ANOMALY DETECTION FOR VEHICULAR NETWORKS USING WIDE-RESNET CONVOLUTIONAL NEURAL NETWORK COMPARED OVER SUPPORT VECTOR MACHINE ACCURACY

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

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

Abstract

Aim: The goal of Vehicular Intrusion is to detect the attackers among Connected vehicles having unique characterstics and high mobility. The Controller Area Network (CAN Bus) is a bus communication protocol that establishes a standard for the simultaneous transmission of data between in-vehicle components. The Machine Learning algorithms are Wide-Resnet Convolutional Neural Network (CNN) and Support Vector Machine (SVM) are the two algorithms (SVM).

Materials and Methods: The data was obtained from the website www.kaggle.com. Sample size of Convolutional Neural Neural Network is (N=20) and the Sample size of Support Vector Machine is (N=20) are the two classes. The increased CAN(Bus) accuracy is 85%, and the Wide-Resnet Convolutional Neural Networks 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 Wide-Resnet Convolutional Neural Network (CNN) than Support Vector Machine.

Keywords: Vehicle Intrusion, Convolution Neural Network, Error Rate, Machine Learning, Support Vector Machine,wide-Resnet, CAN bus.

[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.

1. Introduction

Nowadays Securing the connectivity component of this technology is the most important of all the issues and obstacles facing connected vehicle intrusion in terms of implementation and development today.Connected vehicles, like any other electronic equipment connected to the Internet, are vulnerable to malicious cyberattacks(Hutter, Kotthoff, and Vanschoren 2019; Siuly, Li, and Zhang 2017)). Not to mention that the automation aspect of these technologies is a major contributor to the rise in cyber security attacks. Engine and brake failure, engine overheat, control steering troubles, and door lock issues are all examples of attacks that can be very serious and life threatening. As a result, the goal of this paper is to offer a vehicle Intrusion Detection System that uses Wide-Resnet and a SVM to prevent future security assaults on Connected Vehicles((Hutter, Kotthoff, and Vanschoren 2019; Siuly, Li, and Zhang 2017).

There are 78 articles found on IEEE, and 64 articles were found in the Google Scholar. Information sharing between connected vehicles raises concerns about confidentiality, message integrity, and denial of service, all of which pose security and privacy concerns. This article offers an automated secure continuous on connected vehicles that provides services that meet users' quality of service (QoS) and Quality of Experience (QoE) standards while also enabling an intrusion detection method against attacks (Renault, Mühlethaler, and Boumerdassi 2019). The dataset contains more than 2000 different kinds of messages sent totally at random on the CAN bus and all included in the analysis. Despite the complex structure of the dataset, the proposed method showed high detection accuracy with a low false negative rate. ((Renault, Mühlethaler, and Boumerdassi 2019) An anomaly-based IDS implemented using unsupervised learning to identify intrusions in-vehicle communication networks, in particular, a CAN bus Intrusion (Mhamed et al. 2021).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) (Barolli, n.d.)proposed a Clock-based IDS based Intrusion Detection system to protect in-vehicle Electronic Control Units (ECUs) and identify attacks on in-vehicle intrusion networks. (Marrinan 2021) stated to detect attacks in a CAN bus.They proposed that by using CAN packet frequency between packet sequences can discover anomalies based on the CAN performance on which ECUs interact. (Rahmatian 2014) The difficulties in predicting and generating attack behavior in evaluating the CAN bus system, as well as the need of generalization that is appropriate with the proprietary environment of CAN protocol, thus encourage researchers to propose supervised or semi-supervised anomaly detection methods.

Despite numerous security solutions being presented, the CAN bus communication system remains vulnerable to a variety of attacks attempting to compromise the network's security, in Vehicular intrusion. The landscape is continually evolving and every new connectivity service adds to the number of attack vectors available (Kwon, Yoon, and Park 2020). To overcome the issues of continuous attacks, it is proposed to design an Intrusion detection system using a Novel Wide Resnet Deep Learning Model and its performance is compared over a Support Vector Machine learning model.

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 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 Wide-Resnet Convolutional Neural Network(N=10) as an existing model as group 1 and Support Vector Machine(N=10) as a Proposed model as group 2.

Wide-Resnet Convolutional Neural Networks (Cnn)

By utilizing Wide-Resnet Convolutional Neural Networks calculations with 2 convolutional layers and completely associated layers. Wide-Resnet Convolutional Neural Networks 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 (1)

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

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.
```

Support Vector Machine (Svm)

SVM is a supervised machine learning algorithm, and it can be used for either classification or regression challenges. However, it is mostly used in classification problems. SVM is based on the concept of decision planes that defines decision boundaries.It is a type of graphical approach.

The steps are shown below.

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.
```

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 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 WIDE-RESNET and Support Vector Machine algorithm based methods.The independent variables are datasets of Vehicular 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 WIDE- RESNET and SVM for both methods.

Accuracy for wide-Residual Neural Network and Support Vector Machine algorithms have been calculated primarily based on equation(2)

$$\textbf{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Where,

TP = True Positive

TN - True Negative

FP - False Positive

FN - False Negative

3. Results

From Table2, shows the results of proposed algorithm Novel Wide-Resnet Convolution Neural Network and the existing system Support Vector Machine Algorithm where the accuracy of Wide-Resnet CNN, taken N=10 iterations and mean value is 88.0460 and standard deviation and standard error mean is 0.34727, 0.77652. Group of SVM is N=10 iterations and Mean is 85.7800, standard deviation and standard error rate mean is 0.55202,1.23436. It was observed that the mean accuracy of the Wide-Resnet CNN algorithm was 88% and the Support Vector algorithm was 85%. Table 3, shows the accuracy level of Equal variances assumed in Levene's Test for equality of variances of F is 0.975 and Sig is 0.352and T-Test for equality of means t is 5.008 and df is 8.13and Sig.(2-tailed) is .001 and Mean Difference is 3.26600 and Standard error difference is 0.65217 and 95% Confidence Interval of the Difference of Lower is 1.76209 and Upper is 4.76991. An one more accuracy equal variances not assumed and T-Test for equality of means t is 5.008 and df is 6.737 and Sig.(2-tailed) is 0.02 and Mean Difference and standard error rate difference is 3.26600,0.65217 and 95% confidence interval of the difference of Lower and Upper 1.71159,4.82041. 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 1 it was represented by a simple bar Mean of Accuracy Wide-Resnet Convolutional Neural Network error range (0.99 - 0.98) and SVM error rate range (0.99 - 0.98)

4. Discussions

Wide-Resnet CNN and Support Vector Machine algorithms are applied and compared on vehicle intrusion, which raises many interests largely due to its simplicity and the ability in detecting the attacks efficiently and to enhance the accuracy. From obtained consequences it's concluded that the Wide-Resnet CNN algorithm gives higher accuracy of significance 0.0001 consequences as compared to the Support Vector Machine. 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). (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.

5. Conclusion

The accuracy rate of the WIDE-Resnet Convolution Neural Network algorithm has been improved (88%) & Support Vector Machine, which is having (85%). By applying vehicle intrusion comparing both algorithms, the Novel Wide-Resnet Convolution Neural Network algorithm has high accuracy.

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

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

Barolli, Leonard. n.d. Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 16th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2021). 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.

Hutter, Frank, Lars Kotthoff, and Joaquin Vanschoren. 2019. Automated Machine Learning: Methods, Systems, Challenges. Springer.

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.

Kwon, Hyun, Hyunsoo Yoon, and Ki-Woong Park. 2020. “CAPTCHA Image Generation: Two-Step Style-Transfer Learning in Deep Neural Networks.” Sensors 20 (5). https://doi.org/10.3390/s20051495.

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.

Marrinan, Jean. 2021. Remote Sensor Monitoring: The Home Intruder Detection System: Intrusion Detection.

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.

Rahmatian, Mehryar. 2014. Intrusion Detection for Embedded System Security.

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.

Siuly, Siuly, Yan Li, and Yanchun Zhang. 2017. EEG Signal Analysis and Classification: Techniques and Applications. Springer.

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.

Tables and Figures

Table 1. Data collection for each algorithm N=10 iteration has been taken to calculate Accuracy rate for wide-Residual Neural Networks and Support Vector Machine to gain accuracy(%).

Samples(N)	**Wide-ResnetConvolution Neural Networks(CNN)**	**Support Vector Machine(SVM)**
	Accuracy(%)	**Accuracy(%)**
1	88.00	85.00
2	87.56	84.65
3	86.56	84.78
4	85.00	84.76
5	85.23	84.00
6	96.56	83.87
7	86.56	84.12
8	86.54	83.79
9	87.56	82.89
10	85.26	84.58

Table 2. Comparison of the accuracy of Intrusion Recognition of Wide-Resnet Convolution Neural Networks and SVM .Wide-Resnet Convolution Neural Network algorithm had the highest accuracy (88%). Support Vector Machine had the lowest accuracy (85%) accuracy compared to wide -resnet.

GROUPS		N	Mean	Std Deviation	Std Error Mean
ACCURACY	WRNs CNN	10	88.0460	.77652	.34727
	SVM	10	85.7800	1.23436	.55202

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, SVM has accepted a statistically significant value(p<0.05).

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	0.975	0.352	5.008	8.13	.001	3.266	.6521	1.762	4.769
Equal variances not assumed			5.008	6.737	.002	3.266	0.652	1.711	4.820

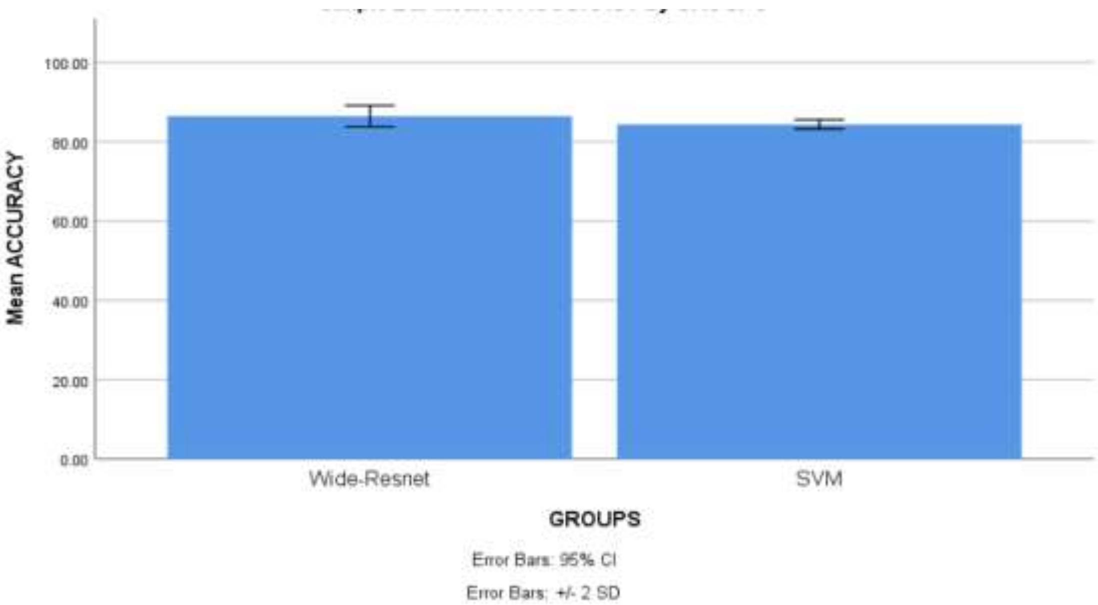

Fig 1. Simple Bar Mean of Accuracy WRNs CNN error range (0.99 - 0.98) and Loss error rate range (2-4) and SVM error rate range (0.98 - 0.99) and for loss error range (0.2-0.3) with Mean accuracy of detection ± 2 SD.X Axis: WRNs CNN vs SVM Y-Axis: Mean accuracy of detection ± 2 SD