Threat Detection and Mitigation in the Realm of Connected Vehicle Systems

Harith Yas[1], Manal M. Nasir [2,*]

[1]Faculty of Management, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

[2]Gwinnett Technical College, 5150 Sugarloaf Pkwy, Lawrenceville, GA 30043, USA

Emails: Harith.albayati@yahoo.com ; mnasir@gwinnetttech.edu

Abstract

Connected Vehicle Systems (CVS) are a combination of transportation and digital technologies that have the potential to revolutionize road safety and efficiency. However, this interconnectivity exposes them to various evolving cyber threats that require proactive detection and mitigation strategies. This study examines the security threat landscape in CVS, focusing on the challenges posed by malicious intrusions, unauthorized access, and vulnerabilities within vehicular networks. By using Deep Neural Networks (DNNs) and conducting an extensive literature review on cybersecurity frameworks, autonomous vehicles, and network vulnerabilities, this research provides a robust methodology for detecting and mitigating attacks in vehicular networks. The results show that the proposed approach is effective with improved predictive capabilities as well as the ability to detect abnormal behaviors. The findings highlight the need for standardized cybersecurity frameworks, cooperation among stakeholders, and continuous improvement of security protocols to ensure safe interconnected vehicular networks in a rapidly changing technological environment.

Keywords: Connected Vehicle; Cybersecurity; Threat Identification; Risk Mitigation Strategies; Automotive Network Security; Intrusion Detection Systems; Vehicle-to-Everything (V2X) Security; Malware Detection; Wireless Communication; Vehicle Telematics Security.

1. Introduction

The evolution of transportation technology has ushered in an era where vehicles are no longer solitary entities but interconnected nodes within complex networks, known as Connected Vehicle Systems (CVS). This integration of vehicles with digital infrastructure has introduced unprecedented conveniences, facilitating real-time communication, enhanced safety features, and novel modes of transportation. However, this interconnectedness has concurrently exposed these systems to a myriad of security threats, prompting a critical examination of cybersecurity measures within the realm of connected vehicles [1]. The interconnected nature of modern vehicles, comprising onboard sensors, communication systems, and computational capabilities, has given rise to an intricate web of data exchange, allowing vehicles to communicate with each other, infrastructure, and external networks [2-3]. This connectivity, while promising advancements in efficiency and safety, has become susceptible to various cyber threats. Malicious intrusions, remote attacks, and unauthorized access pose significant risks to the integrity, privacy, and functionality of these interconnected systems necessitating robust mechanisms for threat detection and mitigation [4].

The vulnerability landscape of Connected Vehicle Systems encompasses multifaceted challenges. Threats can manifest in different forms, ranging from unauthorized access to vehicle control systems, and interception of sensitive data transmitted between vehicles, to the infiltration of infrastructure supporting these networks [5]. Moreover, the integration of wireless communication protocols and the growing complexity of vehicle software systems amplify the potential attack surface, intensifying the urgency to fortify these systems against evolving threats. Addressing the intricacies of cybersecurity within Connected Vehicle Systems requires a comprehensive understanding of the

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

technological landscape, threat vectors, and the development of proactive strategies [6-8]. This paper aims to delve into the critical domain of threat detection and mitigation strategies within the context of connected vehicles. By examining prevalent security challenges, exploring existing detection methodologies, and proposing proactive measures, this study seeks to contribute to the ongoing discourse on fortifying the security posture of Connected Vehicle Systems [8-9].

2. Related Works

This section provides a comprehensive review and synthesis of previous studies, scholarly articles, and industry reports that explain the various dimensions of security threats in Connected Vehicle Systems. Giannaros et al. [10] study is an extensive examination of the autonomous vehicles landscape with a focus on advanced attacks, safety concerns, challenges, open topics, blockchain technology, and future directions. Alqahtani and Kumar [11] conducted a detailed analysis of machine learning applications in enhancing transportation security by specifically looking at electric and flying vehicle systems within the domain of engineering applications of artificial intelligence. Pendleton et al. [12] discuss the perception, planning, control, and coordination aspects of autonomous vehicles which highlight the complex technological requirements necessary for their operation. Kh-Madhloom and Alawadi [13] literature examines fortifications and vulnerabilities in 5G networks revealing emerging challenges in next-generation network security. Taeihagh and Lim [14] investigate governance frameworks for autonomous vehicles by presenting emerging responses to safety, liability, privacy, cybersecurity, and industry risks. Adu-Kyere et al. [16] propose a self-aware cybersecurity architecture catering to autonomous vehicles, focusing on security through system-level accountability. Metwaly and Elhenawy [17] delve into sustainable intrusion detection mechanisms in vehicular Controller Area Networks (CANs), employing machine intelligence paradigms for enhanced security. Ding et al. [18] introduce DeepSecDrive, an explainable deep learning framework designed for real-time cyberattack detection in in-vehicle networks, emphasizing the significance of real-time threat detection mechanisms. Furthermore, Chowdhury et al. [19] conducted a comprehensive survey on attacks targeted at self-driving cars along with countermeasures to mitigate these threats. Islam and Alqahtani [20] provide an overview of autonomous vehicles, covering system functionalities, cybersecurity aspects, associated risks, and prevalent issues, and propose a forward-looking perspective for this evolving technology.

3. Methodology

The empirical research cornerstone of this part of our study outlines the systematic approach used to investigate, analyze, and gain insights into the subject matter. This section explains the research framework and procedural guidelines that were used to explore security threats in Connected Vehicle Systems.

Deep Neural Networks (DNNs) were employed as a fundamental component of our methodology in this study to identify and detect potential cyber threats within Connected Vehicle Systems. DNNs are a subset of artificial neural networks with multiple hidden layers, which have been chosen for their ability to process complex data and extract intricate patterns, making them suitable for anomaly detection tasks within the vehicular network. The application of DNNs involved a multistage process that began with acquiring and preprocessing various datasets that included vehicular communication data, network logs, and sensor information. These datasets were carefully selected to include both normal operating conditions as well as simulated attack scenarios to provide an all-inclusive learning environment for the neural network. Afterward, the DNN architecture was designed and optimized to effectively learn and differentiate between normal vehicular behaviors and anomalous activities. The network's architecture comprised multiple layers, including input, hidden, and output layers, with specific activation functions and optimization algorithms tailored to enhance its learning capacity and discernment of attack patterns. Furthermore, the training phase involved feeding the curated datasets into the DNN, where the network iteratively learned the underlying patterns and features associated with normal vehicular operations while simultaneously discerning deviations indicative of potential attacks. The iterative learning process relied on backpropagation and gradient descent techniques, continually refining the network's parameters to minimize classification errors and enhance its predictive accuracy.

```
1. import tensorflow as tf  # Necessary import for TensorFlow
2.
3. # Creating a custom model inheriting from tf.keras.Model
4. class ModelDense(tf.keras.Model):
5.     def __init__(self):
6.         super(ModelDense, self).__init__()
```


DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

```
7.
8.          # Flatten layer to convert input into a 1D array
9.          self.flatten = tf.keras.layers.Flatten()
10.
11.         # Dense (fully connected) layer with 32 units/neurons
12.         self.dense1 = tf.keras.layers.Dense(32)
13.
14.         # Activation function (Rectified Linear Unit - ReLU) for the first dense layer
15.         self.act1 = tf.keras.layers.Activation('relu')
16.
17.         # Dense layer with 5 units for classification (output layer)
18.         self.dense2 = tf.keras.layers.Dense(5)
19.
20.         # Activation function (Softmax) for the output layer
21.         self.act2 = tf.keras.layers.Activation('softmax')
22.
23.     # Call function defines the forward pass through the network
24.     def call(self, inputs):
25.         x = self.flatten(inputs)  # Flatten the input
26.         x = self.dense1(x)  # Pass through the first dense layer
27.         x = self.act1(x)  # Apply ReLU activation
28.         x = self.dense2(x)  # Pass through the output dense layer
29.         x = self.act2(x)  # Apply Softmax activation for classification
30.         return x
```

Upon completion of the training phase, the DNN underwent rigorous evaluation using distinct performance metrics such, as assessing its ability to accurately classify and detect various types of attacks within the Connected Vehicle System. The evaluation phase aimed to validate the network's effectiveness in discriminating between normal and anomalous vehicular behaviors, ensuring its robustness in identifying potential security threats.

4. Experimental Design

This section constitutes a pivotal component in empirical research, delineating the structured framework and procedures employed to conduct rigorous experiments and analyses within the domain of security threats in Connected Vehicle Systems. To evaluate the detection performance of our model, the following metrics are used:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{1}$$

$$\text{Recall(Sensitivity)} = \frac{TP}{TP + FN} \tag{2}$$

$$\text{Specificity} = \frac{TN}{TN + FP} \tag{3}$$

$$\text{F1} - \text{score} \ \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

In our experiments, we use car-hacking datasets to train and evaluate the proposed model. The details of attack distribution are given in Table 1.

Table 1: Summary of the car-hacking dataset.

Attack Type	DoS Attack	Fuzzy Attack	Spoofing the drive gear	Spoofing the RPM gauze
# of messages	3,665,771	3,838,860	4,443,142	4621702
# of normal messages	3,078,250	3,347,013	3,845,890	3,966,805
# of injected messages	587,521	491,847	597,252	654,897

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

5. Results and Discussion

This section summarizes the results of empirical investigations and analyses aimed at understanding the landscape of security threats in Connected Vehicle Systems. Figure 1 shows learning curves that depict how models' performance has evolved over several iterations or epochs. These curves provide a visual representation of the learning process of the models, showing whether they converge or diverge concerning training and validation data. The visualization helps to understand how the models learn, revealing trends in accuracy, loss, or other relevant metrics across training epochs that are important for determining convergence, detecting overfitting, and improving model performance. Additionally, Figure 2 presents a confusion matrix which is a graphical representation that shows how our classification models performed by indicating true positive, true negative, false positive, and false negative predictions across different classes. This visual aid gives an overall view of the model's predictive ability by breaking down classification errors and accuracies.

Figure 3 presents the Receiver Operating Characteristic (ROC) curve, a graphical representation that illustrates the

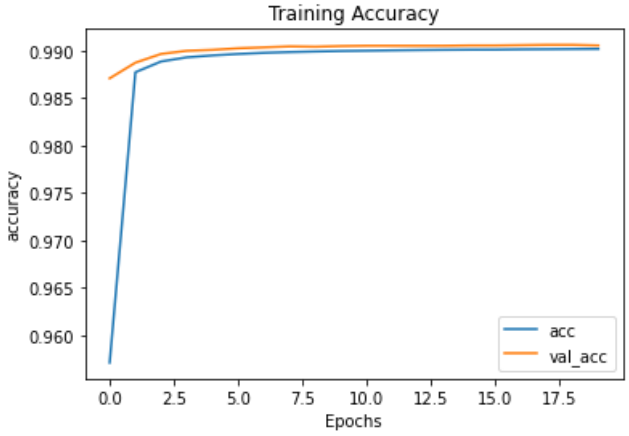

Figure 1: Learning Curves: Evolution of Model Performance over Training Epochs

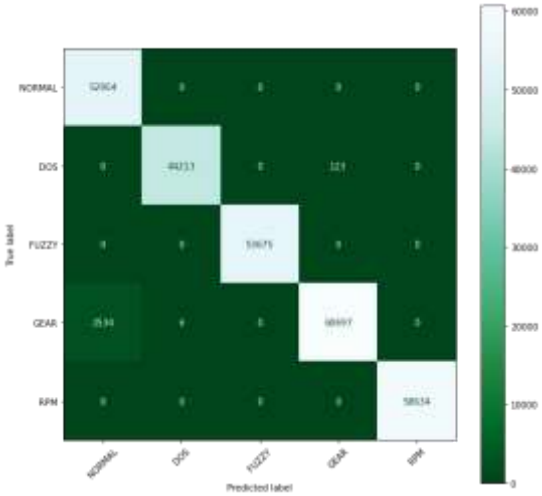

Figure 2: Confusion Matrix: Classification Performance Metrics for the Model

trade-off between a classification model's true positive rate (sensitivity) and false positive rate (1-specificity) across varying threshold values. This visual depiction is instrumental in assessing and comparing the discriminatory power and performance of different classification models. The curve's shape and proximity to the ideal diagonal line (representing perfect classification) signify the model's ability to distinguish between classes. Additionally, the area under the ROC curve (AUC-ROC) quantifies the model's overall performance, with a higher AUC indicating superior

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

discriminatory ability. This visualization aids in evaluating and selecting the most effective model for the task at hand, enabling informed decisions regarding model selection and optimization based on its discrimination capacity.

In Figure 4, we showcase the t-distributed Stochastic Neighbor Embedding (t-SNE) plot, a two-dimensional visualization technique employed to illustrate the high-dimensional data's structure and relationships in a lower-dimensional space. This visualization method reduces the complexity of multi-dimensional data while preserving local structures, offering insights into clusters, patterns, or groupings within the dataset. The t-SNE plot aids in uncovering hidden structures and revealing potential separability or clustering of data points, facilitating an intuitive

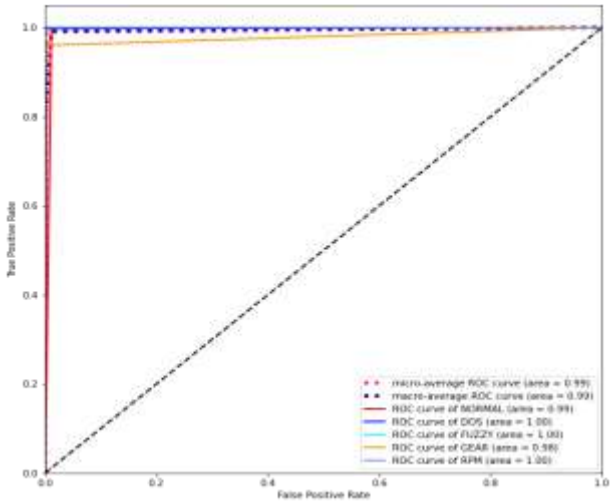

Figure 3: ROC Curve: True Positive Rate vs. False Positive Rate for Classification Models

understanding of the relationships between instances. This visualization assists in discerning intricate data patterns or groupings that might not be immediately apparent in higher-dimensional spaces, thereby aiding in exploratory data analysis and feature understanding.

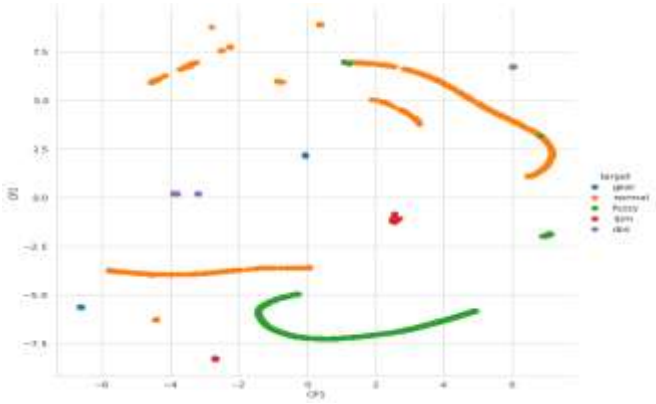

Figure 4: t-SNE Plot: Visualization of High-Dimensional Data in Two Dimensions

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

6. Conclusion

This study underscores the criticality of robust security measures in the realm of Connected Vehicle Systems (CVS), emphasizing the multifaceted landscape of security threats and the imperative need for proactive detection and mitigation strategies. By leveraging advanced technologies like Deep Neural Networks (DNNs) and exploring a comprehensive array of literature encompassing cybersecurity, autonomous vehicles, and network vulnerabilities, this research has illuminated the challenges and opportunities in fortifying the resilience of interconnected vehicular networks. The findings underscore the significance of continual research and development efforts to bolster cybersecurity protocols, establish standardized frameworks, and foster collaboration among stakeholders, laying the foundation for a safer, more secure future of connected mobility systems. As the landscape of technology evolves, the proactive adoption of robust security frameworks and adaptive defenses remains pivotal in ensuring the safety, privacy, and integrity of Connected Vehicle Systems amidst an ever-evolving threat landscape.

References

[1] Elliott, David, Walter Keen, and Lei Miao. 2019. "Recent Advances in Connected and Automated Vehicles." Journal of Traffic and Transportation Engineering (English Edition) 6 (2): 109–31.

[2] Han, Jinpeng, Zhiyang Ju, Xiaoguang Chen, Manzhi Yang, Hui Zhang, and Rouxing Huai. 2023. "Secure Operations of Connected and Autonomous Vehicles." IEEE Transactions on Intelligent Vehicles.

[3] Girdhar, Mansi, Yongsik You, Tai-Jin Song, Subhadip Ghosh, and Junho Hong. 2022. "Post-Accident Cyberattack Event Analysis for Connected and Automated Vehicles." IEEE Access 10: 83176–94.

[4] Bayless, Steven H, Sean Murphy, and Anthony Shaw. 2011. "Connected Vehicle Assessment." ITS America.

[5] Hidalgo, Carlos, Myriam Vaca, Mateusz P Nowak, Piotr Frölich, Martin Reed, Mays Al-Naday, Asterios Mpatziakas, Aikaterini Protogerou, Anastasios Drosou, and Dimitrios Tzovaras. 2022. "Detection, Control and Mitigation System for Secure Vehicular Communication." Vehicular Communications 34: 100425.

[6] McCall, Sophia, Cagatay Yucel, and Vasilios Katos. 2021. "Education in Cyber Physical Systems Security: The Case of Connected Autonomous Vehicles." In 2021 IEEE Global Engineering Education Conference (EDUCON), 1379–85.

[7] Park, Hyungjun, Zulqarnain Khattak, and Brian Smith. 2018. "Glossary of Connected and Automated Vehicle Terms." University of Virginia Center for Transportation Studies.

[8] Ismail, M. and F.Abd El-Gawad , A. (2023) "Revisiting Zero-Trust Security for Internet of Things", Sustainable Machine Intelligence Journal, 3. doi: 10.61185/SMIJ.2023.33106.

[9] El-Rewini, Zeinab, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. 2020. "Cybersecurity Challenges in Vehicular Communications." Vehicular Communications 23: 100214.

[10] Giannaros, Anastasios, Aristeidis Karras, Leonidas Theodorakopoulos, Christos Karras, Panagiotis Kranias, Nikolaos Schizas, Gerasimos Kalogeratos, and Dimitrios Tsolis. 2023. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions." Journal of Cybersecurity and Privacy 3 (3): 493–543.

[11] Alqahtani, Hamed, and Gulshan Kumar. 2024. "Machine Learning for Enhancing Transportation Security: A Comprehensive Analysis of Electric and Flying Vehicle Systems." Engineering Applications of Artificial Intelligence 129: 107667.

[12] Pendleton, Scott Drew, Hans Andersen, Xinxin Du, Xiaotong Shen, Malika Meghjani, You Hong Eng, Daniela Rus, and Marcelo H Ang. 2017. "Perception, Planning, Control, and Coordination for Autonomous Vehicles." Machines 5 (1): 6.

[13] Ismail, M. and F.Abd El-Gawad , A. (2023) "Revisiting Zero-Trust Security for Internet of Things", Sustainable Machine Intelligence Journal, 3. doi: 10.61185/SMIJ.2023.33106.

[14] Taeihagh, Araz, and Hazel Si Min Lim. 2019. "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks." Transport Reviews 39 (1): 103–28.

[15] Heemstra, Jennifer. 2018. "Autonomous Vehicle Technology-The Need for a National Standard on Cybersecurity." Ave Maria L. Rev. 16: 130.

[16] Adu-Kyere, Akwasi, Ethiopia Nigussie, and Jouni Isoaho. 2023. "Self-Aware Cybersecurity Architecture for Autonomous Vehicles: Security through System-Level Accountability." Sensors 23 (21): 8817.

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024

[17] A. Metwaly, A. and Elhenawy, I. (2023) "Sustainable Intrusion Detection in Vehicular Controller Area Networks using Machine Intelligence Paradigm", Sustainable Machine Intelligence Journal, 4. doi: 10.61185/SMIJ.2023.44104.
[18] Ding, W., Alrashdi, I., Hawash, H. and Abdel-Basset, M., 2023. DeepSecDrive: An explainable deep learning framework for real-time detection of cyberattack in in-vehicle networks. Information Sciences, p.120057.
[19] Chowdhury, Abdullahi, Gour Karmakar, Joarder Kamruzzaman, Alireza Jolfaei, and Rajkumar Das. 2020. "Attacks on Self-Driving Cars and Their Countermeasures: A Survey." IEEE Access 8: 207308–42.
[20] Islam, Md Aminul, and Sarah Alqahtani. 2023. "Autonomous Vehicles an Overview on System, Cyber Security, Risks, Issues, and a Way Forward." ArXiv Preprint ArXiv:2309.14213.
[21] Ahmad, Jameel, Muhammad Umer Zia, Ijaz Haider Naqvi, Jawwad Nasar Chattha, Faran Awais Butt, Tao Huang, and Wei Xiang. 2023. "Machine Learning and Blockchain Technologies for Cybersecurity in Connected Vehicles." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, e1515.

DOI: https://doi.org/10.54216/IJWAC.080104
Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024