Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/75/20240523

AI-based IoT attack filtering methods in the context of connected vehicles

Yiwen Lu

Beijing University of Posts and Telecommunications, Beijing, 100876, China

1587261784@bupt.edu.cn

Abstract. With the rapid development of connected vehicle technology, the volume of data generated in the context of connected vehicles is exhibiting an exponential growth trend compared to the traditional automotive industry. This data is closely related to the security of connected vehicles. However, if threats such as malicious intrusions, information tampering, and data theft cannot be effectively resisted, they will pose significant risks and hazards to users, the entire automotive industry, and society. Therefore, researching and implementing security measures for connected vehicles becomes crucial to ensure the sustainable development and widespread application of connected vehicle technology. In this regard, this paper proposes an optimized IoT attack filtering method based on random forest and neural network algorithms in deep learning to predict and filter malicious attacks. The CICIOT2023 dataset is used for training and evaluation, and results are analyzed based on accuracy, recall, precision, and F1 scores. A comparison between models constructed using random forest and neural networks reveals that while both perform similarly in terms of accuracy and precision, the model built with neural networks significantly outperforms random forest in terms of recall and F1 score. Therefore, for IoT attack filtering methods targeted at connected vehicle scenarios, the algorithm using neural networks for attack identification and filtering is recommended, as it can better protect the confidentiality and security of data in connected vehicle scenarios, ensuring user driving safety and safeguarding societal transportation security.

Keywords: Connected Vehicles, Internet of Things (IoT), Malicious Attack Detection, Network Attacks, Deep Learning.

1. Introduction

With the intensifying global demand for smart solutions, various industries are accelerating their transformation from traditional to intelligent, with the automotive industry showing the most noticeable progress. According to official statistics from OICA, global car sales reached an astonishing 85.02 million units in 2022, representing a 3.2% year-on-year increase.

As a new industrial model that integrates various emerging technologies such as the Internet of Things (IoT), Internet Plus (IoP), big data, and cloud computing, the secure development of connected vehicles has long been high on the agenda. China explicitly stated in the "National Comprehensive Three-Dimensional Transportation Network Plan Outline" that it aims to promote the construction of important integrated infrastructure for connected vehicles and enhance security capabilities. Data shows that by 2023, the global number of vehicles equipped with connected car technology will reach 775

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/75/20240523

million units. Faced with such a vast scale of the automotive industry and a massive amount of data, malicious attacks such as intrusion, information tampering, and data theft have also grown exponentially.

For instance, in 2015, security researcher Samy Kamkar discovered vulnerabilities in General Motors' OnStar system, allowing remote control of vehicles and interception of data communications. In 2016, Mitsubishi Outlander plug-in hybrid electric vehicles could be directly located after the WiFi control module key cracked. In 2018, vulnerabilities were found in Volkswagen and Audi's onboard systems, granting root control access, thereby controlling the vehicle's braking system. In 2020, vulnerabilities were identified in the wireless module and Bluetooth key of the Tesla Model S. In 2022, the U.S. Cybersecurity and Infrastructure Security Agency issued warnings regarding multiple security vulnerabilities in the MiCODUS MV720 Global Positioning System (GPS) tracker, affecting over 1.5 million vehicles worldwide [1].

With the leapfrog development of technology, network attacks have gradually emerged as a global primary threat, with countless network devices being subjected to various forms of intrusion on a daily basis. Simply put, network attacks involve the illegal intervention of information systems, aimed at disrupting, stealing, and even tampering with data [2]. In this context, deep learning can learn and train from vast amounts of complex data, thereby identifying and filtering intricate and ever-changing attack patterns, and providing crucial support for the security of connected vehicles.

2. Concept and Architecture of Connected Vehicles

Connected Vehicles, also known as connected cars, utilize wireless communication technology through onboard vehicle devices to effectively utilize dynamic information of all vehicles in an information network platform, providing various functional services during vehicle operation. Fundamentally, it integrates IoT (Internet of Things) technology to upgrade automobiles into intelligent entities. Specifically, it can be structured into three layers based on IoT, namely the perception layer, network layer, and application layer, as shown in Figure 1.

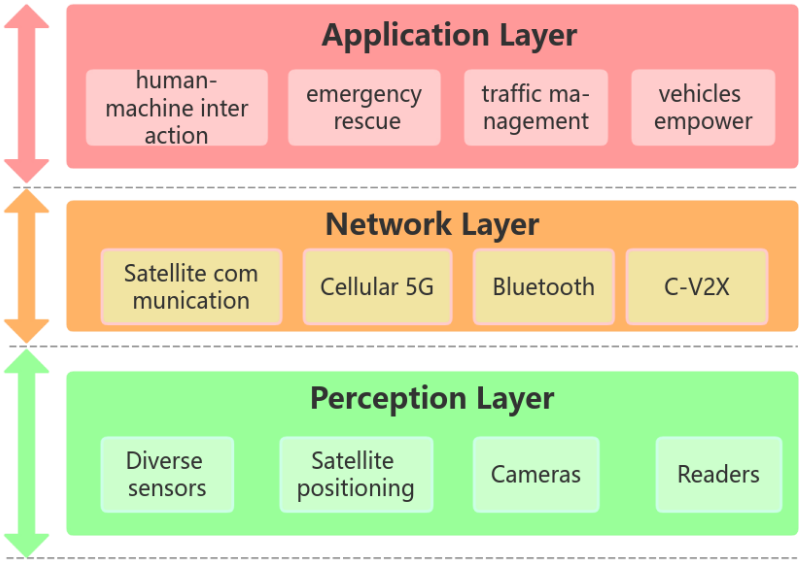


Figure 1. Layered Architecture of Connected Vehicle System

The perception layer serves as the foundation of connected vehicles, acting as the "sensory organs" through which vehicles interact with the external environment. It encompasses various sensing devices such as sensors, Global Positioning System (GPS), cameras, and readers to interact with the surroundings. For instance, it utilizes temperature sensors to perceive outdoor temperature, cameras to capture road conditions, and satellite positioning to accurately locate the driving vehicle, thereby facilitating data and information collection and transformation.

DOI: 10.54254/2755-2721/75/20240523

The network layer acts as the communication medium for connected vehicles, serving as the "language" through which vehicles communicate with the external world. It involves integrating the information and data collected by the perception layer and providing information transmission services to the application layer through network access or by developing network architectures and protocols that meet transmission requirements and adapt to communication environments. Additionally, as an intermediary between the application and perception layers, the network layer transmits relevant instructions issued by the application layer back to the application layer, enabling highly coordinated interactions among humans, vehicles, and objects.

The application layer is the core decision-making component of connected vehicles, functioning as the "brain" through which vehicles interact with the external world. Upon receiving the integrated data from the network layer, the application layer conducts analysis, decision-making, and processing through methods such as data storage, computation, and mining, aiming to achieve compatibility with potential network expansion functions in the future. It provides various application functions for users, enterprises, governments, and society, facilitating application programs and human-machine interaction interfaces.

3. Security threats of connected vehicles

3.1. Threats to Connected Vehicle Terminals

The vehicle perception layer serves as the terminal of connected vehicles, and the sensors in the vehicle's perception layer can generally be divided into two types: traditional sensors and smart sensors. The difference between the two lies in that traditional sensors collect relevant data through physical factors such as pressure, temperature, speed, etc., while smart sensors collect relevant data through means such as infrared radar, biometric features, cameras, etc. Compared to traditional sensors, smart sensors require a larger and more complex amount of data to be collected. Since smart sensors perceive information not only through the physical layer, we need to pay special attention to the security issues of such sensors. If attackers modify or steal data through attacks on sensors, it will greatly affect the judgment of data by the application layer of the network layer, leading to the issuance of incorrect instructions and information, further affecting the safety of vehicle operation.

Smart sensors often need to emit and receive signals during the process of perceiving information [3]. During this process, it is highly susceptible to attacks from malicious actors, such as information eavesdropping, interception, modification, or unauthorized access to launch attacks on vehicles. Therefore, to ensure the security of information during transmission, the terminals of connected vehicles often incorporate a fault diagnosis system. The fault diagnosis system promptly identifies vehicle malfunctions. However, the problem arising from this is that the extensive amount of data and code generated by the fault diagnosis system also becomes a prime target for attackers.

In this context, attacks on the perception layer of connected vehicles can mainly be classified into two types: physical connection and wireless network connection. Attackers use various methods such as sniffing, replay attacks, and spoofing to attack the vehicle bus and onboard systems, aiming to gain control of the vehicle and steal vehicle information. Common attack methods and defense mechanisms against connected vehicle terminals are shown in Table 2. According to the "Global Automotive Cybersecurity Report 2023" published by Upstream, the proliferation of electric smart vehicles has introduced new attack vectors, and electric vehicle charging infrastructure has also become one of the attack targets [4].

Table 2. Common Attack Methods in Connected Vehicles

Typical Attack Methods	Common Defense Measures
Vehicle Botnets	Reputation mechanisms, anomaly detection mechanisms, etc.
Malware Implantation	Access restrictions, etc.
Sniffing Attacks	Port access control, network segmentation, intrusion detection and

DOI: 10.54254/2755-2721/75/20240523

Table 2. (continued).

	prevention systems, etc.
Black Hole Attacks	Introduction of reputation-based routing, etc.
Replay Attacks	Strong encryption methods, virtual private networks, temporal variation, etc.
Witching Attacks	Public-key-based identity and authentication methods, etc.
Timing Attacks	Introduction of random variables to mask temporal features, etc.

3.2. Cloud Threats in Connected Vehicles

Connected vehicle cloud services refer to the storage, computation, analysis, and operation of data through cloud computing-based cloud service platforms, which are the core part of the connected vehicle system. On one hand, the cloud platform provides basic services to relevant departments based on dynamic data, and on the other hand, it provides interactive functions such as vehicle control and vehicle monitoring to users.

Due to the unique application scenarios of the platform, it often becomes the primary target of attackers. Currently, attackers commonly use DDoS, Spoofing, and web-based attacks to target cloud service platforms. Such attacks can result in system paralysis, unauthorized control acquisition, and consequences such as data breaches or permanent deletion.

3.3. Roadside Threats in Connected Vehicles

In the overall system of connected vehicles, communication and coordination are established not only between people and vehicles or between vehicles but also between vehicles and roads, and vehicles and objects. Therefore, roadside threats in connected vehicles mainly refer to basic roadside equipment and digitalized connected vehicle roadside equipment. Basic roadside equipment generally refers to the organic combination of ordinary sensors and communication modules, such as cameras, Light Detection and Ranging (LiDAR), millimeter-wave radar, and other traffic intelligent perception devices. These roadside devices collaborate to capture basic information about vehicles and roads, and therefore, connected vehicle roadside devices mainly interact with onboard terminals and cloud platforms, forming a closed-loop system of connected vehicles. Digitalized connected vehicle roadside equipment is mainly responsible for dynamically perceiving environmental information and traffic signification while delivering it in real-time to onboard terminals and cloud platforms, such as integrating digitalized traffic signals.

Although there are differences in their interaction and perception modes, it is undeniable that roadside equipment in connected vehicles is also one of the most commonly targeted parts by attackers. Roadside infrastructure can provide beyond-line-of-sight perception for connected vehicles, compensating for the limitations of single-vehicle perception. Furthermore, it can aggregate traffic data comprehensively, supporting and realizing refined and real-time traffic control and monitoring. However, it often faces security risks such as illegal intrusion, information tampering, and unauthorized remote control by attackers, resulting in safety hazards for vehicles.

4. Algorithm

4.1. Data Preparation

This experiment utilizes the FIF IOT 2023 dataset, which conducts experiments of six different types: Power, Idle, Interactions, Scenarios, Active, and Attacks, to analyze various protocols and IoT device behavior patterns, vulnerability testing, etc., making it a cutting-edge dataset.

The dataset primarily includes seven types of attack behaviors: DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai.

DDoS Attack: DDoS attacks aim to exhaust the resources of target servers by sending a large number of requests, rendering them unable to provide normal services. Attackers coordinate and control

DOI: 10.54254/2755-2721/75/20240523

multiple infected devices (such as botnets or zombie robots) to launch the attack. These devices simultaneously send a large volume of requests to the target server, causing it to become overloaded.

DoS Attack: Similar to DDoS, DoS attacks also aim to render target servers unable to provide normal services, but attackers use a single device or a small number of devices instead of multiple devices.

Recon Attack: Recon attacks involve attackers scouting and gathering information about the target system. Attackers may attempt to identify weaknesses, vulnerabilities, or sensitive information about the target system in preparation for subsequent attacks.

Web-based Attack: Web-based attacks involve malicious actions targeting web applications, aiming to exploit vulnerabilities or weaknesses in the application to gain access to sensitive information, tamper with data, or execute unauthorized operations [5].

Brute Force Attack: Brute Force Attack is a method of attempting to crack passwords by trying all possible password combinations. Attackers use automated tools to continuously try various passwords until the correct one is found.

Spoofing Attack: Spoofing Attack is a form of impersonation or deception where attackers masquerade as legitimate entities to gain unauthorized access or deceive target users.

Mirai Attack: Mirai is a malicious software designed to infect Internet of Things (IoT) devices, turning them into a large botnet and using them to launch DDoS attacks. The Mirai virus exploits weak passwords or vulnerabilities on many IoT devices, infecting them and turning them into attack tools.

4.2. Solutions

Deep learning is an important branch of machine learning, fundamentally no different from machine learning, both aiming to enable machines to learn and think like humans. Neural networks are a core component of deep learning, which is a computational model consisting of multiple layers that can process input data, learn features of the data, and make predictions. Each layer is composed of many neurons, which gradually adjust their internal parameters through training to minimize prediction errors in the training data. Common neural network structures include feedforward neural networks, convolutional neural networks, and recurrent neural networks [6].

This paragraph introduces the Internet of Things attack filtering method based on artificial intelligence algorithms in the context of connected vehicles, as illustrated in Figure 2.

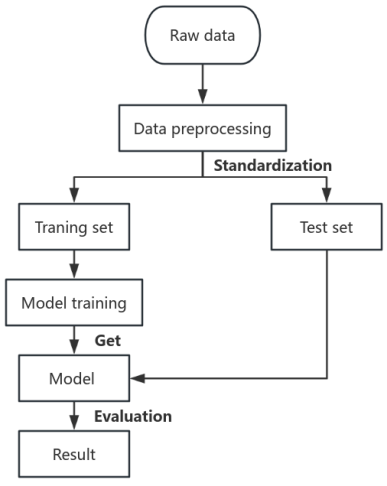


Figure 2. The model framework for detecting malicious attacks using deep learning methods.

Due to the original dataset containing features with different range values, which can cause a bias towards specific layers in both forward and backward propagation of machine learning where different feature values may cause certain weights to update faster than others, it is necessary to preprocess the data centrally. In this method, we standardize the data to have a distribution with a mean of 0 and a standard deviation of 1.

DOI: 10.54254/2755-2721/75/20240523

This study will use both random forest and neural network methods for construction and training separately.

A neural network, also known as an artificial neural network, is a machine learning algorithm inspired by the operation of human brain neurons. It can learn the relationship between input data features and output results to predict the outcome of new input data [7].

A neural network consists of many nodes, each representing a neuron. These neurons communicate with each other through connections and adjust the weights of these connections through forward and backward propagation. By adjusting the connection weights, the neural network minimizes the error between predicted and actual results, thereby changing the output of the entire neural network. In this case, the model we constructed includes two hidden layers, with 128 and 64 neurons respectively.

After preprocessing the data, we divide the dataset into training and testing sets, which are used to train and evaluate the model's performance, respectively. Since the random forest algorithm is an ensemble algorithm, it means that in each training session, we first sample with replacement from the training set N times to form a new training subset D, and then use this new training subset D to learn a complete decision tree [8]. Forming a learner and eventually integrating the training results of multiple sub-learners, such as using a voting method to generate the final training model. Therefore, the random forest has better robustness and noise resistance compared to traditional decision trees, while being less prone to overfitting.

4.3. Evaluation Criteria and Methods

The evaluation results are mainly assessed through four aspects, including accuracy_score, recall_score, precision_score, and F1 score. In the following expressions, we use TP/TN/FP/FN to represent true positive, true negative, false positive, and false negative, respectively.

Accuracy Score: Measures the proportion of correctly classified samples to the total number of samples. Accuracy = (TP + TN) / (TP + TN + FP + FN)

Recall Score: Measures the proportion of positive samples successfully predicted by the model. Recall = TP / (TP + FN)

Precision Score: Measures the proportion of true positive samples among samples classified as positive. Precision Score = TP / (TP + FP)

F1 Score: The harmonic mean of precision score and recall, used to evaluate the comprehensive performance of the model. F1 Score = (2 * Precision Score * Recall) / (Precision Score + Recall)

4.4. Results and Analysis

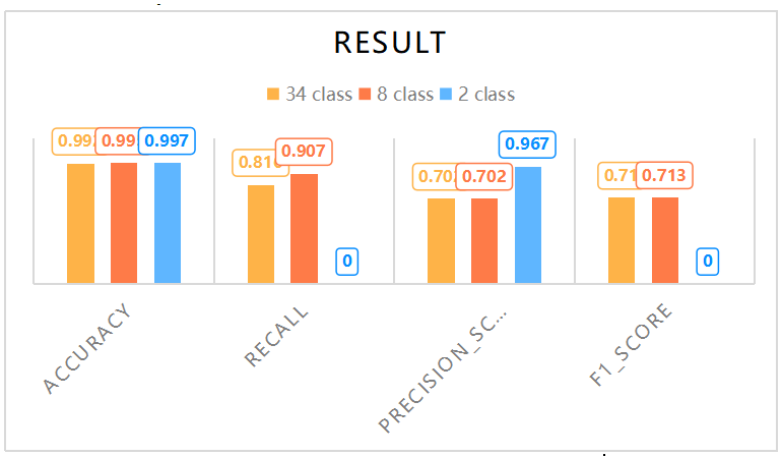


Figure 3. Visualization of Random Forest Results

From above results, it can be seen that the random forest algorithm performs well in predicting and identifying malicious attacks. However, it is evident that there is a trade-off relationship between recall

DOI: 10.54254/2755-2721/75/20240523

rate and precision score. It needs to determine the algorithm's requirements for recall rate and precision based on the specific scenarios.

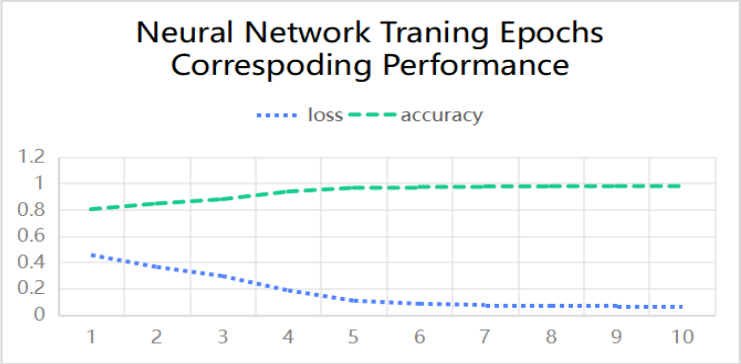


Figure 4. Neural Network Training Epochs and Loss Function Accuracy

During the training process of the neural network, epochs=10 means that the entire training dataset will be repeatedly used 10 times to train the model. An epoch is defined as one complete forward and backward pass of all training steps, including all training samples. Setting epochs=10 means that this process will be repeated 10 times, aiming to improve the model's weights through multiple iterations of training, thereby enhancing the model's performance and accuracy. At the end of each epoch, the model's weights are updated based on observed training data errors. Through multiple epochs of training, the model can better learn data features and patterns. From the results, we can see that the model tends to stabilize around the seventh iteration. The loss stabilizes around 0.068 from 0.4548, and the accuracy stabilizes around 0.97 from 0.8040.

The accuracy_score, recall_score, precision_score, and F1_score are as follows: accuracy_score: 0.9968324477732987, recall_score: 0.9645127044345947, precision_score: 0.9667313162565065, f1_score: 0.9656192284673764.

In summary, comparing the models constructed using random forest and neural networks, it can be concluded that they perform similarly in terms of accuracy and precision. However, the model built with neural networks outperforms random forest in terms of recall rate and F1 score.

5. Conclusion

Attacks in the automotive network are currently a focus of malicious behavior research. This paper uses publicly available CICIOT2023 data to train a model for detecting malicious behavior, and trains and optimizes it using random forest and neural network algorithms in deep learning to identify attack types for filtering purposes. With the increase in training epochs, the models of random forest and neural networks show varying degrees of improvement and decline in accuracy and loss, respectively, and stabilize within a certain number of rounds, more noticeably in the training of neural network models [9]. However, compared to the neural network model, the performance of the random forest in recall rate and F1 score is inferior. This paper concludes that both random forest and neural network algorithms based on deep learning can effectively identify and filter malicious attacks in the automotive network scenario, but the model based on neural networks can more accurately and effectively identify and filter security attacks to protect the privacy of vehicle users.

As the automotive industry rapidly shifts towards intelligence, the automotive network industry has become a globally key development project, and the rapid development of the automotive network industry has led to frequent security issues [10]. This paper mainly analyzes security issues in the automotive network scenario and proposes a method for filtering IoT attacks based on artificial intelligence algorithms. It analyzes various aspects such as the basic development status, concepts and architecture, and security threats of the automotive network, and conducts a series of analyses based on deep learning methods, proposing corresponding algorithm solutions. Ensuring the parallelism of

DOI: 10.54254/2755-2721/75/20240523

intelligence and security, as well as the standardization of networking and privacy, is an important focus of industry development in the interaction loop of people, roads, and things in the automotive network.

References

[1] Shao Xu. Research on H Airlines' Competitive Strategy, Shandong University, Master's Degree, 2022.

[2] Qiu Xuemin. Optimization of Machine Learning Algorithms for Network Attack Detection Systems [J]. Digital Users, 2023(44):140-141.

[3] Pu Jianjie, Yin Zhaoliang. A Malicious Behavior Detection Framework for Internet of Things Based on PyTorch Deep Learning Library [J]. Network Security Technology and Applications, 2023(6):43-45. DOI:10.3969/j.issn.1009-6833.2023.06.020.

[4] Chen Fuyuan, Dong Zhenjiang, Dong Jiankuo, Xu Minjie. Overview of Security Protection Technologies for Connected Vehicles, Telecom Science, 2023-02-22.

[5] Gao Jie. Network Shopping Mall Based on B/S Structure,University of Electronic Science and Technology, Master's Degree, 2011.

[6] Shi Kaiwen. Research on Network Intrusion Detection Based on Deep Learning [D]. Guangxi: Guangxi Normal University, 2023.

[7] Gao S., Zhou M., Wang Y., et al. Dendritic Neuron Model with Effective Learning Algorithms for Classification, Approximation, and Prediction [J]. IEEE Transactions on Neural Networks and Learning Systems, 2018, 30(2): 601-614.

[8] Information Center. A Data Management Method Based on Data Weaving Architecture CN202211504450.5,Yunnan Power Grid Co., Ltd. INVENTION_PUBLICATION; 2022-11-26.

[9] Baoqiang Ma, He Junjiang, Wang Yunpeng. SQL Injection Detection Method under Adversarial Machine Learning Attacks [J]. Network Security Technology and Applications, 2022(4):38-39. DOI:10.3969/j.issn.1009-6833.2022.04.024.

[10] Xinjiao Li, Guowei Wu, Yao Lin, et al. Research Progress and Future Challenges in Machine Learning Security Attacks and Defense Mechanisms [J]. Journal of Software, 2021, 32(2):406-423. DOI:10.13328/j.cnki.jos.006147.