COMPARISON OF ACCURACIES IN RESNET AND WIDE RESNET DEEP LEARNING MODEL IN PREVENTING CONNECTED VEHICLE FROM MALWARE

S. Bhaskara Rao M[1], P. V. Pramila M[2*]

Article History: **Received:** 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Aim: The Purpose of Vehicular Intrusion is to apply Machine Learning methods to determine which Wireless Communication Vehicles have the best accuracy. Residual Neural Network (Resnet) and Wide Residual Neural Network (WRNs) are the two algorithms.

Methods and Materials: The data was obtained from the website www.kaggle.com. Residual Neural Network (N=10) and Wide Residual Neural Network (N=10) are the two classes. The increased CAN (Bus) Residual Neural Network (RNN) accuracy is 90% and the Wide-Resnet (WRNs) accuracy is 88%. The two algorithms are used to determine the CAN Bus Intrusion's enhanced categorization or complexity. In addition, the independent sibling had a satisfied value ($p<0.05$) i.e $\alpha=0.01$ with the confidence level of 95%.

Conclusion: Recognizing In-Vehicle Network Intrusion significantly seems to be better in Residual Neural Network (RNNs) than Wide Residual Neural Network (WRNs).

Keywords: Deep Learning Model, Vehicle Intrusion, Machine Learning, Residual Neural Network, Wide-Residual Network.

[1]Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, 602105.

[2*]Project Guide, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences Saveetha University, Chennai, Tamil Nadu, India, 602105.

Email: pramilapv.sse@saveetha.com

1. Introduction

The exponential growth of autos around the world, vehicle systems can play a vital part in the development of intelligent transportation systems, automated arterial expenditure collecting, perception in self-driving vehicles and corporate deluge control systems.(Ghazali et al. 2019; Alazab and Tang 2019). It is the simplest classification of algorithms available for supervised learning algorithms to identify the attacks. Hacking over the internet as connected vehicles have internet connection, or physical access to the vehicle intelligence system are two further security dangers that smart automotive may face . It allows safety-critical ECUs that are attached to it to sufficiently broadcast information in the form of CAN (Renault, Mühlethaler, and Boumerdassi 2019) packets between them and other connected buses.

Vehicle Intrusion Detection Approaches are carried out by many researchers and scholars by conducting surveys and studies. There are 74 articles which were published in IEEE explore and 43 articles were published in science direct (Mhamed et al. 2021)). The intrusion detection was identified by using Residual Neural Network it was observed accuracy is 90% and for the wide-Residual Neural Network we have observed 88 % accuracy.Our team has extensive knowledge and research experience that has translated into high quality publications (K. Mohan et al. 2022; Vivek et al. 2022; Sathish et al. 2022; Kotteeswaran et al. 2022; Yaashikaa, Keerthana Devi, and Senthil Kumar 2022; Yaashikaa, Senthil Kumar, and Karishma 2022; Saravanan et al. 2022; Jayabal et al. 2022; Krishnan et al. 2022; Jayakodi et al. 2022; H. Mohan et al. 2022)

In recent surveys, The test was conducted on samples of 10,000 CAN message vectors for each dataset. (Ahn and Yeo 2021) Samples were randomly selected, balancing the ratio of CAN ID identifiers, and were split into 80.00% training and 20.00% test sets, again stratifying the CAN ID identifiers for all the datasets with the exception of the dataset. There was a high number of different message identifiers in the unique CAN IDs. The Novel Detection Based Approach Residual Neural Network and Wide Residual Neural Network machine learning predicts th article in which Vehicle is attacked through the internet by performing research. The main drawback is that they have used many attributes. Due to this we are using less attributed algorithms to get a new range with new algorithms.

2. Methods and Materials

The study setting of the proposed work was done in Saveetha School of Engineering, Object Oriented Analysis and Design lab. The sample size was calculated by using clincalc.com by keeping G power_(Mayr et al. 2007)and minimum power of the analysis is fixed as 0.8 and maximum accepted error is fixed as 0.5 with threshold value as 0.05% and Confidence Interval is 95%. Mean and standard deviation has been calculated based on the previous literature for size calculation. The two groups are used, namely Residual Neural Network (N=10) iterations as an existing model as group 1 and Wide Residual Neural Network (N=10) iterations as a Proposed model as group 2.

Residual Neural Network (Resnet)

ResNet is one of the models developed by(Yang et al. 2022). The gain of the ResNets model compared to different architectural models is that the performance of this model does not minimize even though the architecture is getting deeper. Besides, computation calculations are made lighter, and the potential to train networks is better. The ResNet model is applied by way of skipping connections on two to three layers containing ReLU and batch normalization amongst the architectures confirmed that the ResNet model performs higher in intrusion classification than different models, indicating that the intusion facets had been extracted properly via ResNet. Here the residual learning can be applied to multiple layers of layers. The residual block on ResNet is defined as follows in equation (1)

$$y = F(x,W + x) \quad \ldots\ldots(1)$$

where x is the input layer.
y is output layer; and
F function is represented by the residual map.

Pseudo Code

Step 1. Import the dataset.
Step 2. preprocess the imported data.
Step 3. Select the classification and tokenize the data.
Step 4. Computing term frequency and creating document term matrix.
Step 5. Evaluating the data by using an evaluation algorithm.

Wide-Residual Neural Networks (Wrns):-

By utilizing Wide Residual Neural Networks calculations with 2 convolutional layers and completely associated layers. Wide Residual Neural Network comprises first and second convolution layers.This only a few blocks can run valuable representations or many blocks could share very little information with small contributions to the final goal. This problem was tried to be addressed using a special case of dropout applied to residual blocks in which an

identity scalar weight is added to each residual block on which dropout is applied.
The residual block of wide- ResNet is defined as follows in equation (2)

$$Xl + 1 = xl + F(xl, Wl) \quad \ldots.(2)$$

xl+1 and lxl represent the input and output of the l-th unit in the network
F is a residual function
Wl are the parameters

Pseudo Code
Step 1. Import the dataset.
Step 2. preprocess the imported data.
Step 3. Select the classification and tokenize the data.
Step 4. Computing term frequency and creating document term matrix.
Step 5. Evaluating the data by using an evaluation algorithm.
Step 6. At last verify the effectiveness by using Algorithm.
For comparing both the models, the dataset has been trained with five different sample sizes. the accuracy values are recorded. The system configuration is used for the Vehicle intrusion in Deep Learning model algorithm to run in a 64 - bit Operating System, 4GB RAM PC, and using Windows 10, Google Colab, and Microsoft Office for software specification.

Statistical analysis
IBM SPSS version 22 software is used for statistical analysis of RESNET and Wide-Resnet algorithm based methods. The independent variables are datasets of Vehicle intrusion and the dependent variables are predicting accuracy efficiency on intrusion. The independent T test analyses were carried out to calculate the accuracy of the RESNET for both methods Accuracy for Residual Neural Network and Wide-Residual Neural Network algorithms have been calculated primarily based on equation (3)

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad \ldots\ldots\ldots (3)$$

Where,
TP = True Positive
TN - True Negative
FP - False Positive
FN - False Negative

3. Result

From Table2, shows the results of proposed algorithm Novel Residual Neural Network and the existing system Wide-Residual Neural Network Algorithm where the accuracy of RESNET, is taken as N=10 iterations and mean value is 90.0460 and standard deviation 0.62139 and standard error mean is 0.72511. Group of Wide-RNN is N=10 and Mean is 88.0380, and standard deviation is 0.86621and standard error mean is 0.38738.It was observed that the mean accuracy of the RESNET algorithm was 90% and the Wide-Resnet was 88%. From Table 3, shows the accuracy level of Equal variances assumed in Levene's Test for equality of variances of F is 3.482 and Sig is .099 and T-Test for equality of means t is 1.499 and df 18.3 and Sig.(2-tailed) is.172 and Mean Difference 1.23200 and Standard error difference is .8221 and 95% Confidence Interval of the Difference of Lower is .66376 and Upper 3.12776. An one more accuracy equal variances not assumed and T-Test for equality of means t is 1.499 and df is 6.11 and Sig.(2-tailed) one sided p is 0.001 and Mean Difference is 1.23200 and standard error difference is 0.82210 and 95% confidence interval of the difference of Lower 0.77075 and Upper 3.23475. Table 3 represents the Independent Sample T-Test that is applied for the sample collections by fixing the level of significance as 0.005 with a confidence interval of 95 %. After applying the SPSS calculation, SVM has accepted a statistically significant value($P<0.05$). From Figure 2 it was represented by a simple bar Mean of Accuracy Novel Residual Neural Network error range (0.99 - 0.98) and Wide-Resnet error range (0.99 - 0.98).
From Fig.1, shows mean accuracy between Simple Novel Residual Neural Network and Wide-Residual Neural Network Algorithm. From the results, it is shown that connected components are appearing at higher value. The comparison bar graph shows that Novel Residual Neural Network is higher as compared to wide-Resnet.

4. Discussions

RESNET and Wide Resnet are applied in the analysis of vehicular intrusion detection to enhance the security of connected vehicles. From obtained results it is observed that the Novel Residual Neural Network deep learning model gives higher accuracy with significance 0.04 compared to the Wide Resnet model. (Granik and Mesyura 2017) compared SVM (85%). The Neural Networks with a precision of 90 % is superior to the Support vector Machine with an exactness of 85% in perceiving the intrusion (Alazab and Tang 2019). (Li et al. 2022) reported the average detection rate of the KNN algorithm was 84.31 percent and that of the AdaBoost algorithm was 85.06 percent. (Hu et al. 2022) showed in their work that the Mosaic coding approach has greater classification ability of 92% while confronting various sorts of attacks with significantly lower variance in all evaluation

indices.Machine learning algorithms(Palani, Elango, and Viswanathan K 2021) have been used to analyze the information which vehicle is attacked or not by using these algorithms which produce the accuracy by comparing it. In this way the algorithm wide-resnet CNN produces accuracy (88.00%) (Palani, Elango, and Viswanathan K 2021).

5. Conclusion

In this research the algorithm seems to appear with a better accuracy percentage apparently better accuracy (90%) using Resnet Neural Network than Wide-Resnet Neural Network (88%).These vehicle intrusion are designated to various sorts of assaults which lead to consequences for the vehicles' exhibition, dangers to public and private property and street security. In this work, we propose an interruption identification strategy for Deep Learning models CAN transport IDS in vehicles.

Declarations

Conflict of interests

No conflicts of interest in this manuscript.

Authors Contributions

Author SBR was involved in conceptualization, data collection, data analysis, manuscript writing. Author PVP was involved in conceptualization, guidance, and critical review of the manuscript.

Acknowledgments

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding

We thank the following organizations for providing financial support that enabled us to complete the study.

1. SNEW.AI Technologies, Hyderabad
2. Saveetha University
3. Saveetha Institute of Medical and Technical Sciences.
4. Saveetha School of Engineering

6. References

Ahn, Hyojung, and Inchoon Yeo. 2021. "Deep-Learning-Based Approach to Anomaly Detection Techniques for Large Acoustic Data in Machine Operation." Sensors 21 (16). https://doi.org/10.3390/s21165446.

Alazab, Mamoun, and Mingjian Tang. 2019. Deep Learning Applications for Cyber Security. Springer.

Ghazali, Rozaida, Nazri Mohd Nawi, Mustafa Mat Deris, and Jemal H. Abawajy. 2019. Recent Advances on Soft Computing and Data Mining: Proceedings of the Fourth International Conference on Soft Computing and Data Mining (SCDM 2020), Melaka, Malaysia, January 22–□23, 2020. Springer Nature.

Granik, Mykhailo, and Volodymyr Mesyura. 2017. "Fake News Detection Using Naive Bayes Classifier." 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON). https://doi.org/10.1109/ukrcon.2017.8100379.

Hu, Rong, Zhongying Wu, Yong Xu, and Taotao Lai. 2022. "Multi-Attack and Multi-Classification Intrusion Detection for Vehicle-Mounted Networks Based on Mosaic-Coded Convolutional Neural Network." Scientific Reports 12 (1): 6295.

Jayabal, Ravikumar, Sekar Subramani, Damodharan Dillikannan, Yuvarajan Devarajan, Lakshmanan Thangavelu, Mukilarasan Nedunchezhiyan, Gopal Kaliyaperumal, and Melvin Victor De Poures. 2022. "Multi-Objective Optimization of Performance and Emission Characteristics of a CRDI Diesel Engine Fueled with Sapota Methyl Ester/diesel Blends." Energy. https://doi.org/10.1016/j.energy.2022.123709.

Jayakodi, Santhoshkumar, Rajeshkumar Shanmugam, Bader O. Almutairi, Mikhlid H. Almutairi, Shahid Mahboob, M. R. Kavipriya, Ramesh Gandusekar, Marcello Nicoletti, and Marimuthu Govindarajan. 2022. "Azadirachta Indica-Wrapped Copper Oxide Nanoparticles as a Novel Functional Material in Cardiomyocyte Cells: An Ecotoxicity Assessment on the Embryonic Development of Danio Rerio." Environmental Research 212 (Pt A): 113153.

Kotteeswaran, C., Indrajit Patra, Regonda Nagaraju, D. Sungeetha, Bapayya Naidu Kommula, Yousef Methkal Abd Algani, S. Murugavalli, and B. Kiran Bala. 2022. "Autonomous Detection of Malevolent Nodes Using Secure Heterogeneous Cluster Protocol." Computers and Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2022.107902.

Krishnan, Anbarasu, Duraisami Dhamodharan, Thanigaivel Sundaram, Vickram Sundaram, and Hun-Soo Byun. 2022. "Computational Discovery of Novel Human LMTK3 Inhibitors by High Throughput Virtual Screening Using NCI Database." Korean Journal of Chemical Engineering. https://doi.org/10.1007/s11814-

022-1120-5.

Li, Zhongwei, Wenqi Jiang, Xiaosheng Liu, Kai Tan, Xianji Jin, and Ming Yang. 2022. "GAN Model Using Field Fuzz Mutation for in-Vehicle CAN Bus Intrusion Detection." Mathematical Biosciences and Engineering: MBE 19 (7): 6996–7018.

Mayr, Susanne, Edgar Erdfelder, Axel Buchner, and Franz Faul. 2007. "A Short Tutorial of GPower." Tutorials in Quantitative Methods for Psychology. https://doi.org/10.20982/tqmp.03.2.p051.

Mhamed, Mustafa, Richard Sutcliffe, Xia Sun, Jun Feng, Eiad Almekhlafi, and Ephrem Afele Retta. 2021. "Improving Arabic Sentiment Analysis Using CNN-Based Architectures and Text Preprocessing." Computational Intelligence and Neuroscience 2021 (September): 5538791.

Mohan, Harshavardhan, Sethumathavan Vadivel, Se-Won Lee, Jeong-Muk Lim, Nanh Lovanh, Yool-Jin Park, Taeho Shin, Kamala-Kannan Seralathan, and Byung-Taek Oh. 2022. "Improved Visible-Light-Driven Photocatalytic Removal of Bisphenol A Using V2O5/WO3 Decorated over Zeolite: Degradation Mechanism and Toxicity." Environmental Research. https://doi.org/10.1016/j.envres.2022.113136.

Mohan, Kannan, Abirami Ramu Ganesan, P. N. Ezhilarasi, Kiran Kumar Kondamareddy, Durairaj Karthick Rajan, Palanivel Sathishkumar, Jayakumar Rajarajeswaran, and Lorenza Conterno. 2022. "Green and Eco-Friendly Approaches for the Extraction of Chitin and Chitosan: A Review." Carbohydrate Polymers 287 (July): 119349.

Palani, Balasubramanian, Sivasankar Elango, and Vignesh Viswanathan K. 2021. "CB-Fake: A Multimodal Deep Learning Framework for Automatic Fake News Detection Using Capsule Neural Network and BERT." Multimedia Tools and Applications, December, 1–34.

Renault, Éric, Paul Mühlethaler, and Selma Boumerdassi. 2019. Machine Learning for Networking: First International Conference, MLN 2018, Paris, France, November 27–29, 2018, Revised Selected Papers. Springer.

Saravanan, A., P. Senthil Kumar, B. Ramesh, and S. Srinivasan. 2022. "Removal of Toxic Heavy Metals Using Genetically Engineered Microbes: Molecular Tools, Risk Assessment and Management Strategies." Chemosphere 298 (July): 134341.

Sathish, T., R. Saravanan, V. Vijayan, and S. Dinesh Kumar. 2022. "Investigations on Influences of MWCNT Composite Membranes in Oil Refineries Waste Water Treatment with Taguchi Route." Chemosphere 298 (July): 134265.

Vivek, J., T. Maridurai, K. Anton Savio Lewise, R. Pandiyarajan, and K. Chandrasekaran. 2022. "Recast Layer Thickness and Residual Stress Analysis for EDD AA8011/h-BN/B4C Composites Using Cryogenically Treated SiC and CFRP Powder-Added Kerosene." Arabian Journal for Science and Engineering. https://doi.org/10.1007/s13369-022-06636-5.

Yaashikaa, P. R., M. Keerthana Devi, and P. Senthil Kumar. 2022. "Algal Biofuels: Technological Perspective on Cultivation, Fuel Extraction and Engineering Genetic Pathway for Enhancing Productivity." Fuel. https://doi.org/10.1016/j.fuel.2022.123814.

Yaashikaa, P. R., P. Senthil Kumar, and S. Karishma. 2022. "Review on Biopolymers and Composites – Evolving Material as Adsorbents in Removal of Environmental Pollutants." Environmental Research. https://doi.org/10.1016/j.envres.2022.113114.

Yang, Bin, Mingming Chen, Chengfang Zhan, Kexin Liu, Yanhao Cheng, Ting Xie, Peiwen Zhu, et al. 2022. "Identification of OsPK5 Involved in Rice Glycolytic Metabolism and GA/ABA Balance for Improving Seed Germination via GWAS." Journal of Experimental Botany, February. https://doi.org/10.1093/jxb/erac071.

Tables and Figures

Table 1: Data collection for each algorithm is N=10 iterations has been taken to calculate accuracy rate for Residual Neural Network(RNNs) to gain accuracy (%) and WRNs to gain accuracy(%).

Samples(N)	**Residual Neural Networks(RNNs)**	**Wide-Residual Neural Network(WRNNs)**
	Accuracy(%)	**Accuracy(%)**
1	90.00	88.00
2	89.56	87.65

3	88.56	86.78
4	87.00	85.76
5	86.23	87.00
6	85.56	86.87
7	84.56	84.12
8	89.54	83.79
9	87.56	82.89
10	85.26	83.58

Table 2: Comparison of Resnet and Wide-Resnet.The Resnet algorithm had the highest accuracy (90%). Wide-Resnet had the lowest accuracy (88%) as compared to Resnet.

GROUPS		N	Mean	Std Deviation	Std Error Mean
ACCURACY	RNNs	10	90.038	.62139	.72511
	WRNNs	10	86.0380	.86621	.38738

Table 3: Independent Sample T-Test is applied for the sample collections by fixing the level of significance as 0.05 with confidence interval as 95 %. After applying the SPSS calculation, WRNNs has accepted a statistically significant value ($p<0.05$) and error rate.

ACCURACY	Levene's Test for Equality of Variance		T-test for Equality of Means						
	f	Sig	t	df.	Sig(2-tailed	Mean Difference	Std.Error Difference	95% Confidence of the Differences	
								Lower	Upper
Equal variances assumed	3.482	.099	1.499	18.3	.172	1.23200	.82210	.66376	3.12776
Equal variances not assumed			1.499	6.11	.184	1.23200	.82210	.77075	3.23475

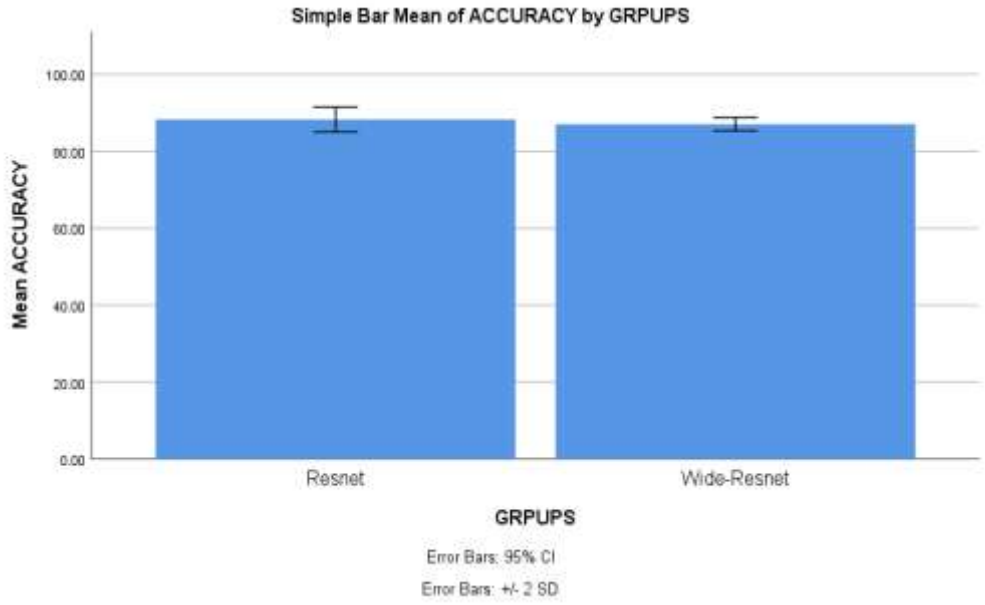

Fig.1: Simple Bar Mean of Accuracy RNNs error range (0.99 - 0.98) and Loss error rate range (2-4) and WRNNs error range (0.98 - 0.99) and for loss error range (0.2-0.3) with Mean accuracy of detection ± 2 SD.X Axis: RNNs vs WRNNs Y-Axis: Mean accuracy of detection ± 2 SD