International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 08, No .01, 2024 ♦ PP. 16–20

Article DOI: https://doi.org/10.54216/IJWAC.080104

FULL LENGTH ARTICLE

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

Received: June 19, 2023 Revised: October 28, 2023 Accepted: January 06, 2024 ⋆ Corresponding author

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 behaviours. 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 technological landscape, threat vectors, and the development of proactive strategies [6, 7, 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] present 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 engineering applications of artificial intelligence.

Pendleton et al. [12] discuss the perception, planning, control, and coordination aspects of autonomous vehicles, highlighting the complex technological requirements necessary for their operation. Kh-Madhloom and Alawadi [13] examine 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.

Heemstra [15] addresses the need for national cybersecurity standards for autonomous vehicle technology. Adu-Kyere et al. [16] propose a self-aware cybersecurity architecture for autonomous vehicles, focusing on security through system-level accountability. Metwaly and Elhenawy [17] investigate 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. 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 employed methodology for detecting and mitigating security threats in connected vehicle systems combines a structured literature review with a Deep Neural Network (DNN)-based detection model. The study first identifies the threat landscape through previous work on cybersecurity, autonomous vehicles, vehicular communications, 5G networks, and intrusion detection. It then develops a learning-based approach to distinguish normal vehicular behaviour from anomalous or attack-related patterns.

The DNN model is designed to classify vehicle-network observations into normal or malicious traffic classes. The architecture flattens input observations, processes them through a dense layer, applies a ReLU activation function, and produces class probabilities using a softmax output layer. The essential structure is illustrated below.

```
class DNN(tf.keras.Model):
    def __init__(self):
        super(DNN, self).__init__()
        self.flatten = tf.keras.layers.Flatten()
        self.dense1 = tf.keras.layers.Dense(32)
        self.act1 = tf.keras.layers.Activation('relu')
        self.dense2 = tf.keras.layers.Dense(5)
        self.act2 = tf.keras.layers.Activation('softmax

    def call(self, inputs):
        x = self.flatten(inputs)
        x = self.dense1(x)
        x = self.act1(x)
        x = self.dense2(x)
        x = self.act2(x)
        return x
```

Upon completion of the training phase, the DNN underwent rigorous evaluation using distinct performance metrics, 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 behaviours, 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 the proposed model, the following metrics are used:

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

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

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

$$\text{F1-score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

In the experiments, car-hacking datasets are used 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 Gauge
# of messages	3,665,771	3,838,860	4,443,142	4,621,702
# 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

The model is assessed using detection accuracy, class-wise predictive behaviour, confusion-matrix outputs, ROC analysis, and low-dimensional visualization of learned representations. These measurements provide complementary insights into whether the model converges during training, detects abnormal patterns reliably, and separates malicious events from legitimate vehicular traffic.

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 the model's performance evolved over several iterations or epochs. These curves provide a visual representation of the learning process, showing whether the model converges or diverges concerning training and validation data. The visualization helps to understand how the model learns, revealing trends in accuracy, loss, or other relevant metrics across training epochs that are important for determining convergence, detecting overfitting, and improving model performance.

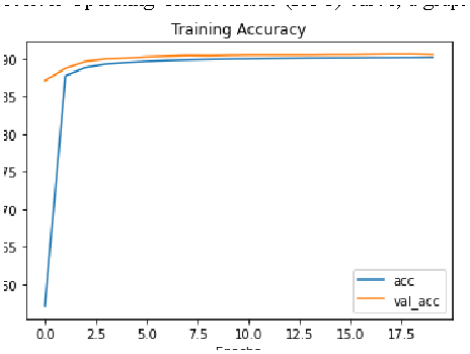

Figure 1. Learning curves: evolution of model performance over training epochs.

Figure 2 presents a confusion matrix, a graphical representation that shows how the classification model 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.

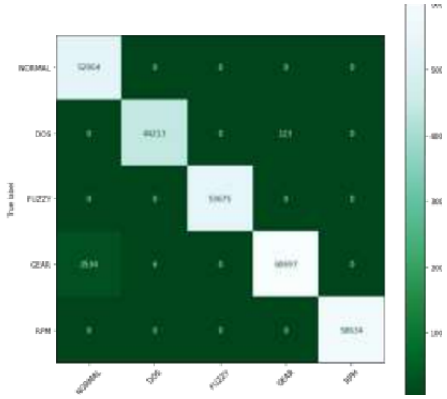

Figure 2. Confusion matrix: classification performance metrics for the model.

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

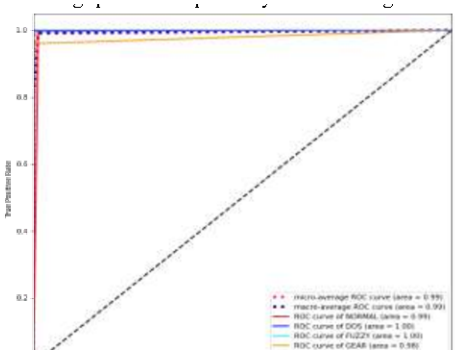

Figure 3. ROC curve: true positive rate vs. false positive rate for classification models.

In Figure 4, the t-distributed Stochastic Neighbor Embedding (t-SNE) plot is showcased as 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, thereby supporting exploratory data analysis and feature understanding.

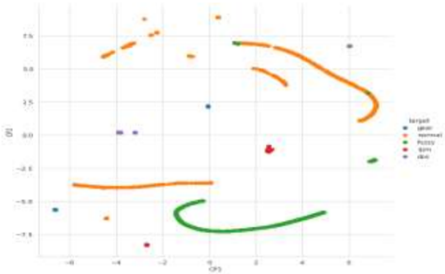

Figure 4. t-SNE plot: visualization of high-dimensional data in two dimensions.

Overall, the obtained results suggest that the proposed DNN-based approach provides improved predictive capabilities and can detect abnormal behaviours in connected vehicular networks. The combination of learning-curve inspection, confusion-matrix analysis, ROC-based discrimination, and t-SNE visualization supports a comprehensive interpretation of the model's detection performance.

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 such as 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 defences remains pivotal in ensuring the safety, privacy, and integrity of Connected Vehicle Systems amidst an ever-evolving threat landscape.

REFERENCES

[1] D. Elliott, W. Keen, and L. Miao, "Recent advances in connected and automated vehicles," *Journal of Traffic and Transportation Engineering (English Edition)*, vol. 6, no. 2, pp. 109–131, 2019.

[2] J. Han, Z. Ju, X. Chen, M. Yang, H. Zhang, and R. Huai, "Secure operations of connected and autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, 2023.

[3] M. Girdhar, Y. You, T.-J. Song, S. Ghosh, and J. Hong, "Post-accident cyberattack event analysis for connected and automated vehicles," *IEEE Access*, vol. 10, pp. 83 176–83 194, 2022.

[4] S. H. Bayless, S. Murphy, and A. Shaw, "Connected vehicle assessment," ITS America, Tech. Rep., 2011.

[5] C. Hidalgo, M. Vaca, M. P. Nowak, P. Frölich, M. Reed, M. Al-Naday, A. Mpatziakas, A. Protogerou, A. Drosou, and D. Tzovaras, "Detection, control and mitigation system for secure vehicular communication," *Vehicular Communications*, vol. 34, p. 100425, 2022.

[6] S. McCall, C. Yucel, and V. Katos, "Education in cyber physical systems security: The case of connected autonomous vehicles," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021, pp. 1379–1385.

[7] H. Park, Z. Khattak, and B. Smith, "Glossary of connected and automated vehicle terms," University of Virginia Center for Transportation Studies, Tech. Rep., 2018.

[8] M. Ismail and A. F. Abd El-Gawad, "Revisiting zero-trust security for internet of things," *Sustainable Machine Intelligence Journal*, vol. 3, 2023.

[9] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[10] A. Giannaros, A. Karras, L. Theodorakopoulos, C. Karras, P. Kranias, N. Schizas, G. Kalogeratos, and D. Tsolis, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, 2023.

[11] H. Alqahtani and G. Kumar, "Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107667, 2024.

[12] S. D. Pendleton, H. Andersen, X. Du, X. Shen, M. Meghjani, Y. H. Eng, D. Rus, and M. H. Ang, "Perception, planning, control, and coordination for autonomous vehicles," *Machines*, vol. 5, no. 1, p. 6, 2017.

[13] M. Ismail and A. F. Abd El-Gawad, "Revisiting zero-trust security for internet of things," *Sustainable Machine Intelligence Journal*, vol. 3, 2023.

[14] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transport Reviews*, vol. 39, no. 1, pp. 103–128, 2019.

[15] J. Heemstra, "Autonomous vehicle technology–the need for a national standard on cybersecurity," *Ave Maria Law Review*, vol. 16, p. 130, 2018.

[16] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability," *Sensors*, vol. 23, no. 21, p. 8817, 2023.

[17] A. A. Metwaly and I. Elhenawy, "Sustainable intrusion detection in vehicular controller area networks using machine intelligence paradigm," *Sustainable Machine Intelligence Journal*, vol. 4, 2023.

[18] W. Ding, I. Alrashdi, H. Hawash, and M. Abdel-Basset, "Deepsecdrive: An explainable deep learning framework for real-time detection of cyberattack in in-vehicle networks," *Information Sciences*, p. 120057, 2023.

[19] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020.

[20] M. A. Islam and S. Alqahtani, "Autonomous vehicles an overview on system, cyber security, risks, issues, and a way forward," arXiv preprint arXiv:2309.14213, 2023.