AN IMPROVED FRAMEWORK FOR C-V2X SYSTEMS WITH DATA INTEGRATION AND IDENTITY-BASED AUTHENTICATION

Rui Huang

Lianyungang Jierui Electronics Co., Ltd.,
city: Lianyungang, zip code: 222061, China

ABSTRACT

Current trends of autonomous driving apply the hybrid use of on-vehicle and roadside smart devices to perform collaborative data sensing and computing, so as to achieve a comprehensive and stable decision making. The integrated system is usually named as C-V2X. However, several challenges have significantly hindered the development and adoption of such systems. For example, the difficulty of accessing multiple data protocols of multiple devices at the bottom layer, and the centralized deployment of computing arithmetic power. Therefore, this work proposes a novel framework for the design of C-V2X systems. First, a highly aggregated architecture is designed with fully integration with multiple traffic data resources. Then a multi-level information fusion model is designed based on multi-sensors in vehicle-road coordination. The model can fit different detection environments, detection mechanisms, and time frames. Finally, a lightweight and efficient identity-based authentication method is given. The method can realize bidirectional authentication between end devices and edge gateways.

KEYWORDS

Network Protocols, Wireless Network, Mobile Network, Virus, Worms & Trojon.

1. INTRODUCTION

Today's technology has made important progress in many fields and shows a cross-fertilization trend. In the integration of transportation systems, with the development of the Internet, a new generation of information technology represented by cloud computing, Internet of Things technology, intelligent sensing / big data mining technology is effectively integrated and applied to rail transportation, road transportation, water transportation and air transportation systems. This makes the integration of transportation systems show the trend of intelligence, networking and collaboration. At present, most of the world's major autonomous driving technology routes are solutions with the car as the intelligent body, i.e., the car itself is made into a mobile intelligent body. Such a solution has high technical requirements, and the system equipment is extremely expensive. This leads to its safety, reliability improvement of the input and output is relatively low as well as autonomous driving is difficult to be widely promoted in a short period of time, thus making it difficult to obtain the benefits of traffic efficiency and traffic safety. In addition, intelligent transportation application scenarios are complex and diverse. In the actual application process, a single public cloud or private cloud solutions are often difficult to meet the needs of intelligent transportation development.

David C. Wyld et al. (Eds): NLPTA, EDU, DSA, IoTE, VLSI, DPPR, ACITY, AIAA, CNDC - 2021
pp. 57-73, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111905

Against the background of the difficulty of enhancing single-vehicle autonomous driving technology and the increasing complexity of the traffic environment, autonomous driving increasingly relies on the development of intelligent road facilities [1]. C-V2X [2] vehicle-road cooperative system can realize different degrees of information interaction and sharing between vehicles and vehicles, vehicles and people, and vehicles and road traffic facilities by building roadside systems with sensing, fusion, path planning, control and communication functions, and vehicles only need to deploy low-cost on-board equipment. It is possible to have autonomous driving capability. This can lower the threshold of self-driving vehicles and shorten the time to realize large-scale autonomous driving, shortening the event of large-scale autonomous driving popularity by 10 to 15 years. Vehicle-road cooperative autonomous driving systems also consider different levels of cooperative optimization of vehicle-road distribution to efficiently and cooperatively perform vehicle and road sensing, prediction, decision making, and control functions.

Vehicle-road cooperative autonomous driving is a low-to-high development process, which mainly includes the following development stages

(1) Information interaction and collaboration, realizing information interaction and sharing between vehicles and roads. Using advanced wireless communication and new generation Internet and other technologies to realize dynamic real-time information interaction and sharing between vehicles and vehicles, vehicles and roads in all aspects, which is mainly reflected in the level of collection and fusion of environmental information by system participants.

(2) Perception prediction decision collaboration, on the basis of (1), to achieve vehicle-road collaboration perception and prediction decision function. With the saturation of vehicle technology progress space and the increase of traffic environment complexity, in addition to real-time information interaction and sharing with the help of communication technology, the realization of autonomous driving perception and decision making also depends on intelligent road facilities and in-vehicle equipment such as radar and cameras. The above facilities and equipment are used to realize the sensing of dynamic traffic environment information in all-time and space, as well as the subsequent functions of data fusion, state prediction and behavioral decision-making. This is mainly reflected in the comprehensive collection of environmental information by system participants and the driving decision level.

(3) Realize advanced vehicle-road cooperative control function. On the basis of (2), it can also realize the vehicle-road cooperative automatic driving control function, and then complete the full coverage of the whole key steps of automatic driving. For example, it can be applied in limited scenarios such as highway lanes, urban expressways and automatic parking, which mainly reflects the comprehensive collection of environmental information by system participants, driving decision and control execution at the whole level.

(4) The vehicle and the road achieve comprehensive synergy, i.e. complete system functions such as vehicle-road cooperative sensing, vehicle-road cooperative prediction and decision making, and vehicle-road cooperative control integration. It further enhances the intelligent role of road infrastructure, so as to realize the comprehensive intelligent collaboration and cooperation between vehicles and roads, i.e., to realize the system integration functions of vehicle-road cooperative sensing, vehicle-road cooperative prediction and decision making, and vehicle-road cooperative control in any scenario. Vehicle-road synergy improves the commercialization of vehicle autonomous driving and forms an integrated development path in which vehicles and roads jointly promote the realization of autonomous driving.

Baidu has brought together autonomous driving and road-vehicle collaboration. For vehicle intelligence, Baidu has launched and open-sourced the Apollo platform [3], which has attracted a large number of developers and manufacturers and has now been updated to Apollo 6.0. Baidu has launched the "ACE Traffic Engine" [4] to build a modern intelligent transportation system with real-time sensing, instantaneous response and intelligent decision-making. Currently, Baidu's "ACE Traffic Engine" integrated solution [5] has been put into practice in nearly 20 cities, including Beijing, Changsha and Baoding. Compared with Baidu, Alibaba is more concerned about the control platform of vehicle-road coordination. Its proposed ET City Brain [6], together with AliOS on the vehicle side, provides global analysis and scheduling at the city level, and has already achieved milestones. In Beijing, through signal timing optimization, the average delay of motor vehicles through intersections has dropped by 6% and the parking ratio has been reduced by 3%. In Shanghai, the prediction accuracy of the neural network model built for the traffic status of the north-south elevated sections has improved by 10% [7].

Vehicle-road cooperative intelligent transportation faces many technical challenges and development bottlenecks, such as the difficulty of accessing multiple data protocols of multiple devices at the bottom layer, and the centralized deployment of computing arithmetic power cannot meet the demand for computing latency of intelligent applications. In the intelligent vehicle-road cooperative system, there are many kinds of sensors and wide distribution, and the in-vehicle sensing system is still in high-speed motion, and the detection environment, detection mechanism, time base, information characteristics and description methods of sensors are different. The problem of fusion of sensor information [8] from multiple locations prevails. In the face of ultra-intensive data volume, as well as the status quo of low tolerance to time delays, existing methods are difficult to play the advantages and characteristics of both sides of the cloud, in order to ensure the safety of road traffic system, usually with the premise of efficiency, to improve the efficiency of road control. We propose a C-V2X vehicle-road collaboration system for road traffic environment, build a vehicle-road collaboration system architecture based on V2X vehicle-road collaboration wireless communication, multi-access edge computing and high-precision positioning, and form a comprehensive solution for city-level vehicle-road collaboration intelligent transportation.

Our contributions:

1. We propose a new vehicle-road collaboration architecture, which fully integrates multiple traffic data resources, as well as control resources such as traffic monitoring, guidance screens, and signal control from three levels: individual vehicles, intersection localization, and regional road network.
2. We propose a multi-level information fusion technology based on multi-sensors in vehicle-road coordination to realize multi-sensor information fusion based on vehicle-road coordination perception, in view of the characteristics of many types of sensors and wide distribution in the vehicle-road coordination system, and the different detection environments, detection mechanisms, time frames, information characteristics and description methods of sensors.

We propose a lightweight identity-based authentication method to improve the authentication protocol for identity-based authentication and realize bidirectional authentication between end devices and edge gateways.

2. RELATED WORK

Existing autonomous driving technologies can be divided into two major technical routes: single-vehicle intelligence and vehicle-road collaboration. Single-vehicle intelligence relies entirely on the input of information from on-board sensors (such as LIDAR, millimeter wave radar and cameras) for environmental perception, and then artificial intelligence technology for environmental change prediction and driving decision generation, such as Waymo, Tesla, Mobileye and other companies in the United States have achieved L2-L4 level autonomous driving to some extent. However, in bad weather such as night, fog, rain and snow or complex traffic scenarios such as intersections and curves, the accuracy and reliability of on-board sensors are difficult to guarantee, thus making it impossible to achieve autonomous driving.

2.1. Single Vehicle Intelligence

The Society of Automotive Engineers (SAE) has defined five levels of driving automation. In this taxonomy, level zero represents no automation at all. Primitive driver assistance systems, such as adaptive cruise control, antilock braking systems and stability control, start at Level 1. Level 2 is partial automation, into which advanced assistance systems such as emergency braking or collision avoidance are integrated. The third level is conditional automation. During normal operation, the driver can focus on tasks other than driving, however, he/she must respond quickly to emergency alerts from the vehicle and be ready to take over. No level of human attention is required at Levels 4 and 5. However, Level 4 can only operate in limited ODDs where special infrastructure or detailed maps exist. In the case of leaving these areas, the vehicle must stop the trip by automatically stopping. A fully automated system, Level V, can operate on any road network and in any weather conditions. There are no production vehicles capable of Level 4 or Level 5 automation.

Self-driving cars use sensors such as cameras, radar and LIDAR to sense their surroundings. Due to the high price of LIDAR, Tesla wants to achieve fully autonomous driving without the use of LIDAR and proposes Autopilot [9] to be loaded on all Tesla production cars in the future. autopilot has achieved L3 level of autonomous driving by collecting image data through 8 cameras and 12 millimeter wave radars to assist in perception, but it is difficult to continue to improve. Waymo, which ranks first in the world in the field of autonomous driving, is mainly dedicated to the research of autonomous driving algorithms, building its own radium map through short-range, medium-range and long-range lidar, and choosing electromagnetic wave radar with better environmental adaptability than ultrasonic radar, but the requirements for cameras are also higher.

Baidu's Apollo has now achieved L4 level autonomous driving capability in a semi-enclosed environment. In the latest versions of Apollo, it is gradually moving closer to V2X, making Apollo with high level autonomous driving capabilities even more advantageous. Tencent, on the other hand, is more focused on providing services [10] for autonomous driving with the help of high-precision maps [11].

2.2. Cellular-Vehicle to everything

The Internet of Vehicles includes Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P), and Vehicle to Network (V2N) interactions. Network (V2N) interaction. Telematics will rely on information and communication technology to provide comprehensive information services through all-round connection and data interaction, forming a new industrial form with deep integration of automobile, electronics, information and communication, road transport and other industries.

The V2X network architecture based on vehicle-road cooperation can be generally divided into three levels: perception layer, decision layer and execution layer. The perception layer mainly involves environment perception technology and vehicle positioning technology to obtain the location of the vehicle and the surrounding traffic status; the decision layer mainly involves environment change prediction technology and driving decision technology, i.e., to predict the movement trajectory of the surrounding people and vehicles and generate optimized driving decisions accordingly; the execution layer mainly performs driving decisions through mechanical control. In the V2X network architecture, cloud, edge-side and vehicle-side are included, and each part is involved in various aspects of smart transportation, including data sensing, analysis and simulation, and decision control. The cloud has the lowest real-time performance, the edge side is in the middle, and the vehicle side has the highest real-time performance. Quasi-real-time data fusion and downlink in the edge cloud enables driverless vehicles to gain the ability to acquire information that breaks through visual dead spots or across occlusions. The perception, policy and control related to real-time vehicle control are performed at the vehicle side, and the analysis and calculation are done by the cloud-side fusion control platform.

2.3. Communication technology for C-V2X

C-V2X defines V2X technology based on cellular communications, including LTE-V2X, 5G-V2X [12]. it leverages the already existing LTE network facilities to enable V2V, V2N, V2I information interaction. The most attractive aspect of this technology is its ability to keep up with changes, adapt to more complex security application scenarios, meet low latency, high reliability and satisfy bandwidth requirements. LTE V2X defines two communication methods for vehicle applications [13]: centralized (LTE-V-Cell) and distributed (LTE-V-Direct). The centralized type, also known as cellular type, requires a base station as the control center, which defines the communication between the vehicle and roadside communication unit and base station equipment; the distributed type, also known as direct type, does not require a base station as support. 2006's CoCar project achieved an end-to-end delay of less than 500ms [14]. 2017's LTE-V2X technology from Bosch and Huawei achieved direct communication coverage of 1km and more. above, which can effectively provide the performance of two cars following each other face-to-face at 500km/h, with communication latency less than 20ms in high-density congested traffic scenarios and message sending success rate over 90%.

5G-V2X is the V2X standard for 5G communication. Because 4G-LTE technology was not fully considered at the beginning of the design, and with the rapid development of smart cars, 4G-LTE technology [15] became insufficient. V2X will be part of the 5G network, and 5G-V2X has the potential to integrate LTE-V2X and DSRC [16] to provide safer and more efficient operation capabilities for cars [17]. In July 2020, 3GPP completed the first 5G framework-based 5G-V2X standard Rel-16, which realizes the cooperative sensing and path planning, thus effectively avoiding accidents.

2.4. C-V2X security issues

Automated vehicles in vehicle-road collaboration interact with the surrounding environment through wireless communication technology [18], so it is of great significance to achieve a secure and reliable communication method to guarantee the security of Telematics [19][20]. The literature [21] proposes a security scheme for Telematics communication based on public key architecture and edge computing. The authors use the location information of the vehicle as well as the RSU as the reference basis for key pair distribution, so that key pre-distribution can be performed based on the prediction of the vehicle location. However, the security assurance scheme based on public key architecture requires certificate delivery and verification during the communication process, which greatly increases the load on the network. In the literature [22], an efficient anonymous, bulk authentication scheme is proposed to address the problem of security privacy protection in vehicular networking, thus reducing the message loss rate of vehicles and RSUs.

3. System Model

We propose a C-V2X vehicle-road collaboration system for road traffic environment, which is divided into a central cloud platform, an edge computing system, roadside devices and terminal devices.

The C-V2X vehicle-road collaboration system for road traffic environment defines the architecture and functional requirements of the central cloud platform and the edge computing system, and proposes the improvement of multi-sensor fusion and safety warning technology based on high-precision positioning.

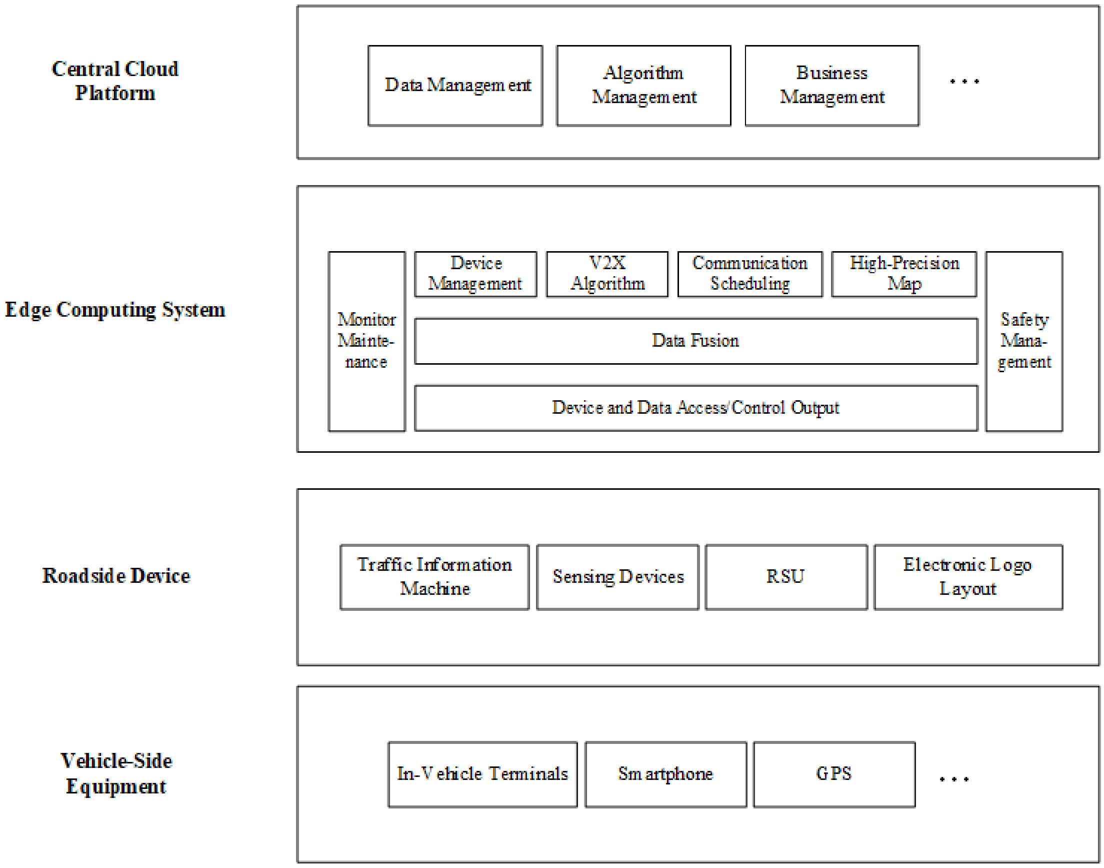

Figure 1. System Architecture

3.1. Central cloud platform

The core of C-V2X vehicle-road coordination system in the central platform assumes the functions of macroscopic decision-making and unified command dispatch. By converging the panoramic sensing data of people, vehicles, roads and environment in the vehicle-road cooperation scenario, it provides support for vehicle-road and vehicle-brain, and vehicle-vehicle cooperation decision based on big data and AI.

Distributed object storage enables storage of all data types, solving the problems associated with storage of massive amounts of all data forms, and making it more available, fault-tolerant, and scalable than a single data center. Make the system scalable by referring to objects using IDs instead of filenames. Associate large amounts of metadata with specific objects. Perceptual device layer convergence access to the cloud computing platform to provide basic data support for the cloud computing platform.

The functions of the central cloud platform include:

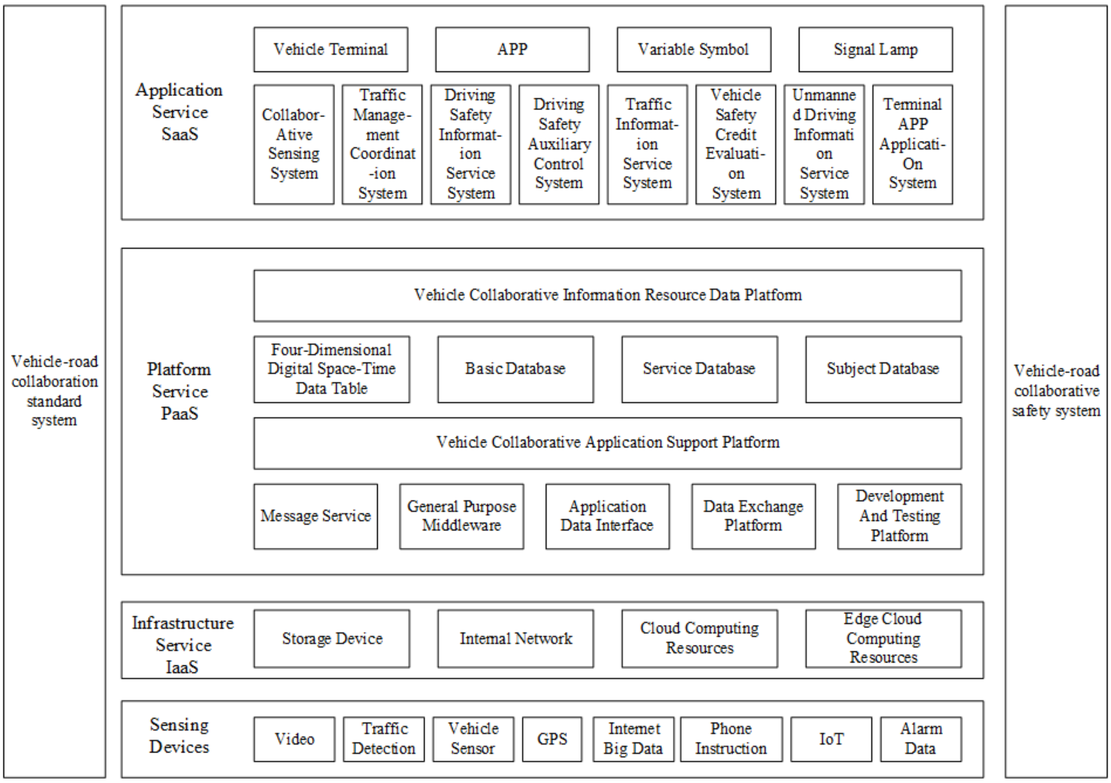
Vehicle-road collaboration standard system
Application Service SaaS
Vehicle Terminal
APP
Variable Symbol
Signal Lamp
Collabor-Ative Sensing System
Traffic Manage-ment Coordinat-ion System
Driving Safety Informat-ion Service System
Driving Safety Auxiliary Control System
Traffic Informat-ion Service System
Vehicle Safety Credit Evaluati-on System
Unmanned Driving Information Service System
Terminal APP Applicati-On System
Platform Service PaaS
Vehicle Collaborative Information Resource Data Platform
Four-Dimensional Digital Space-Time Data Table
Basic Database
Service Database
Subject Database
Vehicle Collaborative Application Support Platform
Message Service
General Purpose Middleware
Application Data Interface
Data Exchange Platform
Development And Testing Platform
Infrastructure Service IaaS
Storage Device
Internal Network
Cloud Computing Resources
Edge Cloud Computing Resources
Sensing Devices
Video
Traffic Detection
Vehicle Sensor
GPS
Internet Big Data
Phone Instruction
IoT
Alarm Data
Vehicle-road collaborative safety system

Figure 2. Central System Architecture

(1) Data management: Aggregate a huge amount of front-end devices, including pictures, videos, status and other timing data of vehicles, traffic signal control machines and many other devices. Distributed storage architecture is adopted for persistent storage of massive data.

(2) Data fusion: Relying on the processing power of the big data platform and the integrated data processing algorithms and models, the multi-source traffic data are automatically analyzed and processed for optimization under the set rules. It provides data-level fusion, feature-level fusion and decision-level fusion services to complete the required traffic control decision and prediction and early warning.

(3) Edge cloud collaboration:

1) Security collaboration: Provide perfect security policies, including traffic cleaning, traffic analysis, etc. In the process of security policy collaboration, the center can block malicious traffic if it is found to exist at an edge to prevent malicious traffic from spreading throughout the edge cloud platform.

2) Application collaboration: The cloud realizes lifecycle management of value-added network applications at edge nodes, including application push, installation, uninstallation, update, monitoring and logging. The central node can incubate and start the already existing application images on different edge clouds to complete the high availability guarantee and hot migration of applications.

(4) GBA security authentication function: In addition to grouping terminals with high similarity, security authentication and device management of the cloud platform are decoupled and decentralized for deployment to the edge gateway authorized through authentication. The designed lightweight certificate-free authentication protocol proposes a distributed authentication mechanism with the edge gateway as the core, thus improving the authentication efficiency.

Device management: centralized management of various devices accessed by the system, including vehicles, guidance screens, traffic signal controllers, and sensors.

3.2. Edge System

Edge computing system is the roadside core system of C-V2X vehicle-road cooperation system for road traffic environment, and it is the main undertaking system for communication and authentication services of C-V2X.

The edge computing system is deployed at the edge side of the front end of the vehicle-road collaboration system near the traffic road and traffic data sources. This system incorporates an open platform of network, computing, storage, and application core capabilities, and provides computing and intelligence services. It extend cloud computing and intelligence capabilities to edge nodes close to end devices. This avoids the problems of longer network latency, network congestion, and degraded quality of service that can be caused by putting computing on the cloud. This satisfies the requirements of high real-time and high computing capability of the vehicle-road collaboration system. The structure is shown in Figure 3.

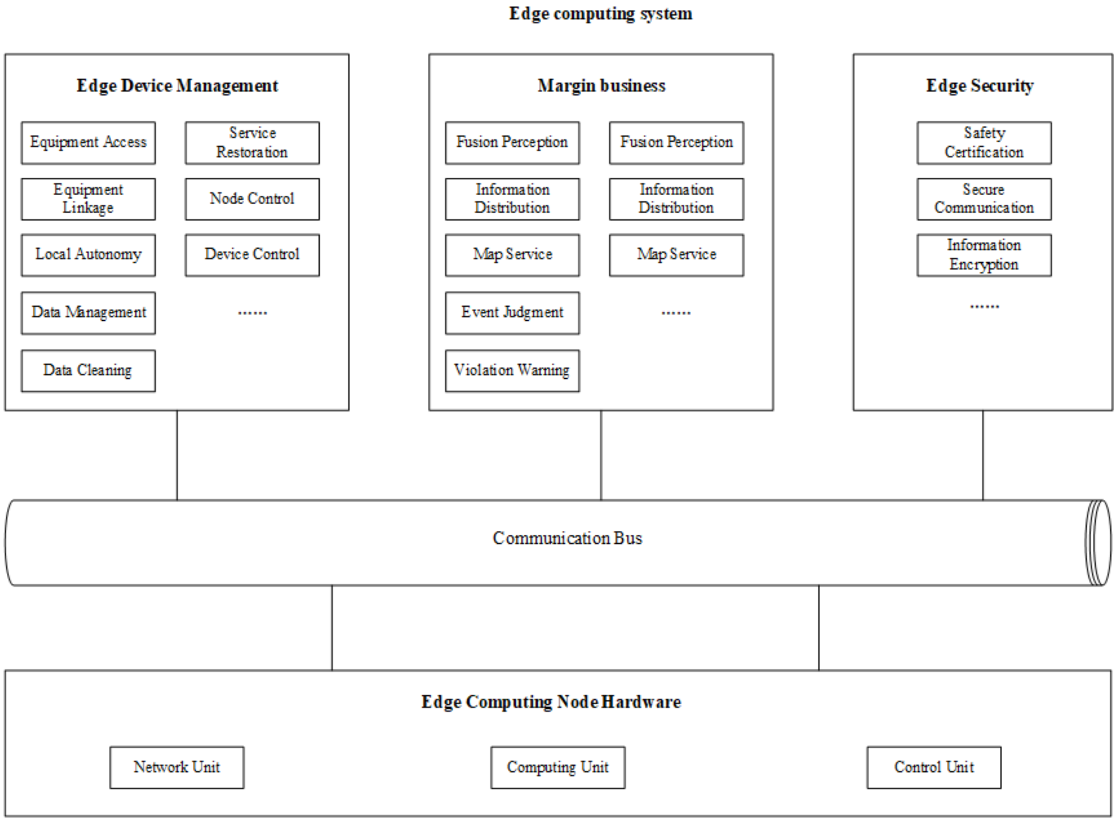

Figure 3. Edge Computing System Architecture

The edge layer includes two main parts, edge nodes and edge management. The edge node is the hardware entity, which is the core of carrying edge computing services. The presenting core of edge management is software, and the main function is to provide unified management of edge nodes.

The physical composition of the edge computing nodes for vehicle-road collaboration includes three basic modules: network, computing and storage. The service execution of C-V2X vehicle-road cooperative edge computing for road traffic environment is inseparable from the support of communication network. The network of edge computing is characterized by the need to satisfy both the determinism of transmission time and data integrity of control-related services, and the ability to support flexible deployment and implementation of services. Time-sensitive network (TSN) and software-defined network (SDN) technologies will be important fundamental resources for the network part of edge computing. Heterogeneous computing is the key computing hardware architecture at the edge. Edge devices have to handle both structured data and unstructured data at the same time. A local database is used to store high-precision map data, high-resolution image data, etc. It supports functions such as fast writing of time-series data, persistence, and multi-dimensional aggregated queries.

The edge computing node of vehicle-road collaboration logically contains three functional units: control, analysis and optimization. The control function unit perceives the environment timely and accurately, and uses edge computing to enhance local computing capabilities and reduce the response latency caused by cloud-centric computing. The control functional unit mainly includes the functions of environment sensing and execution, real-time communication, entity abstraction, control system modeling, device resource management, and program operation executor. The analysis functional unit mainly includes streaming data analysis, video image analysis, intelligent computing, and data mining. The algorithms such as neural network and machine learning related to artificial intelligence are applied at the edge side to complete the solution of complex problems using intelligent computing.

The integration of edge computing system with C-V2X can enhance the end-to-end communication capability of C-V2X. It can also provide auxiliary computing and data storage support for C-V2X vehicle-road cooperation application scenarios for road traffic environment.

The GBA secure communication system runs in a multi-access edge computing system. It provides complete security authentication and session channel encryption services for application layer services such as vehicle networking, road infrastructure networking, and vehicle-road collaboration. In the C-V2X vehicle-road cooperation system for road traffic environment, GBA secure communication connects the vehicle terminal and USIM card with the wireless access network, core network, GBA platform, and CA server. This guarantees the communication security of V2X.

3.3. Traffic information sensing module

Traffic targets in the vehicle-road cooperative environment refer to multi-source multi-dimensional traffic information such as vehicles, pedestrians, signage, and intersection environment. Multi-source multidimensional traffic information acquisition is achieved by sensors such as radar detectors, video detectors, and small meteorological data collectors. We propose a multi-channel intermingled information fusion method based on radar and video to achieve more accurate traffic target recognition by fusing traffic information from multiple sensors.

The point of video vehicle detection is that it can provide the impact situation of the road surface, and has a more excellent detection performance for beating cars and dense small cars in the image area under ideal lighting conditions. The recognition of different vehicle models and pedestrians is also good. But video vehicle detection is greatly affected by the light situation and weather conditions. For example, the recognition performance at night becomes poor, rain and fog weather basically cannot work, and adhere to the limited distance, generally not more than 100 meters.

Radar vehicle detection can detect a section of the road and can quickly derive precise position and speed information of the target, which is less affected by weather conditions. However, radar vehicle detection cannot give image information, cannot detect stopping targets, is not effective for hitting vehicles, and cannot effectively distinguish between various types of vehicles and pedestrians.

The fusion of traffic information from video vehicle detection and radar vehicle detection has two advantages, respectively: first, a sufficiently large detection area, sufficiently accurate data, and unaffected by climatic conditions is guaranteed by radar. Second, it can provide image information by video detection to accomplish stationary targets, large vehicle detection and distinguish various vehicle categories.

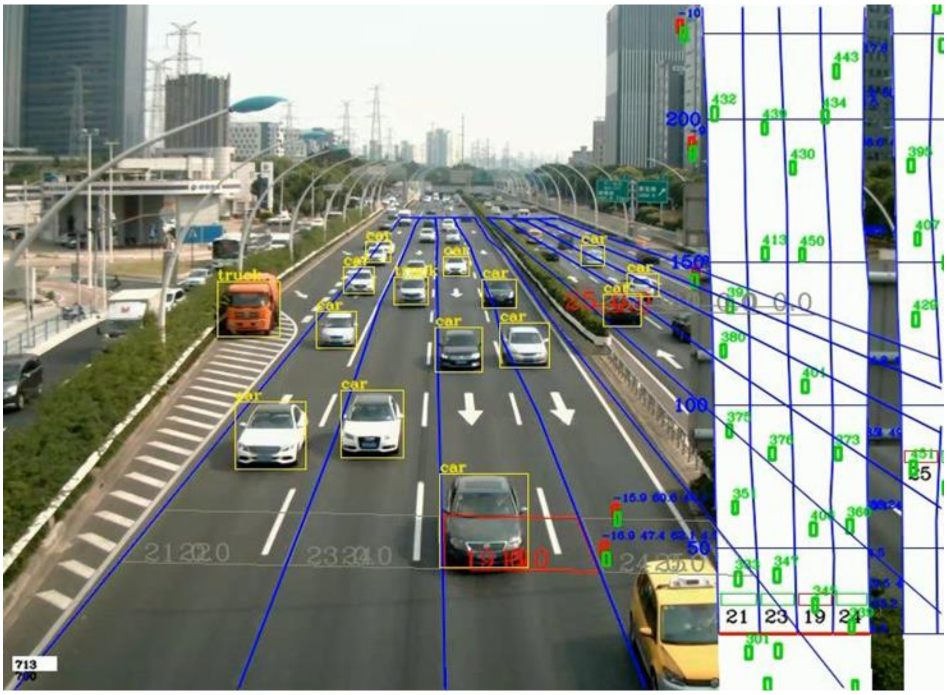

Figure 4. Radar and Video Traffic Information Fusion Perception

For the same target, both radar and video detect the target with high confidence. Both radar and video detect the target, but with high or low confidence. Only one of the radar and video detects the target. Only one of the radar and video detects this target. Neither radar nor video detects this target. The target data obtained by using both detection methods are weighted by confidence to obtain the final target data, and the final target data is used to update the target tracking status.

Since the type, style, and clarity of data collected by various other sensors are different, it is first necessary to perform spatial coordinate system conversion and temporal calibration on these multidimensional data. After the calibration, the fusion of radar video data with the same time stamp in the same coordinate system is achieved. The fusion centers after spatio-temporal alignment appear in clusters and are roughly distributed around the target true value. According to this characteristic using the idea of clustering in pattern recognition theory, the data belonging to the same target in different detectors can be clustered into one class and the data that are not targets can be separated. The video centers clustered into one class are estimated to calculate the fusion center, so that the tracking of multi-dimensional traffic targets is converted into a single video multi-target tracking problem.

The converted but video target data is input to the neural network. The MobileNet-SSD model is used as the core algorithm of the detection module. the basic structure of the SSD vehicle detection model is shown in Figure 5.

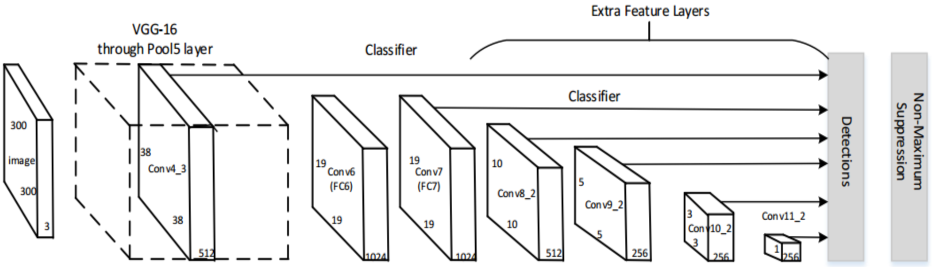

Figure 5. SSD vehicle inspection model

Firstly, the video to be detected by vehicle is pre-processed frame by frame so that the network input is an image of size 300*300*3. 300 denotes the number of pixels of image length and width, and 3 denotes the three channels R, G, and B. The SSD uses a feature pyramid structure for detection. Its base network structure is VGG-16, and the last two fully connected layers are changed to convolutional layers, and subsequently four convolutional layers are added to construct the network structure. The decreasing size of the convolutional layers layer by layer enables the network to make predictions at multiple scales. The convolutional layers extract different vehicle features and the size of the output feature map becomes smaller layer by layer. The size of the feature image obtained from each layer is 38*38, 19*19, 10*10, 5*5, 3*3, and 1*1, respectively.

For each additional feature layer added, a series of convolution kernels are used to perform convolution operations by means of sliding windows to produce the corresponding predictions. The output (feature map) of each of the five different convolutional layers is convolved with two different 3x3 convolutional kernels. One output is classified using confidence, with each default box generating 2 category confidences, and the other output is regressed using localization, with each default box generating 4 coordinate values (x,y,w,h). Specifically for a feature layer of size mxn with p channels, using a small convolution kernel of 3x3xp, a score or coordinate offset with respect to the default box is generated at each position of mxn for the attributed category. These 5 feature maps also go through the PriorBox layer to generate the priority box (the default box selected in practice). The number of default boxes in each layer of the above 5 feature maps is given, and the total number of obtained prior boxes in all feature maps is 8732.

The position of each box is fixed with respect to the feature lattice corresponding to it. In each feature lattice, the displacement from the default box needs to be predicted and the score (probability of belonging to a certain class) of the objects contained in each box. So, for each box in a set of k boxes at a location, c classes, the score of each class, and 4 offsets of that box compared to its default box can be calculated. Therefore, (c+4)*k results are generated for each location in the feature map. For a feature map of size m*n, then (c+4)*k*m*n outputs are generated.

MobileNet-SSD is evolved from SSD. It is a lightweight deep network model proposed for application to mobile, replacing the VGG-16 base feature extraction network in the SSD network with the MobileNet network. It can significantly improve the computational efficiency with guaranteed accuracy. The main use of Depthwise Separable Convolution decomposes the standard convolutional kernel to reduce the computational effort. Depthwise Separable Convolution is a standard convolution kernel divided into a depthwise convolution kernel and a pointwise convolution kernel of 1*1. The ratio of kernel computation is: (DK*DK*M* DF*DF+M*N* DF*DF)/(DK*DK*M*N*DF*DF)=1/N+1/(DK*DK), the computation is greatly reduced.

The detection results directly output by the detection network will contain a large number of duplicate frames, here we use the non-maximum suppression algorithm to filter out the duplicate detection frames and get the vehicle detection results. The main idea of the non-maximum suppression algorithm is as follows: for any detection target, the redundant detection frames should be eliminated, leaving only the frames with the highest confidence. The final remaining window within the sequence is then outputted as the final detection result. Thus, the recognition of multidimensional targets is achieved.

3.4. Security Module

The identity-based authentication protocol is improved to address the problem of limited communication and computational resources of IoT end devices. The resulting authentication scheme with lower computational complexity and higher efficiency is proposed. This achieves bi-directional authentication of end devices and edge gateways.

The identity-based bidirectional authentication protocol is divided into three main phases: as shown in Figure 6

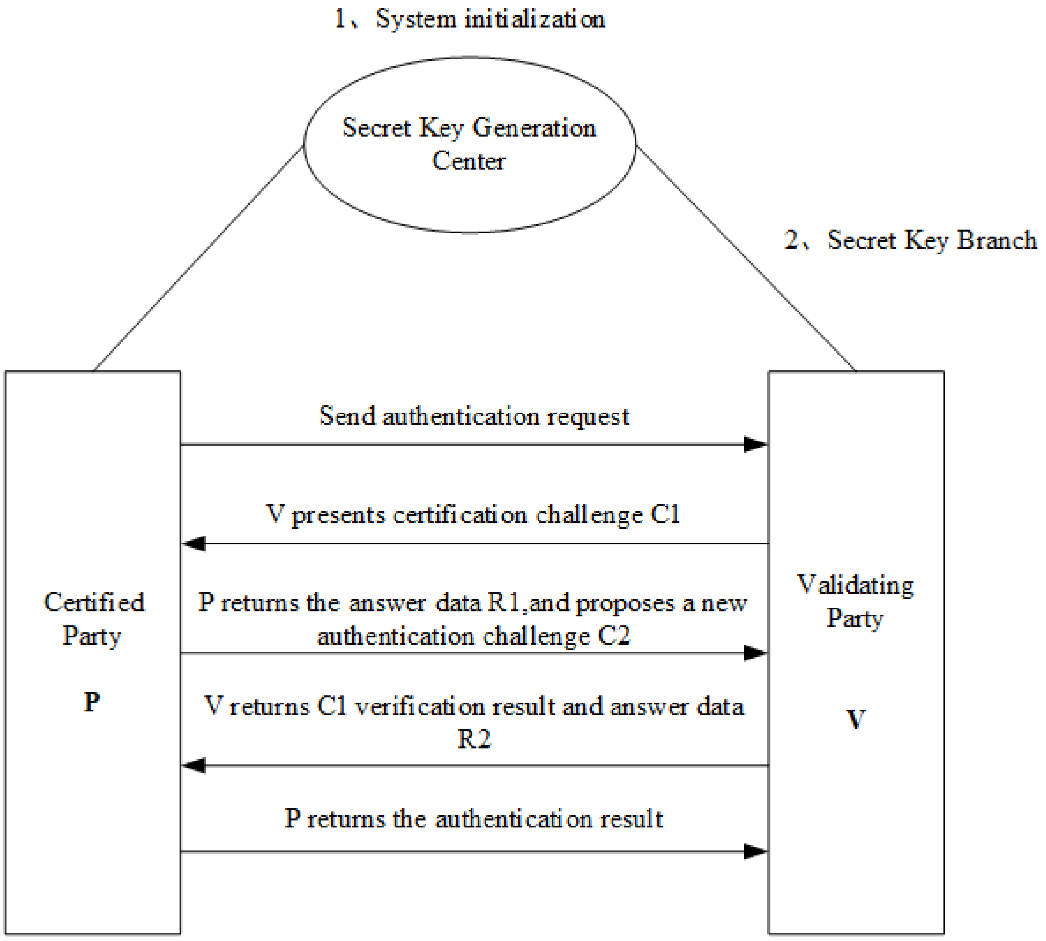
1、System initialization
Secret Key Generation Center
2、Secret Key Branch
Certified Party
P
Send authentication request
V presents certification challenge C1
P returns the answer data R1,and proposes a new authentication challenge C2
V returns C1 verification result and answer data R2
P returns the authentication result
Validating Party
V

Figure 6. Two-way authentication protocol

(1) Initialization phase

At the completion of the private key generation center (PKG), the PKG picks the additive cyclic group G_1 and the multiplicative cyclic group G_2. Both G_1 and G_2 are prime q-order. P is an arbitrarily chosen generating element of G_1. Denote the bilinear pair as:

$$e: G_1 \times G_2 \rightarrow G_1$$

Given a security parameter 1^k, select the random number $sk_m \grave{o} Z_p^{*}.$, sk_m is the master key (i.e., the system private key), and compute the master public key (i.e., the system public key).

$$P_{pub} = sk_m P$$

Select hash function.

$$h_1 : \{0,1\}^* \rightarrow G_1$$

$$h_2 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$$

The master key cannot be made public by the PKG alone, and the system reference $\left(G_1, G_2, e, q, P, P_{pub}, h_1, h_2\right)$ is published to all users in the system.

(2) Key extraction stage

Completed in the PKG, the corresponding public key is calculated based on the unique identification ID of the user in the system:

$$Q_{ID} = h_1(ID)$$

The private key corresponding to the user is then generated from the master key:

$$sk_{ID} = sk_m Q_{ID}$$

After that, the user key pair (Q_{ID}, sk_{ID}) is sent to the corresponding user through a secure channel (online or offline).

(3) Two-way authentication phase

T is the authentication initiator (i.e., terminal device) and S is the authentication server (edge gateway). To improve security, two-way authentication of T and S is required.

(a) T selects the random number $r_T \grave{o} Z_q^*$, the timestamp t_T and the hash function h_2 to calculate

$$c_T = h_2(r_T, t_T)$$

(b) S decrypts c_T after receiving the data, first verifies the validity of the timestamp t_T, selects the random number r_SòZ_q^* when the detection result is a valid timestamp, and calculates

$$\begin{gathered} m_S = (r_S + r_T) sk_S \\ c_S = h_2(r_S, t_S) \\ Q_T = h_1(ID_T) \end{gathered}$$

Re-transmitting authentication challenge information to the end device T.

(c) T decrypts c_S after receiving the data, verifies the validity of timestamp t_S, and if the timestamp is valid, calculates the public key of S.

$$Q_S = h_1(ID_S)$$

and test whether the equation holds:

$$e\left(m_S, -(r_S + r_T)P\right) = e\left(Q_S, P_{pub}\right)$$

If the equation does not hold then it shows that T fails to authenticate to S, i.e., S is not a legitimate edge gateway for the end device and T disconnects from the connection; otherwise it proves that T authenticates to S successfully and calculates.

$$m_T = (r_S + r_T) sk_T$$

return an answer message to S upon completion.

d) S decrypts and verifies that the equation holds after receiving a successful message from T and verifying that the timestamp is successful

$$e\left(m_S, -(r_S + r_T)P\right) = e\left(Q_S, P_{pub}\right)$$

If the equation does not hold, it indicates that S fails to authenticate T, the identity of the terminal device is considered illegitimate, a failure frame is returned, the data uploaded by terminal T is rejected and the connection is disconnected; otherwise, it indicates that S authenticates T successfully, a success frame is returned and the data uploaded by T starts to be received.

4. CONCLUSIONS

This paper proposes a novel framework for C-V2X system design. The framework can integrate multi-source data and perform collaborative analysis, which may benefit numerous services like autonomous driving. To achieve this goal, a highly aggregated architecture is proposed to hierarchically fuse the data resources. Then a multi-modal information fusion method is proposed to further aggregate the multi-sensor data generated within the C-V2X system. The method is flexible for different detection tasks and scenarios. Finally, the paper also introduces a fast and reliable authentication method to enhance the security level of the whole system. In our future study, we will focus on the detailed methods and models used for our C-V2X systems.

REFERENCES

[1] Wang Y, Chao W L, Garg D, et al. Pseudo-lidar from visual depth estimation: Bridging the gap in 3d object detection for autonomous driving[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019: 8445-8453.

[2] Chen S, Hu J, Shi Y, et al. A vision of C-V2X: technologies, field testing, and challenges with chinese development[J]. IEEE Internet of Things Journal, 2020, 7(5): 3872-3881.

[3] Fan H, Zhu F, Liu C, et al. Baidu apollo em motion planner[J]. arXiv preprint arXiv:1807.08048, 2018.

[4] Liu Z, Lu F, Wang P, et al. 3D Part Guided Image Editing for Fine-Grained Object Understanding[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 11336-11345.

[5] Du L, Ye X, Tan X, et al. Associate-3ddet: perceptual-to-conceptual association for 3d point cloud object detection[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020: 13329-13338.

[6] Yu Z, Liang S, Wei L, et al. MaCAR: Urban Traffic Light Control via Active Multi-agent Communication and Action Rectification[J].

[7] Chu W, Liu Y, Shen C, et al. Multi-task vehicle detection with region-of-interest voting[J]. IEEE Transactions on Image Processing, 2017, 27(1): 432-441.

[8] Zou L, Wang Z, Hu J, et al. Moving horizon estimation meets multi-sensor information fusion: Development, opportunities and challenges[J]. Information Fusion, 2020, 60: 1-10.

[9] Pan T, Song Y, Yang T, et al. Videomoco: Contrastive video representation learning with temporally adversarial examples[J]. arXiv preprint arXiv:2103.05905, 2021.

[10] Jia K, Kenney M, Mattila J, et al. The application of artificial intelligence at Chinese digital platform giants: Baidu, Alibaba and Tencent[J]. ETLA reports, 2018 (81).

[11] Ding L, Feng C. DeepMapping: Unsupervised map estimation from multiple point clouds[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019: 8650-8659.

[12] Molina-Masegosa R, Gozalvez J. LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications[J]. IEEE Vehicular Technology Magazine, 2017, 12(4): 30-39.

[13] Chen S, Hu J, Shi Y, et al. LTE-V: A TD-LTE-based V2X solution for future vehicular network[J]. IEEE Internet of Things journal, 2016, 3(6): 997-1005.

[14] Gonzalez-Martín M, Sepulcre M, Molina-Masegosa R, et al. Analytical models of the performance of C-V2X mode 4 vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2018, 68(2): 1155-1166.

[15] Vukadinovic V, Bakowski K, Marsch P, et al. 3GPP C-V2X and IEEE 802.11 p for Vehicle-to-Vehicle communications in highway platooning scenarios[J]. Ad Hoc Networks, 2018, 74: 17-29.

[16] Ghafoor K Z, Guizani M, Kong L, et al. Enabling efficient coexistence of DSRC and C-V2X in vehicular networks[J]. IEEE Wireless Communications, 2019, 27(2): 134-140.

[17] Boban M, Kousaridas A, Manolakis K, et al. Use cases, requirements, and design considerations for 5G V2X[J]. arXiv preprint arXiv:1712.01754, 2017.

[18] Wang J, Wu J, Li Y. The driving safety field based on driver–vehicle–road interactions[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(4): 2203-2214.

[19] Nassi B, Mirsky Y, Nassi D, et al. Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 293-308.

[20] Jarašūniene A, Jakubauskas G. Improvement of road safety using passive and active intelligent vehicle safety systems[J]. Transport, 2007, 22(4): 284-289.

[21] Zhang J M, Zhao Y J, Jiang H B, et al. Research on protection technology for location privacy in VANET[J]. Journal on Communications, 2012, 33(8): 180.

[22] Jing T, Pei Y, Zhang B, et al. An efficient anonymous batch authentication scheme based on priority and cooperation for VANETs[J]. EURASIP Journal on Wireless Communications and Networking, 2018, 2018(1): 1-13.

AUTHORS

Rui Huang, born in June 1984 in Xuzhou, Jiangsu Province, with a bachelor's degree, he is now the deputy general manager of smart city business department. His main research direction is traffic control and big data analysis, computer software development and application, system integration and security.