Essential Technics of Cybersecurity for Intelligent Connected Vehicles: Comprehensive Review and Perspective

Yang Shichun, Zuo Zheng, Ma Bin, Zheng Yifan, Zhou Sida, Liu Mingyan, Lu Yu, Li Qiangwei, Zhou Xinan, Zhang Mengyue, Hua Yang, Chen Fei, and Cao Yaoguang

***Abstract*—Along with the promotion of intelligent connected vehicles (ICVs), the problems of network attacks have rapidly increased, and thus the cybersecurity has drawn much attention. Unfortunately, although remarkable progress has been achieved both in technics and standard, it still remains vague for designing vehicular cybersecurity. In this article, the general technical profile of cybersecurity for ICVs has been comprehensively reviewed, including threat analysis and risk assessment, static defense, and intrusion detection. The potential attacking vulnerabilities for ICVs are summarized, within in-vehicle network and mobile networks. Then, the identity authentication and secure communication methods are introduced from static defense, where the conventional and novel intelligent approach are included. And the intrusion detection is introduced as the active methods, including conventional and novel ones. Moreover, the general procedure and management for designing the vehicular cybersecurity are also summarized according to the current standard system. It hopes that the review of research progress on technical method may help researchers and manufactures, and delivers the potential direction for future cybersecurity development.**

***Index Terms*—Cybersecurity, encryption, intelligent connected vehicles (ICVs), intrusion detection, standard system.**

NOMENCLATURE

ICVs	Intelligent connected vehicles.
IoV	Internet of Vehicles.
GPS	Global positioning system.
CA	Certification authority.
CAN	Controller area network.
CRL	Certificate revocation list.
TARA	Threat analysis and risk assessment.
V2X	Vehicle to everything.
DoS	Denial of Service attacks.
PLF	Piecewise Lyapunov functional.
OTA	Over-the-air technology.
AES	Advanced encryption standard.
DES	Data encryption standard.
RSA	Rivest–Shamir–Adleman.
DSA	Digital signature algorithm.
ECC	Elliptic curve cryptography.
ECU	Electronic control unit.
V2G	Vehicle-to-grid.
CAN-FD	Controller area network with flexible data rate.
GANs	Generative adversarial networks.
LSTM	Long short-term memory networks.
LTE-V2X	Long term evolution-V2X.
ETSI	European telecommunication standards institute.
ITSs	Intelligent transport systems.
EVITAs	E-safety vehicle intrusion protected applications.
TPD	Tamper proof device.
PKI	Public key infrastructure.
PRESERVE	Preparing secure vehicle-to-X communication systems.
HEAVENS	Healing vulnerabilities to enhance software security and safety.
OBU	On board unit.
RSU	Road side unit.
OCTAVE	Operationally critical threat, asset, and vulnerability evaluation.
TVRA	Threat, vulnerabilities, and implementation risks analysis.
SOTIF	Safety of the intended functionality.
CSMS	Cybersecurity management system.
MEC	Mobile edge computing.
WAVEs	Wireless access in vehicular environments.
VTA	Vehicle type approval.
SUMS	Software upgrade management system.

Manuscript received 30 September 2022; revised 1 June 2023 and 15 June 2023; accepted 24 July 2023. Date of publication 4 August 2023; date of current version 7 December 2023. The work of Yang Shichun, Zhou Sida, Chen Fei, and Cao Yaoguang was supported in part by the National Key Research and Development Program of China under Grant 2021YFB2501300 and Grant 2022YFB3104900, and in part by the National Natural Science Foundation of China under Grant U22A2042. *(Corresponding authors: Chen Fei; Cao Yaoguang.)*

Yang Shichun is with the School of Transportation Science and Engineering, Beihang University, Beijing 100191, China, and also with the Technology Innovation Center of New Energy Vehicle Digital Supervision Technology and Application for State Market Regulation, Beijing 100120, China.

Zuo Zheng, Zheng Yifan, Zhou Sida, Liu Mingyan, Lu Yu, Li Qiangwei, Zhou Xinan, and Chen Fei are with the School of Transportation Science and Engineering, Beihang University, Beijing 100191, China (e-mail: cf2020@buaa.edu.cn).

Ma Bin is with the College of Communication Engineering, Jilin University, Changchun 130012, China.

Zhang Mengyue is with the School of Transportation Science and Engineering, Beihang University, Beijing 100191, China, and also with the High Technology Research and Development Center, Ministry of Science and Technology of China, Beijing 100862, China.

Hua Yang is with the Core and Basic Technology Institute, Beijing SWORD Electric Industrial Company Ltd., Beijing 100176, China.

Cao Yaoguang is with the Research Institute for Frontier Science, Beihang University, Beijing 100191, China (e-mail: caoyaoguang@buaa.edu.cn).

Digital Object Identifier 10.1109/JIOT.2023.3299554

CCMS	Cooperative-ITS security certificate management system.
SCMS	Security credential management system.
VANET	Vehicle ad hoc network.
TSP	Telematics service provider.

I. Introduction

ALONG with the rapid innovation of vehicular technologies, ICVs have been gradually promoted worldwide and lead the direction of technical development for the next generation of vehicles. Perception, controlling, and decision methods help ICVs to understand driving situations and guarantee the safety. Moreover, the diversified communications methods provide more approaches for ICVs to realize surrounding environments and make decisions. Presented as Fig. 1, the diversity of communication is one of the typical characteristics for ICVs, where the vehicle may access to cloud-platform (vehicle-to-Internet), surrounding vehicle (vehicle-to-vehicle) and people (vehicle-to-person). Diverse accessing approach results in abundant functions and contributes to improve the user's experience. Unfortunately, the abundance of functions leads to another problem—the risking attacks. Moreover, ICVs always incorporate various intelligent sensors, such as lidar, video camera, GPS, and others. The diverse sensors significantly benefit the perception of the dynamic environment, but they also increase the potential risking cyber-attack and result in threats for cybersecurity.

Fig. 2 shows the typical in-vehicle network classification and associated data transmission rate. CAN [Fig. 2(b)] and FlexRay bus [Fig. 2(c)] are classical communication methods in ICVs, which have been promoted for decades. Authentication, encryption or other methods help improve security during communication. However, there still numbers of attack accidents occurring each year by intruding CAN network. Considering the increasing amounts of accidents and severe consequences, cybersecurity has drawn much attention and gradually becomes necessary during the vehicular design process. Cybersecurity is defined as a condition in ISO 21434, in which assets are sufficiently protected against threat scenarios. Cybersecurity is more emphasizing the protection from artificial attacks rather than the failure of electrical units. Different from conventional vehicular technics, cybersecurity is not independent and must associate with specific technology. For example, there is an ICV first and then it can be attacked; thus, the cybersecurity is born to defend the attack. Before 2010s, cybersecurity problems do not raise concerns for researchers or suppliers. In 2015, two famous hackers, Charlie Miller and Chris Valasek, remotely invaded a Jeep via an on-board infotainment system. They obtained the read/write permission of the CAN bus in the vehicle, and then sent unauthorized messages to control vehicle deviating from the driving direction and finally rushing into a slope. Owing to the threatening vulnerability, the incident leads Chrysler to recall nearly 1.4 million vehicles. In 2018, Tesla was revealed that its cloud server account was hacked, and a series of sensitive data was leaked, including telemetry data, map information, and vehicle maintenance records. Some classic cases of cyber-attack in recent years are presented in Table I. Owing to the increasing

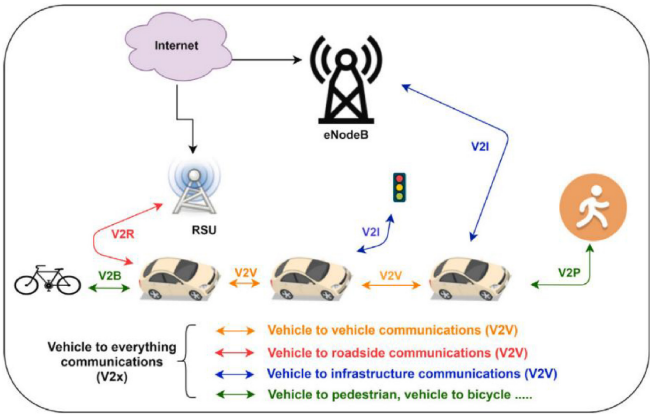

Fig. 1. Landscape of vehicular ad-hoc networks [1].

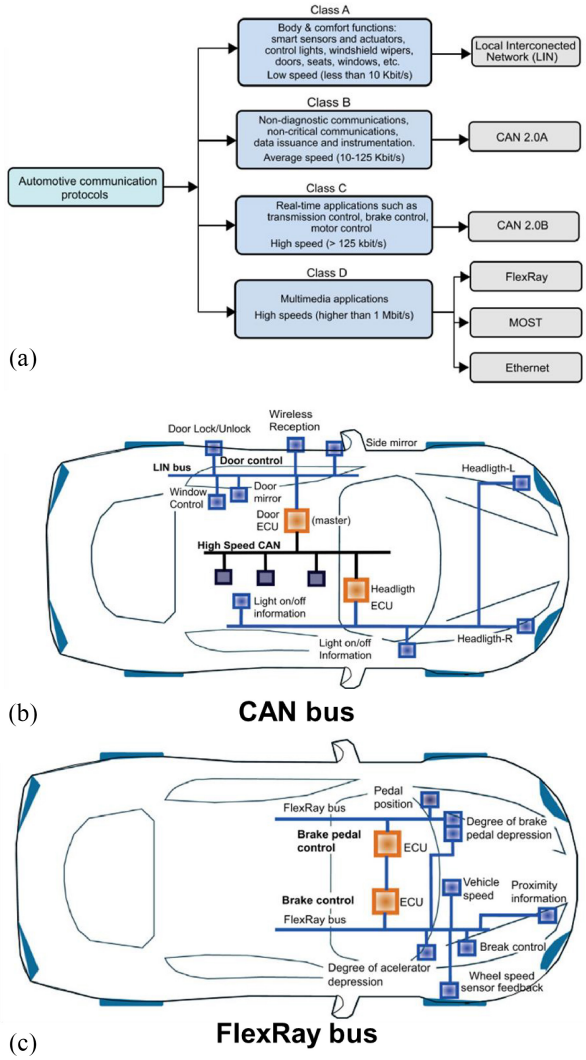

Fig. 2. In-vehicle network and communications. (a) General classification. (b) Typical protocol of CAN bus. (c) Typical protocol of FlexRay bus.

concerns of personal information protection, more statutes and standards are released recently, especially for ISO 21434, which is recognized as the most important one to standardize the general management process of vehicular cybersecurity. Cybersecurity has achieved great progress along with the research of the communication method.

TABLE I
TYPICAL CYBER-ATTACK FOR VEHICLES IN RECENT YEARS

Year	Manufacturer	Event
2013	Toyota	Charlie Miller & Chris Valasek cracked the Toyota Prius through OBD.
2014	-	Charlie Miller & Chris Valasek released a report of vehicle safety problem for 12 models.
2014	Tesla	360 company cracked remote control function of Tesla model.
2015	BMW	BMW's connected drive function has vulnerabilities, resulting in a recall of 2.2 million vehicles
2015	General Motors	Samy Kamker cracked the OnStart system of General Motors.
2015	JEEP	Charlie Miller & Chris Valasek remotely cracked Jeep cars and resulting in a recall of 1.4 million vehicles.
2015	BYD	360 company cracked automobile cloud service and remote driving function of BYD models.
2015	Tesla	360 company cracked automobile millimeter wave (wireless access in vehicular environments) radar system of Tesla.
2018	Volkswagen	The infotainment system of Golf GTE is detected for remote code execution vulnerability.
2018	Honda	The personal information of more than 50000 users was leaked owing to improper cloud-server configuration.
2019	Mercedes-Benz	The on-board application was cracked, causing more than 100 cars to be stolen.
2019	Toyota	Cohen Lab released four security vulnerabilities in the navigation device of 2017 NX300 model.
2020	Mercedes-Benz	9765 vehicles were recalled owing to communication module software problems.
2020	Volkswagen	The hacker obtains the key through the digital signature transponder.
2021	QNX Operating System	Multiple security vulnerabilities in automotive operating system QNX were found by 360 Company.
2022	Honda Motor	Key rolling code has defect and the wireless signal can be replayed. The expired opening instruction was reproduced.
2023	Toyota	Due to a misconfiguration of the cloud environment, any unauthenticated visitor was able to access some of the databases managed by Toyota Connected Corporation.

Considering the complexity of cybersecurity technologies, this article reviews the general technical profile for designing the vehicular cybersecurity, including TARA, static defense, and intrusion detection. Attacking vulnerabilities are also summarized from the general in-vehicle and outside communication networks. Moreover, the standards on the management of cybersecurity are also summarized. This article hopes to generally analyze the research progress for essential technologies, and provides guidance for researchers to understand the potential perspective for future vehicular cybersecurity.

II. ESSENTIAL TECHNIQUES OF CYBERSECURITY

As the increasing amounts of attacking vulnerabilities for ICVs, the techniques are broadly researched for protecting the vehicles from intrusion. Generally, three components help establish the lifespan cybersecurity, including TARA, static defense, and intrusion detection. Then, the development of cybersecurity can be divided accordingly. Threat analysis is the fundamental basis of risk assessment, which aims at defining the potential attack and their influences of ICVs. Currently, the methods of threat analysis consist of process-driven methods, event-driven methods, and others. Owing to that TARA only delivers the potential risk and hazard of attack, effective defense measures are still needed to address the attack problems. The current defense measures can be divided into active/passive ones in general, where the former one aims at preventing the abnormal information or potential attacks, and the latter one is designed for safely communicating with scheduled encryption.

Considering to concentrate on the specifical techniques and provide general guidance for cybersecurity researchers, in this article, three main parts are detailly introduced during the cybersecurity design process, and the pros and cons of current available methods are also discussed, presented as Fig. 3. Considering the actual development of vehicular cybersecurity, the current promoted standards are also analyzed. This article hopes to help the researchers and developers realize the comprehensive designing process of cybersecurity, and may acquire the potential direction of future research in perspective.

III. ATTACKING VULNERABILITIES OF ICVS

Along with the increasement of vehicle functions, abundant interfaces are attached to vehicles, including hardware access or remote access. Considering the large amounts of sensors, ECUs in vehicles, the design of cybersecurity generally has great difficulties on protecting all known/unknown threats. Assuming that there is a hacker trying to intrude a vehicle, diverse categories of means can be applied via various communication interfaces between the vehicle and environments. In general, the interfaces of ICVs can be roughly separate into external communication (including radio, keyless

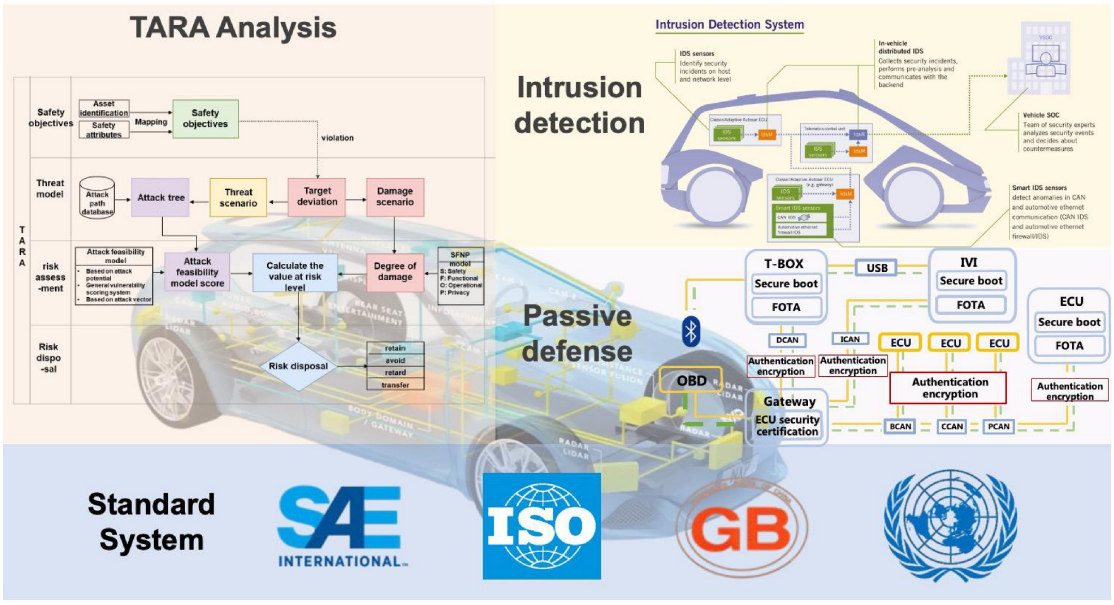

Fig. 3. General profile of vehicular cybersecurity.

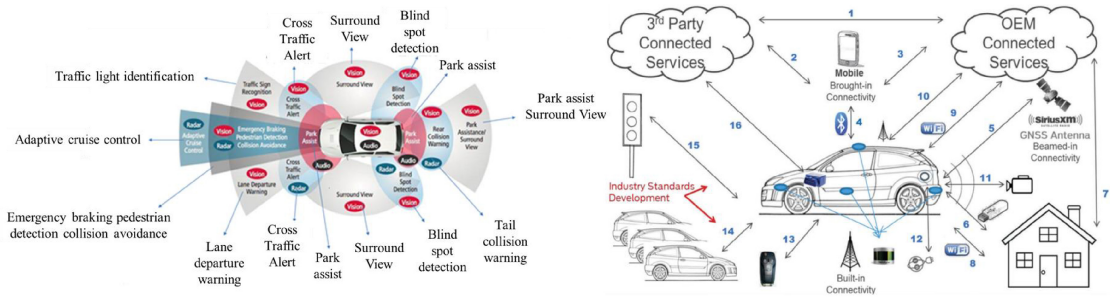

Fig. 4. Increasing interfaces for connected vehicles, especially for sensors and electrical units. (a) Diverse sensors for automotive vehicles. (b) 16 potential attacking vulnerabilities for vehicles [2].

entry, and sensor charging interface) and internal communication (including USB, Bluetooth, diagnostic interface, GPS, or Internet), where an instance for automotive vehicles is performed in Fig. 4(a). Fortunately, most attacks can be simulated and analyzed during the design process according to threat analysis method. In this section, the potential attack modes are systematic analyzed based on existing cyber-attack accidents or experiments, and the challenges of cybersecurity are also discussed.

Before to decompose system threats of ICVs, it is necessary to explore the potential weakness in communication mode. In Fig. 4(b), the current communication methods and relationship of input/output are presented, where common weak components are divided into eight categories of potential vulnerable communication modes: mobile network (servers and mobile applications), keyless entry, infotainment system, USB, Bluetooth, and in-vehicle network. Moreover, according to Upstream (presented in Fig. 5), the most common attack is cloud servers, which takes a percentage of 36%. And the attack of keyless entry is the second common one, which has 23% parts. As the promotion of cloud servers, the attack of is will be more often and become hard to defend.

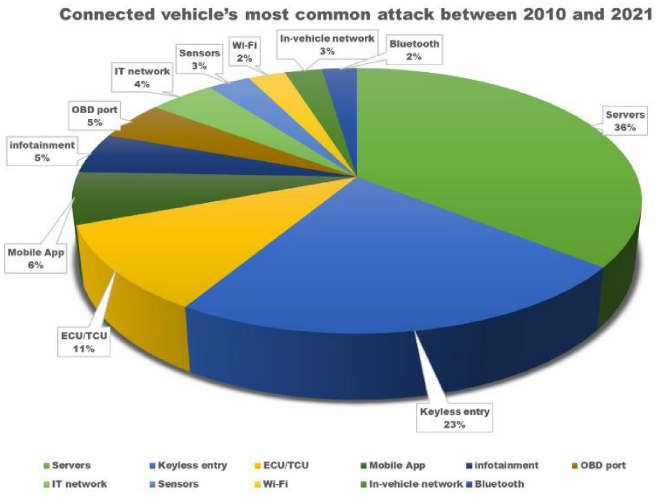

Fig. 5. Connected vehicle's most common attack between 2010 and 2021. (Data from Upstream).

A. Mobile Network

As the promotion of the V2X technology, the mobile network is applied for connecting the vehicle with other

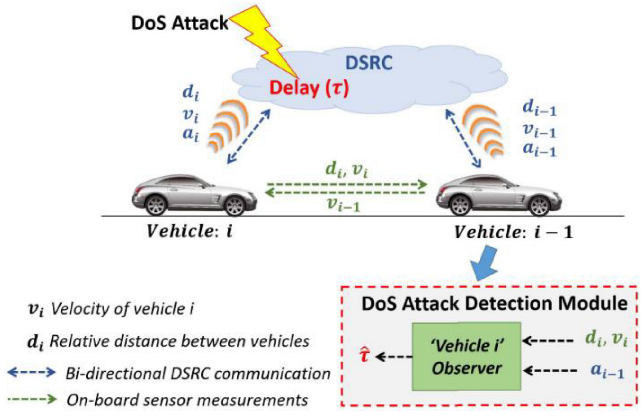

Fig. 6. DoS attack detection and estimation scheme from Zoleikha (2018) [8].

vehicles or facilities, and more possibilities for cyber-attack are accordingly generated [3]. Via cracking mobile network, the attackers can get access to the internal networks of vehicles from anywhere, and they can also monitor drivers, track driving traces, or interfere signals without the notice of drivers.

DOS is one of the classic attack modes for vehicle mobile networks, which intrudes the communication protocol for exhausting the resources of objects, presented in Fig. 6. DOS is regarded as one of the most severe threats for cybersecurity of ICVs, which may lead to traffic jams and other safety issues [5]. Exploiting the vulnerabilities in CAN protocol is most common methods of DOS and it has difficulty to detect. Such cases have been broadly researched both for vehicle and computers. Nissan Connect application equipped one Nissan Leaf was been exposed by DOS vulnerability which allowed hackers to reconfigure fans and then drained out the on-board battery. Li et al. [6] introduced a real-time edge detection scheme for sybil DOS, where they used the entropy theory to quantify the traffic distribution, and further design an algorithm named fast quartile deviation check to recognize and locate the attack. Ma et al. [7] introduced an event-triggering communication scheme to enhance the efficiency of network resource utilization, and exponential stability analysis was carried out according to the PLF approach. Zhang et al. [4] introduced switched time-delay system model for solving the problem of distributed secure platoon control of connected vehicles subject to DoS attack, where the associated theory is established based on the Lyapunov stability theory and Jensen's Inequality method.

Black-hole attacks have similarity with DOS, which intercept some messages to block the communication. Hassen et al. [9] introduced an intelligent black hole attack detection scheme, and used hop count, destination sequence number, packet delivery ratio, and end-to-end delay as key parameters.

Sybil attack is senior attack method, which uses a few nodes in a network to control multiple false identities, so as to control or affect other nodes. Chang et al. [10] proposed a footprint method for investigating sybil attack detection by location-hidden authorized message generation scheme, where authorized messages used for long-term identification are prohibited. According to a footprint method, vehicles generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages, and then sybil attacks can be detected by utilizing social relationship among trajectories. Shrestha et al. [11] presented a lightweight solution for sybil attacks based on received signal strength by determining the optimal threshold value which minimizes false detection probabilities.

Malware is another attack form by installing software, without the notice of drivers, to monitor the driver privacy information, driving traces, or other critical malfunctions [12], [13]. Diverse methods can be utilized for installing malwares, including onboard diagnostic ports, OTA, embedded Web browsers, and other media ports [14]. Elkhail et al. [15] presented a comprehensive review of the malware detection system and provides a specific taxonomy, and delivers a detailed contrast of signature-based malware detection techniques. Zhang et al. [16] delivered a cloud-assisted vehicle malware defense framework for address the challenges of malware issues.

B. Keyless Entry

The keyless entry has become the second most common attack within multicategories cyber-attacks, which can be attributed to the simplified design of remote keys for user's convenience. Owing to the ability to open doors or trunk, the keyless entry performs significance on protecting vehicle safety. However, the keyless entry usually applies radio for communication, and is easier to be intruded. The attacked keyless entry can crack encryption algorithms, block original signals, and consume the power, even that the vehicles can be stolen with nothing out of ordinary. Ansaf and Mahmud [17] summarized the common attacks against the security of keyless-entry systems of vehicles and also compared the vulnerability of the system under different attacks. Transmitter, receiver, recorder, signal analyzer, and mathematician are typical tools for attacking key-less system on vehicles. Beek and Leferink [18] introduced a receiver with a synchronous detector for tackling pulsed noise interference, which would be less vulnerable against hacking attacks relying on jamming the wireless link. In 2021, the 360 Radio security research department released research on keyless entry attack report. By cracking the wireless communication protocol, the hackers may extend the sensing distance of the remote key and mistakenly deceive the vehicle to trust the nearby key. According to the result, some signal shields may be effective for defending the attacks on keyless entry, but they also will cause problems for regular uses.

C. Wi-Fi

Generally, the on-board infotainment system usually has the ability to communicate via Wi-Fi, including flashing program in maintenance shop, or transferring logs locally. Especially for autonomous driving application, Wi-Fi are also applied to help locate the vehicle position. Different from mobile network attack, the intrusion of Wi-Fi often occurs when the vehicle attempts to connect to the cracked Wi-Fi. Consequently,

the attacker can implant malware on vehicles, and also can intercept or send wrong messages. Mousavinejad et al. [19] introduced the potential defects of cybersecurity on vehicle platooning control system, wherein intervehicle information is propagated via a wireless communication network; moreover, a distributed attack detection algorithm is proposed and some recovery methods are also discussed for improving the security during information propagation. Rana [20] presented the influence of Internet of Things on vehicle sensors, and also introduced a distributed state estimation and stabilization algorithm for electric vehicles.

D. Infotainment System

As a time of software-defined vehicle come, the infotainment system is of crucial importance for improving user experience. The current infotainment system has the ability for vehicle-cloud integration, and can get access to both external network and internal network. Thus, the cracked infotainment system can be utilized for diverse intrusion, including installing malware, maliciously accessing to CAN network, or presenting false information to the driver.

In 2021, based on an experimental environment, the Tencent Cohen laboratory released three vulnerabilities on the infotainment system for Mercedes Benz ICVs, including buffer overflows, remote code execution, and out-of-bounds access. The researchers first get access to the vehicle authority through physical contact, and then realize the remote control of the on-board infotainment system. Moreover, by cracking the vehicles, the researchers can remotely control other functions, such as displaying images on the screen or sending any CAN data by T-Box.

E. USB, Bluetooth, and CAN

The intrusion of USB and Bluetooth is a relatively conventional attacking measure. The cracked USB can install malware, tampered updating software even make USB interface short circuit to damage the automotive system. Similarly, the crack of Bluetooth may also result in the same consequences. Cheah et al. [21] proposed a framework for a systematic method of security testing for automotive Bluetooth interfaces, where the core concept of the framework is the initial reconnaissance of any test interface, and which forms the basis for all future vulnerability hypotheses and threat models. Dardanelli et al. [22] delivered a hierarchically distributed control system architecture for tackling the security between smart phone and vehicles, an ad-hoc, end-to-end security layer is designed to demonstrate how a smartphone can interact securely with a modern vehicle without requiring modifications to the existing in-vehicle network.

As the main communication means of the internal network, CAN performs an essential significance on guaranteeing the vehicle operation in electronic and electrical architecture. The encryption mechanism of CAN helps prevent most attacks, such as false message or network jam, but there is still some potential intrusion of CAN, which results in consequences. The cracked CAN can activate the vehicle without the input of key, and also damage the communication between different ECUs, leading to vehicle electrical system paralysis [23]. Araujo-Filho et al. [24] introduced two machine learning algorithms for detecting fuzzing and spoofing attacks, and also proposed a system for intrusion prevention, which is deployed on a single additional device connected to the CAN bus under surveillance.

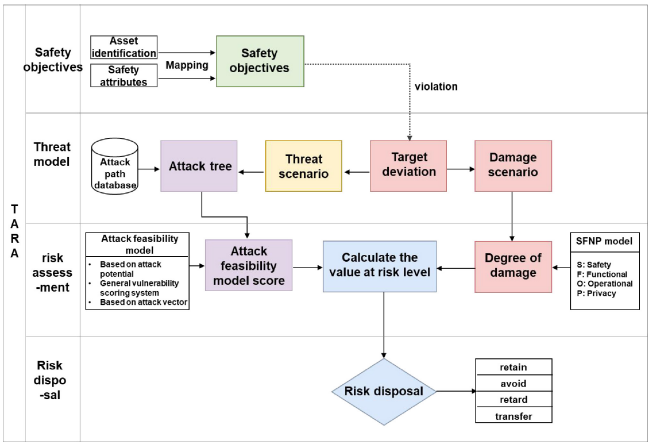

Fig. 7. Typical process of TARA.

IV. Threat Analysis and Risk Assessment

As the beginning of the design for vehicular cybersecurity, the TARA process delivers guidance on determining vulnerabilities and assessing the potential risks; moreover, TARA should provide the basic requirements for developers. Normally, TARA is more process-oriented compared against specific technics; thus, in this article, only the essential information about TARA will be presented and help to understand the complete process on designing cybersecurity, as shown in Fig. 7.

Threat analysis should identify and evaluate potential threats associated with assets according to typical application scenarios, and finally describe the relationship between threats and security to help establish risk assessment. The threat model is one of the efficient methods to find the threat analysis, including the basic components, software/hardware equipment, internal communication, on-board operating system, and external terminal. The main purpose of threat analysis is to determine the protected assets, potential attack surfaces, and vulnerability.

Asset identification should give the data diagram based on specific cases of assets, exemplified as Table II. Not all assets should be protected or easy to be attacked; thus, the asset identification can help reduce the complexity during evaluating the risk of intelligent networked vehicles.

Threat identification should give the potential threats and their influencing security attributes. Generally, the normal threats can be divided into six categories, including counterfeiting, tampering, repudiation, information disclosure, denial of service, and privilege promotion; and the influencing security attributes can be separated into authenticity, integrity, confidentiality, availability, timeliness, and anti-repudiation.

TABLE II
TYPICAL PROTECTED ASSETS IDENTIFICATION AND POTENTIAL THREATS

Typical protected assets identification		
Assets	Typical content	
Electronic control units	Accessed controlling function, execution environment, on-board communication.	
Information associated with vehicle and driver	Vehicle ID, vehicle status (location, speed), driver information (identity authentication, history)	
On-board software	Operating system, application software	
Infotainment content	Video, music, navigation map	
Vehicle configuration	Software/hardware system configuration information	
potential threats and influencing security attributes		
Threat category	description	influencing security attributes
counterfeiting	Attacker impersonates user to intrude.	Authenticity, timeliness
tampering	Attacker artificially changes the transmitted and stored data.	integrity
repudiation	The actions of attacker cannot be traced back.	anti-repudiation, timeliness
information disclosure	Attacker gets the access to transmitted or stored data.	confidentiality
denial of service	Attacker can interrupt the normal operation of the system.	availability
privilege promotion	Attacker can access to unauthorized behavior.	confidentiality

Vulnerability identification should conduct penetration test based on scanning tool, audition, and analytical strategy. The results perform the description of the relationship between vulnerabilities and damage of threats by attacking vulnerabilities. Attack tree is one of the typical methods for determining vulnerability.

The main purpose of risk assessment is to evaluate the influencing level and severity level, and forms the final evaluating results of threats and their harmfulness. The former should quantify the impact of threats based on adverse consequences, including leaked user privacy, economic loss, and user personal safety. And the latter one will quantify the information security of the on-board terminal, and finally form the quantitative evaluation by combining the threat and impact assessment.

Generally, the process of risk assessment can be divided into three steps: 1) identification; 2) analysis; and 3) evaluation. In the risk identification step, it is necessary to determine the important units within the system and find out the potential risk according to the operational situations. The judgment of the risk is of crucial importance and the coverage has great influences on results. In the secondary step, the system and inside units will be detailed analyzed to characterize the risk, along with clearing the definitions and potential harmful consequences of risks. Finally, the risk evaluation step will perform a clear quantitative assessment of the final impact of the risk based on the influence on possibility and consequences. As the risk assessment is only the beginning of the whole process, the results are to help the researcher understand the value of designed electronic units and improve the vulnerability in the subsequent designing process.

V. RESEARCH PROGRESS OF STATIC DEFENSE

In order to ensure the normal operation of the communication system of intelligent vehicle networking, all parts of the IoVs need to carefully consider security, the security of IoV has become a crucial research part in the 5g era. The attacks faced by the IoV include false message attacks, eavesdropping attacks, message tampering attacks, DoS, replay attacks, etc. [25]. Among the various security mechanisms used in the IoV, ensuring security through the authentication technology is a crucial part. At the same time, due to the high-speed mobility of vehicles, an ideal authentication scheme must be efficient and practical. In addition, the IoV security system needs to protect the privacy of users and vehicles. Therefore, it is very important to propose a safe and efficient authentication scheme for the IoV to protect the privacy of users' information. The current security communication system of the IoV is mainly designed and implemented based on PKI. The CA center issues digital certificates for all parties involved in the communication, and carries out identity authentication and secure communication with the support of the digital certificates [26], [27], [28]. However, in the traditional PKI system, the digital certificate contains a lot of personal information, so there is a problem of personal information leakage during

the communication process [28]. On the other hand, the big data analysis of the IoV can also easily lead to the leakage and abuse of the car owner's geographic locations, behavior habits, family residences, and other private information, which violates the car owner's legitimate rights and interests, and may also cause leakage and theft of owner's personal privacy, daily life, private wealth, and other security threats [29]. At the same time, in recent years, more and more attention has been paid to personal information and privacy protection. The state has also issued a number of laws and regulations to emphasize that privacy is the legitimate rights and interests of citizens, and personal information is protected by law. Therefore, if the problem of personal information and privacy protection cannot be well solved, it will become a serious shackle for the further development of the IoV. Various countries are currently conducting research on this issue. Presently, the entire IoV security protection technology is divided into two parts: 1) identity authentication technology and 2) privacy protection technology and secure encrypted communication, which will be explained in the following.

A. Identity Authentication and Privacy Protection Technology in the IoV

The identity authentication technology is designed to verify the legitimacy of each entity's identity in the vehicle network, which can be recognized as the first line of defense for cybersecurity system. The identity authentication can be classified into static one and dynamic one. Account and password are the basic method of static authentication, whereas they still suffer from large security risks to be easily attacked owing to the static memory of password. Dynamic authentication mode utilizes the updating password to authentic, where the password may be updated for days or months. More often to dynamic update the password, more security can be achieved for the system. As for the online authentication application in vehicles, the common methods for identity authentication have diverse categories, including anonymous certificate, digital signature, intelligent authentication, and others, and these guarantee the legality of both entities and confidentiality during communication. The privacy protection technology includes group signature technology, ring signature technology, and pseudonym protection technology. It can not only ensure the secure communication of the IoV, but also prevent the leakage of personal information and privacy. Group signature technology and ring signature technology take RSU as the center and vehicles as the group. The members of the group themselves encrypt the data with their private keys and verify the authenticity with the public keys of the group. The Pseudonym certificate system is an improved scheme based on the PKI system, which involves many key links, including certificate generation, certificate use, certificate management, certificate switching, certificate revocation, etc. Studying these key technologies and designing a safe, reasonable, efficient, and usable pseudonym authentication system will have rich theoretical research and practical value for the development of China's future IoV system and architecture. Specific IoV identity authentication and privacy protection technologies are shown in Table III.

1) Research Status of Traditional Identity Authentication Technology at Home and Abroad: The digital signature method delivers a private group key to each vehicle, and it will be used for certifying the messages. When a message will be broadcasted, the message signature is processed through the distributed group private key. Thus, the identity of the signer is not known. When other members use the group public key to verify the signature, the security of privacy for identity can be guaranteed. Existing identity authentication mainly includes identity authentication based on embedded security module and identity authentication based on the encryption mechanism. The former builds a trusted architecture to assist in authentication by integrating security modules such as TPD on the mobile terminal, and uses hardware to ensure the security and authentication efficiency of the solution. However, different manufacturers have different definitions of security module standards, which make it difficult to unify the security standards. The latter verifies whether the mobile terminal has the correct key and password, which requires low hardware requirements but requires high computational overhead. So far, scholars at home and abroad have done a lot of research on how to ensure communication security and identity authentication in the IoV. The details are shown in Table IV.

IEEE 1609.2 is an international standard for secure communication of the IoV. By using the traditional PKI certificate architecture for reference, it defines the secure message format and certificate type of WAVE, and realizes the mutual trust of terminals through a complete certificate generation, issuance, revocation, and update process. Generally speaking, the main modules of traditional digital certificates include root CA, enrollment CA, digital CA, etc. [37], [38]. To sum up, based on IEEE1609.2 and combined with China's IoV communication standards and management system, it is a very important and urgent task to study the security communication system of the IoV in line with China's national conditions.

2) Research Status of Traditional Identity Authentication Technology at Home and Abroad: With the continuous evolution of technology, the blockchain technology has gradually evolved into a distributed platform coupled with multiple technologies, such as distributed storage, consensus, information encryption, digital signatures, smart contracts, etc., which realizes users' independent interaction, security sharing, and privacy protection without a central server. Due to the many advantages of the blockchain technology, a large number of studies have applied it to IOVs scenarios, aiming to make up for the data management problems caused by large-scale vehicle access and alleviate the processing pressure of centralized servers. With the help of the MEC technology, according to the different blockchain architectures, the blockchain technologies in the existing IoVs can be roughly divided into three categories.

a) Public blockchain: In this structure, each vehicle acts as a blockchain node, encapsulates the data interaction process with other vehicles into a transaction format, broadcasts the transaction to the whole network, and records and links the transaction using the consensus mechanism. In the whole

TABLE III
SUMMARY OF IDENTITY AUTHENTICATION AND PRIVACY PROTECTION METHODS OF IOV

	Items	Authentication method	Implementation method	Pros	Cons
Identity authentication technology of IoV	Static authentication	Static account and password	Identity authentication protection based on traditional account and password	Easy to use, low complexity, low cost	Simple passwords are easy to be cracked, and easy to implant Trojan horses for monitoring
	Dynamic authentication	PKI (digital certificate)	Provide encryption and decryption, signature, identity authentication services, and the CA center provides full life cycle guarantee services for the IoV system.	High safety, realize the guarantee service in the whole life cycle of the vehicle	Certificate storage and revocation occupy resources, and it is difficult to protect users' privacy
		Certificateless public key cryptosystem	Part of the private key is provided by a third-party trusted organization, and part is generated by the user himself. The user identity and public key are not bound by the certificates.	Avoid complex certificate management problems, and the processing efficiency is high.	The security performance is low, and privacy is difficult to guarantee. The solution itself is only in the theoretical stage, and its practicability needs to be discussed.
		Identity-based cryptography	The user identity information is used as the public key, and the third-party trusted institution generates the private key.	Higher efficiency, and easier resource management than PKI.	The security is not as good as PKI, the privacy is difficult to guarantee, and the system security completely depends on the third-party trusted institution.
		Block-chain methods	Building a decentralized IoVs security system based on blockchain security communication protocol.	De-centralization, traceability, public transparency, anonymous	The decentralized system makes the security guarantee unable to be certified by authoritative

process, there is no need for traffic infrastructure assistance, and each vehicle user has a unique identity address identifier in the whole network. Under this structure, the network has high anti-attack capability, and the security of data transactions can be greatly improved. However, this structure requires all vehicles in the entire network to store a copy of other people's

TABLE III
(Continued.) SUMMARY OF IDENTITY AUTHENTICATION AND PRIVACY PROTECTION METHODS OF IOV

				transaction, consensus mechanism.	organizations, and the blockchain itself is not recognized, which leads to difficulties in landing.
Privacy protection technology of IoV	Security and privacy protection authentication	Group signature technology/ ring signature technology	Advantage: With the RSU as the center and vehicles as the group, the group members encrypt data with their own private key, and use the group public key to verify the authenticity of the information. Disadvantages: (1) The high-speed movement of the vehicle leads to frequent group changes, which is only suitable for low-speed moving scenarios. (2) The signature verification is proportional to the number of groups, and the maintenance pf CRL (certificate revocation list) is expensive. (3) The security performance is average.		
		Pseudonym certificate technology	Advantage: (1) Replacing the communication certificates with pseudonym certificates, which can ensure the safety of the vehicles under the premise of ensuring high efficiency and safety. (2) The replacement frequency of pseudonym certificates is 1-2 weeks, so there is no need to replace them frequently. Disadvantages: (1) To issue multiple pseudonym certificates at one time, it is necessary to ensure that there is no link between each certificate. (2) Revoking multiple pseudonym certificates at one time costs a lot to maintain CRL.		

ledger, resulting in poor network scalability. At the same time, the interaction of the whole network caused by the consensus process causes large communication overhead, which poses a great challenge to network resources. Although some existing researches have optimized the public chain structure by reducing the computational difficulty in the consensus algorithm, optimizing the ledger storage structure, and offloading and deploying storage data, the public chain still faces many challenges for latency-sensitive IoV scenarios.

b) Private blockchain: The private chain can be regarded as a public chain structure with a small number of nodes. The difference is that the identity of vehicles in the private chain is only considered legal in the current chain, and they cannot interact with other vehicles in the rest of the chain. Therefore, private chains are often configured with one or more vehicle identity legality management facilities. Due to the small scale of nodes in the private chain, the amount of data that the vehicle needs to store is correspondingly reduced, and the communication overhead required in the consensus process is further reduced, which improves the scalability of the system [39]. At the same time, due to the identity management facility in the private chain to review and control the vehicle identity, the security in the transaction process can also be guaranteed [40]. However, the cross-chain behavior of nodes under the private chain depends on identity reassignment and review. In the high-speed mobile IoVs environment, the frequent cross-region behavior of vehicles increases the complexity of identity management and affects the efficiency of interaction between vehicles.

c) Alliance blockchain: This structure combines the advantages of the public chain and the private chain. With the help of the communication, storage, and computing capabilities of the transportation infrastructure, the vehicle itself is only responsible for generating transactions and maintaining lightweight accounts, while offloading the ledger storage, block packaging and verification, and consensus process migration in the blockchain to the infrastructure. It innovates and reshapes the operation mode of the blockchain in a hierarchical manner, which is widely recognized and studied. So far, scholars at home and abroad have done a lot of research on the alliance blockchain. The details are shown in Table V.

The blockchain technology provides a new solution for data sharing under the IoVs. By abstracting data sharing between vehicles as the transaction process between nodes in the blockchain, and using consensus algorithms to verify and account for transactions, data sharing is recorded in the

TABLE IV
RESEARCH HISTORY OF TRADITIONAL IDENTITY AUTHENTICATION TECHNOLOGY

Year and researcher	Detailed research content
IEEE1609.2 Committee [26]	The PKI authentication technology is applied to secure communication in the IoVs for the first time.
2007, Hubaux et al [30]	The researchers proposed to obtain a large number of digital certificates and key pairs in the keystore with the help of the CA center. The sender of the information used the key pair to digitally sign and encrypted the information through the certificate, and the receiver verified the signature and decrypted the information through the public key in the corresponding key pair. However, a large number of certificates cause a waste of resources.
2010, Lu et al [27]	The researchers optimized the above PKI algorithm, and proposed better measures for identity authentication and message accuracy assurance. However, the problem is that when the certificates are revoked and updated, the process will be very cumbersome.
2011, Verma [31]	The researchers improved the certificate update and revocation time to further improve the authentication efficiency.
2012, Almeida et al [32]	This article proposed a PKI-based key distribution protocol for the IoVs, which has lower resource consumption than traditional PKI systems in performance. However, the OBU (On Board Unit) of each vehicle stores many different types of keys, which leads to troublesome certificate storage and revocation.
2016, Lo et al [33]	This article proposed a new identity signature method based on elliptic curve cryptosystem, and designed a conditional privacy protection authentication scheme without the need to pair and connect at the same time.
2017, Das et al [34]	In this article, the communication identity authentication technology of each end is implemented by embedding security chips in vehicles, roadside units and mobile terminals. However, the security protection of each end is not considered, which leads to the risk of information leakage. At the same time, the scheme does not consider the identity authentication scheme at each end, which leads to the risk of man-in-the-middle attack.
2017, Sun et al [35]	Sun et al. proposed a mutual authentication framework based on identity signature scheme as a conditional privacy protection, and the protocol used internal authentication and cross-region authentication to improve authentication efficiency.
2017, Maryam et al [36]	In order to reduce the computation of VANET (Vehicle ad hoc network) roadside units, Maryam et al. proposed an identity-based message authentication method using proxy vehicles. Through the elliptic curve discrete logarithm model of random Oracle model, it is proved that the underlying signature cannot be forged in adaptive selective message feeding and identity attack.
2018, U.S. Department of Transportation [37]	The U.S. Department of Transportation takes the lead in proposing a security credential management system to verify the workflow of the V2X-based system through small-scale testing and research.
2018, automobile manufacturers in European Union [ETSI TS 102 940-2018]	They proposed a Cooperative-ITS (intelligent transport systems) security certificate management system. By strengthening the management of the root certificate access mechanism in the architecture design scheme, the automobile manufacturers pay attention to technical limitations and system performance requirements in the case of full deployment of V2X functions

blockchain system in a distributed manner. Hash encryption is used to encrypt data to ensure data privacy and security [47], [48]. The chain structure and timestamp ensure the contextual coherence of vehicle data-sharing transactions and ensure the auditability of data sharing [49], [50]. Using the embedded virtual currency system, the blockchain can provide a good incentive mechanism for data sharing between vehicles, thereby ensuring the data quality of the sharer [51], [52], [53].

TABLE V
RESEARCH HISTORY OF ALLIANCE BLOCKCHAIN

Year and researcher	Detailed research content
2012, Lei et al [41]	This article proposed an edge computing system supporting blockchain, in which the alliance blockchain architecture is introduced to ensure the security of the results in the computing process.
2019, Li et al [42]	This article proposed a quality-of-service-oriented car-sharing strategy aimed at ensuring trust and fair payment in the sharing process.
2020, Yang et al [43]	This article proposed a lightweight directed acyclic graph blockchain to represent the attachment relationship of vehicle transactions, and used RSU to record and update the ledger to adapt to dynamic scenarios in the IoVs.
2020, Dwivedi et al [44]	Dwivedi et al. designed a block chain-based framework, using cloud servers to design vehicle authentication protocols and a consensus mechanism to verify transactions, thus solving the single point of failure and realizing the sharing of critical information among all road units.
2021, Baza et al [45]	Based on the research of Li et al., this article proposed a conditional privacy scheme to protect vehicle privacy.
2022, Anju Devi [46]	Anju Devi et al. proposed a blockchain-based on-board network trust framework to reduce security issues such as trust issues. By improving the two-stage auction algorithm and block selection method based on the discrete particle swarm algorithm, various security parameters are used to improve the reliability of
	blockchain-based data sharing in the IoVs.

More importantly, with the help of the smart contract technology, vehicles can adaptively customize appropriate sharing rules according to their own resource status and shared data characteristics, truly realize user autonomous data sharing, and reduce the pressure of user data management under the IoVs [54]. Although blockchain can provide security and autonomy of distributed users in the process of vehicle data sharing, it still needs to occupy more computing, storage, and communication resources due to its own flat architecture and global node consensus. How to simplify the complex blockchain system, serve the diverse data sharing needs under the IoVs, and promote it nationwide with a large number of national recognitions has become an urgent concern in the future.

3) Research Status of Privacy Protection Technology at Home and Abroad: The core building block of a vehicle security and privacy protection system is the Vehicle PKI, which provides the vehicle with multiple anonymous credentials known as pseudonyms These pseudonyms are used to ensure the authenticity and integrity of messages while protecting the privacy of vehicles (and passengers). There are many technical aspects involved in the pseudonym certificate system, and at present, many scholars are carrying out relevant research. The details are shown in Table VI.

The pseudonym authentication method distributes the number of pseudonym public/private keys and the corresponding public key certificates to the vehicles through the certification center, and realizes the authentication through the matching of the keys and the certificates. Accordingly, nodes that publish fake messages based on published keys can be tracked. However, the pseudonym mechanism needs to manage a large number of keys and pseudonym certificates, and the requirements for storage space and computing capacity also increase. On this basis, how to optimize the scheme of the pseudonym mechanism has also become a hot topic in recent years, as shown in Table VII.

Generally speaking, although the concepts related to the IoVs have appeared for many years, the privacy protection of the domestic IoVs system is still in its infancy, and the privacy protection technology based on pseudonyms is still in its initial trial stage. Based on the above research foundation, and on the basis of learning from foreign SCMS and CCMS systems, how to propose a brand-new pseudonym certificate identity authentication architecture for LTE-V2X based on the latest IEEE1609.2 protocol for IoVs communication. and apply it to the development and design of domestic IoVs security system to ensure confidentiality, integrity, privacy, and nonrepudiation in data transmission has become the focus of domestic research.

4) Other Security and Privacy Protection Technologies: Other hybrid or innovative methods are also gradually applied to the IoVs environment to ensure vehicle safety and privacy. The details are shown in Table VIII.

B. Secure and Encrypted Communication Technology in IoV

There are numbers of potential attack modes on vehicle communication and hard to be defended. Thus, the secure communication has drawn much attention for developers. Generally, the communication between vehicles and others can be divided into authentication, transmission, and protocol. The methods to achieve secure identity authentication have been discussed in Section V-A, and others will be

TABLE VI
RESEARCH HISTORY OF VEHICLE PRIVACY AND SAFETY PROTECTION

Year and researcher	Detailed research content
2013, W.Whyte et al [55]	This article proposed a vehicle security certificate management system based on the vehicle-to-vehicle communication system. This system is developed in cooperation with the U.S. Department of Transportation. Under the premise of ensuring the rationality of the system, the pseudonym certificate mechanism is proposed to provide security and privacy protection to the maximum extent. The disadvantage is that this system is only aimed at vehicle-to-vehicle communication and cannot prevent attacks from inside
2017, W.Whyte et al [37]	This article proposed a security credential management system for vehicle-to-terminal communication based on pseudonym mechanism, which is the main scheme to support the United States to establish a nationwide V2X-based PKI. However, this design is not suitable for the communication system of IoVs in China
2018, European Union [ETSI TS 102 940-2018]	The Cooperative-ITS security certificate management system proposed in the article is the main scheme to support the EU to establish a secure V2X system based on PKI. This scheme is based on the pseudonym mechanism and complies with the privacy protection requirements of general data protection regulation. However, this design is also not suitable for the communication system of IoVs in China
Bruno Fernandes et al [56]	A new simulation PKI system based on IEEE 1609.2 of the United States and ETSI ITS of the European Union was proposed, and a pseudonym mechanism was added on this basis. However, the communication delay needs to be verified by the authority
2019, Eric R. Verheul et al [57]	This article proposed a pseudonym certificate mechanism that is issued first and then activated. This scheme is a security improvement of SCMS (Security Credential Management System) and CCMS (Cooperative-ITS security Certificate Management System), and is ahead of the existing standard schemes of the European Union and the United States. However, it is still at the design level, and the actual performance verification is not ideal.

TABLE VII
RESEARCH HISTORY OF PSEUDONYM CERTIFICATE SCHEME OPTIMIZATION

Year and researcher	Detailed research content
2018, Gao et al [58]	This article proposed an anonymous authentication scheme based on proxy mobile IPv6. The scheme combines the group signature mechanism with the IoVs by using pseudonym, identity password mechanism and various authentication protocols. The experimental results show that the scheme is superior to the typical pseudonym authentication scheme in computing cost, communication cost and signal command,
2021, Chen Wang et al [59]	A novel lightweight authentication protocol was proposed, which can complete mutual identity authentication with the nearest roadside unit without repeating tedious calculations.
2021, Yuan et al [60]	This article proposed an optimized identity authentication protocol, which is composed of three stages and seven authentication processes to ensure the forward and backward security of the protocol.

presented as follow. The transmission risk can be attributed to the lack of encryption capability, where the insufficiently encrypted information is vulnerable to attack, resulting in the leakage, illegal tampering, and destruction of communication information. The protocol risk refers to the crack of the protocols or protocol-complying false messages, which may result in the information disclosure even illegal control of vehicles.

Encryption is a common security mechanism for data confidentiality protection, which is the main method to protect communication security. Classical encryption methods can be roughly divided into symmetric encryption, asymmetric encryption, and hash algorithm. In symmetric key encryption, the sender and receiver will use the same key to encrypt and decrypt data, which greatly enhances the encryption and decryption speed and has advantages in tackling large amounts of data. Unfortunately, the detection is also obvious that the private key management between sender and receiver has difficulty in protection. Typical symmetric encryption methods include AES and DES and others.

Asymmetric key encryption utilizes pair of keys to complete the encryption and decryption operations, respectively, which refers to a published public key for senders and the private key

TABLE VIII
RESEARCH HISTORY OF OTHER SECURITY AND PRIVACY PROTECTION TECHNOLOGIES

Year and researcher	Detailed research content
2019, Shimaa et al [61]	Shimaa et al. introduced a light-weight security protocol using a notion of hash-chain key generation to protect vehicle-to-vehicle communication. The proposed authentication protocol is used to protect the privacy of vehicle condition, and the security level is improved along with the reduction of the communication cost.
2020, Wang et al [62]	The article proposed a privacy-protecting authentication mechanism without any pseudonym, and realized the key exchange between electric vehicles and local aggregators in this mechanism. According to experimental results, the scheme can satisfy the requirements of anonymity, confidentiality, unlikability, non-repudiation, traceability and revocability.
2020, Zhang et al [63]	Zhang et al. proposed a combing 5G and privacy protection authentication framework on the fringes of computing technology. The authentication protocol includes the choice of edge to calculate vehicle certification.
2020, Reza Fotohi et al [64]	The article proposed a self-protection method of unmanned aerial vehicles based on an agent, which uses a multi-agent system like artificial immune system to detect the attacking unmanned aerial vehicle and select the safest path. Moreover, it uses routing request messages and self-protection methods to verify the evaluation results, which performs high accuracy.
2021, Ikram Ali et al [65]	The article designed a conditional privacy protection authentication scheme based on short signature by improving the bilinear pair to elliptic curve cryptosystem and changing the hash function mapped to point to the general hash function, along with allowing multiple signatures to be verified. The proposed scheme guarantees the security of the existence and unforgeability against adaptive selective message attack while significantly reducing the communication cost.

for users. Typical asymmetric key encryption methods consist of the RSA algorithm, DSA, ECC, and others. Although the asymmetric encryption scheme has been very mature, the lightweight IoVs communication encryption scheme based on asymmetric encryption still becomes one of the research focuses in recent years.

The Hash algorithm is a one-way algorithm, where users can generate a hash value for the target information through the hash algorithm, but it cannot be got the target information again through this hash value. The performances of tamper-proof and anonymous can be guaranteed according to the Hash algorithm. Similarly, in recent years, the application of the hash algorithm in the IoVs has gradually tended to be lightweight and efficient. In recent years, scholars at home and abroad have made a lot of research on the security and encrypted communication technology of the IoVs, as shown in Table IX.

Combined with the above technical characteristics, the actual security communication process of each end of the IoVs based on symmetric, asymmetric, hash algorithm, and identity authentication is shown in Fig. 8. The orange line represents hash encryption, the blue line represents asymmetric encryption, the green line represents symmetric encryption, and the black line represents secure transmission channel. The whole process uses the asymmetric key encryption technology and digital digest technology to ensure the identity authenticity of the communication parties [59]. The digital signature can not only ensure the integrity of the information sent, but also verify the identity of the sender. The sender extracts the digest from the sent data through the hash function and encrypts the digest with its own private key to form a digital

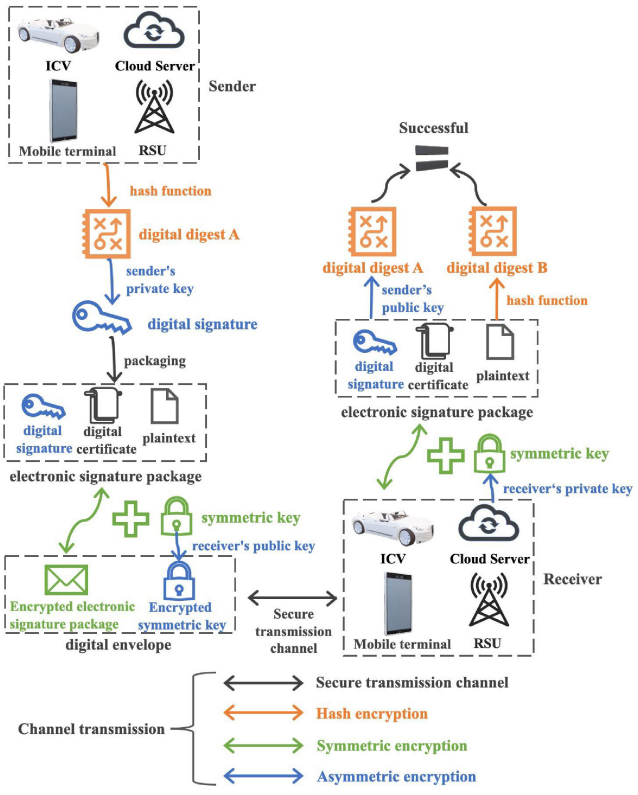

Fig. 8. Actual security communication process of each end of the IoVs.

signature. The digital signature, the sender's digital certificate, and plaintext are packaged to form an electronic signature package. The sender encrypts the electronic signature package with the symmetric key negotiated by both parties, and

TABLE IX
RESEARCH HISTORY OF SECURITY AND ENCRYPTED COMMUNICATION TECHNOLOGY

Year and researcher	Detailed research content
2016, Pedro J. Femandez et al [66]	The article reviewed the security problems in the V2X domain, analyzed the semantic gaps of existing security solutions, and outlined the possible problems that need to be solved.
2020, Song et al [67]	The article proposed a vehicle identity security authentication scheme based on elliptic curve cryptography. By dividing the vehicle network into multiple ellipses, the security authentication of vehicles outside the ellipse and the security monitoring of other vehicles can be realized. In the security authentication layer, this article proposed a deep learning scheme to achieve real-time security of the IoVs, thereby reducing the burden of accurate and dynamic security authentication in a high-speed driving environment.
2020, Castiglione et al [68]	Castiglione et al. studied the possibility of using lightweight block ciphers to protect on-board devices and the feasibility of using symmetric encryption algorithms to protect the information exchanged on the CAN bus.
2020, Limbasiya et al [69]	The article proposed an efficient and secure vehicle-to-vehicle data transmission protocol, which uses one-way hash functions to quickly send valuable information to the receiver, and has been proven to have good performance in terms of execution time and storage cost.
2020, Han et al [70]	Han et al. proposed an ICV communication architecture with security attribute isolation, which introduced attributes into ECUs to achieve authorized access between ECU (electronic control unit) nodes. By classifying the functional attributes of ECUs, a security attribute isolation communication architecture was presented.
2021, Amin et al[71]	Amin et al. integrated software definition network technology into the IoVs system for vehicle-to-vehicle communication, established a universal session key for secure communication, and carried out simulation verification through Scyther tool.

TABLE X
COMPARATIVE EVALUATION OF DIFFERENT ENCRYPTION METHOD

Categories of encryption	Typical algorithms	Calculating speed	Calculating cost	Security
Symmetric encryption	DES	★★★	★★	★
	3DES	★★	★	★★
	AES	★	★★★	★★★
Asymmetric encryption	RSA	★	★	★★★
	DSA	★	-	★★★
	ECC	★★	★★	★★★
Hash algorithm	-	★★	★★	★★
Block-chain-based encryption	-	★★	★	★★★
Hybrid encryption	RSA+AES	★	★	★★★

encrypts the symmetric key with the receiver's public key. The encrypted electronic signature package and the encrypted symmetric key form a digital envelope, which is sent to the receiver through a secure transmission channel. The receiver decrypts the encrypted symmetric key with the receiver's private key, and uses the decrypted symmetric key to obtain the electronic signature package. The public key of the digital certificate in the electronic signature package is used for signature authentication to obtain digital digest A. The receiver calculates the plaintext in electronic signature package through the same hash function to obtain the digest B and compares it with the digest A to determine whether the message has been modified to achieve an efficient identity authentication guarantee.

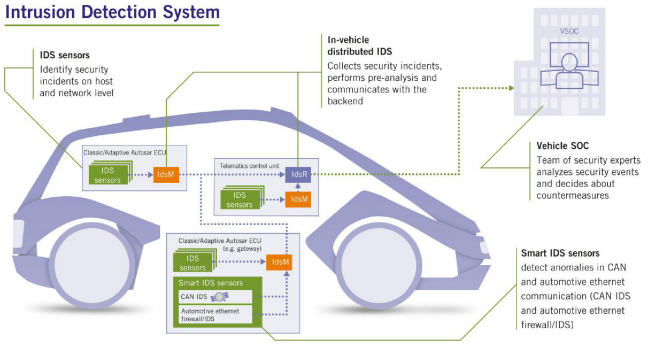

Fig. 9. Multicategories of distributed attack detection for vehicles, algorithm-based or nonalgorithm-based methods [74].

In summary, according to the experience and applying performances for different encryption methods, a comparative classification is presented as Table X.

VI. RESEARCH PROGRESS OF INTRUSION DETECTION

Different from identity authentication and communication encryption technologies, the intrusion detection methods are generally recognized as the active defense technology, where the defense system will proactively detect illegal invasion in the network, illustrated as Fig. 9. Owing to the innovation on electrical/electronic architecture, connected vehicles have been broadly promoted for better performances, whereas the openness of vehicles is also enlarged, where the categories and numbers of communication interfaces between vehicles and the environment have also greatly risen. Especially for

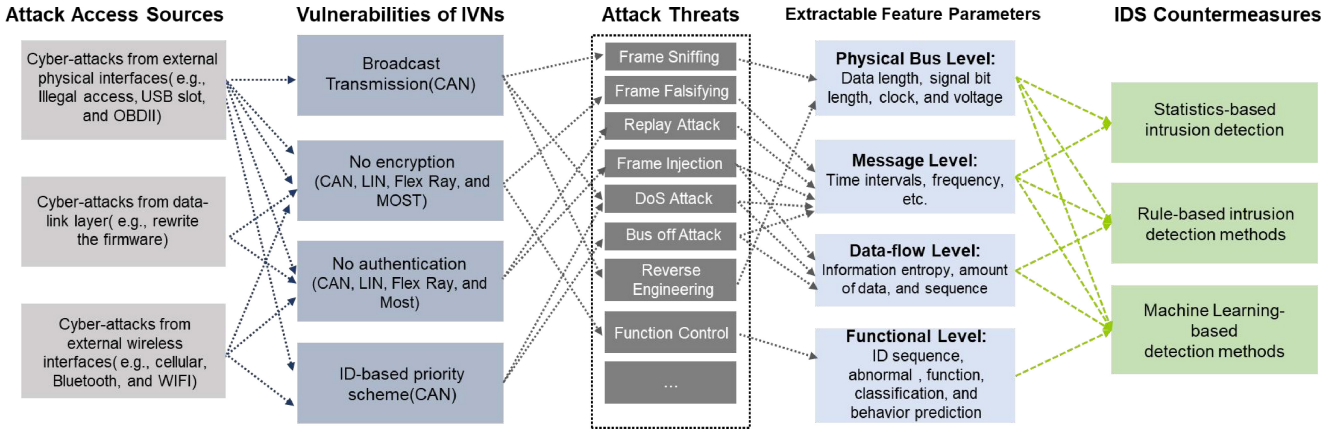

Fig. 10. Intrusion detection for in-vehicle networks and classification.

automotive vehicles, amounts of sensor networks have been attached for image detection and decision-making, where hundreds of ECUs are applied and millions of codes are attached, enlarging the potential attacking vulnerabilities [73]. Owing to the endless attack modes for vehicles, the intrusion detection is of crucial importance to guarantee the common security of communications.

Considering CAN is the most promoted in-vehicle network and the hijack of CAN has large hazards on vehicular cybersecurity, most of intrusion detection methods are concentrating on the protection of CAN, where the CAN messages are rather concise and simple but crucial with core data [75], [76]. Moreover, the gateway and Ethernet also have necessity for attaching intrusion detection methods. As the algorithms should be applied on embedded system in vehicles, the lightweight and real-time performances still should be considered. Generally, intrusion detection methods can be divided into statistics-based methods, rule-based methods, and machine-learning methods, as shown in Fig. 10. Wu et al. [77] delivered a survey of intrusion detection for in-vehicle networks, and the advantages and drawbacks are detailed summarized. Al-Jarrah et al. [78] provided a structured and comprehensive review of the state of the art of the intravehicle intrusion detection systems, and presented outstanding research challenges and gaps in intravehicle IDS research.

Statistics-based intrusion detection methods usually utilize the experienced model established by capturing messages to express random behaviors during communications [79]. Information theory is always applied for statistics according to probability methods, where the regular load of normal communication can be memorized to distinguish illegal intrusion. Such methods take the advantages of statistics without the knowledge of priori of the attack, and have the ability for updating and detecting the latest attack behavior in real time according to the previous data. Lightweight and simplicity contribute to the online applications without much calculating burden. Unfortunately, the disadvantages of these methods are also obvious where they have poor performance for complex information, and the setting of abnormal threshold also affects the performance of detection. Donmez et al. [80] studied an intrusion detection system for detecting anomalies in vehicular CAN bus traffic by analyzing message identifier sequences, which is established based on a heavy-duty truck over a period of several months. Bozdal et al. [81] introduced a wavelet-based approach to locating the behavior change in the CAN traffic by analyzing the CAN network's transmission pattern, which confirms the effectiveness of traditional methods. Yu and Wang [82] proposed a novel intrusion detection method based on the verification of network topology for CAN-FD, where external intruding devices can be reliably detected through a simple random walk based on network topology construction and subsequent verification. Groza and Murvay [83] proposed an intrusion detection mechanism based on bloom filtering, which can test frame periodicity based on message identifiers and parts of the data field which facilitates detection of potential replay or modification attacks. Ji et al. [84], [85] comprehensively analyzed the vulnerability of in-vehicle networks and investigated a unique detection method based on clock drift of ECUs. The results confirm that performances on both recognition accuracy and application range are compared with the method based on information entropy theory.

Rule-based intrusion detection methods take advantages of prior-known knowledge, also named rules, where the normal data and abnormal data have been artificially divided and applied to train algorithm for classification [86]. Finite state machine and support vector machine are two of typical methods on rule-based methods. The rule-based methods have satisfactory performance on achieving good classification effect and robustness, but the process of detection and decision making is rather complex. Moreover, the result often depends on the professional decision-making capacity and ability of experts, which has dependency on sufficient prior knowledges. Larson et al. [87] introduced the draft of CAN 2.0 and CAN 3.01 protocol open standards, and the applicability of specification-based detection is explored. D'Angelo et al. [88] introduced a cluster-based multidimensional approach for detecting attacks based on the clustering and data-driven anomaly detection algorithm, where the former one is used to learn the behavior of messages passing on the CAN bus and the latter one is used to perform real-time classification of messages for early alerting. Liang et al. [89] proposed a

hidden Markov model based on a filtering model for intrusion detection, where the state mode of each vehicle was modeled as a hidden Markov model, and the Baum–Welch algorithm was used through scheduling, filtering, and updating.

As the great progress of machine learning algorithm theory and calculating ability of calculation units, machine learning methods become hotspot for intrusion detection [90], [91], [92]. As classified according to functionality, data-driven intrusion detection methods consist of signature-based methods and anomaly based methods, where the former one has advantages on reporting the abnormal pattern signatures of known intrusions, and the latter one analyzes the network data to detect attacks according to the abnormal behaviors of network data [93]. Both two methods have their own defect. The main issue of the signature-based methods is the weakness for the intrusions from the novel and unknown attacks, and the anomaly based methods suffer from the high false alarm rate. As for specific algorithms, Bayesian network algorithm, neural network algorithm, heuristic search algorithm, and classification algorithm are all applied for detecting potential intrusion [94], [95], [96]. Moulahi et al. [97] summarized the current applied machine learning methods on intrusion detection, and delivered comparative study of the most common machine learning techniques. Xie et al. [98] introduced GANs for intrusion detection technique of CAN network, where the enhanced GAN is applied to generate usable attacked samples to supplement the training samples with higher accuracy. Tanksale [99] introduced LSTM networks to perform anomaly detection for CAN network, which focuses on the efficient design and testing of functions that are attack-resistant. Sun et al. [100] proposed a novel intrusion detection model named CNN-LSTM with the attention model, which extracts the abstract features of the signal values at each time step and feeds it into LSTM network to extract the time dependence. Nam et al. [101] introduced an intrusion detection model, which composes of two generative pretrained transformer networks in a bi-directional manner to allow both past and future CAN IDs to be used. Luo et al. [102] introduced a scheme which creatively incorporates identity authentication into key distribution without trusted third party, and the improvements help the security of communication in public networks. Unfortunately, although the machine learning method has been verified with better performances on solving various intrusion detection problems, it still suffers from the issue of online deployment which should be attributed to the limited calculating ability of online embedded systems. Li et al. [103] proposed an intrusion detection scheme based on transfer learning to solve the problems of traditional machine learning which needs amounts of data to achieve model training. Additionally, a cloud-assisted update scheme and a local update scheme were proposed for IoV. Kosmanos et al. [91] proposed a probabilistic cross-layer intrusion detection system based on machine learning, which use relative velocity position verification to compare the distance between two communication nodes observed by the on-board unit.

Apart from classical methods, more hybrid methods are also proposed for enhancing the performances on intrusion detection. Yang et al. [104] introduced a multitiered hybrid intrusion detection systems, which incorporates a signature-based intrusion detection systems and an anomaly based intrusion detection systems to detect both known and unknown attacks on vehicular networks, and the experimental results confirm the effectiveness on tackling the intrusion of CAN network. Liu et al. [105] proposed a blockchain and federated learning method for collaborative intrusion detection in vehicular edge computing, where blockchain is used for the storage and sharing of the training models. Experimental results validate the achievement of cooperative privacy preservation for vehicles while reducing communication overhead and computation cost. van Wyk et al. [106] developed an anomaly detection approach through combining a convolutional neural network with a well-established anomaly detection method, and Kalman filtering with a $\chi 2$-detector, to detect and identify anomalous behavior. The multicoupling method helps achieve satisfactory performances on intrusion detection in connected and automated vehicles. Sedjelmaci et al. [107] introduced a hierarchical detection and response system to detect malicious anomalies, including GPS spoofing attack's detection rule, jamming attack's detection rule, and false information dissemination attack's detection rule. The hierarchical detection methods do help improve the performances on detecting diverse attack threat according to the confirming experiments. Loukas et al. [108] introduced offloaded intrusion detection prototype to calculate and save energy of the detection algorithm, and results confirmed the application in online robotic vehicles. Jin et al. [109] proposed an intrusion detection method by combining oversampling, outlier detection, and metric learning. Particularly, the proposed method can achieve better performances in three special ways: 1) oversampling the minority classes; 2) using a new feature with the basis of imbalance ratio; and 3) reducing the outliers and rescaling original samples actively.

VII. Security Management and Standards

Considering that the main content of cybersecurity should consist of threat analysis, risking assessment, and attack defense, amounts of rules or references should be taken into consideration during the full-lifespan design. To standardize the process of designing cybersecurity and guarantee the safety of vehicle, serial standard systems have been established worldwide and help to improve the understanding of cybersecurity for researchers or developers. The standards normalize the general process, in which they deliver some typical threat defects or provide the full lifespan design process. Currently, the standardization research has been carried out in Europe, America, China, and other countries/organizations. In this section, the currently valid standards are summarized and accordingly, and the prospect of future standards settings is also discussed. The development history of standards for cybersecurity is as follows.

As cybersecurity is an associated technology with the development of communication methods, the importance of cybersecurity draws much attention after some accidents and discovered risks. In 2010, GPS remote intrusion incident

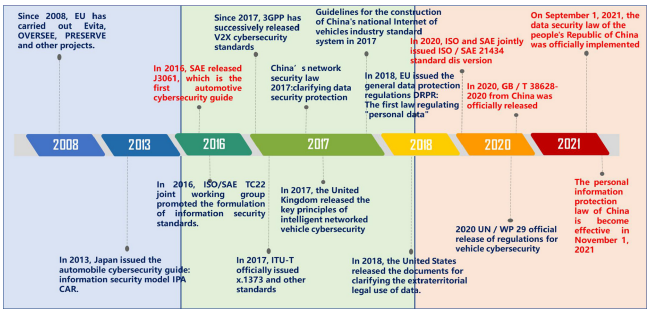

Fig. 11. General progress of the establishment of cybersecurity standard system.

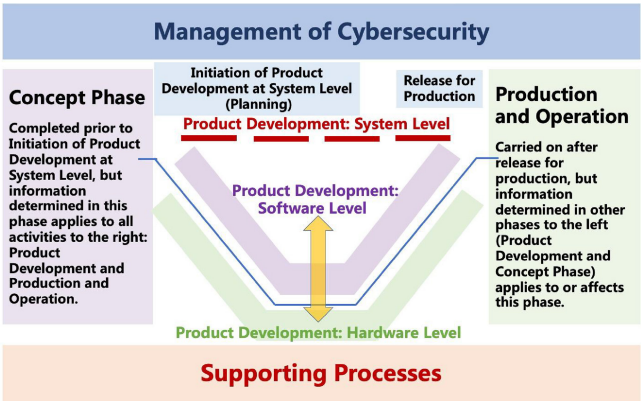

Fig. 12. Management of cybersecurity based on J3061.

occurred in Texas, and the University of Washington released a comprehensive analysis of vehicular attacking vulnerabilities. Such incidents enhance the importance of cybersecurity for Internet of Things, and then diverse efforts have been paid for investigating the protection of network, both for vehicles and others. Beginning from 2008, various projects are activated for exploring the potential solution of cybersecurity, including EVITAs, and PRESERVE in Europe.

Along with some research progress of cyber-attack analysis and protection methods, some guidance documents are proposed to provide some suggestions and mandatory provisions, which helps the improvement of cybersecurity for manufacturers and suppliers. In 2013, Japan introduced a guidance of vehicular cybersecurity, where the attack modes and methods are analyzed from the perspective of vehicle reliability, and a model named IPA CAR is introduced. Then, in 2016, SAE released the worldwide first vehicular cybersecurity guide-J3061, presented as Fig. 12, realizing a well-defined and well-structured vehicular cybersecurity management process. From 2016 to now, the research and application of cybersecurity technologies come into a new stage, where the detailed standard system, essential technologies and applications gradually become the important composition for the design of vehicles. Especially after 2020, more mandatory or recommended standards are delivered, including ISO/SAE 21434 and GB/T 38628-2020. Moreover, 3GPP and UN/WP 29 also delivers some standards and procedures, which helps the worldwide cybersecurity standard construction. More detailed information about the specific standards is discussed as follows. The general progress of the development of cybersecurity standard system is performed in Fig. 11.

A. SAE J3061

As the first guidance on cybersecurity for vehicle networks, SAE J3061 is of crucial importance on the full-lifespan design of vehicle networks, providing a significant accordance for the development of cybersecurity of vehicle network. Generally, the main content of SAE J3061 can be divided into two parts: 1) typical methodologies of TARA and 2) the development process.

1) Methodologies of threat analysis and risking assessment, including E-safety EVITA Method, HEAVENS, OCTAVE, TVRA, and attack trees method.
2) Development process, including the management, core cybersecurity engineering activities, and supporting process. The core cybersecurity engineering activities are of crucial importance which are directly associated with the developing process, and can be divided into concept phase, product development phase (consisting software, hardware, and system), and integration and test phase.

The V-model process proposed in J3061 is one of the characteristics and has become the common process during the design of ECUs. The V-model process is strict and orderly, and a stage can only be started with the completion of the previous one. Moreover, each development stage is corresponding to a testing stage, so as to effectively ensure the quality of software. Generally, the Complete V-model process consists of seven symmetrical stages: 1) requirements analysis; 2) architecture design; 3) unit design; 4) software development; 5) unit testing; 6) integration testing; and 7) system testing.

Apart from J3061, both SAE J3101 and J3138 also contribute to the development of cybersecurity. J3101 delivers the requirements of vehicular cybersecurity based on hardware protection, and J3138 address the Safety communication guide for connecting OBDII equipment.

B. ISO/SAE 21434

Owing to that J3061 is only the programmatic standard and cannot cover the whole process from concept design to product operation, ISO/SAE 21434 is established and finally released in August 2021, and the main framework is shown in Fig. 13. The design of ISO/SAE 21434 mainly aims at solving the defect of the structured process of vehicular cybersecurity design. During the standard setting process, ISO/SAE organizations and hundreds of vehicle manufacturers/suppliers involve and jointly design a framework of vehicular cybersecurity.

The main content of ISO/SAE 21434 can be divided into four parts.

1) Introduction and other necessary information. This part consists of chapters 1 to 4, including the scope of standards, referenced standards, terms and definitions, and precautions.

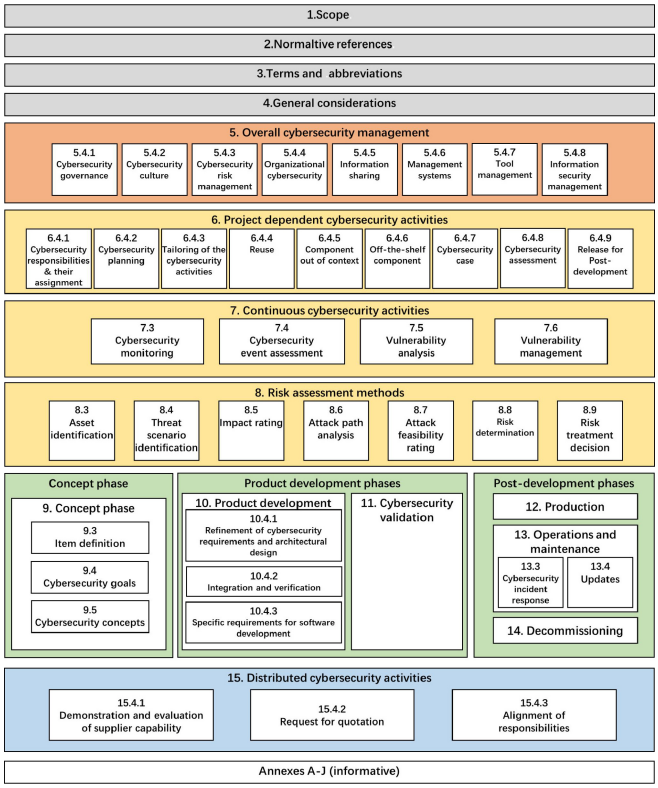

Fig. 13. Architecture of ISO 21434.

2) The general management requirements of vehicular cybersecurity from a macro perspective. This part consists of chapters 5 to 7, including overall network security management, project-based network security management, and continuous network security activities.
3) The general development requirements from TARA and concept design to operating and retirement, this part consists of chapters 8 to 14, including risk assessment, concept development, verification to production, operation and maintenance, and retirement.
4) Other requirements under distributed cooperative development mode. This part consists of chapter 15, including the requirements for asset identification, request quotation, and responsibility distribution.

V-process is the main development process for electric units, both for functional safety, SOTIF, and cybersecurity. According to ISO 21434, V-process helps improve the security of products from standardized process management, which has the tendency for integration of SOTIF and functional safety, shown in Fig. 14.

ISO/SAE 21434 introduces seven categories of common threats, and delivers the analysis and prevention method of potential system weakness. The details about typical threat and weakness are summarized as Table XI.

C. UN R155 and R156

Both SAE J3061 and ISO/SAE 21434 deliver the general process of vehicular cybersecurity design, but some technical problems still remain and should be tackled. Based on ISO/SAE 21434, UN R155 and R156 are established as

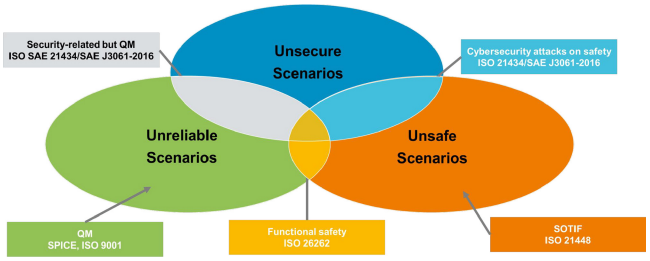

Fig. 14. General V-process of cybersecurity design and the integration with others.

TABLE XI
TYPICAL THREATS AND WEAKNESS FROM ISO 21434 (DIS)

Item	Threats	Typical weakness
1	external data servers	information cracking, internal attack, unauthorized access
2	remote communication function	code injection, relay attack
3	personnel mis-operation	operation without the established process
4	function upgrade	maliciously tampered upgrading package, OTA attacked during upgrade, DDoS
5	near-filed communication	USB, OBD, WIFI, NFC
6	vehicle data and codes	malicious access and tampering with data, system diagnostic data
7	weakness in functional design	encryption defect, code bug, data physical damage

statute to guarantee the vehicle with fundamental ability on cybersecurity.

R155 carries out CSMS certification and VTA evaluation and certification for OEM-specific models in specific countries. R156 carries out SUMS evaluation and certification for OEM-specific models in specific countries, as illustrated in Fig. 15. Further analysis of R155 and R156 is presented in Table XII.

VIII. RESEARCH PROGRESS OF INTRUSION DETECTION

As the promotion of connected vehicles, problems of cybersecurity still draw much attention for researchers. According to various investigations and data review, combined with the above research basis, automobile information security knowledge mapping is summarized as shown in Fig. 16. Although diverse efforts have been pained for improving the performances, there still some challenges on theories and applications to be solved. According to our engineering experience, four essential technologies should be researched based

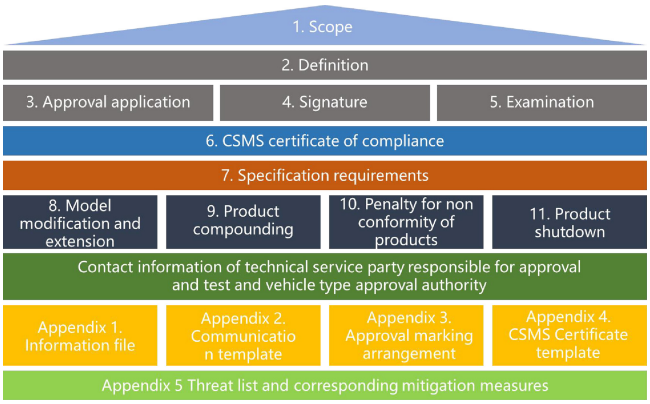

Fig. 15. Regulatory framework of R155.

TABLE XII
COMPARISON BETWEEN R155 AND R156

	R155	R156
Name	Regulations on network security and network security management system	Regulations on software upgrade and software upgrade management system
Document type	statute	statute
Applicable object	Passenger cars, commercial vehicles, buses, and autonomous vehicles above L3	Passenger cars, commercial vehicles and buses that allow software updates
Expected activation time	July 2022	July 2022
Partial detailed regulations	Should launch the cybersecurity management system.	Should ensure the safe transmission of software upgrade package.
	Should have management process of risk assessment, analysis and risk identification.	Should have restore function when the upgrading fails.
	Should have measures to detect and prevent cyber attacks	Should ensure safe upgrade procedures
	Should upload vehicle monitoring data to the appropriate regulatory authority	

on the evolution of electronic and electrical architecture for vehicles.

A. Cybersecurity Protection for Domain Electronic and Electrical Architecture

Domain electronic and electrical architecture has become the mainstream for ICVs. However, there still difficulties on cybersecurity protection for domain controllers and gateways in domain electronic and electrical architecture. Diverse essential technologies still remains questionable, including network isolation, intrusion detection security upgrade, and so on. Before the wide promotion of domain electronic and electrical architecture, it is urgent for establishing the all-round safety protection technology schemes, and the following points may help improve cybersecurity.

1) Research the implementation of network isolation technology on vehicle gateway, domain controller, and communication protocols, especially for CAN-FD and Ethernet.
2) Apply authentication and encryption based on hardware encryption module.
3) Deliver a cybersecurity algorithm application platform with unified software and hardware implementation, with the adaptation to operational scenarios. Research on the intrusion detection technology for network traffic across protocol layer, and providing predefined early warning, log recording, and emergency response algorithm.

B. Testing Platform of Cybersecurity for Intelligent Networked Vehicles

Although diverse cybersecurity methods have been proposed and validated, it still remains deficiency for testing platforms for intelligent networked vehicles. Both SAE J3061, ISO/21434 and WP/29 mention that it is necessary for testing the penetration performances, while it is still unclear how to carry out the experiments, and the associated tools or platform is remaining blank [111]. In the consideration of amounts of actual scenarios which increases the difficulty for testing, and the operational efficiency of the cybersecurity algorithm is questionable. The construction of the testing platform may be engineering, but there are still some suggestions as follows.

1) Research the network vulnerability mining platform for intelligent networked vehicles and surrounding ecology, including white hat management, security supervision, vulnerability submission, and verification.
2) Based on vulnerability analysis, research the integration of multisource vulnerability information and evaluation technology.
3) Research the cybersecurity testing method integrating the physical characteristics of ICV, including static code detection, dynamic attack testing, data computing security, and trusted access verification.
4) Research automatic attack load generation technology.
5) Formulate unified, modular, service-oriented, scalable and scenario-oriented standards, specifications, and processes related to the cybersecurity testing. Develop a cybersecurity testing platform for ICV, including network topology analysis, dynamic/static code detection and penetration test, data security and credibility verification, and implementing driving scenarios.

C. Lightweight Protection Method of Heterogeneous Network for Intelligent Networked Vehicles

As the promotion of ICVs, the domain electronic and electrical architecture has become more popular and necessary owing to better communication capability and accessibility.

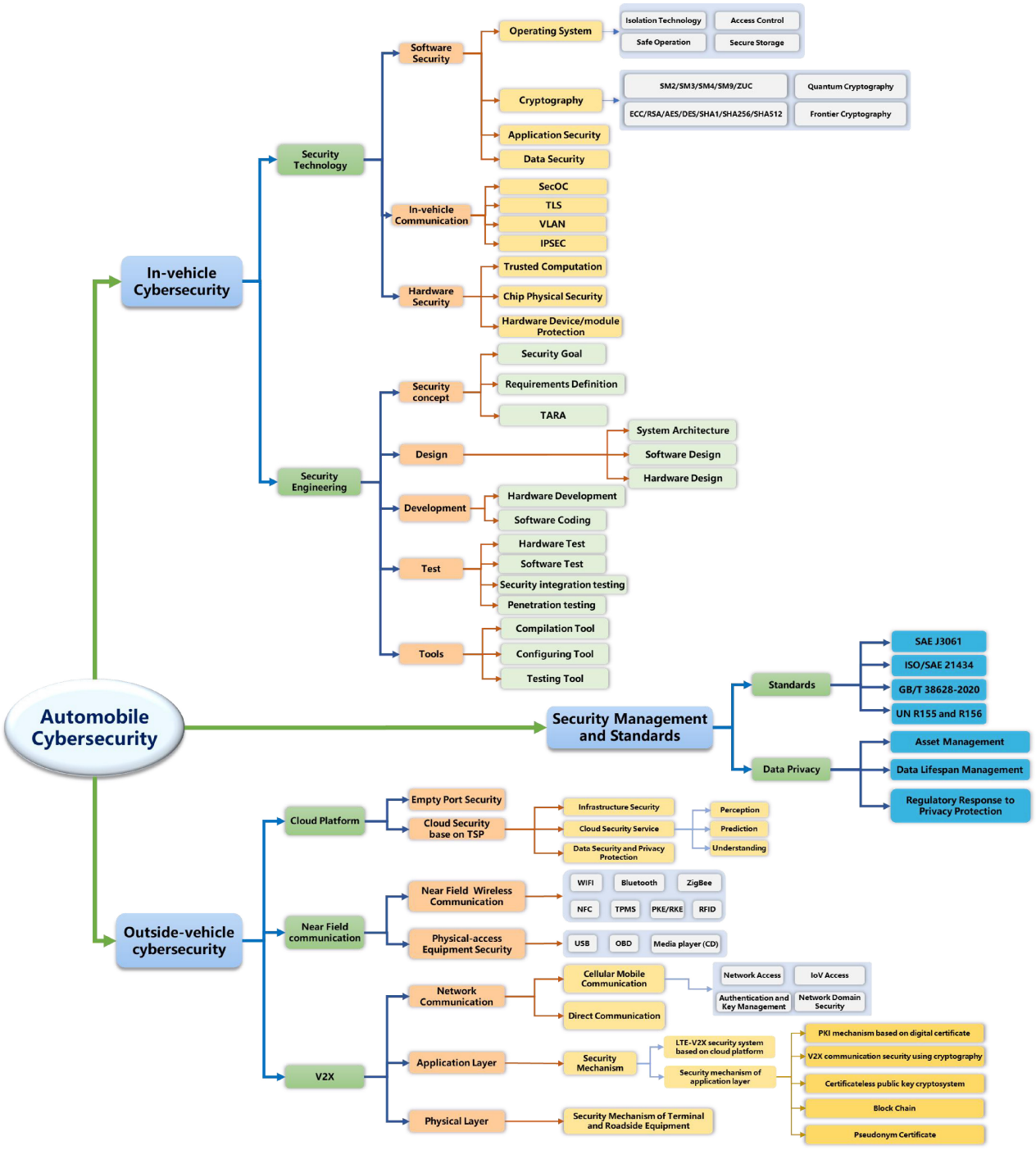

Fig. 16. Knowledge mapping of automobile information security [110].

However, most of the current cybersecurity protection methods are established for distributed electronic and electrical architecture, and the serious lack of on-board protection method in vehicle layered security defense has drawn much attention. The main courses of unavailability for traditional solutions can be attributed to limited computing, storage resources, and cost, which results of efficiency problems and enlarge the importance of the lightweight identity authentication, message encryption, and decryption and firewall technology. The following hotspots may help improve the online cybersecurity implementation.

1) The propose a lightweight security algorithm for embedded ECU is necessary and should be solved in the future, which can include the lightweight identity authentication method and message encryption algorithm for MCU and MPU.
2) Research the lightweight of message load for delivery/transmission, and the lightweight of the security system resource occupation.
3) Deliver the deployment scheme of the lightweight method based on physical isolation, logical isolation, and virtualization technology.

IX. Summary

Along with the promotion of ICVs, the problems of network attacks have rapidly increased in the past ten years, and the cybersecurity has drawn much attention for worldwide researchers and manufactures. Unfortunately, although remarkable progress has been achieved both in technics and standard, there still remains vague for designing vehicular cybersecurity. In this article, the general technical profile of cybersecurity for ICVs has been reviewed, including TARA, static defense, and intrusion detection. Moreover, the general procedure and management for designing the vehicular cybersecurity are also summarized according to a current standard system, including ISO 21434 and R155.

This article highlights the comprehensive reviews on cybersecurity technical system. Considering that the TARA is the fundamental basement for designing the system cybersecurity which provides the common vulnerabilities inside the communication methods, this article first summarizes the potential attacking vulnerabilities for ICVs, within the in-vehicle network and mobile networks. Then, the identity authentication methods and secure communication methods are introduced from static defense, where the conventional and novel intelligent approaches are provided. Next, the intrusion detection is introduced as active methods, which performs a large contribution on solving the problems of out-vehicle attacks. Finally, the current valid standard system for cybersecurity is also demonstrated, where both the development history and current system are generally introduced. Associated with our experiences on engineering, some perspective suggestions are provided at the end of this article, and hopes to help researchers improve the theoretical and technical methods on cybersecurity.

As the promotion of ICVs and other vehicles, the cybersecurity will perform significance for protecting vehicular safety, and it has risen to a new level equal to functional safety. We hope that the review of research progress on technical method may help researchers and manufactures, and delivers the potential direction for future cybersecurity development.

References

[1] M. Safwat, A. Elgammal, E. G. AbdAllah, and M. A. Azer, "Survey and taxonomy of information-centric vehicular networking security attacks," *Ad Hoc Netw.*, vol. 124, Jan. 2022, Art. no. 102696.

[2] Y. Xie, Y. Zhou, J. Xu, J. Zhou, X. Chen, and F. Xiao, "Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges," *Softw. Pract. Exp.*, vol. 51, no. 11, pp. 2108–2127, 2021.

[3] M. Dibaei et al., "Attacks and defences on intelligent connected vehicles: A survey," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 399–421, 2020.

[4] D. Zhang, Y.-P. Shen, S.-Q. Zhou, X.-W. Dong, and L. Yu, "Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 11, pp. 7269–7278, Nov. 2021.

[5] S. Ohira, A. K. Desta, I. Arai, H. Inoue, and K. Fujikawa, "Normal and malicious sliding windows similarity analysis method for fast and accurate IDS against DoS attacks on in-vehicle networks," *IEEE Access*, vol. 8, pp. 42422–42435, 2020.

[6] J. Li, Z. Xue, C. Li, and M. Liu, "RTED-SD: A real-time edge detection scheme for Sybil DDoS in the Internet of Vehicles," *IEEE Access*, vol. 9, pp. 11296–11305, 2021.

[7] Y. Ma, Z. Nie, S. Hu, Z. Li, R. Malekian, and M. Sotelo, "Fault detection filter and controller co-design for unmanned surface vehicles under DoS attacks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1422–1434, Mar. 2021.

[8] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[9] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[10] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[11] R. Shrestha, S. Djuraev, and S. Y. Nam, "Sybil attack detection in vehicular network based on received signal strength," presented at the Int. Conf. Connected Veh. Expo (ICCVE), Vienna, Austria, 2014, pp. 745–746.

[12] P. Faruki et al., "Android Security: A survey of issues, malware penetration, and defenses," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 998–1022, 2nd Quart., 2015.

[13] C. S. Ramaiah, S. Z. Hussain, S. A. Hussain, and Y. A. Balushi, "Smart vehicle security system for defending against collabrative attacks by malware," presented at the 3rd MEC Int. Conf. Big Data Smart City (ICBDSC), Muscat, Oman, 2016, pp. 1–5.

[14] J. F. Roscoe, O. Baxandall, and R. Hercock, "Simulation of malware propagation and effects in connected and autonomous vehicles," presented at the Int. Conf. Comput., Electron. Commun. Eng. (iCCECE), Southend, U.K., 2020.

[15] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 162401–162437, 2021.

[16] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[17] A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," *IEEE Trans. Veh. Technol.*, vol. 54, no. 1, pp. 41–50, Jan. 2005.

[18] S. van de Beek and F. Leferink, "Vulnerability of remote keyless-entry systems against pulsed electromagnetic interference and possible improvements," *IEEE Trans. Electromagn. Compat.*, vol. 58, no. 4, pp. 1259–1265, Aug. 2016.

[19] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.

[20] M. M. Rana, "Attack resilient wireless sensor networks for smart electric vehicles," *IEEE Sens. Lett.*, vol. 1, no. 2, pp. 1–4, Apr. 2017.

[21] M. Cheah, S. A. Shaikh, O. Haas, and A. Ruddle, "Towards a systematic security evaluation of the automotive Bluetooth interface," *Veh. Commun.*, vol. 9, pp. 8–18, Jul. 2017.

[22] A. Dardanelli et al., "A security layer for smartphone-to-vehicle communication Over Bluetooth," *IEEE Embedded Syst. Lett.*, vol. 5, no. 3, pp. 34–37, Sep. 2013.

[23] X. He, E. Hashemi, and K. H. Johansson, "Distributed control under compromised measurements: Resilient estimation, attack detection, and vehicle platooning," *Automatica*, vol. 134, Dec. 2021, Art. no. 109953.

[24] P. F. De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for can: Hindering cyber-attacks with a low-cost platform," *IEEE Access*, vol. 9, pp. 166855–166869, 2021.

[25] M. A. Rahman, M. S. Hossain, M. M. Rashid, S. Barnes, and E. Hassanain, "IoEV-Chain: A 5G-based secure inter-connected mobility framework for the Internet of electric vehicles," *IEEE Netw.*, vol. 34, no. 5, pp. 190–197, Sep./Oct. 2020.

[26] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," presented at the VTC Spring IEEE Veh. Technol. Conf., Singapore, 2008.

[27] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[28] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[29] J. Cao et al., "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.
[30] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.
[31] B. K. Chaurasia and S. Verma, "Infrastructure based authentication in VANETs," *Int. J. Multimedia Ubiquitous Eng.*, vol. 6, no. 2, pp. 41–54, 2011.
[32] J. Almeida, S. Shintre, M. Boban, and J. Barros, "Probabilistic key distribution in vehicular networks with infrastructure support," presented at the IEEE Global Commun. Conf., 2012.
[33] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.
[34] A. Abdallah and X. S. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615–2629, Mar. 2017.
[35] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.
[36] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5409–5423, Jun. 2018.
[37] B. Brecht et al., "A security credential management system for V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3850–3871, Dec. 2018.
[38] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by Internet of Vehicles," *IEEE Access*, vol. 8, pp. 117593–117614, 2020.
[39] C. Qiu, F. R. Yu, F. Xu, H. Yao, and C. Zhao, "Blockchain-based distributed software-defined vehicular networks via deep Q-learning," presented at the Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl., 2018.
[40] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Permissioned blockchain and deep reinforcement learning for content caching in vehicular edge computing and networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4312–4324, Apr. 2020.
[41] L. Lei, Z. Zhangdui, L. Chuang, and S. Xuemin, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96–104, Jun. 2012.
[42] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.
[43] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A lightweight DAG-based blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5749–5759, Jun. 2020.
[44] S. K. Dwivedi, R. Amin, S. Vollala, and R. Chaudhry, "Blockchain-based secured event-information sharing protocol in Internet of Vehicles for smart cities," *Comput. Elect. Eng.*, vol. 86, Sep. 2020, Art. no. 106719.
[45] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr.–Jun. 2021.
[46] A. Devi, G. Rathee, and H. Saini, "Secure blockchain-Internet of Vehicles (B-IoV) mechanism using DPSO and M-ITA algorithms," *J. Inf. Security Appl.*, vol. 64, Feb. 2022, Art. no. 103094.
[47] K. Kim, T. Kim, and I. Y. Jung, "Blockchain-based information sharing between smart vehicles for safe driving," presented at the IEEE 91st Veh. Technol. Conf., 2020.
[48] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of using blockchain to protect the privacy of drone big data," *IEEE Netw.*, vol. 35, no. 1, pp. 44–49, Jan./Feb. 2021.
[49] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1189–1201, Apr.–Jun. 2021.
[50] A. Davenport and S. Shetty, "Air gapped wallet schemes and private key leakage in permissioned blockchain platforms," presented at the IEEE Int. Conf. Blockchain (Blockchain), 2019.
[51] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1625–1640, Mar. 2020.
[52] A. Devi, G. Rathee, and H. Saini, "Using optimization and auction approach: Security provided to vehicle network through blockchain technology," presented at the 6th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC), 2020.
[53] Y. Wang, Z. Su, Q. Xu, R. Li, and T. H. Luan, "Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue," presented at the IEEE INFOCOM Conf. Comput. Commun., 2021.
[54] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, "Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3681–3692, May 2020.
[55] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," presented at the IEEE Veh. Netw. Conf., 2013.
[56] B. Fernandes, J. Rufino, M. Alam, and J. Ferreira, "Implementation and analysis of IEEE and ETSI security standards for vehicular communications," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 469–478, 2018.
[57] E. Verheul, C. Hicks, and F. D. Garcia, "IFAL: Issue first activate later certificates for V2X," presented at the IEEE Eur. Symp. Security Privacy (EuroS&P), 2019.
[58] T. Gao, X. Deng, N. Guo, and X. Wang, "An anonymous authentication scheme based on PMIPv6 for VANETs," *IEEE Access*, vol. 6, pp. 14686–14698, 2018.
[59] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14248–14257, Sep. 2021.
[60] Y. Lei, L. Zeng, Y.-X. Li, M.-X. Wang, and H. Qin, "A lightweight authentication protocol for UAV networks based on security and computational resource optimization," *IEEE Access*, vol. 9, pp. 53769–53785, 2021.
[61] S. A. A. Hakeem, M. A. Abd El-Gawad, and H. Kim, "A decentralized lightweight authentication and privacy protocol for vehicular networks," *IEEE Access*, vol. 7, pp. 119689–119705, 2019.
[62] Q. Wang, M. Ou, Y. Yang, and Z. Duan, "Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks," *IEEE Access*, vol. 8, pp. 217592–217602, 2020.
[63] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020.
[64] R. Fotohi, E. Nazemi, and F. S. Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100267.
[65] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1278–1291, Feb. 2021.
[66] P. J. Fernandez, J. Santa, F. Bernal, and A. F. Skarmeta, "Securing vehicular IPv6 communications," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 46–58, Jan./Feb. 2016.
[67] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: A fog-based identity authentication scheme for privacy preservation in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5403–5415, May 2020.
[68] A. Castiglione, F. Palmieri, F. Colace, M. Lombardi, D. Santaniello, and G. D'Aniello, "Securing the Internet of Vehicles through lightweight block ciphers," *Pattern Recognit. Lett.*, vol. 135, pp. 264–270, Jul. 2020.
[69] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," *IEEE Syst. J.*, vol. 14, no. 1, pp. 520–529, Mar. 2020.
[70] M. Han, A. Wan, F. Zhang, and S. Ma, "An attribute-isolated secure communication architecture for intelligent connected vehicles," *IEEE Trans. Intell. Veh.*, vol. 5, no. 4, pp. 545–555, Dec. 2020.
[71] R. Amin, I. Pali, and V. Sureshkumar, "Software-defined network enabled vehicle to vehicle secured data transmission protocol in VANETs," *J. Inf. Security Appl.*, vol. 58, May 2021, Art. no. 102729.
[72] R. W. van der Heijden, S. Dietzel, T. Leinmuller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 1st Quart., 2019.

[73] W. Wang, H. Huang, Q. Li, F. He, and C. Sha, "Generalized intrusion detection mechanism for empowered intruders in wireless sensor networks," *IEEE Access*, vol. 8, pp. 25170–25183, 2020.

[74] E. Knauel, J. Gramm, and J. Holle, "Automotive cybersecurity—Efficient risk management for the entire life cycle of vehicles," *ATZelectronics Worldwide*, vol. 15, pp. 18–22, Nov. 2020.

[75] O. Avatefipour et al., "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127580–127592, 2019.

[76] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.

[77] W. Wu et al., "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.

[78] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

[79] R. Mitchell and C. Ing-Ray, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 5, pp. 593–604, May 2014.

[80] T. C. M. Donmez, "Anomaly detection in vehicular CAN bus using message identifier sequences," *IEEE Access*, vol. 9, pp. 136243–136252, 2021.

[81] M. Bozdal, M. Samie, and I. K. Jennions, "WINDS: A wavelet-based intrusion detection system for controller area network (CAN)," *IEEE Access*, vol. 9, pp. 58621–58633, 2021.

[82] T. Yu and X. Wang, "Topology verification enabled intrusion detection for in-vehicle CAN-FD networks," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 227–230, Jan. 2020.

[83] B. Groza and P.-S. Murvay, "Efficient intrusion detection with bloom filtering in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 1037–1051, 2019.

[84] H. Ji, Y. Wang, H. Qin, X. Wu, and G. Yu, "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ECUs," *IEEE Access*, vol. 6, pp. 49375–49384, 2018.

[85] H. Ji, Y. Wang, H. Qin, Y. Wang, and H. Li, "Comparative performance evaluation of intrusion detection methods for in-vehicle networks," *IEEE Access*, vol. 6, pp. 37523–37532, 2018.

[86] J. Ning, J. Wang, J. Liu, and N. Kato, "Attacker identification and intrusion detection for in-vehicle networks," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1927–1930, Nov. 2019.

[87] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," presented at the IEEE Intell. Veh. Symp., Eindhoven, The Netherlands, 2008.

[88] G. D'Angelo, A. Castiglione, and F. Palmieri, "A cluster-based multidimensional approach for detecting attacks on connected vehicles," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12518–12527, Aug. 2021.

[89] J. Liang, M. Ma, M. Sadiq, and K.-H. Yeung, "A filter model for intrusion detection system in vehicle ad hoc networks: A hidden Markov methodology," *Knowl.-Based Syst.*, vol. 163, pp. 611–623, Jan. 2019.

[90] Z. Cao et al., "An effective railway intrusion detection method using dynamic intrusion region and lightweight neural network," *Measurement*, vol. 191, Mar. 2022, Art. no. 110564.

[91] D. Kosmanos et al., "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, Mar. 2020, Art. no. 100013.

[92] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101974.

[93] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-driven intrusion detection for intelligent Internet of Vehicles: A deep convolutional neural network-based method," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2219–2230, Oct.–Dec. 2020.

[94] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," *IEEE Access*, vol. 8, pp. 185489–185502, 2020.

[95] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.

[96] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 5, pp. 1143–1153, May 2017.

[97] T. Moulahi, S. Zidi, A. Alabdulatif, and M. Atiquzzaman, "Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus," *IEEE Access*, vol. 9, pp. 99595–99605, 2021.

[98] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021.

[99] V. Tanksale, "Design of anomaly detection functions for controller area networks," *IEEE Open J. Intell. Transp. Syst.*, vol. 2, pp. 312–321, 2021.

[100] H. Sun, M. Chen, J. Weng, Z. Liu, and G. Geng, "Anomaly detection for in-vehicle network using CNN-LSTM with attention mechanism," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10880–10893, Oct. 2021.

[101] M. Nam, S. Park, and D. S. Kim, "Intrusion detection method using bi-directional GPT for in-vehicle controller area networks," *IEEE Access*, vol. 9, pp. 124931–124944, 2021.

[102] J. Luo, S. Yao, J. Zhang, W. Xu, Y. He, and M. Zhang, "A secure and anonymous communication scheme for charging information in vehicle-to-grid," *IEEE Access*, vol. 8, pp. 126733–126742, 2020.

[103] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of vehicles," *Inf. Sci.*, vol. 547, pp. 119–135, Feb. 2021.

[104] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, Jan. 2022.

[105] H. Liu et al., "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021.

[106] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1264–1276, Mar. 2020.

[107] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.

[108] G. Loukas, Y. Yoon, G. Sakellari, T. Vuong, and R. Heartfield, "Computation offloading of a vehicle's continuous intrusion detection workload for energy efficiency and performance," *Simulat. Model. Pract. Theory*, vol. 73, pp. 83–94, Apr. 2017.

[109] F. Jin, M. Chen, W. Zhang, Y. Yuan, and S. Wang, "Intrusion detection on Internet of Vehicles via combining log-ratio oversampling, outlier detection and metric learning," *Inf. Sci.*, vol. 579, pp. 814–831, Nov. 2021.

[110] *Automotive Information Security Knowledge Competency Panorama (2020)*, Automotive Inf. Security Org., Washington, DC, USA, 2021.

[111] F. Luo, X. Zhang, and S. Hou, "Research on cybersecurity testing for in-vehicle network," presented at the Int. Conf. Intell. Technol. Embedded Syst. (ICITES), 2021.