Causal Inference-Based Network Anomaly Detection for Internet of Vehicles

Ming Dai[1],†, Heng Gao[2],†, Zengri Zeng[2],*, Aimei Kang[2], Xinming Wang[3]

[1] Institute of Applied Artificial Intelligence of the Guangdong-Hong Kong-Macao Greater Bay Area, Shenzhen Polytechnic University, Shenzhen 518055, China
[2] Hunan University of Humanities, Science and Technology, Loudi 417000, China
[3] School of Chemical Engineering, University of Science and Technology Liaoning, Anshan 114051, China

* Corresponding author. E-mail: zengzr@nudt.edu.cn
† These authors contributed equally to this work.

Abstract. 5G-V2X technology and connected and autonomous vehicles are deeply integrated. The Internet of Vehicles (IoV) has become the core support of an intelligent transportation system. Its heterogeneous architecture and high-dynamic characteristics bring serious cybersecurity risks. Traditional anomaly detection methods rely on correlation reasoning. They have high false positive rates. They are not easy to interpret. They can't adapt to combined attacks. They also lack real-time performance. This paper puts forward a causal inference-based anomaly detection algorithm (IoV-NDCML). It is specially designed for the IoV scenario. The algorithm reconstructs a multi-dimensional causal interpretable feature set. It designs a dynamic causal intervention screening method. The method integrates scenario weights. It builds a lightweight hierarchical SCM model. It improves the counterfactual diagnosis method. The algorithm realizes accurate anomaly detection. It also achieves causal attribution.Experiments show that the proposed algorithm achieves 99.2% accuracy in single-attack scenarios and 97.5% accuracy in combined-attack scenarios, with an end-to-end latency below 50 ms on edge devices. Its comprehensive performance outperforms comparative algorithms, providing technical support for security defense in the Internet of Vehicles.

Keywords. causal inference; Internet of Vehicles (IoV); V2X communication; network anomaly detection; causal intervention; counterfactual diagnosis; structural causal model (SCM)

1 Introduction

1.1 Research Background and Significance

5G-V2X technology is deployed widely. Intelligent connected vehicles are used on a large scale. The Internet of Vehicles (IoV) realizes heterogeneous communication. It

involves multiple nodes. These nodes include vehicles, roads, clouds and users. It provides critical support for some applications. These applications are autonomous driving and cooperative traffic management. The IoV has high dynamics. It also has heterogeneity. It has strict real-time requirements. The IoV faces common network attacks. It also faces unique threats. These threats include fake base station spoofing, false message injection and CAN bus hijacking. These threats can easily cause abnormal vehicle control. They can lead to traffic disorder. They may even cause traffic accidents. Existing detection methods can barely meet IoV scenario requirements. Causal inference can decouple spurious correlations. It achieves accurate attribution. It provides a new solution to these problems. Developing causal detection algorithms is important. These algorithms need to adapt to the IoV. It has great theoretical and engineering significance.

1.2 Research Status at Home and Abroad

Current research on IoV anomaly detection has three categories. All of them have obvious limitations:

1. Traditional methods rely on statistical correlation. They can't adapt to IoV scenarios. These scenarios are highly dynamic and high-noise. They lead to high false positive and negative rates.
2. General causal detection algorithms exist. For example, NDCML in Ref. [1]. They eliminate noise through causal intervention. They are not optimized for IoV heterogeneous communication. They are also unoptimized for combined attacks. They can't be applied directly.
3. Preliminary causal inference applications exist in IoV. They only introduce causal ideas. They don't have scenario-specific customization. They lack dedicated causal feature sets. They also lack lightweight models. They can't solve combined attacks. They can't address real-time performance. They fail to solve other core issues.

Existing methods can barely meet IoV detection requirements. Designing a dedicated causal inference algorithm is necessary. It should be for the IoV. This is the research starting point of this paper.

1.3 Main Research Contents and Innovations of This Paper

1.3.1 Main Research Contents

This paper solves the key pain points of IoV anomaly detection. The main research contents are as follows: Analyze IoV traffic features. Analyze attack types and detection requirements. Verify the adaptability of causal inference. Reconstruct a multi-dimensional causal interpretable feature set. Develop a corresponding feature extraction tool. Design a dynamic causal intervention screening method. It integrates scenario weights. It is used to eliminate scenario noise. Build a lightweight hierarchical SCM model. It adapts to combined attacks. It also adapts to edge deployment. Optimize the counterfactual diagnosis method. Improve real-time performance. Realize interpretable output. Verify the overall algorithm performance. Verify the effectiveness of each module. Use simulation experiments to do this.

1.3.2 Core Innovations

1. A multi-dimensional causal feature set is reconstructed for the Internet of Vehicles. It extracts features. These features have clear causal correlations to attacks. They come from the network layer, application layer, in-vehicle physical layer and node state layer. It breaks through the limitations of general features.

2A dynamic causal screening method is put forward. It integrates scenario weights. The IPW strategy is improved. Scenario and communication link weights are introduced. The threshold is adjusted dynamically. It reduces the false positive rate.

3. A lightweight hierarchical SCM model is built. It has a three-layer structure. The structure is attack-feature-scenario. An attack coordination factor is introduced. It adapts to combined attacks. Node pruning is used. It achieves lightweight deployment. Scenario exogenous variables are added. They eliminate attribution bias.

4. The counterfactual diagnosis method is improved. The prior causal probability table is pre-calculated. Scenario correction coefficients are introduced. It achieves millisecond-level response. It also realizes structured interpretable output.

1.4 Thesis Structure

This thesis has six chapters. Chapter 1 introduces the research background. It introduces the state-of-the-art. It also introduces main contents and innovations. Chapter 2 presents the Internet of Vehicles architecture. It presents core theories of causal inference. It shows their compatibility. Chapter 3 analyzes key issues. These issues are about network anomaly detection in the Internet of Vehicles. Chapter 4 elaborates the detailed design. The design is of the IoV-NDCML algorithm. Chapter 5 verifies the algorithm performance. It uses experiments to do this. Chapter 6 summarizes the research achievements. It discusses limitations. It proposes future research directions.

2 Theoretical Foundation

2.1 Fundamentals of IoV Network Architecture and Anomaly Detection

The Internet of Vehicles uses a collaborative "edge + cloud" architecture. Edge nodes are in charge of local traffic collection. They also handle real-time lightweight detection and defense. The cloud carries out global feature fusion. It also does complex attack attribution and model update. IoV attacks are divided into two types. One is common attacks that affect communication transmission. The other is specific attacks that threaten vehicle control. Anomaly detection in IoV must meet four core requirements. These requirements are high accuracy, strong real-time performance, interpretability and edge deployability.

2.2 Core Theories of Causal Inference

Causal inference and correlation inference have key differences. Causal inference can reveal the essential causal relationships among variables. It can decouple spurious correlations. It achieves stronger robustness and interpretability. This paper takes the Structural Causal Model (SCM) as the core model. The SCM is composed of causal graphs, structural equations, counterfactuals and intervention logic. This paper combines the potential outcome framework to calculate causal effects. Causal intervention is used to eliminate confounders. Counterfactual reasoning clarifies the causal roles of variables. It helps realize accurate attribution. The three principles of causal inference are clearly defined in Ref. [2]. They provide a theoretical basis for the application of causal inference in this paper.

2.2.1 Confounders and the SCM Model

Confounders are key factors. They stop correlation inference from accurately identifying causal relationships between variables. They refer to bias path variables in a directed acyclic graph. These variables affect both the cause variable and the outcome variable at the same time. For example, in the Internet of Vehicles, there is a concealed attack host Z. It is controlled by an attacker. The attacker forges an IP (X) to launch attacks. This leads to abnormal traffic characteristics (Y). In this case, Z is a confounder.

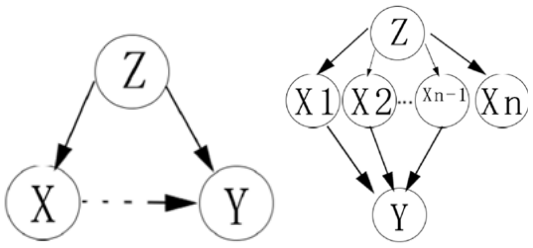

Fig. 1. Confounding Factor Graph

2.2.2 Causal Intervention and Counterfactual Reasoning

Causal intervention uses the do-operator to change the state of a variable and analyze its effect on the outcome. The core formula is as follows:

$$P_M(x|do(y)) = P_{M_y}(x)$$

(Formula 1: Post-intervention distribution of the do-operator)

$$P(X = x/Y = y) \neq P(X = x/do(Y = y))$$

(Formula 2: Formula for the difference between statistical inference and causal intervention inference)

$$P' = P\left(\varepsilon = e' | \varepsilon = e, do(X' = x)\right)$$

(Formula 3: Probability formula of feature abnormality in counterfactual reasoning)

2.3 Adaptability of Causal Inference to Anomaly Detection in IoV

Causal inference is highly compatible with the requirements of anomaly detection in the Internet of Vehicles.Causal intervention can decouple spurious correlations. It can eliminate scenario noise such as vehicle mobility and equipment perception errors.Counterfactual reasoning can clarify the causal relationship between “attacks and anomalous features”. It improves the interpretability of detection.The SCM can incorporate exogenous scenario variables including vehicle driving state and traffic density. It can clearly characterize the causal relationships among multiple variables. It can eliminate attribution bias. It thus meets the modeling requirements of IoV.

3 Analysis of Core Issues in IoV Network Anomaly Detection

Network anomaly detection in the Internet of Vehicles faces four core issues. These issues have become application bottlenecks for existing methods:

Traffic characteristics have four key properties. They are highly dynamic, heterogeneous, transient and periodic. Network topology changes in real time. General feature sets cannot adapt to these properties. They easily mix up periodic features with attack features. There is a prominent problem in traffic feature extraction. It is the "distorted correspondence between features and attacks caused by lossy compression". This problem is more obvious in IoV scenarios.

Scenario and collaborative noise are very similar to attack features. Traditional correlation inference can’t tell them apart effectively. This leads to a high false positive rate. The problem of spurious correlations caused by confounders is more complex. It’s even more complicated in the highly dynamic IoV environment.

Traditional SCM models rely on the "single-attack assumption". They are hard to model combined attacks. Besides, general models have complex structures. Scenario exogenous variables are difficult to quantify. This makes them unsuitable for edge deployment. The NDCML algorithm in Ref. [1] solves single-attack detection. But it does not adapt to IoV combined attacks. It also fails to meet edge deployment requirements.

IoV has strict real-time requirements for detection. General causal algorithms have high computational complexity. They also have large latency. They cannot meet the demand for millisecond-level response. The IoV-NDCML algorithm to be designed later will solve the above issues one by one.

4 Design of IoV Network Anomaly Detection Algorithm Based on Causal Inference (IoV-NDCML)

4.1 Overall Framework Design of the Algorithm

The IoV-NDCML algorithm is improved based on the NDCML framework in Ref. [1]. It adopts a distributed edge-cloud collaborative architecture. This architecture forms a closed loop: edge detection → cloud attribution → edge defense. A lightweight algorithm version is deployed on edge nodes.It is used for feature collection, normalization, causal screening and simple attack detection.It reports data to the cloud.
The full version runs on the cloud.It integrates global features.It constructs the SCM for complex attack attribution.It updates the prior probability table synchronously.It issues defense instructions to edge nodes.

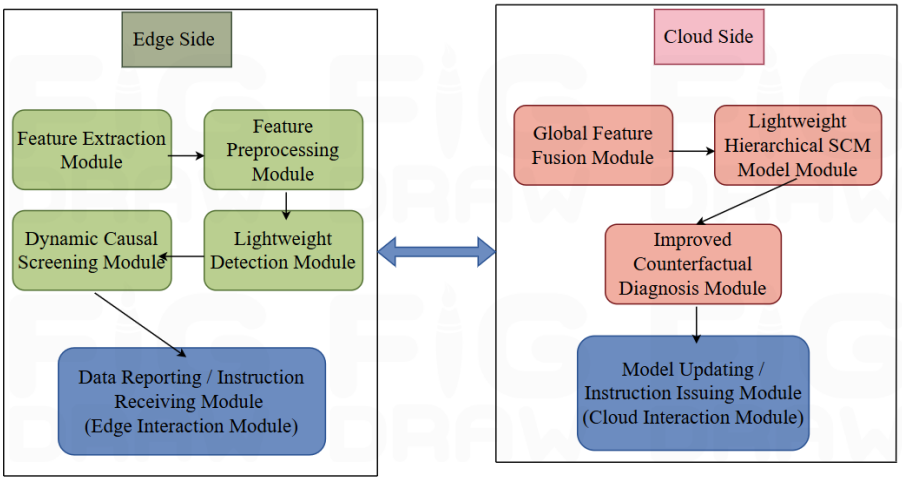

Fig. 2. IoV-NDCML Algorithm Framework Diagram

4.2 Extraction and Normalization of Causally Interpretable Features for IoV

After extracting IoV features, traffic flows are divided according to flow ID.Core features are calculated.
Twenty-eight core features are extracted from four dimensions. These features have clear causal correlations to attacks. They form a multi-dimensional causally interpretable feature set. Partial core features are shown in the table below:

Table 1. Causally Interpretable Core Features

Feature Name	Description	Belonged Layer
Flow ID	Flow ID (composed of source address, destination address, and protocol number)	Network Layer
Flow Duration	Flow duration (μs)	Network Layer
Fwd PL Mean	Mean size of forward packets	Network Layer
CAN Bus Data Transmission Delay	Time consumption of in-vehicle CAN bus data transmission	In-vehicle Physical Layer
RSU Node Load Ratio	Real-time load ratio of Road Side Unit	Node State Layer

Linear normalization is applied to map the features into the interval [0, 1], with the formula as follows:

$$YD_{ij} = Round[(\frac{Y_{ij} - min(Y_{ij})}{\max(Y_j) - min(Y_j)}) * N]$$

(Formula 4: Feature normalization formula)

Special fluctuation elimination is performed on periodic features in the IoV, providing a high-quality feature foundation for subsequent causal inference.

4.3 Dynamic Causal Intervention Feature Screening Fused with Scenario Weights

Three types of scenario noise features are defined.The do-operator is performed on each feature.Its average causal effect (ACE) on the attack label is calculated.This measures the causal correlation strength between the feature and the attack.The calculation formula of average causal effect is as follows:

$$Lj = E[X = 1|do(Yj = 1) - E[X = 1|do(Yj = 0)]$$

(Formula 5: Calculation formula of average causal effect)

On the basis of IPW weighting, scenario weights and communication link weights are introduced to improve the weighted causal effect calculation method. The formula is as follows:

$$L_j = \left(Y^T{}_j \sum W\, Y_{-j}/n\right) - \left(Y^T{}_j W/n\right).\left(Y^T{}_{-j} W/n\right)$$

(Formula 6: Improved weighted causal effect calculation formula)

Instead of the fixed threshold scheme, the screening threshold is dynamically adjusted according to vehicle driving state and network topology.It eliminates noise features.In

addition, the binary decomposition method is used.It decomposes continuous features into Bernoulli distribution features.This satisfies the modeling assumptions of the model.

4.4 Construction of Lightweight Hierarchical SCM Causal Model for IoV

a A three-layer SCM causal model is built. It is an attack-feature-scenario model.The attack layer includes 6 common attacks. It also includes 6 IoV-specific attacks.The feature layer is made up of the extracted core causal features. Causal edges are established between the feature layer and the attack layer.
The scenario layer contains exogenous variables. These variables include driving speed and traffic density.Causal edges are established between the scenario layer and the feature layer. This helps eliminate attribution bias.An attack coordination factor is introduced. It is used to improve the Noisy-OR model.This improvement enables effective modeling of combined attacks.Irrelevant nodes are pruned. This achieves model lightweighting.Structural equations are used. They quantify the influence of scenario variables.This meets the deployment requirements of edge nodes.

4.5 Improved Real-Time Counterfactual Diagnosis Method

a dual-network SCM model with factual and counterfactual networks is constructed.
In the counterfactual network, only the target attack is set to the non-occurrence state, while the rest of the network structure remains consistent with the factual network.

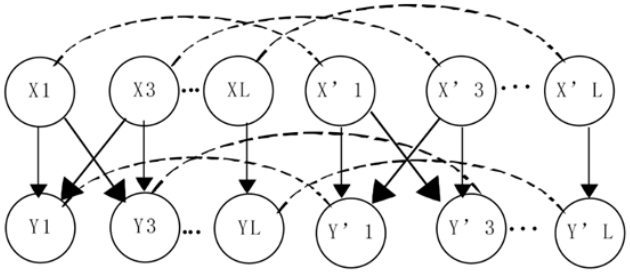

Fig. 3. Dual-network SCM graph

When performing the do-operator, only the target attack, core features and key scenario variables are retained. This reduces computational complexity.The prior causal probability tables of 12 common attacks are precomputed. This improves detection efficiency.A scenario correction coefficient is introduced. It is used to improve the counterfactual expectation formula, as shown below:

$$E(Xa,\varepsilon) := \sum_{Y'} |Y'_+|\, P(Y'|\varepsilon, do(Pa(Y_+)\backslash Xa = 0))P(Y'_+, Xa|\varepsilon)$$

(Formula 7: Improved counterfactual expectation formula)

Clear attribution decision rules are designed.In single-attack scenarios, the attack type with the maximum counterfactual abnormal feature expectation is selected.In combined-attack scenarios, collaborative anomalies are identified.The contribution degree of each attack is calculated.Structured diagnosis results are output.This solves the pain point of "only alarm without explanation" in traditional detection.

5 Experimental Design and Result Analysis

5.1 Experimental Environment and Dataset Construction

The experiment adopts an “edge + cloud” hardware architecture:Edge nodes are based on NVIDIA Jetson Nano to simulate RSU and on-board edge boxes.The cloud is deployed on an Intel Core i7-12700H server to realize global attribution.
OpenV2X is used to build the simulation scenario, and a self-built IoV-CICIDS dataset is constructed with reference to the labeling rules of CICIDS2019.48 hours of IoV operation data are collected to generate 100,000 samples (40,000 normal, 60,000 attack).The dataset is split into training and test sets at a ratio of 7:3.Samples cover 28 core features and 12 attack types, with balanced distribution and strong scenario representativeness.

5.2 Evaluation Metrics and Experimental Scheme

Detection accuracy (ACC), false positive rate (FPR), false negative rate (FNR), detection latency (DL), and causal interpretability score (CIS) are selected as the core evaluation metrics.The calculation formulas of ACC, FPR, and FNR are as follows:

$$ACC = (TP + TN)/(TP + TN + FN + FP)$$

(Formula 8: Calculation formula of ACC)

$$FPR = FP/(FP + TN)$$

(Formula 9: Calculation formula of FPR)

$$FNR = FN/(TP + FN)$$

(Formula 10: Calculation formula of FNR)

Comparative experiments and ablation experiments are designed to verify the algorithm performance.In the comparative experiments, 3 traditional machine learning algorithms, the original NDCML, and 2 existing IoV algorithms are selected as benchmarks, tested under both single-attack and combined-attack scenarios.In the ablation experiments, 4 versions of the algorithm are constructed by successively removing core modules, so as to verify the effectiveness of each module.

5.3 Experimental Results and Analysis

5.3.1 Comparative Experimental Results

The IoV-NDCML algorithm achieves significantly better overall performance than all comparison algorithms:

In the single-attack scenario:ACC reaches 99.2%, FPR is 0.3%, edge-side DL is 38 ms, and CIS is 9.2.Among the comparison algorithms: Bayesian BN has an accuracy of 92.1%, the original NDCML has a latency of 120 ms, and LSTM-V2X has an accuracy of 96.5%.
In the combined-attack scenario:The algorithm achieves an ACC of 97.5%, FNR of 1.8%, and cloud-side DL of 82 ms.In contrast, the accuracy of the original NDCML drops to 88.7%, and LSTM-V2X only reaches 90.3%,showing obvious performance degradation for all comparison methods.
The performance comparison of different algorithms is shown in the table below:

Table 2. Performance Comparison of Different Algorithms

Classifier	**No. of features**	**Precision**	**TPR**	**F-Measure**	**DL(ms)**	**CIS**
KNN	80	0.96	0.96	0.96	150	6.5
ID3	80	0.80	0.80	0.80	120	5.8
BN	80	0.92	0.92	0.92	110	7.0
Original NDCML	29	0.89	0.89	0.89	120	8.5
LSTM-V2X	35	0.96	0.96	0.96	95	7.2
IoV-NDCML	29	0.99	0.99	0.99	38 (edge)	9.2

5.3.2 Ablation Experiment Results

Ablation experiments verify the necessity of each core module:
Removing the scenario-weighted screening module increases the false positive rate to 2.8%.
Removing the attack coordination factor reduces the ACC in combined-attack scenarios to 89.3%.
Removing the improved counterfactual diagnosis module increases detection latency to 132 ms and decreases CIS to 7.1.
The ablation experiment results are shown in the table below:

Table 3. Ablation Experiment Results

Algorithm Version	**ACC (Single Attack)**	**ACC (Combined Attack)**	**FPR**	**DL(ms)**	**CIS**
IoV-NDCML (Full Version)	99.2%	97.5%	0.3%	38	9.2

Algorithm Version	ACC (Single Attack)	ACC (Combined Attack)	FPR	DL(ms)	CIS
Without scenario-weighted screening	97.8%	95.2%	2.8%	36	9.0
Without attack coordination factor	98.9%	89.3%	0.4%	37	8.9
Without improved counterfactual diagnosis	98.5%	96.8%	0.5%	132	7.1

5.3.3 Robustness Test Results

In high-noise scenarios, the ACC of the IoV-NDCML algorithm still reaches 96.7%, showing superior anti-noise ability compared with competing algorithms (original NDCML 88.5%, BN 85.3%, KNN 90.2%).

Four typical attack types are selected for confusion matrix analysis to verify the classification accuracy. The results are shown in the table below:

Table 4. Confusion Matrix Results for Different Attack Types

class	UDP	Syn	NetBIOS	Fake Base Station Spoofing	BENIGN
UDP	11227	0	0	0	68
Syn	0	60568	0	0	8
NetBIOS	0	0	9099	0	1
Fake Base Station Spoofing	0	0	0	8762	5
BENIGN	2	0	31	4	427

In summary, through the synergy of multiple modules, the IoV-NDCML algorithm effectively solves the four core problems of IoV anomaly detection. It has high detection accuracy, low latency, strong robustness, and good interpretability, meeting the requirements of edge deployment.

6 Conclusion and Future Work

6.1 Main Research Conclusions

This paper completes a series of studies focusing on IoV network anomaly detection, with the core conclusions as follows:The four core problems of IoV anomaly detection are clarified, and the adaptability of causal inference is verified.The constructed multi-dimensional causally interpretable feature set and IoV-Flowmeter tool can realize efficient collection of multi-link features.The designed dynamic causal intervention screening method improves the anti-noise ability and detection accuracy of the algorithm.The constructed lightweight hierarchical SCM model solves the problems of combined attack modeling and edge deployment.The improved counterfactual diagnosis method achieves millisecond-level response and interpretable output.Simulation experiments show that the comprehensive performance of the IoV-NDCML algorithm is superior to existing comparison algorithms, which can realize accurate IoV anomaly detection and causal attribution.

6.2 Limitations and Future Work

Limitations of this study are as follows:The dataset used in the experiments is simulation data, which differs from real-world scenarios.The research on combined attacks is limited, and high-complexity combined attacks are not thoroughly investigated.The lightweight degree of the algorithm can be further optimized, and it is not fully adapted to low-computing edge devices.Dynamic and adversarial attack scenarios are not considered.

Future research directions:Collect real IoV data to optimize the algorithm.Expand the scope of combined attack research and refine the attack coordination factor.Promote extreme lightweight of the algorithm to adapt to low-computing devices.Introduce dynamic and adversarial attack scenarios and study anti-interference strategies.Explore the integration of causal inference with deep learning and federated learning to build a multi-agent collaborative detection framework.Combine causal discovery techniques to solve data missing problems and improve the generalization ability of the algorithm.

ACKNOWLEDGMENTS

This work was supported in part by the Shenzhen Science and Technology Program under Grant JCYJ20250604140051064; the Guangdong Basic and Applied Basic Research Foundation under Grant 2024A1515011688; Hunan Provincial Natural Science Foundation of China (No. 2025JJ70343); the Innovation Engineering Project of Shenzhen Polytechnic University under Grant 2024CXGC017 and in part by the Post-doctoral Later-stage Foundation Project of Shenzhen Polytechnic University under Grant 6023271024K1.

References

1. Zeng, Z.R., Peng, W., Zeng, D.T. A Network Anomaly Detection Method Based on Causal Reasoning. Unpublished manuscript, submitted for publication, 2026.
2. Hu, Y.S., Xu, T.Y., Cui, X.Y., Cheng, Q.S.: Inferring Uncertain Knowledge Based on Bayesian Networks. In: Computer Integrated Manufacturing Systems-CIMS, vol. 12, pp. 65–68 (2001). https://doi.org/10.13196/j.cims.2001.12.66.huysh.014
3. Li, X.H., Zhong, C., Chen, Y., Zhang, H.L., Weng, J.: A Survey on Internet of Vehicles Security. In: Journal of Information Security Research, vol. 4, no. 3, pp. 17–33 (2019). https://doi.org/10.19363/J.cnki.cn10-1380/tn.2019.05.02
4. Editorial Board of China Journal of Highway and Transport. Overview of China's Automotive Engineering Academic Research: 2023. In: China Journal of Highway and Transport, vol. 36, no. 11, pp. 1–192 (2023). https://doi.org/10.19721/j.cnki.1001-7372.2023.11.001
5. Li, J.N., Xiong, R.B., Lan, Y.Y., Pang, L., Guo, J.F., Cheng, X.Q.: A Survey on Advances in Causal Machine Learning. In: Journal of Computer Research and Development, vol. 60, no. 1, pp. 59–84 (2023). https://doi.org/10.7544/issn1000-1239.2023.20220544
6. Wang, S.C., Zheng, F., Zhang, L.: Learning Temporal Causal Relationships Based on Bayesian Networks. In: Journal of Software, vol. 32, no. 10, pp. 3068–3084 (2021). https://doi.org/10.13328/j.cnki.jos.006012
7. Chen, S.Z., Hu, J.L., Shi, Y., Zhao, L.: LTE-V2X Vehicular Networking Technology, Standards and Applications. In: Journal of Communications, vol. 39, no. 5, pp. 1–12 (2018). https://doi.org/10.11959/j.issn.1000-436x.2018165
8. Chen, S.Z., Ge, Y.M., Shi, Y.: Development, Applications and Prospects of Cellular Vehicle-to-Everything (C-V2X) Technology. In: Journal of Communications, vol. 43, no. 2, pp. 1–15 (2022). https://doi.org/10.11959/j.issn.1000-436x.20220345