An Algorithm for Detecting Wireless Communication Attacks on Intelligent Vehicles Based on Air Interface Identification

Xiaotong Zhou*

School of Management and Engineering, Capital University of Economics and Business, Beijing, China
**Corresponding author: 2278725142@qq.com*

Abstract: *Based on the threat to user privacy posed by intelligent vehicle networks, this paper proposes an intelligent vehicle wireless communication attack detection algorithm based on air interface traffic identification. The technique determines whether there is a threat to user privacy by monitoring the vehicle network communication signals, analyzing the signals and the type of business being carried, and combining the type of business with whether it has the attribute of steganography attack, which includes location tracking, wireless eavesdropping and video echo of eavesdropping. Using the software radio platform, the wireless air interface electrical signals are collected and transmitted to the signal analysis platform, and the neural network model based on the CNN model achieves the identification of the three types of traffic: audio, image and video, and the accuracy of the simulation experiment results is 90.34%.*

Keywords: *Smart Vehicle Security Risk, Internet of Vehicles, Abnormal Traffic Identification, CNN Neural Network, Wireless Attack Detection*

1. Introduction

The development of intelligent vehicles and the popularity of mobile communication services have greatly facilitated people's lives, but at the same time introduced a new type of network security risks. Compared with traditional vehicles, the current smart vehicles are equipped with intelligent operating systems, audio and video sensors, and high-speed wireless communication modules. By exploiting the vulnerabilities of the operating system, attackers can obtain the operating privileges of the audio and video and wireless communication modules, for example, by using Trojan horse attacks, implanting a stealing device inside the vehicle, and other illegal means to obtain the user's private information. Remote control of vehicle operation status is also carried out, for example, Miller and Valasek [1], researchers in the field of smart car security, demonstrated the process of remote attack targeting the infotainment system of a JEEP Cherokee car to achieve remote control of the car's steering wheel, brakes, and engine in the 2015 DEFEND conference.Woo et al [2] used a mobile phone APP to connect to the OBD diagnostic interface module device inside the car via WiFi to attack the ECU node inside the car to achieve the effect of changing the dashboard display, switching off the engine, etc. Francillon et al [3] used the relay information between the car and the smart car key to successfully enter the interior of the vehicle and start the vehicle by using a repeater. Based on the above problems, in-vehicle operating systems and various types of sensors have become the main channels for user information leakage. For this reason, detecting and identifying unauthorised mobile terminals and steganographic attacks based on mobile communication links are of great significance to the development of smart vehicles.

For the monitoring of wireless communication attacks, existing technical methods include obtaining mobile communication traffic data in a specific region through a mobile network operator and performing analysis, such as obtaining downlink network traffic, port number, and resource allocation information in a specific region on the base station side, and detecting abnormal steganographic transmission behaviour through a traffic identification model. Typical schemes include port number-based analysis, which completes traffic type [4], protocol analysis [5] anomaly detection [6] based on port rules developed by the Internet Corporation for Assigned Names and Numbers , which is low in computational complexity but gradually loses its effectiveness with the popularity of port obfuscation and forwarding techniques [7]. Subsequently, researchers used Deep Packet Inspection (DPI) method to analyse and match the traffic datagrams to distinguish different flows [8], the algorithm has high accuracy but high computational complexity, and with the update of encryption protocols, the administrators are gradually unable to obtain the data content of the traffic packets [9]. Subsequent researchers have also proposed the encrypted traffic algorithm based on statistical features, which analyses the header data of encrypted packets by mean, variance and standard deviation, and adopts machine learning methods such as SVM, Random Forest, and Plain Bayes to classify the encrypted traffic [10]. However, the algorithm has a short timeliness and needs to be constantly updated when the mobile terminal is upgraded or changes occur. The above methods need to be processed based on IP data, and this type of data needs authorisation from the operator to be obtained, which makes it difficult to obtain experimental data and also poses a threat to user privacy.

Aiming at the above problems, this paper proposes an algorithm for detecting wireless communication attacks on intelligent vehicles based on air interface traffic identification, which uses air interface interaction signals to detect and identify uplink traffic based on the characteristics of the resource blocks occupied by the air interface signals. For abnormal video and audio traffic, the software radio is used to collect the air interface signals and obtain the time-frequency resource map to achieve the identification of service types. The work in this paper includes collecting IQ sample data, drawing time-frequency resource maps according to the time and frequency resource granularity of air interface signal transmission by the existing Vehicle Networking physical layer protocols, identifying the time-frequency resource structure of different types of services by summarising the different time-frequency resource structures and change trends, and learning the time-frequency resource features by using CNN neural network training, combining the physical layer resource block power information and the link layer time-frequency resource scheduling information to achieve multi-terminal service identification within the vehicular network. The work in this paper no longer needs to demodulate the uplink signal, is completely based on IQ sample analysis, has low computational complexity, passively collects electromagnetic signals in the air, does not require the cooperation of operators, does not resolve to obtain user information, and does not pose a threat to user privacy.

2. Wireless Attack Detection Model for Telematics

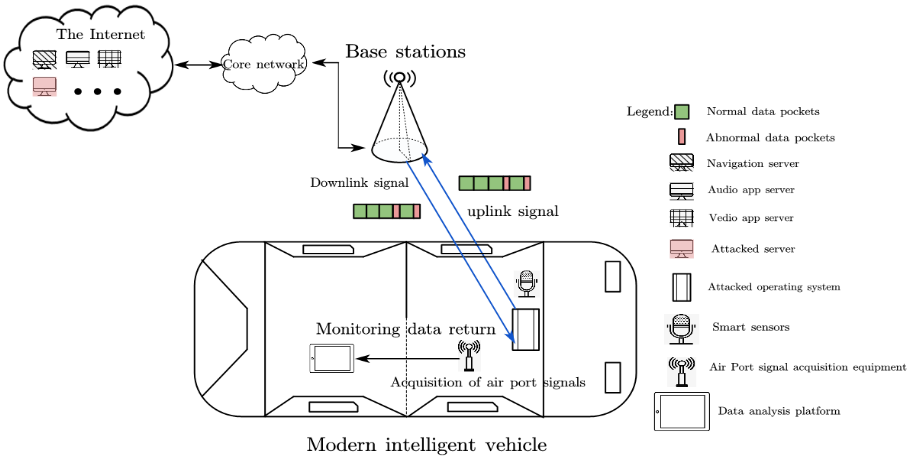

Figure 1: Modelling Wireless Steganography Attacks on Smart Vehicles.

In this paper, we take the example of steganography attack against user's private information to illustrate the car networking attack scenario, as shown in Figure 1. Intelligent vehicles are equipped with an operating system with 5G wireless communication technology in the driving area, which not only has the function of high-speed transmission of information, but also can connect to various types of servers, such as navigation, video, and audio APP servers through base station signal transmission. At the same time, the vehicle operating system is mostly based on Android system, the eavesdropper can use the loopholes that exist in the Android system [11], through remote installation of Trojan viruses and other illegal means to obtain access to sensitive data such as audio, video, and vehicle operation information in the vehicle central control, and even use the vehicle's own 5G communication module wireless transmission technology back to the eavesdroppers in the database, which poses a threat to the user's privacy.

For the above steganography attack scenarios, in order to protect the privacy of users, this paper will install the air interface signal acquisition equipment and traffic analysis equipment in the vehicle. The air interface signal acquisition equipment is based on a software radio receiver, which continuously monitors and collects the upstream and downstream interaction signals between the vehicle intelligent wireless terminal and the base station. And the collected data is transmitted back to the traffic monitoring and analysis equipment to analyse whether the air interface signal contains abnormal uplink audio and video traffic.

For the attacker, this paper assumes that it has the ability to obtain terminal control privileges, such as implanting a malicious Trojan horse to obtain privileges in the process of vehicle repair and maintenance. The control privileges include audio and video acquisition and the invocation of wireless communication modules. The attacker can use the wireless link can remote control to start the attack and stop the attack. For example, during the time range when the user is not using the vehicle, by obtaining the operating privileges of the wireless transmission module, the acquired user information is transmitted back. For the monitoring of abnormal traffic at the air interface, this paper assumes that it knows the communication frequency band of the vehicle intelligent terminal and the base station, and it can collect the traffic of various APPs in the vehicle with the assistance of the user, and actively learn the upstream and downstream signal time-frequency occupancy behaviours corresponding to the traffic as the basis for distinguishing and judging the abnormal traffic.

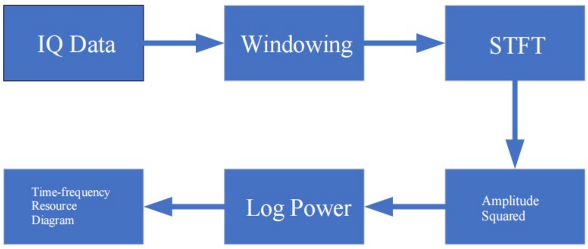

Figure 2: Data Processing Procedure.

As shown in figure 2,The signal acquisition module includes an antenna and a signal receiver for receiving the wireless communication signal s(t): $s(t)=a(t)e^{j[2\pi(f_c+n\Delta f)t+\phi(t)]}$,where the carrier frequency fc varies with time. The received radio frequency signal is reduced to the intermediate frequency, and the digital baseband positive classification and digital baseband in-phase components are obtained through a digital low-pass filter, which are respectively recorded as: $x(1)n=a(n)\cos\phi(n)$, $x(1)n=a(n)\cos\phi(n)$, Then through the time-frequency conversion module, discrete Fourier transform is performed on the received signal: $STFT[m,n]=\sum_{k=0}^{N-1}x(k)g^{*}[kT-mT]e^{-j2\pi(nF)k}$, Where g(t) is the window function, m is the length of the window function, * is the complex conjugate, T (> 0) is the sampling period of the time variable, F (> 0) is the sampling period of the frequency variable, m and n are integers .Combine the transformed data into a time-frequency waterfall , as Figure 3 shown below:

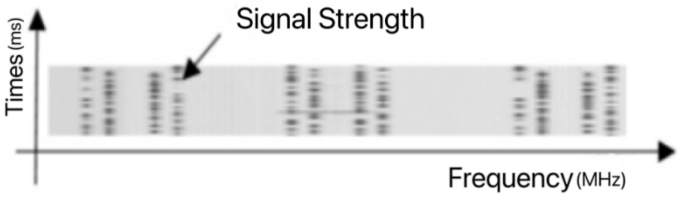

Figure 3: Time-frequency Waterfall Chart.

Since the IQ samples are too large to be processed by ordinary computers, after the data collection is completed, the collected data are transferred to the server via FileZilla for data processing, and the data processing flow is shown in Figure 3. First of all, short-time Fourier transform (STFT) is applied to the IQ data, and its main parameters are shown in Table 1. The main parameters are shown in Table 1. Among them, the window overlap is to make the spectrum energy more concentrated and reduce the spectrum leakage. According to Parseval's theorem, the power calculation in the time domain is converted to the frequency domain to reduce the complexity of calculation. Finally, the time-frequency resource map is performed according to the horizontal and vertical coordinate granularity specified by the physical layer communication protocol of Telematics.

Table 1: Drawing Parameters of Time-Frequency Resource Map

Parametric	size
Window length	2048
Overlap	1024
FFT Number of points	2048
Sampling rate	30.72M

In this paper, the air interface steganography traffic monitoring and analysis system is set into three operation modes: learning mode, time-sharing focused monitoring and full-time intelligent monitoring. Firstly, users can use the learning mode of the system to back up the legitimate traffic types within the intelligent vehicle in advance, which serves as the basis for the system to judge the abnormal traffic. Secondly, the time-sharing focused monitoring mode can set the monitoring time according to the different needs of users and monitor the intelligent vehicles within a specific time range. Finally, the full-time intelligent detection mode, based on the data samples already available in the first two learning modes, can operate within an all-weather time range, actively analyse the types of traffic within the intelligent vehicle, analyse different types of traffic and types of business, and actively identify and screen out abnormal traffic through the traffic monitoring and analysis platform, which can provide users with a reliable guarantee of information security within an arbitrary time range. The full-time intelligent detection mode uses an artificial neural network model to actively learn different traffic types, which can screen out abnormal traffic in a wider range, and has stronger learning capability and business type expansion capability than the time-sharing focused monitoring mode.

3. CNN neural network based air interface traffic analysis algorithm

Based on the differences in spectrum of different service types of services, service type identification is completed according to the shape of the time-frequency resource map and the trend of change in the number of features, and feedback of the service type identification results is carried out when the accuracy of service type identification is lower than 90% until the identification accuracy meets the algorithm requirements. This process converts the multi-terminal and multi-service recognition task into single terminal and single service recognition, reducing the complexity of the algorithm. The data includes three different business types, QQ, WeChat, and Bluetooth, and the audio, video, and picture traffic generated by them are recognized respectively.

3.1. Data Preprocessing

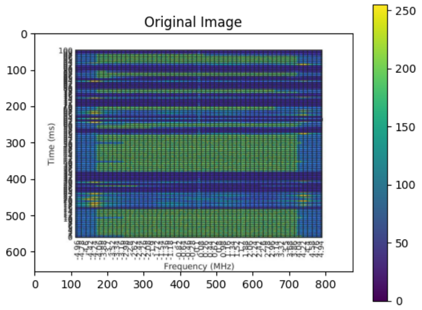

Figure 4: Original Image(a).

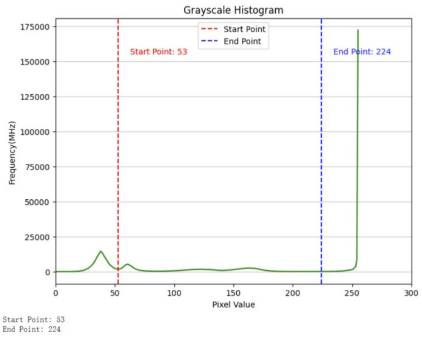

Figure 5: Greyscale Histogram of Time-frequency Resource Map ‘a’.

Based on a set power threshold that separates those signals with the highest power from other signals, an assumption can be made that the monitoring equipment should be able to receive signals with the maximum power when there is an abnormal terminal operating inside the vehicle. This assumption is based on the relationship between signal power and anomalous terminals because anomalous terminals usually communicate with the highest power, so by detecting signals with the highest power, we can look for potential anomalies or anomalous devices. This operation is designed to improve the accuracy and reliability of anomaly detection for better safety and stability of the in-vehicle environment. In this study, considering the computational complexity and the difficulty of implementation, a multi-threshold segmentation method is chosen, in which the image is segmented into multiple parts representing different terminals by means of several different thresholds. Due to the complexity of the actual environment, including the variation of noise and terminal transmitting power, this study realizes the adaptive adjustment of the thresholds by means of the gray scale histogram to adapt to different environmental conditions. The results are shown in Figures 4 and 5.

3.2. Data learning

1) Firstly, the data are processed to generate time-frequency resource maps, and its detailed steps are shown in Figure 2;

2) Import 6000 collected time-frequency resource maps and set the map height and width size to 180 pixel values, and the number of batch processing is 32 times. Which set the ratio of training dataset and test dataset as 8:2, i.e., the training dataset images are 4960 and the test dataset images are 1240.

3) Normalize the data to ensure that the range of pixel values in the image data in the training dataset is limited to the [0,1] interval after normalization. Improve the stability of model training and accelerate the convergence speed of the model.

4) Input the time-frequency resource map into the CNN artificial neural network for feedback validation of the uplink signal recognition results, perform model training with Epoch of 80 times, and when the recognition probability of the number of model output terminals is lower than 90%, the algorithm re-returns to the data processing part, and adjusts the CNN model architecture, such as the number of layers of convolutional kernel, the size, the step size, the learning rate, and other parameters until the results reach 90% above the validation level.

At last, the specific model structure is shown in Table 2 and the network structure is shown in Figure 6.

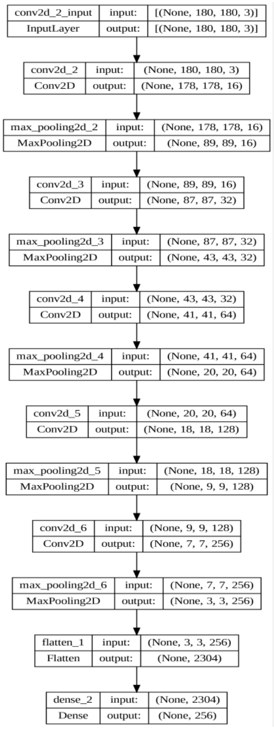
conv2d_2_input | input: | [(None, 180, 180, 3)]
InputLayer | output: | [(None, 180, 180, 3)]
conv2d_2 | input: | (None, 180, 180, 3)
Conv2D | output: | (None, 178, 178, 16)
max_pooling2d_2 | input: | (None, 178, 178, 16)
MaxPooling2D | output: | (None, 89, 89, 16)
conv2d_3 | input: | (None, 89, 89, 16)
Conv2D | output: | (None, 87, 87, 32)
max_pooling2d_3 | input: | (None, 87, 87, 32)
MaxPooling2D | output: | (None, 43, 43, 32)
conv2d_4 | input: | (None, 43, 43, 32)
Conv2D | output: | (None, 41, 41, 64)
max_pooling2d_4 | input: | (None, 41, 41, 64)
MaxPooling2D | output: | (None, 20, 20, 64)
conv2d_5 | input: | (None, 20, 20, 64)
Conv2D | output: | (None, 18, 18, 128)
max_pooling2d_5 | input: | (None, 18, 18, 128)
MaxPooling2D | output: | (None, 9, 9, 128)
conv2d_6 | input: | (None, 9, 9, 128)
Conv2D | output: | (None, 7, 7, 256)
max_pooling2d_6 | input: | (None, 7, 7, 256)
MaxPooling2D | output: | (None, 3, 3, 256)
flatten_1 | input: | (None, 3, 3, 256)
Flatten | output: | (None, 2304)
dense_2 | input: | (None, 2304)
Dense | output: | (None, 256)

Figure 6: The Network Structure.

Table 2: The Specific Model Structure

Typology	Parametric	Convolution kernel size	Number of convolution kernels	Strides	activation function
modelling structure	COV2D_1	3*3	16	1	relu
	COV2D_2	3*3	32	2	relu
	COV2D_3	3*3	64	1	relu
	COV2D_4	3*3	128	2	relu
	COV2D_5	3*3	256	1	relu
hyperparameterisation	Batch Size		32		
	Learning Rate		0.0001		
	optimiser		Adam		
	Epochs		80		
	Dropout Rate		0		

Input Layer: The input layer of the model uses a Rescaling layer to normalise the pixel values of the image to the range [0, 1].

Convolutional Layer (Conv2D): First Convolutional Layer: 16 3x3 convolutional kernels, ReLU activation function, "same" padding. Second convolutional layer: 32 3x3 convolutional kernels, ReLU activation function, step size (2, 2), "same" padding. Third convolutional layer: 64 3x3 convolutional kernels, ReLU activation function, "same" padding. Fourth convolutional layer: 128 3x3 convolutional kernels, ReLU activation function, step size (2, 2), "same" padding. Fifth convolutional layer: 256 3x3 convolutional kernels, ReLU activation function, "same" padding.

Fully connected layer (Dense layer): after the convolutional layer, the model includes two fully connected layers. The first fully connected layer has 256 neurons with ReLU activation function, the second fully connected layer has a number of neurons equal to the number of classes (num_classes).

Optimiser and loss function: the model uses the Adam optimiser with a learning rate of 0.0001 and a loss function of SparseCategoricalCrossentropy.

The performance metric of the model is accuracy.Training cycles (Epochs): the model will be trained on the training data for 80 cycles.Total params: 459171 (1.75 MB),Trainable params: 459171 (1.75 MB) ,Non-trainable params: 0 (0.00 Byte).

After a large number of experiments, we get the best recognition rate of 90.03%, the model for the time-frequency resource map with obvious features can be accurately identified, the results are shown in Figure 7, the model in the training process in the training set and the test set of the recognition of the accuracy of the steady increase, and the loss rate performance is good, into a downward trend, no oversaturation performance.

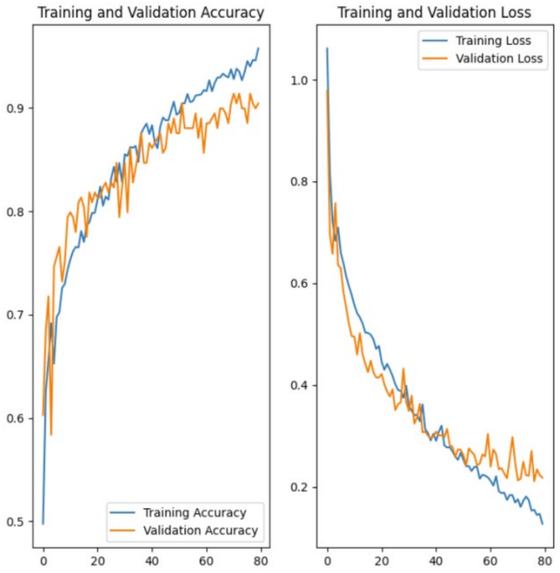

Figure 7: Trends in Accuracy and Loss Rates for Test and Training Sets.

3.3. Evaluation Criteria

In order to measure the performance of the network, it is difficult to judge the advantages and disadvantages of the algorithm by only one index, so this paper adopts the four parameters of Accuracy, Precision, Recall and F1 as the evaluation criteria.

In order to calculate the above four evaluation indicators, it is necessary to first understand the following concepts.TP: positive sample predicted as positive category; TN: negative sample predicted as negative sample predicted to be in the negative category; FP: negative sample predicted to be in the positive category; FN: positive sample predicted to be in the negative category. Based on the above four concepts, the four evaluation indicators are calculated as follows:

$$A\text{ccuracy} = \frac{TP+TN}{TP+FP+FN+TN} \tag{1}$$

$$\text{Pr}\,ecision = \frac{TP}{TP+FP} \tag{2}$$

$$\text{Re}\,call = \frac{TP}{TP+FN} \tag{3}$$

$$F1 = \frac{2TP}{2TP+FP+FN} \tag{4}$$

4. Practical Scenarios and Experimental Analysis

This subsection introduces abnormal traffic identification, which classifies terminal services into two categories, normal and abnormal, by identifying the characteristics of the object for a specific classification target. Due to the limited business types in this paper, the theoretical feasibility is demonstrated only on the basis of the completed business identification. In the future, more terminal business types will be added to meet practical needs. Considering the actual situation, in a particular area, authorised terminals can make voice calls through the mobile communication network, but video calls and other services are not allowed. After identifying the number of terminals and services using the algorithm in this paper, if unauthorised services (e.g. video calls) are found, an alarm will be triggered to provide basic conditions for subsequent processing.

4.1. Experimental Environment Setup

In order to verify the effect of different environments on the performance of the algorithm, we used srsLTE to build a laboratory base station. In order to avoid the interference of data collection by terminals in the existing network, we choose the n2 frequency band, which has been realised but not deployed in the current network, as the experimental base station according to the 3GPP protocol. The uplink frequency point of this band is 1880MHz, and it has been confirmed by the spectrometer test that there is no other interfering signal within the 10MHz bandwidth. Therefore, the bandwidth of the experimental environment is set to 10 M. According to srsLTE, the base station should be configured with mobile phone SIM card information. To achieve this requirement, we used the GRSIMWrite card writing software to write the identity information such as the mobile phone IMSI into a programmable white card, and installed the white card into the test terminal. On the test terminal, we configured the APN information to be srsLTE and verified that the terminal was connected to an analogue base station using the IMSI information to ensure the accuracy of the collected data. The acquisition equipment and setup were exactly the same as in Section 2.

4.2. Experimental analysis under different signal-to-noise ratio conditions

In data processing, this paper takes the signal power as the terminal identification feature, and adopts the simplified estimation method of power spectral density, i.e. power/bandwidth, in order to improve the frequency resolution and reduce the computational complexity. Considering that the transmit power of mobile terminals cannot be controlled, this paper simulates different signal-to-noise ratio environments to verify the generality of the algorithm.

In this paper, the video resource map is divided into two parts, noise floor and terminal data, and processed with the noise floor as the benchmark, and the power value of terminal data is subtracted from the noise floor to generate a new time-frequency resource map, which further improves the frequency resolution. In this paper, the performance of the algorithm in the range of 10dB to 40dB is verified, and the accuracy of the terminal data set on the validation set under different power conditions is demonstrated through Figure 8.

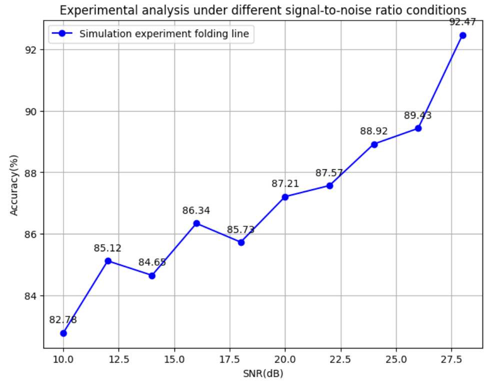

Figure 8: Simulation experiments under different signal-to-noise ratio conditions.

As can be seen from Figure 8 the performance of all networks on the validation set under different power conditions is basically the same. In addition, in order to evaluate the algorithm performance more comprehensively, this paper also validates the test set by calculating the four evaluation metrics introduced in Section 3.3, and the results are shown in Table 3.

Table 3: Experimental results of simulation under different signal-to-noise ratio conditions.

SNR(dB) Evaluation criteria	10-20	12-14	14-16	16-18	18-20	20-22	22-24	24-26	26-28	28-30
Accuracy	82.78	85.12	84.65	86.34	85.73	87.21	87.57	88.92	89.43	92.47
Precision	83.43	86.25	84.77	87.84	85.87	87.46	88.62	90.23	89.32	92.88
Recall	82.65	85.08	84.22	86.13	85.26	87.11	87.49	88.74	89.36	92.44
F1	83.65	86.22	84.64	86.56	85.79	87.31	88.54	89.42	89.51	92.76

By changing the size of the signal transmitting power, the time-frequency resource diagrams under different signal-to-noise ratios are produced, and different data are inputted into the model in batches to be identified again, and the experimental results in the above table are obtained. According to the chart, the results can be obtained, when the signal-to-noise ratio is set to the interval of 10dB-18dB, the accuracy of the model prediction results fluctuates greatly, and becomes a wave-like upward trend. When the signal-to-noise ratio is 18dB-30dB, the accuracy of the model prediction results increases steadily and reaches the maximum value (92.47%) at 30dB, according to which it can be concluded that the optimal signal-to-noise ratio interval is within the range of 18dB-30dB.

4.3. Experimental analysis of image enhancement for similar power values

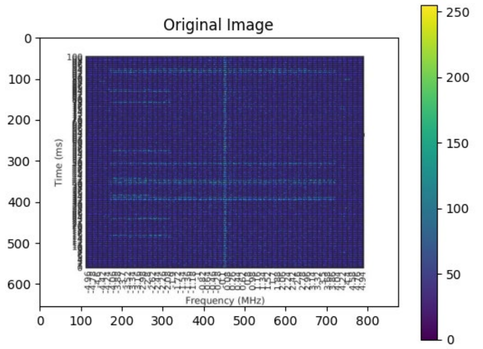

Figure 9: Original Image(b).

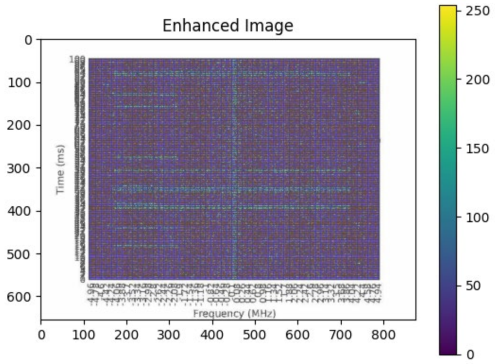

Figure 10: Colour enhancement 2x image 'b'.

In the validation phase of uplink signal identification, this study uses linear enhancement to adjust the time-frequency resource maps of terminals with close power values. During the user identification process, it is recognised that there are some differences in the power values of different users, which are reflected in different colours after generating the time-frequency resource maps. Similar power values correspond to similar colours, so we processed the colours of the images to highlight the differences between similar powers. We used three channels of RGB to enhance the images and fed two different datasets, the original image and the RGB enhancement, into the Terminal Quantity Identification Network (Figure9-10). We also used the four evaluation metrics described in Section 3.3 to compare network performance, and the experimental results are shown in Table 4.

Table 4: Experimental Results of Similar Power Time-frequency Resource Map Simulation.

Evaluation criteria / Imagery	Accuracy	Precision	Recall	F1
Original Image	90.03	90.52	90.09	90.11
RGB Enhanced 2x Image	95.29	95.33	95.36	95.32

4.4. Experimental analysis of increasing interference signals

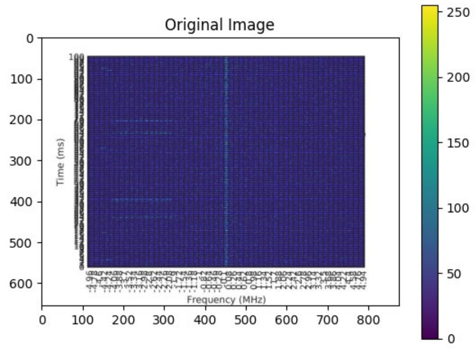

Figure 11: Original Image(c).

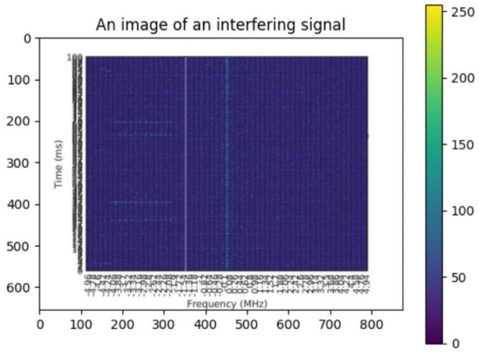

Figure 12: Image after adding an interfering signal to the time-frequency resource map 'c'.

In this paper, the python tool is used to batch process the original time-frequency resource map and add 1-5 interfering signals in the range of 1 to 5. Figure 11 shows the original time-frequency resource map, and Figure 12 shows the time-frequency resource map in the case of adding 1 interfering signal. In this paper, the new images under the conditions of different number of interference signals are fed into the CNN model again, and the experimental results shown in Figure 13 are obtained with other conditions being the same.

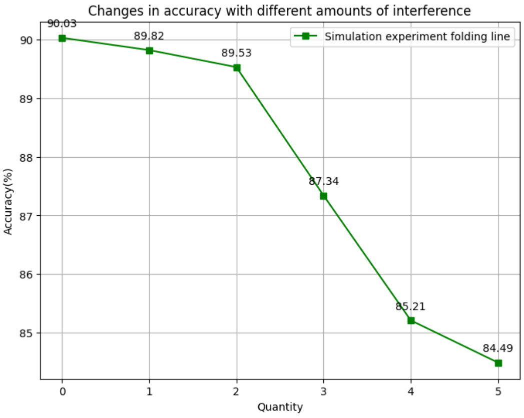

Figure 13: Image of the change in accuracy when the interference signal is 1-5.

The above results are obtained by adding different number of interfering signals to the original picture and then inputting them into the model. With the increase of interfering signals, the accuracy of model recognition gradually decreases, when the number of interfering signals is 3, the accuracy is lower than 88% of the verification level (87.34%), the model recognition is affected to a certain extent, with the increase of the interfering signals to 4, 5, the accuracy of the model recognition decreases dramatically, in the number of interfering signals 5, the accuracy of the recognition of 84.49, which is less than 85% of the verification level. Based on the algorithm proposed in this paper, it can cope with abnormal traffic detection when the number of interfering signals is less than 4, and when the number of interfering signals gradually increases the model needs to be further optimised.

5. Conclusion

Aiming at the problem of steganographic anomalous traffic identification for intelligent vehicles, this paper proposes an algorithm for communication service identification based on uplink time-frequency resource occupancy, uses CNN artificial neural network model training to identify the time-frequency resource map features of different service types, completes the work of identifying the video, audio, and picture traffic of three different service types, namely, QQ, Wechat, and Bluetooth, and verifies the simulation experimental analysis under different signal-to-noise ratios, different RGB data sets and different number of interfering signals. The algorithm achieves 90.03% recognition accuracy on the test set. In the future, this paper will further improve the algorithm to enhance the recognition accuracy of the model, and continue to collect signal features to cope with the detection of anomalous traffic recognition in different business types.

References

[1] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle [J]. Black Hat USA, 2015.
[2] Woo S, Jo H J, Lee D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN [J]. Intelligent Transportation Systems, IEEE Transactions on, 2015, 16(2): 993-1006.
[3] Francillon A, Danev B, Capkun S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars[C]//NDSS. 2011.
[4] Hyun J, Li J, Im C T, et al. A VoLTE traffic classification method in LTE network[C]. The 16th Asia-Pacific Network Operations and Management Symposium. IEEE, 2014: 1-6.
[5] Wang Z. The applications of deep learning on traffic identification[J]. BlackHat USA, 2015, 24(11): 1-10.
[6] Qian B, Lu S. Detection of mobile network abnormality using deep learning models on massive network measurement data[J]. Computer Networks, 2021, 201: 108571.
[7] Sengupta S, Yadav V K, Saraf Y, et al. MoViDiff: Enabling service differentiation for mobile video

apps[C]. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2017: 537-543.

[8] Dong C, Zhang C, Lu Z, et al. CETAnalytics: Comprehensive effective traffic information analytics for encrypted traffic classification[J]. Computer Networks, 2020, 176: 107258.

[9] Aceto G, Ciuonzo D, Montieri A, et al. Mobile encrypted traffic classification using deep learning[C]. 2018 Network traffic measurement and analysis conference (TMA). IEEE, 2018: 1-8.

[10] Z. Geng, H. Yan, J. Zhang and D. Zhu, "Deep-Learning for Radar: A Survey," in IEEE Access, vol. 9, pp. 141800-141818, 2021, doi: 10.1109/ACCESS.2021.3119561.

[11] Qin Jiawei, Zhang Hua, Yan Hanbing, He Nengqiang, Tu Tengfei. Context-aware Android application vulnerability detection research [J]. Journal of Communication, 2021, 42(11):13-27.