When the warning level is triggered, YELLOW tokens are taken, but no frames are dropped until the dropping level is triggered. Table 9 shows the performance of the system with and without abnormal traffic when ADS is applied and is not applied.

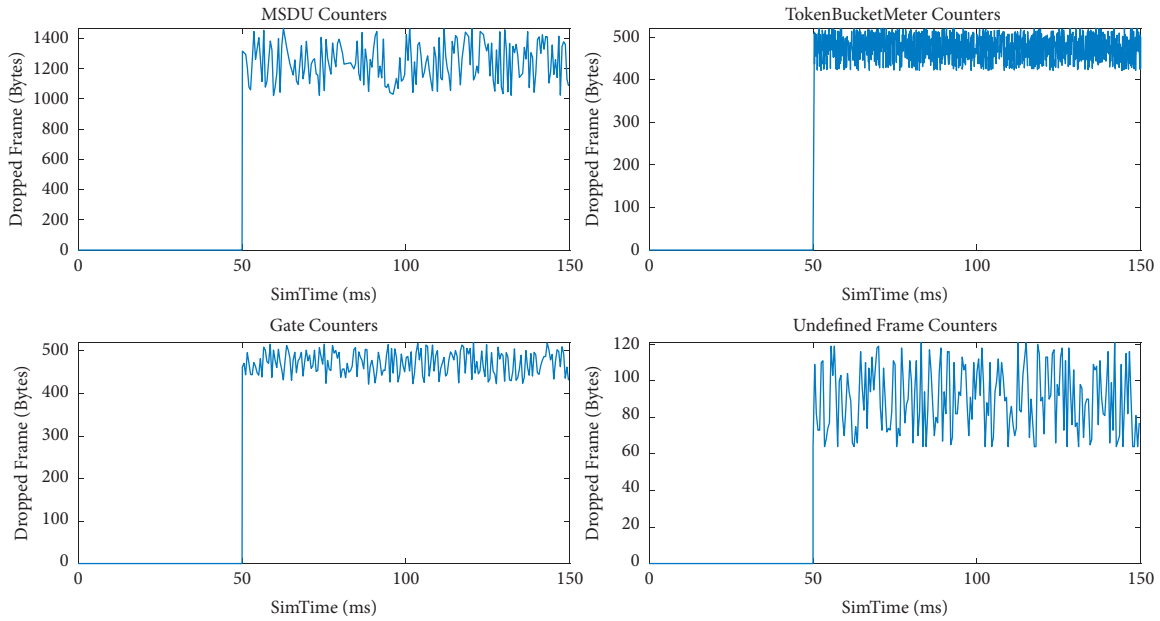

Figure 15: Effects of ADS on four different kinds of abnormal traffic.

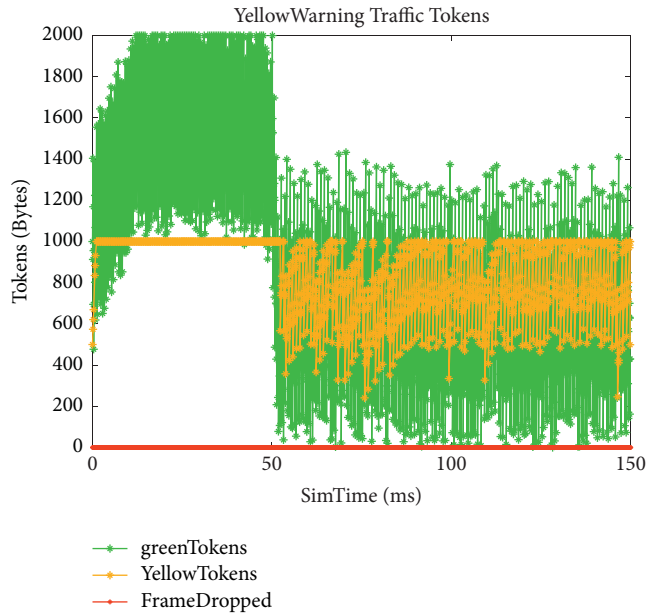

Figure 16: The behavior of the warning level.

Table 9: The performance of the system with and without abnormal traffic when ADS is applied and is not applied.

Stream info	Source	Destination	[5]E2E delay1 (us)	[6]E2E delay2 (us)	[7]E2E delay3 (us)	[8]E2E delay4 (us)	[9]Diff.1 (us)	[10]Diff.2 (us)	[11]Diff.3 (us)
Forward camera	AV1	CentralHost	132.6	1088	132.6	159.9	955.4	0	−928.1
Forward camera	AV2	CentralHost	132.9	2498	132.9	799.1	2365	0	−1699
Radar data	Radar	CentralHost	48.19	190.9	48.19	76.70	142.7	0	−114.2
Control data	ZonalHost	CentralHost	33.55	95.05	33.55	33.55	61.50	0	−61.50

[5]E2E delay1 = E2E mean delay without abnormal traffic when ADS is not applied. [6]E2E delay2 = E2E mean delay with abnormal traffic when ADS is not applied. [7]E2E delay3 = E2E mean delay without abnormal traffic when ADS is applied. [8]E2E delay4 = E2E mean delay with abnormal traffic when ADS is applied. [9]Diff.1 = difference between E2E delay2 and E2E delay1. [10]Diff.2 = difference between E2E delay3 and E2E delay1. [11]Diff.3 = difference between E2E delay4 and E2E delay2.

It can be seen that the real-time performance of the control data is not significantly affected when ADS is applied.

6. Conclusions

In this paper, the security of an automotive TSN as a backbone E/E architecture was analyzed through the MS STRIDE threat model. In the architecture, denial of service attacks is the biggest hidden danger and needs to be emphasized. To form a comprehensive protection strategy for automotive Ethernet security combining the traditional Ethernet and TSN security mechanisms, the protection countermeasures of each layer were listed according to the OSI model, and the countermeasures were divided into three categories: isolation and filtration, detection and defense, and authentication and encryption. Then, according to the definition of PSFP defined in IEEE 802.1Qci, an anomaly detection system was designed. Finally, according to the OMNeT++ simulation tool, the performance of ADS was analyzed and evaluated. Experimental results showed that the ADS successfully identified and discarded four different abnormal traffic events. The application of ADS can thus reduce the impact of abnormal traffic, especially the denial of service attacks. Among them, ADS can make the highest priority control messages not affected by abnormal messages, achieving the goal of ADS design. In future work, the performance of ADS will be further evaluated through hardware based on the simulation design method and model.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was financially supported by the Shanghai Automotive Industry Science and Technology Development Foundation (1806) and Prospective Study Funding of Nanchang Automotive Innovation Institute, Tongji University (no. TPD-TC202010-13).

References

[1] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 534–545, 2014.

[2] S. Sommer, A. Camek, K. Becker et al., "Race: a centralized platform computer based architecture for automotive applications," in *Proceedings of the 2013 IEEE International Electric Vehicle Conference (IEVC)*, October 2013.

[3] J. L. Messenger, "Time-sensitive networking: an introduction," *IEEE Communications Standards Magazine*, vol. 2, no. 2, pp. 29–33, 2018.

[4] J. Lindberg, *Security Analysis of Vehicle Diagnostics Using DoIP*, Chalmers, Gothenburg, Sweden, 2011.

[5] N. Herold, S.-A. Posselt, O. Hanka, and G. Carle, "Anomaly detection for SOME/IP using complex event processing," in *Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, IEEE, Istanbul, Turkey, April 2016.

[6] R. Boatright and J. Tardo, "Security aspects of utilizing ethernet AVB as the converged vehicle backbone," *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, vol. 5, no. 2, pp. 470–478, 2012.

[7] IEEE Standard for Local and Metropolitan Area Networks, *Timing and Synchronization For Time-Sensitive Applications*, pp. 1–421, IEEE, Piscataway, NJ. USA, 2020, https://ieeexplore.ieee.org/document/9121845.

[8] IEEE Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks, *Amendment 25: Enhancements for Scheduled Traffic*, pp. 1–57, IEEE, Piscataway, NJ. USA, 2016, https://www.ieee802.org/1/pages/802.1bv.html.

[9] IEEE Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks, *Amendment 26: Frame Preemption*, pp. 1–52, IEEE, Piscataway, NJ. USA, 2016, https://ieeexplore.ieee.org/document/7553415.

[10] IEEE Standard for Local and Metropolitan Area Networks-- Bridges and Bridged Networks, *Amendment 28: Per-Stream Filtering and Policing*, pp. 1–65, IEEE, Piscataway, NJ. USA, 2017, https://ieeexplore.ieee.org/document/8064221.

[11] IEEE Standard for Local and Metropolitan Area Networks-- Bridges and Bridged Networks, *Amendment 29: Cyclic Queuing and Forwarding*, pp. 1–30, IEEE, Piscataway, NJ. USA, 2017, https://standards.ieee.org/standard/802_1Qch-2017.html.

[12] IEEE Standard for Local and Metropolitan Area Networks-- Bridges and Bridged Networks, *Amendment 34:Asynchronous Traffic Shaping*, pp. 1–151, IEEE, Piscataway, NJ. USA, 2020, https://standards.ieee.org/standard/802_1Qcr-2020.html.

[13] IEEE Standard for Local and Metropolitan Area Networks, *Frame Replication and Elimination for Reliability*, pp. 1–102, IEEE, Piscataway, NJ. USA, 2017, https://ieeexplore.ieee.org/document/8091139.

[14] P802.1DG, *TSN Profile for Automotive In-Vehicle Ethernet Communications*, IEEE, Piscataway, NJ. USA, 2020, https://1.ieee802.org/tsn/802-1dg/.

[15] Committee VCSE, *Cybersecurity Guidebook for cyber-physical vehicle systems*, SAE International, Warrendale, PA. USA, 2016.

[16] Committee VCSE, *Road vehicles - cybersecurity engineering*, SAE International, Warrendale, PA. USA, 2020.

[17] UNECE, *Working Party on Automated/Autonomous and Connected Vehicles*, UNECE, Geneva, Switzerland, 2020, https://unece.org/transportvehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction.

[18] F. Sommer, J. Dürrwang, and R. Kriesten, "Survey and classification of automotive security attacks," *Information*, vol. 10, no. 4, p. 148, 2019.

[19] B. Carnevale, F. Falaschi, D. Pacini, G. Dini, and L. Fanucci, "A hardware accelerator for the IEEE 802.1 X-2010 key hierarchy in automotive applications," in *in Proceedings of the IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, November 2015.

[20] B. Carnevale, F. Falaschi, D. Pacini, G. Dini, and L. Fanucci, "An implementation of the 802.1 AE MAC Security Standard for in-car networks," in *Proceedings of the IEEE 2nd World*

Forum on Internet of Things (WF-IoT), IEEE, Milan, Italy, December 2015.

[21] B. Carnevale, L. Fanucci, S. Bisase, and H. Hunjan, "Macsec-based security for automotive ethernet backbones," *Journal of Circuits, Systems, and Computers*, vol. 27, no. 5, Article ID 1850082, 2018.

[22] J.-H. Choi, S.-G. Min, and Y.-H. Han, "MACsec extension over software-defined networks for in-vehicle secure communication," in *Proceedings of the 10th International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2018.

[23] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi et al., "Ultra-low latency (ULL) networks: the IEEE TSN and IETF DetNet standards and related 5G ULL research," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 88–145, 2019.

[24] L. Lo Bello and W. Steiner, "A perspective on IEEE time-sensitive networking for industrial communication and automation systems," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 1094–1120, 2019.

[25] D. Ergenç, C. Brülhart, J. Neumann, L. Krüger, and M. Fischer, "On the security of IEEE 802.1 time-sensitive networking," in *Proceedings of the IEEE International Conference on Communications Workshops*, (ICC Workshops), Montreal, Canada, June 2021.

[26] D. Grimm, M. Weber, and E. Sax, "An extended hybrid anomaly detection system for automotive electronic control units communicating via ethernet," in *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems - Volume 1 VEHITS*, Funchal, Portugal, March 2018.

[27] M. H. Farzaneh, S. Shafaei, and A. Knoll, "Formally verifiable modeling of in-vehicle time-sensitive networks (TSN) based on logic programming," in *Proceedings of the IEEE Vehicular Networking Conference (VNC)*, December 2016.

[28] M. H. Farzaneh and A. Knoll, "Time-sensitive networking (TSN): an experimental setup," in *Proceedings of the IEEE Vehicular Networking Conference (VNC)*, November 2017.

[29] S. Brunner, J. Rodger, M. Kurcera, and T. Waas, "Automotive E/E-architecture enhancements by usage of ethernet TSN," in *Proceedings of the 13th Workshop on Intelligent Solutions in Embedded Systems (WISES)*, June 2017.

[30] R. Mahfouzi, A. Aminifar, S. Samii, and P. Eles, "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.

[31] V. M. Navale, K. Williams, A. Lagospiris, M. Schaffert, and M.-A. Schweiker, "(R) evolution of E/E a," *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, vol. 8, no. 2, pp. 282–288, 2015.

[32] IEEE, *TSN Ethernet as Core Network in the Centralized Vehicle E/E Architecture: Challenges and Possible Solution*, IEEE, Piscataway, NJ. USA, 2019, https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/eipatd-presentations/2019/D1-02_BENGTSSON-TSN_ethernet_as_core_network_in_EE_architecture.pdf.

[33] Microsoft, *Microsoft STRIDE threat model*, Microsoft, Redmond, WA, USA, 2021, https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

[34] IEEE, *IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security*, IEEE, Piscataway, NJ. USA, 2018, https://ieeexplore.ieee.org/document/8585421.

[35] IEEE, *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control*IEEE, Piscataway, NJ. USA, 2020, https://standards.ieee.org/standard/802_1X-2020.html.