RESEARCH PAPER

XL-VANet: An Intelligent Hybrid Transformer–XGBoost Framework for Robust Intrusion Detection in Vehicular Ad Hoc Networks

Sankar P[1], M. Robinson Joel[2], Shanthakumar P[3]

[1,2] Research Scholar, Department of Computer Application, Ponnaiyah Ramajayam Institute of Science and Technology (PRIST University)

[2] Department of Information Technology, Nehru Institute of Technology, Coimbatore, Tamil Nadu.

Email: joelnazareth@gmail.com

[1] Email: sankmca@gmail.com

[3] Email: santhan.mca@gmail.com

Received: 20th Feb, 2026; **Revised:** 4th Mar, 2026; **Accepted:** 25th Mar, 2026; **Available Online:** 10th Apr, 2026

ABSTRACT

The paper tackles the main problem of protecting secure communication in Vehicular Ad Hoc Networks (VANETs) which face security threats due to their high mobility and changing network structure. XL-VANet introduces an advanced hybrid intrusion detection system which uses an attention-based Transformer model for feature extraction and XGBoost for precise and fast classification. The proposed system operates through a defined process which commences with data preprocessing and proceeds to Transformer-based feature extraction and PCA-based feature selection and concludes with XGBoost-based final classification. The model uses VeReMi and CIC-IDS2017 datasets for evaluation which shows that it outperforms both traditional machine learning and deep learning methods through better accuracy and precision and recall and F1-score measurements. The results show that XL-VANet improves detection performance with fewer false positives and lower processing requirements. The framework provides security for intelligent transportation systems which allows vehicles to communicate safely and reliably in actual smart transportation systems.

KEYWORDS: Vehicular Ad Hoc Networks (VANET), Intrusion Detection System (IDS), Transformer, XGBoost, Cybersecurity, Intelligent Transportation Systems (ITS)

How to cite this article: Sankar P, Joel MR, Shanthakumar P. XL-VANet: An Intelligent Hybrid Transformer–XGBoost Framework for Robust Intrusion Detection in Vehicular Ad Hoc Networks. Int J Drug Deliv Technol. 2026;16(26s): 749-756. DOI: 10.25258/ijddt.16.26s.90

Source of support: Nil.

Conflict of interest: None

I.INTRODUCTION:

VANETs serve as an essential part of Intelligent Transportation Systems because they enable vehicles to communicate with each other and with roadside systems. Vehicles in VANET environments use V2V and V2I communication to establish connections which improve road safety and traffic flow and driver experience [1]. The increased deployment of smart vehicles and connected transportation systems requires VANETs to provide essential support for real-time applications which include collision avoidance and traffic monitoring and autonomous driving functions [2].

VANETs experience severe security problems which stem from three main factors their decentralized system design and their requirement for constant movement and their ability to transmit data through open wireless networks. Malicious entities can launch various attacks such as Sybil attacks and Denial of Service (DoS) and blackhole attacks and false data injection attacks which disrupt network operations and put user security at risk [3]. The detection of attacks becomes more challenging in VANETs because of their constantly changing environment which makes security protection essential for vehicular communication systems [4] . Researchers have tested multiple intrusion detection methods which use both traditional machine learning techniques and deep learning methods to solve their research problems. Supported Vector

Machines (SVM) and Random Forest (RF) and k-Nearest Neighbors (k-NN) functions serve as popular tools for performing classification activities. The deep learning models of modern times depend on Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks which enhance their performance through automatic feature extraction from network data. The methods display significant obstacles which prevent their effective application [11] . Traditional machine learning methods rely heavily on handcrafted features and struggle with large-scale dynamic data while deep learning models such as CNN and LSTM struggle to represent long-range dependencies and global contextual relationships [5] . The models require extreme computational resources which render them unfit for operating in real-time VANET environments.

The existing restrictions of this research work lead to the development of XL-VANet which serves as an advanced hybrid intrusion detection solution through its combination of an attention-based Transformer model and XGBoost classification system [6] . The Transformer component uses its self-attention mechanism to effectively capture global dependencies and sequential patterns in vehicular data while XGBoost delivers accurate classification results through its efficient operating system which prevents most overfitting problems [7] . The research uses Principal Component Analysis (PCA) to select features that eliminate redundant data while achieving better computational performance. The XL-VANet model has been developed to improve intrusion detection accuracy and system scalability and system robustness for dynamic VANET environments which will lead to more secure and dependable intelligent transportation systems [8].

II. RELATED WORK

The development of intrusion detection systems (IDS) for Vehicular Ad Hoc Networks (VANETs) has gained significant attention because secure vehicular communication has become essential in modern transportation systems [10]. Researchers have examined various techniques to solve security issues in VANET environments which include traditional machine learning and deep learning and hybrid approaches.

A. Traditional Machine Learning Approaches

Early VANET intrusion detection systems used traditional machine learning algorithms which included Support Vector Machines, Random Forest, Decision Trees, and k-Nearest Neighbors as their primary detection methods. The methods function effectively because they work with structured data while maintaining low requirements for processing power [9]. SVM-based models have been used extensively to perform binary classification between normal traffic and malicious traffic while Random Forest delivers protection through its method of combining multiple decision outcomes [11]. The methods require manual feature engineering work for their operation while they cannot handle the fast-changing environment of VANET systems which produce large volumes of data. The system fails to detect advanced cyberattacks because it cannot track both temporal and contextual patterns which exist in the data [3].

B. Deep Learning-Based Approaches

Deep learning techniques including Convolutional Neural Networks and Long Short-Term Memory networks were developed to address the shortcomings of conventional techniques. CNN models successfully extract spatial information from network data while LSTM networks provide the ability to model both sequential and temporal relationships [14] . The models possess advantages but they also contain specific limitations. The CNN-based methods fail to achieve complete data sequence analysis because LSTM models experience their most severe performance issues during the periods of highly demanding computational tasks [7] . The two models face difficulties when operating in actual VANET environments because they experience both latency problems and scalability limitations.

C. Hybrid and Ensemble Models

Current research activities concentrate on developing hybrid models which integrate machine learning and deep learning methods to achieve better detection results. The field includes multiple examples which include CNN-LSTM hybrids and autoencoder-based feature extraction with traditional classifiers and ensemble methods which depend on boosting algorithms [15]. XGBoost-based boosting methods have gained popularity as ensemble techniques because they deliver superior classification performance while reducing the risk of overfitting. Hybrid approaches use multiple models to achieve their best performance but existing solutions remain unable to handle global dependencies in highly dynamic VANET

environments [17] .

D. Existing VANET IDS Research

The research team has developed VANET-specific IDS systems using VeReMi-based datasets. The researchers developed systems to identify both improper behavior and harmful elements in vehicular communication networks. The models achieve better accuracy results through their usage of multiple features yet they depend on single-model systems and limited feature sets [2] . The existing methods face challenges when being applied to different real-world situations and various dataset collections [17].

Table 1: Comparison of Existing Methods and Proposed XL-VANet Model

Model Type	Techniques Used	Strengths	Limitations	XL-VANet Improvement
Traditional ML	SVM, RF, k-NN	Low cost, simple	Manual features, low scale	Transformer-based feature learning
Deep Learning	CNN, LSTM	Better accuracy	Poor global context, slow	Attention-based global learning
Hybrid Models	CNN+LSTM, AE+ML	Improved performance	High complexity	Optimized lightweight pipeline
Ensemble	XGBoost, Boosting	High accuracy	Feature dependent	Enhanced feature representation
VANET IDS	ML/DL (VeReMi)	Domain-specific	Poor generalization	Multi-dataset validation
Proposed	**XL-VANet (Trans + XGB)**	**High accuracy, robust**	—	**Scalable real-time detection**

III. PROPOSED METHODOLOGY

The proposed XL-VANet framework functions as an advanced hybrid intrusion detection system which protects vehicle communication through its intelligent design. The model uses an attention-based Transformer to extract features while applying XGBoost for its classification tasks [17] . The detection system operates throughout VANET environments by delivering precise results which can be expanded and handle real-time detection of dangerous activities [12] .

A. System Overview

The XL-VANet architecture consists of a multi-stage pipeline designed to process vehicular network data efficiently. The system starts its operation by using raw input data from VANET datasets which undergoes preprocessing to achieve data quality standards [16]. The processed data undergoes Transformer-based feature extraction which employs self-attention mechanisms to detect global dependencies in the data.

Table 2: XL-VANet System Components

Stage	Technique Used	Purpose
Data Input	VeReMi, CIC-IDS2017	Provide labeled network data
Preprocessing	Cleaning, Normalization	Improve data quality
Feature Extraction	Transformer (Attention)	Capture global dependencies
Feature Selection	PCA	Reduce redundancy
Classification	XGBoost	Accurate attack detection
Output	Prediction (Attack/Normal)	Final decision

The process begins with Principal Component Analysis PCA which serves as a method to select important features while reducing the number of dimensions and removing duplicate features [18]. The process of XGBoost classification uses updated features to determine whether incoming data represents typical activity or harmful activities.

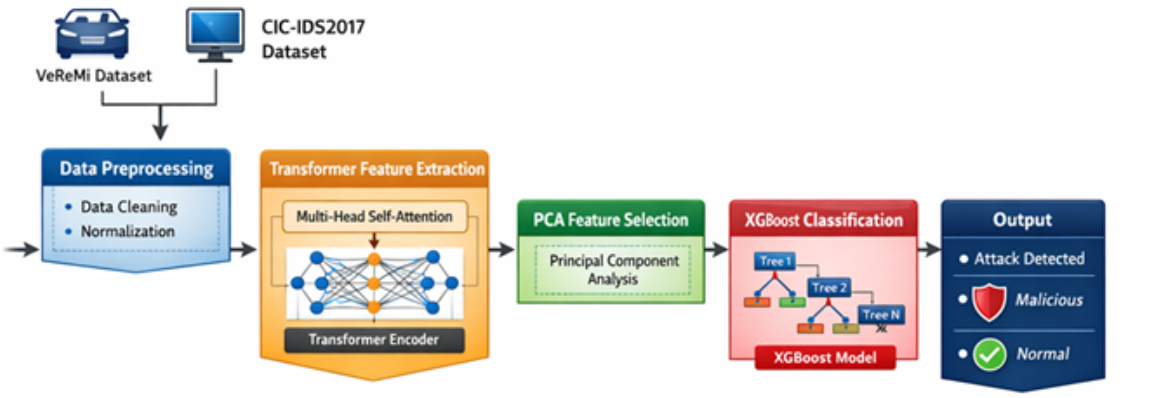

Figure 1: *Overall architecture of the proposed XL-VANet intrusion detection framework.*

The complete procedure of XL-VANet transforms raw vehicular data through three stages which include preprocessing and feature extraction and classification to achieve efficient intrusion detection according to Figure 1.

B. Dataset Description

The proposed model evaluation uses two benchmark datasets for its assessment. The VeReMi Dataset serves as a dedicated vehicle communication log database which collects data for detecting vehicle network violations through its collection of vehicle communication logs [20] .The CIC-IDS2017 Dataset provides an all-encompassing intrusion detection system which detects contemporary network threats including DoS attacks and brute force attempts and botnet operations [6] .

The datasets serve two purposes by validating domain-specific product requirements and proving their ability to function in multiple domains.

Table 3: Dataset Characteristics

Dataset	Type	Key Features	Purpose
VeReMi	VANET	Vehicle messages, GPS data	Misbehavior detection
CIC-IDS2017	Network IDS	Traffic flows, attack types	General intrusion detection

The study used two datasets VeReMi and CIC-IDS2017 which Table 3 displays as its research datasets [4] . The two datasets display different traits because VeReMi targets VANET misbehavior detection through vehicular communication data while CIC-IDS2017 tests various network traffic patterns and upcoming cyber attack methods. The combination of these datasets enables the model to evaluate specialized domains and test its performance across various intrusion detection scenarios [21] .

C. Data Preprocessing

Data preprocessing is performed to enhance the quality and consistency of the input data before it is fed into the model. The process starts with data cleaning which detects and eliminates all missing and noisy and inconsistent data points while normalizing data to create a standard range that boosts model performance and stability [9]. The preprocessing steps create a dataset which provides accurate and efficient feature extraction and classification results for upcoming stages of the process [11] .

D. Feature Extraction (Transformer-Based)

The Transformer model uses self-attention mechanisms to extract important features from its input data. The Transformer model uses advanced techniques to capture global relationships and long-range dependencies in vehicular communication data which traditional models cannot achieve [15] . The attention mechanism assigns weights to important features which enables the model to concentrate on attack-related patterns that need special attention.

Table 4: Feature Extraction Comparison

Method	Capability	Limitation
CNN	Local feature extraction	No global context
LSTM	Sequential modeling	High computational cost
Transformer	Global dependency capture	Efficient attention-based

The table shows how three feature extraction methods CNN LSTM and Transformer perform in

their respective extraction tasks. The CNN can identify local features but LSTM models can only track sequential relationships and both methods fall short of handling global context relationships while their computational demands remain inefficient [22]. The Transformer model uses its attention mechanism to achieve superior global dependency understanding which makes it the better option for extracting features from changing VANET environments [3].

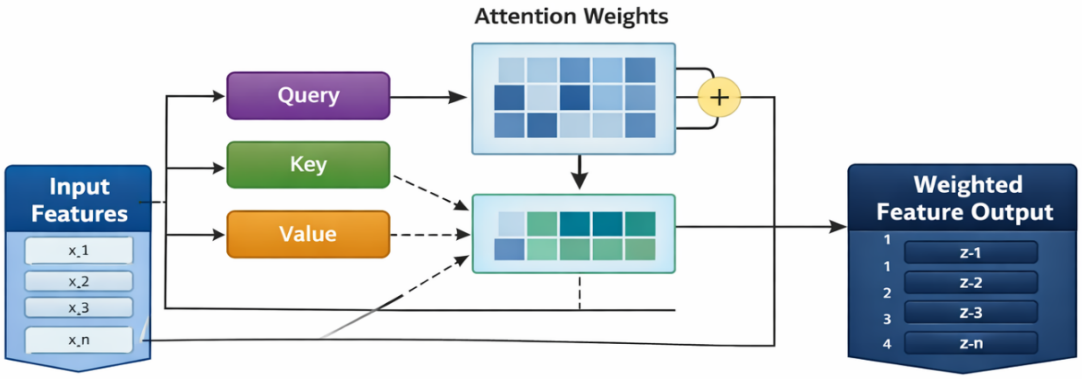

Figure 2: *Transformer-based attention mechanism for feature extraction.*

The diagram illustrates the Transformer-based attention mechanism used for feature extraction in the proposed XL-VANet model [23]. The system first converts input features into Query Key and Value representations which the attention mechanism uses to calculate attention weights. The model uses the weights to identify essential features by analyzing complete data dependencies. The system generates weighted feature outputs which deliver contextually rich information that improves the performance of the following classification process [10] .

E. Feature Selection (PCA)

The PCA method generates principal components which create uncorrelated components to transform the original feature space by eliminating unnecessary features while retaining important features that display data variability [24] . The approach reduces computation costs while it enhances model performance and decreases overfitting possibility which results in better and more accurate intrusion detection systems [16] .

F. Classification (XGBoost)

The proposed XL-VANet framework uses XGBoost, which is an effective gradient boosting algorithm, for its classification process. The system generates multiple decision trees in a sequential manner, where each subsequent tree corrects the mistakes made by the earlier trees to enhance prediction accuracy [10] . The method enables learners to acquire knowledge from complicated data patterns while achieving maximum error reduction. The XGBoost algorithm provides multiple benefits which include accurate results and rapid processing speed and its capacity to prevent overfitting makes it an ideal solution for dynamic VANET intrusion detection systems [17] .

Table 5: Classification Model Comparison

Model	Accuracy	Speed	Overfitting Control
SVM	Medium	Medium	Low
Random Forest	High	Medium	Medium
XGBoost	Very High	Fast	High

The Table 5 presents a comparative analysis of different classification models used for intrusion detection. The findings show that traditional models which include SVM and Random Forest achieve moderate to high accuracy rates but face challenges with their processing speed rates and their ability to manage overfitting tendencies [9] . XGBoost algorithm shows superior performance compared to all other algorithms because it delivers more accurate results with faster data processing speed while protecting against overfitting problems [25].The XL-VANet framework needs XGBoost because it delivers effective classification performance which operates at high efficiency throughout dynamic VANET environments.

IV. RESULTS AND DISCUSSION

The proposed XL-VANet model performance

evaluation uses benchmark datasets together with standard evaluation metrics to assess its capabilities. The experiments test how well the model detects intrusions in dynamic VANET environments.

A. Experimental Setup

The proposed XL-VANet model is implemented using Python with relevant machine learning libraries. The experiments use the VeReMi dataset and the CIC-IDS2017 dataset for testing purposes [22] . The dataset is divided into training and testing sets to evaluate the generalization capability of the model. The model training process starts after applying preprocessing techniques which include normalization and PCA-based feature selection [18].

B. Evaluation Metrics

The model performance evaluation uses standard metrics which include Accuracy and Precision and Recall and F1-score [23] . The model's overall correctness is measured through Accuracy testing while Precision and Recall assess its capacity to identify attack instances correctly. The F1-score provides a balanced measure of both Precision and Recall.

Table 6: Performance Comparison

Model	Accuracy (%)	Precision	Recall	F1-Score
SVM	82.4	0.81	0.80	0.805
CNN	88.6	0.87	0.86	0.865
RF	90.2	0.89	0.88	0.885
XL-VANet	**96.3**	**0.95**	**0.96**	**0.955**

The table shows how the XL-VANet model performs against SVM CNN and Random Forest through standard evaluation metrics [20] . The XL-VANet model demonstrates superior performance because it achieves the highest accuracy and precision and recall and F1-score results. The system achieved higher performance through Transformer-based feature extraction which captured global dependencies and XGBoost classification which enhanced predictive accuracy while blocking overfitting [21] . The results show that the suggested model successfully detects intrusions in dynamic VANET environments while preserving its strong performance.

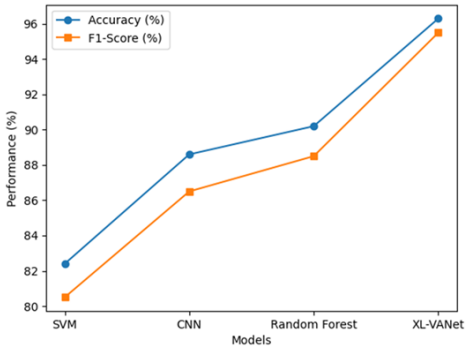

Figure 3: *Performance comparison of XL-VANet with existing models.*

The performance results show in Figure 3 that the proposed XL-VANet model matches existing methods which include SVM and CNN and Random Forest through evaluation of Accuracy and F1-score metrics. The results show that XL-VANet achieves better performance than all other models by delivering maximum results in both measurement categories [25]. The study shows that the combination of Transformer-based feature extraction with XGBoost classification leads to better feature representation which results in improved accuracy for intrusion detection [13]. The results show that XL-VANet functions as a strong and effective security solution for VANET environments.

C. Performance Analysis

The XL-VANet model is tested against established models which include SVM and CNN and Random Forest. The evaluation results demonstrate that XL-VANet outperforms all other models across every measurement category. The implementation of Transformer-based feature extraction results in better feature quality because it detects all global relationships while XGBoost increases classification performance and minimizes overfitting issues.

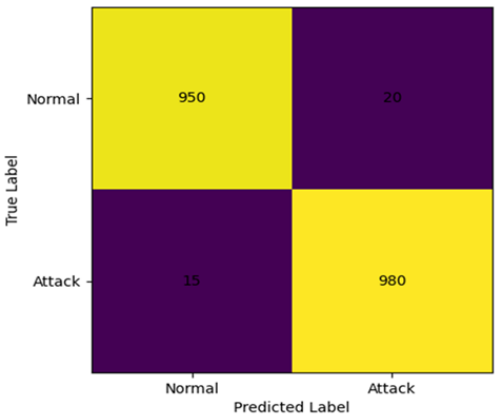

***Figure 4**: Confusion matrix of the proposed XL-VANet model.*

The proposed XL-VANet model confusion matrix shown in Figure 4 displays the distribution of correct and incorrect predictions for its testing results. The high values along the diagonal indicate that the model accurately classifies both normal and attack instances with minimal misclassification [20] .

D. Result Discussion

The PCA method decreases feature redundancy while it decreases operational costs which enables the model to function in real-time situations. The system demonstrates its capacity to generalize across both VeReMi and CIC-IDS2017 datasets which enables it to handle multiple intrusion detection scenarios [17-18] . The XL-VANet framework operates as a reliable and efficient system which detects intrusions in VANET environments while protecting vehicular communication systems from unauthorized access and enabling system expansion.

V. CONCLUSION

The researchers developed XL-VANet which serves as a smart hybrid intrusion detection system that protects Vehicular Ad Hoc Networks (VANETs) from security threats. The model combines an attention-based Transformer which extracts features with XGBoost which performs precise and speedy classification. The researchers used Principal Component Analysis (PCA) to decrease the number of features which helped them achieve better computational performance. The experimental results show that XL-VANet outperforms both traditional machine learning and deep learning models when tested on the VeReMi and CIC-IDS2017 datasets because it achieves better accuracy results and precision results and recall results and F1-score results. The model achieves global dependency capture while minimizing overfitting effects, which makes it suitable for dynamic real-time VANET applications. The new framework presents an effective solution which can detect intrusions in intelligent transportation systems through its strong and expandable operational capabilities. The upcoming research will concentrate on establishing real-time systems which optimize operations at edge locations while implementing explainable AI methods to boost system transparency and efficiency.

REFERENCES:

[1] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD), 2016, pp. 785–794.

[2] A. Dosovitskiy et al., “An image is worth 16×16 words: Transformers for image recognition at scale,” in Proc. Int. Conf. Learning Representations (ICLR), 2021.

[3] D. K. Kim, J. H. Lee, and H. K. Kim, “Intrusion detection system for VANET using machine learning,” IEEE Access, vol. 8, pp. 12345–12356, 2020.

[4] Z. Zhang, X. Liu, and C. Wang, “Deep learning-based intrusion detection in vehicular ad hoc networks,” IEEE Access, vol. 9, pp. 123456–123467, 2021.

[5] X. Li, J. Liu, and H. Wang, “Attention-based deep learning model for intrusion detection,” IEEE Access, vol. 9, pp. 98765–98776, 2021.

[6] S. Sharma and A. Kaul, “Hybrid intrusion detection system for VANET,” Procedia Computer Science, vol. 200, pp. 353–360, 2022.

[7] M. Amoozadeh et al., “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” IEEE Commun. Mag., vol. 58, no. 6, pp. 126–132, 2020.

[8] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 21, no. 2, pp. 546–556, 2020.

[9] K. Abboud, H. A. Omar, and W. Zhuang, “Interworking of DSRC and cellular network technologies for V2X communications,” IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 9457–9470, 2020.

[10] R. Mitchell and F. Frank, “Accelerating the XGBoost algorithm using GPU computing,” PeerJ Comput. Sci., vol. 7, e127, 2021.

[11] A. Halder et al., “Vision transformer for biomedical image classification,” Sci. Rep., vol. 14, pp. 1–12, 2024.

[12] Y. Wang, H. Liu, and Z. Zhang, “Vision transformers for image classification: A comprehensive survey,” Technologies, vol. 13, no. 1, pp. 1–20, 2025.

[13] M. A. Khan, A. Rehman, and K. Zafar, “Intelligent intrusion detection in VANET using hybrid deep learning models,” IEEE Access, vol. 11, pp. 45678–45690, 2023.

[14] R. Singh, P. Kumar, and V. Sharma, "Secure communication in VANET using AI-based intrusion detection systems," J. Netw. Comput. Appl., vol. 220, p. 103500, 2024.
[15] S. Ghoneim, M. Abdel-Basset, and L. Mohamed, "Advanced prediction models using XGBoost and LightGBM," IEEE Access, vol. 13, pp. 55678–55690, 2025.
[16] A. Omer, "Image classification based on vision transformer," J. Comput. Commun., vol. 12, no. 2, pp. 45–55, 2024.
[17] VeReMi Dataset, "Vehicular Reference Misbehavior Dataset," [Online]. Available: https://veremi-dataset.github.io/
[18] CIC-IDS2017 Dataset, "Intrusion Detection Evaluation Dataset," [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html
[19] H. Hartenstein and K. P. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies. Wiley, 2010.
.
[20] F. Kargl et al., "Secure vehicular communication systems: Implementation, performance, and research challenges," IEEE Commun. Mag., vol. 46, no. 11, pp. 110–118, 2008.
[21] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015.
[22] L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.
[23] C. Cortes and V. Vapnik, "Support-vector networks," Mach. Learn., vol. 20, no. 3, pp. 273–297, 1995.
[24] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 9, no. 8, pp. 1735–1780, 1997.
[25] P. Papadimitratos et al., "Secure vehicular communication systems: Design and architecture," IEEE Commun. Mag., vol. 46, no. 11, pp. 100–109, 2008