WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n1.11
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Review of Anomalous Behavior Detection in Internet of Vehicles

Jun Ren

School of Information Engineering, Henan University of Science and Technology, Luoyang 471000, China
rjun2024@163.com

ABSTRACT

The intelligent transportation system with the Internet of Vehicles as its core is gradually penetrating into the lives of urban residents, but it has also exposed security threats such as remote control of vehicles and leakage of personal information of car owners. Compared to the security issues at the level of vehicle end devices and vehicle networking service platforms, the article focuses on the security issues of abnormal behavior in vehicle networking. Based on this, the article reviews the relevant research on abnormal behavior detection mechanisms in the Internet of Vehicles environment in recent years. Firstly, the definition of abnormal behavior was analyzed, and the basic framework for detecting abnormal behavior was provided; Then, the classification of abnormal behavior detection mechanisms was discussed from three aspects: deep learning based abnormal behavior detection, spatiotemporal fusion based abnormal behavior detection, and visual based abnormal behavior detection; Finally, the unresolved technical issues and future research trends in the current abnormal behavior detection mechanism for the Internet of Vehicles were summarized.

KEYWORDS

Internet of Vehicles; Abnormal Behavior Detection; Deep Learning

1. INTRODUCTION

Vehicle self-organizing network (VANET) is a special type of network developed from mobile self-organizing network (MANET) [1-4], which is a completely self-organizing network. The communication in VANETs is facilitated by various short distance and remote wireless technologies to establish communication between vehicles and between vehicles and the roadside. However, due to the lack of processing and communication capabilities, VANETs are unable to process global information collected from other vehicles and systems, resulting in limited contemporary applications. In order to adapt to a wide range of contemporary applications, Vehicles in VANETs need to communicate with infrastructure, the Internet and people. These evolved VANETs are known as the Internet of Vehicles (IoVs) and largely follow the paradigm of the Internet of Things (IoT). The IoVs is a new type of Ad Hoc network [5, 6] composed of basic communication units of mobile vehicles and the surrounding environment. It has the sensing, computing, storage and wireless communication capabilities of running on the road, and realizes the communication between vehicles, vehicles and roadside units (RSUs), vehicles and people, and vehicles and the Internet.

Currently, with the continuous development of the IoVs pilot program, the system may inevitably face security threats from unknown attackers, such as attacking the in car bus, interfering with IoVs communication, and attacking IoVs service platforms. Such attacks may cause serious consequences

(such as reducing traffic efficiency) and even endanger the lives of drivers and pedestrians (such as interfering with electronic control units of engines and braking systems).

The essence of detecting abnormal behavior in the IoVs is to use current anomaly detection algorithms and model frameworks to train and learn from the data samples collected by vehicles. The challenges faced in detecting abnormal behavior in the current IoVs are mainly reflected in the following three aspects:

1) Abnormal behavior is complex and diverse: Intrusion detection, as an important detection method for vehicle road safety, plays an important role. However, due to the rapid changes in the structure of the vehicle network and the complex and diverse forms of intrusion, traditional detection methods cannot guarantee their accuracy and real-time requirements, and cannot be directly applied to the detection of abnormal behavior caused by network attacks in the vehicle network [7].

2) Large scale, diversity, and complexity of data: Abnormal behavior detection in the IoVs requires processing a large amount of diverse and complex data, which comes from multiple sensors and has high heterogeneity and heterogeneity. How to effectively process and analyze these data is one of the main challenges faced by abnormal behavior detection in the IoVs for digital twins.

3) High real-time performance: The IoVs environment is constantly changing, and the types of attacks are uncertain. Traditional anomaly detection mechanisms cannot provide real-time response to data [8].

This article mainly focuses on the security of the IoVs, and focuses on the research of abnormal behavior detection technology in response to the security threats and needs it faces.

2. ABNORMAL BEHAVIOR DETECTION METHODS

There are many classification methods for abnormal behavior detection in the IoVs, and most researchers tend to classify it from the source of abnormal behavior detection data, which can be divided into node centered abnormal behavior detection and data centered abnormal behavior detection.

(1) Node centered anomaly behavior detection: The idea of node centered detection mechanism is to use known datasets to detect malicious vehicle messages. A typical use case is PKI based signature authentication, which verifies the identity of the message sender through signature verification. Node centered detection mechanisms can be divided into behavior based and trust based: behavior based detection mechanisms[9, 10]. Focusing on the behavior of a specific node, focusing on identifying nodes that send messages too frequently or modify message content in a way that does not comply with protocol standards; Trust based detection mechanism [11, 12]. Similar to behavior based detection mechanisms, by establishing credibility metrics between nodes and assigning them to corresponding nodes, aggregation can effectively filter out malicious nodes. The node centered detection mechanism analyzes data based on past inappropriate behavior by setting a trust threshold. If the trust threshold is exceeded, it will be judged as abnormal behavior. However, the disadvantage of this method is that when two originally trusted nodes receive a conflict, it can lead to the inability to determine whether the message was malicious at the time of sending, and the node centered detection mechanism will fall into a dilemma, unable to detect abnormal behavior.

(2) Data centric abnormal behavior detection: The data centric detection mechanism analyzes the relationship between data packets, determines whether they are normal, and thus determines whether there are abnormal behaviors and nodes. It often analyzes the consistency and rationality of data packets, with consistency based detection [13-15]. Using the relationship between data packets, the credibility of newly received data is determined based on multiple communication vehicles from the vehicle network. For example, by analyzing the speed of multiple data packets to obtain the average

speed of this section of the road, and then determining whether the speed in the data packet is trustworthy.

2.1. Basic Framework for Abnormal Behavior Detection

The basic model for detecting abnormal behavior is shown in Figure 1. Collect and organize data containing normal and abnormal behaviors, construct an abnormal behavior detection dataset, discover hidden abnormal behavior characteristics in the data through data mining, deep learning training, spatiotemporal fusion, and other methods. Through continuous parameter optimization, finally form a suitable abnormal behavior detection model. During detection, the collected new data is input into the abnormal behavior detection model, and the detection results are output to the response processing module. According to the threat level of abnormal behavior, hierarchical response processing is carried out.

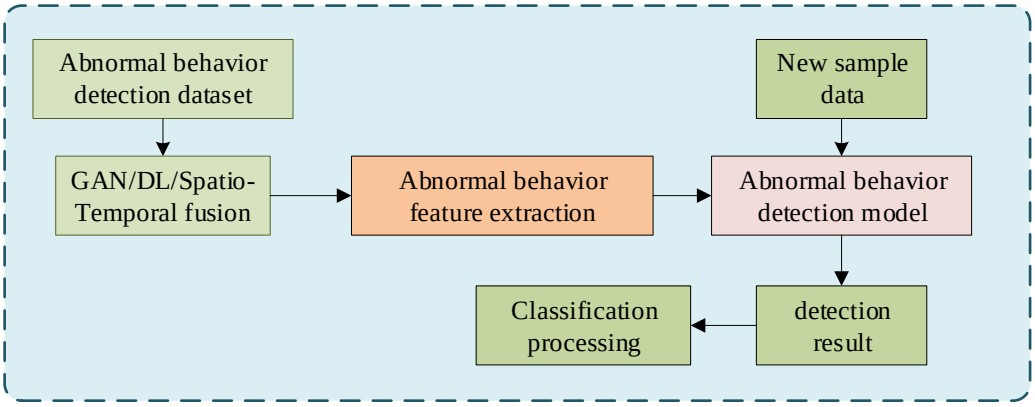

Figure 1. Basic process of abnormal behavior detection

Data collection and preprocessing: Using sensor devices on vehicles in the IoVs, collect information about the surrounding environment of vehicles, including images, videos, radar, LiDAR GPS and other vehicle status and surrounding environmental information. The process of data collection needs to pay attention to the quality and validity of the data, and perform normalization preprocessing operations on the data for subsequent processing and analysis.,

Feature extraction: For the collected data, feature extraction is required to extract representative and discriminative features for subsequent abnormal behavior detection. The methods of feature extraction include frame based feature extraction, trajectory based feature extraction, timeline based feature extraction, and spatial structure based feature extraction. Store and manage the features extracted by the vehicle perception and processing module. This module mainly consists of data storage devices and data management systems, used for real-time storage and management of vehicle perception data.

Model training and learning: After completing feature extraction, it is necessary to train and learn an anomaly behavior detection model based on machine learning or deep learning algorithms. Common machine learning algorithms include support vector machines, decision trees, naive Bayes, etc. Common deep learning algorithms include convolutional neural networks, recurrent neural networks, long short-term memory networks, etc. In the process of model training and learning, it is necessary to separate the training and testing sets for cross validation and model optimization to improve the accuracy and robustness of the model.

Abnormal behavior detection: Identify and classify abnormal behaviors from the features extracted from the behavior recognition module. After completing model training and learning, it is necessary to use the learned model to monitor and analyze the behavior of vehicles [16], Thus achieving the detection of abnormal vehicle behavior. The detection process includes inputting feature data into the model, which involves extracting abnormal behavior features and inputting new data samples into the

already trained model for testing. And predict and classify through the model, ultimately output classification results and detect abnormal behavior.

2.2. Visual Based Anomaly Detection Method

The general process of visual based vehicle abnormal behavior detection is shown in Figure X. It mainly includes preprocessing, behavior modeling, and anomaly detection modules. Firstly, extract various dynamic and static information of moving targets in the scene for behavioral feature representation. Then, the behavior modeling module takes the behavioral features extracted by the preprocessing module as input data, learns the behavior of moving targets in the scene, and forms certain rules, models, or databases. The abnormal behavior detection module compares the behavior of the test object with the learned behavior model or database, and obtains the category label or abnormal index of the current behavior. Mainly using video surveillance equipment to extract video or image features of vehicle driving paths in traffic scenes. Extracting features from videos of vehicles driving in traffic scenes collected from video surveillance devices [17]. Then utilize deep learning [18]. Train the model using other methods to detect abnormal behavior of the vehicle.

The review literature on visual based detection of abnormal behavior in traffic scenes is as follows. Li et al [19]. A smart vehicle behavior analysis framework for digital twins has been proposed. Firstly, implement vehicle detection based on deep learning, utilizing Kalman filtering and feature matching to track vehicles. Subsequently, the tracked vehicles were mapped to a digital twin virtual scene developed in the Unity game engine, and each vehicle's abnormal behavior was tested based on customized detection conditions set in the scene. Miao et al [20]. Propose an anomaly behavior detection method based on pix2pix and continuous video frames. In this literature, unmanned aerial vehicles and fixed ground equipment are used to conduct multi-level and multimodal behavior perception of large-scale crowds. A hybrid model is deployed in edge clouds to extract global features from the behavior data of large-scale crowds, and then these global features are used to construct a good action recognition and behavior semantic cognitive classification algorithm. Finally, danger intention prediction based on abnormal behavior learning: By integrating cognitive data over a period of time, behavior information is associated with possible danger intentions. Tian et al [21]. Provide a detailed introduction to traffic monitoring video processing technology based on computer vision, and also propose vehicle abnormal behavior detection based on background modeling and non-background modeling. Sodemann et al [22]. Systematically introduce abnormal behavior detection technology in traffic surveillance videos from the aspects of feature extraction, learning methods, and behavior classification methods.

In summary, visual based vehicle abnormal behavior detection methods have the following drawbacks: (1) inability to detect hidden behavior: Visual detection methods mainly rely on videos or images captured by video devices, which leads to only seeing external behavior of the vehicle and unable to observe behavior inside the vehicle, thus unable to detect hidden behavior that may occur inside the vehicle; (2) Privacy and security issues: The behavior inside the vehicle is highly protected by privacy, and visual detection methods can easily infringe on the personal privacy of passengers inside the vehicle, which may cause social disputes and legal issues; (3) Model training is required: Visual detection methods require model training, which requires a large amount of annotated data and time to complete. At the same time, models in different scenes may need to be retrained; (4) Requires a large amount of computing resources: Visual detection methods based on deep learning and other technologies require a large amount of image processing and computation, which requires high computing resources and also requires a long processing time, affecting real-time performance.

2.3. Deep Learning Based Abnormal Behavior Detection Methods

Deep learning is a type of machine learning based on artificial neural networks. Technology, which mainly consists of multiple hidden layers. Deep learning automatically learns multi-level

representations based on input data through backpropagation algorithms and applies them to tasks such as classification, regression, and anomaly detection. In the detection of abnormal behavior in the IoVs, three common deep learning algorithms can be used: convolutional neural networks [23], Recurrent neural network [24]. And generate adversarial networks [25].Among them, Convolutional Neural Network (CNN) is a type of feedforward neural network that includes convolutional computation and has a deep structure, and is one of the representative algorithms of deep learning; Recurrent Neural Network, RNN is a type of recursive neural network that takes sequence data as input, recurses in the direction of sequence evolution, and all nodes (loop units) are connected in a chain like manner; Generative Adversarial Networks, GAN is a deep learning model and a popular unsupervised learning algorithm in recent years.

In the detection of abnormal behavior in the IoVs, digital twin models can model the operating status of vehicles and compare the actual vehicle status with the model status to detect abnormal behavior. The implementation of digital twin models can also utilize deep learning methods. For example, LSTM based digital twin models can be used to establish accurate anomaly detection capabilities for vehicles in the vehicular network [26].

Deep learning methods focus on extracting advanced features of vehicle appearance and motion from videos, in order to more effectively extract normal and abnormal behavior. The methods of deep learning can be divided into supervised learning, unsupervised learning, and weakly supervised learning. Supervised learning mainly utilizes deep neural networks to extract high-level features of labeled images, and classifiers classify the features into two categories: normal behavior and abnormal behavior. However, due to the real-time and high mobility characteristics of connected vehicles in the IoVs, it is difficult to obtain sufficient abnormal behavior label data. Unsupervised or weakly supervised learning methods are usually used to establish behavior models for video data containing only normal behavior, detect behaviors that do not comply with this model, and identify them as abnormal behavior.

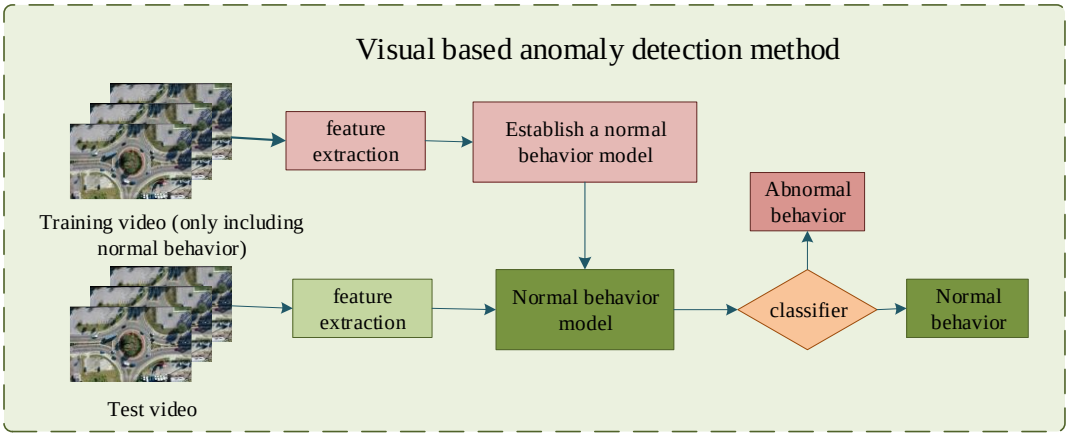

Figure 2. The basic process of detecting abnormal behavior in deep learning

The adaptability and adaptability of deep learning methods can be further optimized to adapt to more complex scenarios. Therefore, deep learning will continue to play an important role in detecting abnormal behavior in the IoVs. Although deep learning methods have achieved a series of successes in detecting abnormal behavior in the IoVs, they also face some problems and challenges. For example, as deep learning models become more complex, the complexity of training and debugging also increases significantly. In addition, the quality and quantity of data have a significant impact on the training and performance of the model in detecting abnormal behavior in the IoVs.

2.4. Spatio-Temporal Fusion Based Abnormal Behavior Detection Methods

The anomaly behavior detection method based on spatiotemporal fusion is a method that combines temporal and spatial information, mainly aimed at anomaly behavior detection in the field of video

surveillance. This method treats each frame of the video sequence as a single data point in the temporal dimension, and considers the spatial position of each pixel in the video as another dimension. Then, deep learning models are used to model spatiotemporal information, learn patterns of normal behavior, and detect behaviors that do not match normal patterns during monitoring.

Reference [27] first proposed a spatiotemporal flow anomaly detection framework based on Bayesian fusion. Firstly, video samples were collected using vehicle sensors or monitoring devices, which are generally composed of spatial and temporal components. The anomaly detection model is mainly divided into spatial flow convolutional networks and temporal flow convolutional networks. Calculate the spatial flow reconstruction error and the time flow reconstruction error after training the time and spatial flows; Then, through Bayesian fusion, the reconstruction errors of the two are fused, and finally, the final fusion reconstruction error is used to determine abnormal behavior. This method can accurately detect abnormal behavior, but there are still some real-time and vehicle trajectory issues. To solve the real-time problem of high vehicle mobility, it is necessary to train spatial and temporal flow models separately.

In response to the issues of real-time performance and multiple monitoring variables, reference [28] proposes an anomaly detection algorithm for spacecraft telemetry data based on spatiotemporal fusion generative adversarial network (GAN). This algorithm is based on a GAN model, combining Convolutional Neural Networks (CNN) and Long Short Term Memory Networks (LSTM) to extract temporal and spatial features of data. This not only helps to automatically and simultaneously represent the non negligible temporal features of monitoring variables and the complex correlations between variables. These features can also be used to detect various abnormal behavior data. In addition, the literature also proposes an anomaly score design suitable for GAN based algorithms, which significantly helps with the accuracy of anomaly behavior detection. The main reason for abnormal behavior in the IoVs is caused by network intrusion methods. Vehicles in the IoVs are subjected to network attacks, causing the received or sent information to be tampered with, resulting in abnormal driving behavior. Reference [29] proposes a network spoofing framework based on spatiotemporal cost combination. Firstly, determine the interest points of collaborative vehicle networking participants, establish baseline trajectories, and determine typical trajectory distributions; Secondly, use statistical models to calculate trajectory distribution, cost, travel direction, and destination. At the same time, the vehicle nodes are transformed into evolution maps to detect abnormal behavior in local road sections. Finally, based on the perception of abnormal road environments, analyze the causes of abnormal trajectories. Reference [30] proposes an AA distributed combination deep learning method for intrusion detection in vehicular networks based on the Apache Spark framework. This method applies machine learning methods to intrusion detection systems and uses support vector machines and naive Bayesian algorithms for normalization and feature simplification for analysis and comparison. Mainly using LSTM and CNN to extract features and data of vehicle intrusion detection from large-scale vehicle networking data streams, and discover anomalies. In the network environment, deep learning technology has good self-learning function, associative storage function, and high-speed optimization function, which is very suitable for processing current complex network traffic data, especially in complex connected vehicle environments.

The above methods all use 2D convolution to extract spatiotemporal features, and 3D CNN is an extension of 2D convolution, adding a time dimension, and can model both appearance and motion information simultaneously [31]. Reference [32] proposes an intelligent vehicle behavior analysis framework. The vehicle trajectory and two-dimensional coordinates in the video coordinate system can be obtained through deep learning algorithm YOLOv5 and tracking algorithm. Create a mapping relationship for virtual scenes based on the video, and convert 2D coordinates into 3D coordinates. Then, three-dimensional reconstruction is performed on each detected vehicle in the virtual scene, and the reconstructed vehicle model can interact with the behavior detection conditions set in the virtual scene. As a result, the abnormal behavior detection module integrates binary classifiers and

multi classifiers used to distinguish multiple specific abnormal classes, which can detect more distinguishable detailed features and improve detection accuracy.

In summary, the method based on spatiotemporal fusion generally relies on training methods such as convolutional neural networks or deep learning to train the model. This method can extract spatiotemporal features from video and sequence data to fuse appearance and motion trajectories, and can capture more differences in advanced features of normal and abnormal behavior. The use of spatiotemporal fusion can achieve high accuracy and solve real-time issues.

3. PERFORMANCE EVALUATION

The application of the IoVs cannot be separated from the detection and prediction of abnormal vehicle behavior, so performance evaluation has become an essential part. This article measures its performance from the following three aspects.

Accuracy: Accuracy is an important indicator of the performance of anomaly detection algorithms, which is usually defined as the degree of consistency between the algorithm's predicted results and the actual results. Common accuracy indicators include precision, recall F1 score, etc.

$$precision = \frac{TP}{TP + FP} \tag{1}$$

$$recall = \frac{TP}{FP + FN} \tag{2}$$

Where true positive (TP) refers to the number of correctly predicted vehicle anomalies, false positive (FP) refers to the number of incorrectly predicted vehicle anomalies, and false negative (FN) refers to the number of incorrectly predicted vehicle anomalies.

$$F1 = \frac{2 * precision * recall}{precision + recall} \tag{3}$$

Computational complexity: Computational complexity is commonly used to measure the computational cost and performance of anomaly detection algorithms. Common computational complexity indicators include model size, model training time, model inference time, etc. Among them, model size refers to the number of parameters required by the model; The model training time is the time required to train the model; Model inference time refers to the time it takes for the model to perform inference after inputting feature data.

Robustness: Robustness refers to the anti-interference ability of abnormal behavior detection algorithms against data noise, interference, and environmental changes. Common robustness indicators include misjudgment rate, stability, etc. Among them, the misjudgment rate refers to the probability of algorithm anomaly detection errors; Stability refers to the adaptability and stability of an algorithm to changes in the environment and data.

This article provides an overview of the current research status of abnormal behavior detection, and classifies the current research achievements in this field. Several methods for abnormal behavior detection are introduced, each with its unique characteristics. For different application needs, their analysis and comparison results are listed in Table 1. It can be seen that their applicability to traffic scenarios, performance, and other aspects are not the same. Through comparative analysis, these types of anomaly detection methods all have high accuracy and precision, but their performance varies in

terms of real-time performance, computational overhead, data requirements, and the complexity of model establishment.

4. SUMMARY AND FUTURE RESEARCH DIRECTIONS

Although existing literature has proposed corresponding detection methods for multiple typical abnormal behaviors, there are still the following unresolved issues in this field.

(1) A rigorous identity authentication scheme not only prevents unauthorized nodes from accessing the network, but also leads to greater computational and communication costs, making it unsuitable for vehicle networking applications with latency sensitive requirements. Therefore, a balance must be made between the costs of identity authentication, computation, and communication, and it is recommended that the vehicle terminal be equipped with a tailored identity authentication scheme that meets the requirements of the IoVs;

(2) Currently, applying machine learning technology to intrusion detection systems is a hot research area. In order to maximize the effectiveness of machine learning, we need to create a representative large-scale dataset that includes the communication characteristics of the connected vehicle network. Dempsey and other researchers used VANET simulation tools to create a reference dataset for abnormal vehicle behavior called VeReMi in order to address the issue of vehicle location data forgery. This dataset covers various cases of positional forgery. Subsequently, the dataset was further expanded to include more realistic sensor error models and more complex position forgery strategies to provide richer testing scenarios. However, currently most of the relevant datasets still mainly come from simulation experiments. These datasets still exhibit certain limitations when faced with real-world scenarios in vehicle networking communication systems with large scale, high data heterogeneity, and high environmental complexity. Therefore, generating representative datasets that can truly reflect the connected car environment is a significant challenge. In addition, evaluating the differences between simulation results and real-world testing is also an urgent issue that needs to be addressed.

(3) The privacy protection mechanism of the IoVs usually requires frequent identity changes (pseudonyms), which conflicts with the long-term identity requirements of security mechanisms. At the same time, the frequent use of pseudonyms makes nodes have multiple identities at the same time, which can easily trigger Sybil attacks. In addition, the frequent changes in pseudonyms greatly increase the difficulty of tracking message sources and associating messages from the same node, adding additional obstacles to the detection of malicious nodes. In summary, overly strict security mechanisms can violate user privacy, while excessive privacy protection can limit security mechanisms. Therefore, there is an urgent need for a balance between the two.

REFERENCES

[1] Jirkovský V, Obitko M, Mařík V. Understanding data heterogeneity in the context of cyber-physical systems integration[J]. IEEE Transactions on Industrial Informatics, 2016, 13(2): 660-667.

[2] Zhang Y, Pan J, Qi L, et al. Privacy-preserving quality prediction for edge-based IoT services[J]. Future Generation Computer Systems, 2021, 114: 336-348.

[3] Xu X, Fang Z, Zhang J, et al. Edge content caching with deep spatiotemporal residual network for IoV in smart city[J]. ACM Transactions on Sensor Networks (TOSN), 2021, 17(3): 1-33.

[4] Bindu R, Preethi Sejal M, Chetan H. A Survey Paper on Evolution of Vanet Towards IOV[M]//Optical and Wireless Technologies: Proceedings of OWT 2021. Singapore: Springer Nature Singapore, 2022: 99-113.

[5] Ding N, Ma H X, Zhao C G, et al. Driver's emotional state-based data anomaly detection for vehicular ad hoc networks[C], IEEE International Conference on Smart Internet of Things. IEEE, 2019: 121-126.

[6] Ding N, Ma H, Zhao C, et al. Data anomaly detection for internet of vehicles based on traffic cellular automata and driving style[J]. Sensors, 2019, 19(22): 4926.

[7] Wang Z, Gupta R, Han K, et al. Mobility digital twin: Concept, architecture, case study, and future challenges[J]. IEEE Internet of Things Journal, 2022, 9(18): 17452-17467.

[8] Wu J, Yang Y, Cheng X U N, et al. The development of digital twin technology review[C]. Chinese Automation Congress. IEEE, 2020: 4901-4906.

[9] Puñal O, Aguiar A, Gross J. In VANETs we trust? Characterizing RF jamming in vehicular networks[C]//Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications. 2012: 83-92.

[10] Chen C, Wang X, Han W, et al. A robust detection of the sybil attack in urban vanets[C]//2009 29th IEEE International Conference on Distributed Computing Systems Workshops. IEEE, 2009: 270-276.

[11] Sowattana C, Viriyasitavat W, Khurat A. Distributed consensus-based Sybil nodes detection in VANETs[C]//2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE). IEEE, 2017: 1-6.

[12] Raya M, Papadimitratos P, Aad I, et al. Eviction of misbehaving and faulty nodes in vehicular networks[J]. IEEE journal on selected areas in communications, 2007, 25(8): 1557-1568.

[13] Raya M, Papadimitratos P, Aad I, et al. Eviction of misbehaving and faulty nodes in vehicular networks[J]. IEEE journal on selected areas in communications, 2007, 25(8): 1557-1568.

[14] Ding N, Ma H, Zhao C, et al. Data anomaly detection for internet of vehicles based on traffic cellular automata and driving style[J]. Sensors, 2019, 19(22): 4926.

[15] Sabokrou M, Khalooei M, Fathy M, et al. Adversarially learned one-class classifier for novelty detection[C]. IEEE conference on computer vision and pattern recognition. 2018: 3379-3388.

[16] Alshehri A, Khan N, Alowayr A, et al. Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics[J]. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 2023, 44(2): 1679-1689.

[17] Ding N, Ma H, Zhao C, et al. Data anomaly detection for internet of vehicles based on traffic cellular automata and driving style[J]. Sensors, 2019, 19(22): 4926.

[18] Chiroma H, Abdulhamid S M, Hashem I A T, et al. Deep learning-based big data analytics for internet of vehicles: taxonomy, challenges, and research directions[J]. Mathematical Problems in Engineering, 2021, 2021: 1-20.

[19] Li L, Hu Z, Yang X. Intelligent Analysis of Abnormal Vehicle Behavior Based on a Digital Twin[J]. Journal of Shanghai Jiaotong University (Science), 2021, 26: 587-597.

[20] Miao Y, Yang J, Alzahrani B, et al. Abnormal Behavior Learning Based on Edge Computing toward a Crowd Monitoring System[J]. IEEE Network, 2022, 36(3): 90-96.

[21] Tian B, Yao Q, Gu Y, et al. Video processing techniques for traffic flow monitoring: A survey[C]//2011 14th international IEEE conference on intelligent transportation systems (ITSC). IEEE, 2011: 1103-1108.

[22] Wang W, Xia F, Nie H, et al. Vehicle trajectory clustering based on dynamic representation learning of internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(6): 3567-3576.

[23] Tay N C, Connie T, Ong T S, et al. A robust abnormal behavior detection method using convolutional neural network[C]. Computational Science and Technology, 2019: 37-47.

[24] Alshehri A, Khan N, Alowayr A, et al. Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics[J]. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 2023, 44(2): 1679-1689.

[25] Alqahtani H, Kavakli-Thorne M, Kumar G. Applications of generative adversarial networks (gans): An updated review[J]. Archives of Computational Methods in Engineering, 2021, 28: 525-552.

[26] Ugli D B R, Kim J, Mohammed A F Y, et al. Cognitive Video Surveillance Management in Hierarchical Edge Computing System with Long Short-Term Memory Model[J]. Sensors, 2023, 23(5): 2869.

[27] Jiang J, Wang X Y, Gao M, et al. Abnormal behavior detection using streak flow acceleration [J]. Applied Intelligence, 2022: 1-18.

[28] Contreras-Cruz M A, Correa-Tome F E, Lopez-Padilla R, et al. Generative Adversarial Networks for anomaly detection in aerial images[J]. Computers and Electrical Engineering, 2023, 106: 108470.

[29] Kong X, Zhu B, Shen G, et al. Spatial-temporal-cost combination based taxi driving fraud detection for collaborative internet of vehicles[J]. IEEE Transactions on Industrial Informatics, 2021, 18(5): 3426-3436.

[30] Alferaidi A, Yadav K, Alharbi Y, et al. Distributed deep CNN-LSTM model for intrusion detection method in IoT-based vehicles[J]. Mathematical Problems in Engineering, 2022, 2022.

[31] Tran D, Bourdev L, Fergus R, et al. Learning spatiotemporal features with 3d convolutional networks[C]//Proceedings of the IEEE international conference on computer vision. 2015: 4489-4497.

[32] Li L, Hu Z, Yang X. Intelligent Analysis of Abnormal Vehicle Behavior Based on a Digital Twin[J]. Journal of Shanghai Jiaotong University (Science), 2021, 26: 587-597.