Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

A Review on Connected Vehicle Cyber-Attacks and Various Intrusion Detection Techniques

Segun Ebenezer Olaniyan
Federal University of Technology
Minna, Niger State, Nigeria.
E-mail: segunthescribe@gmail.com
Phone: +2347066680988

ABSTRACT

In today's world, self-driving and connected vehicles are becoming more interconnected with the internet. This integration allows for many features and services, such as cellular service, Wi-Fi, and Bluetooth. However, this increased connectivity comes with increased vulnerability to cyber threats, making automotive systems more attractive targets for potential cyberattacks. It is imperative to prioritise intrusion detection when securing the network of vehicles, particularly self-driving cars and vehicles with open connectivity. This paper presents an overview of cyberattacks that can threaten connected and autonomous vehicles and various intrusion detection techniques that can be used to avoid them.

Keywords: Connected vehicle, Internet of Things (IoT), Cyber-attack, Intrusion Detection, Automotive, Network, Internet.

Proceedings Citation Format
Segun Ebenezer Olaniyan (2024): A Review on Connected Vehicle Cyber-Attacks and Various Intrusion Detection Techniques. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 35-42. https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/ dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P3

1. INTRODUCTION

The Internet of Things (IoT) has brought about a significant transformation in how automotive networks function. Nowadays, cars are capable of connecting with various infrastructures and devices that were previously unknown to them. The Internet of Things (IoT) is a global network of interconnected devices and technologies that allows cloud-based communication.

The primary factor that facilitates this function is the Internet. The modern vehicle has evolved into a complex cyber-physical system, combining traditional mechanical components with sophisticated electronics and software. Electronic Control Units (ECUs) play a crucial role in this system by managing various functions within the vehicle (Lampe & Meng, 2023). The ECUs (Electronic Control Units) are in charge of multiple vehicle functions, including driving and comfort, and they communicate through various in-vehicle networks. These networks often use technologies like Ethernet and CAN (Controller Area Networks), a type of bus technology specifically designed for communication within a vehicle. The communication between ECUs and specific peripherals is made easy by utilising a shared bus and a simple protocol (Zenden et al., 2023).

Modern vehicles, including electric, hybrid, and driverless cars, require constant communication between different modules to function correctly. Various applications of CAN have been rapidly developed to facilitate this exchange of information. Additionally, there are other complex in-vehicle network architectures, such as Media-Oriented Systems Transport (MOST), FlexRay, Local Interconnect Networks (LIN), and Automotive Ethernet (AE) (Rathore et al., 2022). According to Hammood et al. (2023), cybersecurity experts forecast increased cyberattacks with the increasing usage of vehicle communication systems. It is imperative to employ robust detection techniques to prevent such threats. An Intrusion Detection System (IDS) is a security system that can improve vehicles' safety without requiring significant infrastructure changes (Lampe & Meng, 2023). It depicts excellent potential for enhancing connected vehicle security.

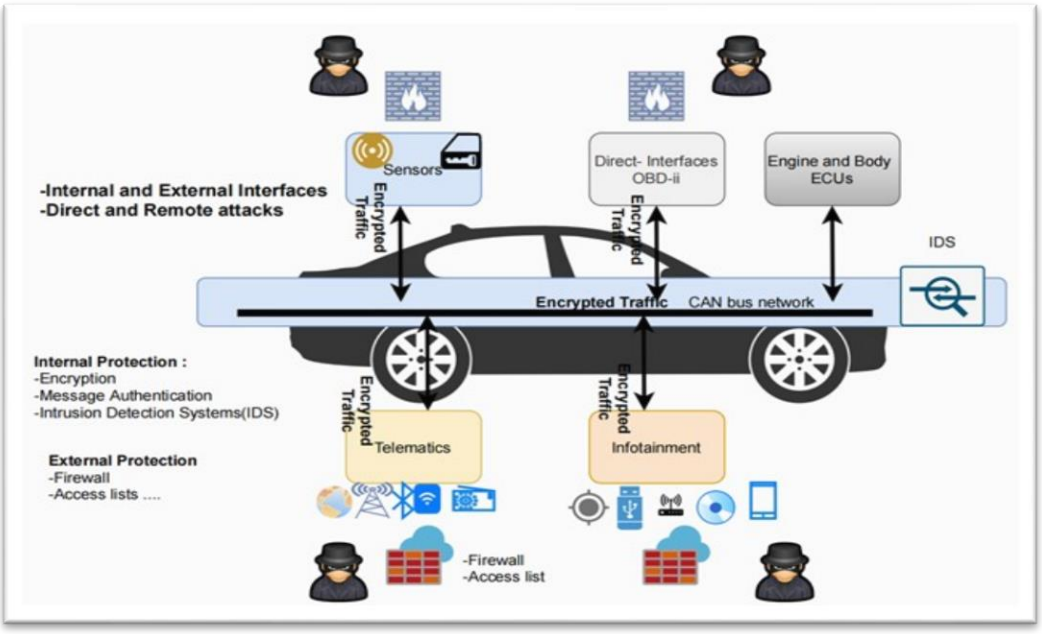

Figure 1: A connected vehicle with entry points for data injection: Telematics, Infotainment, Direct interfaces, and Sensors. Security measures include Cryptography, IDS, Firewalls, and Access Control Lists to prevent physical and remote attacks according to the research (Aliwa et al., 2021).

The figure above clearly represents the techniques used to input and output data between the vehicle system and the external environment. Telematics allow for communication between the vehicle and external networks or servers. They enable remote diagnostics, over-the-air updates, and navigation services. However, infotainment provides occupants with entertainment, navigation and communication features. These systems are connected via Bluetooth, USB, or Wi-Fi to external devices such as smartphones. In addition, vehicles have physical interfaces and ports, such as USB or diagnostic ports (OBD-II), which could be referred to as direct interfaces for legitimate purposes such as diagnostics, maintenance, or firmware updates.

Modern vehicles have many sensors for various purposes; they also include advanced driver assistance systems (ADAS) and autonomous driving features (Khandelwal & Shanker Shreejith, 2022). These sensors collect and feed data to the vehicle's control systems. All these components enhance vehicles' open connectivity and are susceptible to cyberattacks. This paper focuses on the types of cyberattacks that can target connected vehicle systems and various techniques used for intrusion detection. This paper further outlines the following sections: Section II covers different connected vehicle cyberattacks. Section III discusses various techniques for intrusion detection, and Section IV concludes the article.

2. CONNECTED VEHICLE CYBER-ATTACK

Any malicious activity that takes advantage of vulnerabilities within a vehicle's network or the open connectivity features of motor vehicles can be called a connected vehicle cyber-attack. These attacks can target various vehicle entry points, components, or systems to compromise their operation, safety, privacy, or data integrity. One of the critical components of the automotive system is the Controller Area Network (CAN). The CAN protocol is commonly used in vehicles to transfer data between ECUs and sensors. A CAN bus controller within the vehicle connects crucial components like the engine and body control modules, including gears, speed, brakes, and more. However, since the CAN protocol lacks message authentication, it is susceptible to cyber-attacks like CAN frame injections (Aliwa et al., 2021).

Furthermore, Nguyen et al. (2023) provided insight into the typical network attacks that cyber attackers can execute on the CAN bus. The cyber-attacks are as follows:

Flood Attack: One of the most common types of attacks on computer systems is a denial-of-service (DoS) attack. It involves the use of a flood attack, where a large number of legitimate requests are sent, overwhelming the processing capabilities of the CAN bus. The attacker aims to destroy the system's infrastructure and destabilise its operations.

Fuzzy Attack: The CAN Bus is repeatedly injected by using random messages. To interfere with the vehicle's operations, the attacker analyses the CAN packets containing in-vehicle information and chooses specific CAN IDs to trigger unexpected actions.

Spoofing Attack: Intruders can launch a spoofing attack, also known as a malfunction (Mal) attack, using acquired CAN IDs to identify particular subsystem functions within a vehicle. Changing the payload generates abnormal messages.

Replay Attack: A legitimate message being seized and carelessly introduced into the CAN bus poses a potential threat. This could force vehicles to repeat actions that might result in dangerous consequences. Detecting such attacks is only possible if the sequential patterns in the CAN are carefully examined. Other potential cyberattacks that could occur against autonomous and connected vehicles include:

Remote Exploitation: involves exploiting vulnerabilities in the vehicle network, software, or associated systems to gain unauthorised access and control of vehicle functions. Attackers can remotely modify critical brakes, steering, and speed systems. If a hacker accesses sensor data and enters false information, it can cause the vehicle's management systems to make incorrect decisions, affecting safety and performance.

Data Manipulation: Attackers can inject false information into a vehicle's sensors or systems, causing the vehicle's management system to make incorrect decisions. For example, changes in sensor data related to environmental or road conditions can lead to risky or unpredictable behaviours. Additionally, telematic systems can be vulnerable to unauthorised access or malicious attacks that could result in data modification or control of certain vehicle functions.

Ransomware: Modern cars are connected to the internet; attackers could shut down its system and take it hostage, demanding payment to return control to the owner. Attackers can insert malicious code or gain unauthorised access to a vehicle's network to shut down its system.

Eavesdropping and Surveillance: The transmission of private information between a vehicle's components or to outside servers can be intercepted and stolen by cybercriminals. This poses a potential risk to the passengers' privacy inside the vehicle.

3. ANALYSIS OF VARIOUS INTRUSION DETECTION TECHNIQUES

Nguyen et al. (2023) proposed an innovative intrusion detection system (IDS) for detecting potential attacks on in-vehicle CAN buses. The system uses transformer-based attention network (TAN) technology, which can categorise attacks without relying on RNNs. The TAN employs a self-attention mechanism to identify replay attacks by aggregating sequential CAN IDs. Unlike other models, the TAN can identify intrusion messages without requiring message labelling, even when sequential CAN IDs are used. The experimental results have demonstrated that the TAN is more efficient than the baselines for different input data types and datasets. Additionally, the TAN uses transfer learning to improve the performance of models trained on small data from other vehicle models, inheriting the benefits of transformers.

Yang et al. (2022) designed a remarkable IDS system named Leader Class and Confidence Decision Ensemble (LCCDE). It utilises three state-of-the-art algorithms (XGBoost, LightGBM, and CatBoost) to identify the most effective model for each type of cyber-attack. By leveraging the predicted confidence values, the class leader models can accurately detect an array of cyberattacks. The results of experiments conducted on two public IoV security datasets (Car-Hacking and CICIDS2017) demonstrate that LCCDE is a reliable solution for detecting intrusions on intra-vehicle and external networks.

According to Yang et al. (2022), the LCCDE model proposed demonstrated exceptional performance on the Car-Hacking dataset, achieving an almost perfect F1-score of 99.9997%. Additionally, it significantly elevated the F1-score of the CICIDS2017 dataset from 99.792% to 99.811%. These results emphasise the advantages of utilising the highest-performing base models for each category to construct the LCCDE ensemble model.

Yang and Shami (n.d.) proposed an Intrusion Detection System (IDS) for IoV systems that uses transfer learning and ensemble learning techniques based on Convolutional Neural Networks (CNNs) and hyperparameter optimisation. Experiments were conducted on two widely recognised public IoV security datasets - the Car-Hacking and CICIDS2017. Based on the experiments conducted, it was observed that the proposed IDS framework could accurately detect different types of attacks with higher F1-scores of 100% and 99.925% than other state-of-the-art methods used on the two benchmark datasets.

Khandelwal and Shanker Shreejith (2022) presented a machine-learning model to detect various in-vehicle attacks effectively. The model used Xilinx's Deep Learning Processing Unit IP on a Zynq Ultrascale+ (XCZU3EG) FPGA and was trained and tested using the public CAN Intrusion Detection dataset. The model boasts an accuracy rate of over 99% and a false positive rate of only 0.07%, making it highly reliable in detecting denial of service and fuzzing attacks. Its performance is comparable to the most advanced techniques existing. The IDS execution consumes only 2.0 W with software tasks running on the ECU, resulting in a 25% reduction in per-message processing latency compared to current implementations. This deployment is an excellent option for real-time IDS in in-vehicle systems as it requires minimal task modifications and allows the ECU function to coexist with the IDS.

Schell and Kneib (2023) designed SPARTA to detect and prevent intrusions on the CAN bus. It is highly reliable and uses an active prevention mechanism to minimise the impact of attacks. SPARTA can identify transmission authenticity violations and recognise denial-of-service (DoS) attack attempts. It is designed to require minimal resources and can meet the real-time constraints of automotive systems. The system was tested on different CAN and CAN-FD setups and has proven efficient, high-performing, and adaptable to dynamic environments.

To evaluate SPARTA's attack detection, Yang and Shami (n.d.) adjusted the settings of every node to have a 10% chance of sending unauthorised messages with an identifier from a randomly selected node. SPARTA successfully detected all 13,550 random attack messages with a 100% detection rate, without any false positives or negatives, and identified the attacker in each instance.

Aldhyani and Alkahtani (2022) presented an advanced solution that proactively uses AI technology to protect vehicle networks from potential cyber threats. A security system based on deep learning approaches to protect autonomous vehicles from intrusions. This was tested on a real automatic vehicle network dataset, which includes spoofing, replay attacks, FL flood, and benign packets. A dataset underwent preprocessing to convert categorical data into numerical data. The dataset was processed using two models to identify attack messages: the convolutional neural network (CNN) and a hybrid network that combines CNN and long short-term memory (CNN-LSTM).

The proposed system has been empirically demonstrated to have an impressive accuracy rate of 97.30%. This approach surpasses existing systems by significantly improving detection and classification accuracy, making it the top-performing system for ensuring real-time CAN bus security (Aldhyani & Alkahtani, 2022). Vita Santa Barletta et al. (2023) established a vehicle-security operation centre for improving automotive security (V-SOC4AS). The centre monitors intra-vehicle communication subsystems in real-time, such as CAN, LIN, FlexRay, MOST, and Ethernet. V-SOC4AS deploys security information and event management (SIEM) to detect malicious attacks in intra-vehicle and inter-vehicle communications, including messages transmitted between vehicle ECUs, infotainment and telematics systems, and vehicular ports.

SOC analysts can automatically identify potential threats and enhance incident response processes leveraging V-SOC4AS. Furthermore, V-SOC4AS can classify messages as malicious or non-malicious, obtain more information about the type of attack, and reduce detection time, thus facilitating support for response activities. An open-source dataset was used to simulate vehicles and evaluate denial of service (DoS) and fuzzing attacks. V-SOC4AS employs a rule-based mechanism to analyse packets a vehicle sends and instantly alerts SOC analysts if the payload contains a CAN frame attack (Vita Santa Barletta et al., 2023).

Zhang and Ma (2022) identified the two primary approaches for intrusion detection as rule-based and machine learning-based. Furthermore, it was noted that the rule-based approach is efficient but limited in detection accuracy. In contrast, machine learning detection has comparably higher detection accuracy but higher computation costs at the same time. Therefore, a unique hybrid intrusion detection system was developed, combining the advantages of rule-based and machine learning-based methodologies.

Zhang and Ma (2022), the approach utilises machine learning techniques to attain a high detection rate while minimising the computational resources needed by leveraging a rule-based component. The extensive testing on CAN traces obtained from four distinct vehicle models proved the efficacy and efficiency of the proposed hybrid IDS solution. Islam et al. (2022) proposed an intrusion detection algorithm called the graph-based Gaussian naive Bayes (GGNB). This algorithm uses graph properties and PageRank-related features to enhance its accuracy. When tested on the raw CAN data set, it detected denial of service (DoS), fuzzy, spoofing, replay, and mixed attacks with 99.61%, 99.83%, 96.79%, and 96.20% accuracy, respectively. The Opel Astra data set also accurately detected DoS, diagnostic, fuzzing CAN ID, fuzzing payload, replay, suspension, and mixed attacks, with percentages ranging from 97.75% to 100%. The GGNB-based methodology requires significantly less training and test time than the SVM classifier used in the same application.

Cheng et al. (2022) proposed a TCAN-IDS model that uses a temporal convolutional network with global attention to detect network intrusion in vehicles. The model encodes 19-bit features, including an arbitration bit and data field, into a message matrix that recalls historical messages. The feature extraction model extracts spatial-temporal detail features using global attention to focus on essential changes. Finally, a two-class classification component monitors anomalous traffic. According to experimental results, TCAN-IDS can be monitored in real time and offers high detection performance on known attack datasets. This model is expected to provide high information security and prevent illegal intrusion.

4. CONCLUSION

The Internet of Things and open connectivity have given rise to the Internet of Vehicles, allowing vehicles to communicate with other vehicles, infrastructures and the external world. While this innovation in the automotive industry is exciting, it also increases the risk of cyber-attacks on self-driving cars and connected vehicles. Therefore, it is crucial to implement effective intrusion detection techniques to identify potential attacks on in-vehicle networks. This paper evaluates several types of connected vehicle cyber-attacks and the various intrusion detection techniques used to avoid them.

REFERENCE

Aldhyani, T. H. H., & Alkahtani, H. (2022). Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors*, *22*(1), 360. https://doi.org/10.3390/s22010360

Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and Countermeasures for In-Vehicle Networks. *ACM Computing Surveys*, *54*(1), 1–37. https://doi.org/10.1145/3431233

Cheng, P., Xu, K., Li, S., & Han, M. (2022). TCAN-IDS: Intrusion Detection System for Internet of Vehicle Using Temporal Convolutional Attention Network. *Symmetry*, *14*(2), 310. https://doi.org/10.3390/sym14020310

Hammood, L., Doğru, İ. A., & Kılıç, K. (2023). Machine Learning-Based Adaptive Genetic Algorithm for Android Malware Detection in Auto-Driving Vehicles. *Applied Sciences*, *13*(9), 5403. https://doi.org/10.3390/app13095403

Islam, R., Devnath, M. K., Samad, M. D., & Jaffrey Al Kadry, S. M. (2022). GGNB: Graph-based Gaussian naive Bayes intrusion detection system for CAN bus. *Vehicular Communications*, *33*, 100442. https://doi.org/10.1016/j.vehcom.2021.100442

Khandelwal, S., & Shanker Shreejith. (2022). *A Lightweight Multi-Attack CAN Intrusion Detection System on Hybrid FPGAs*. https://doi.org/10.1109/fpl57034.2022.00070

Lampe, B., & Meng, W. (2023). A survey of deep learning-based intrusion detection in automotive applications. *Expert Systems with Applications*, *221*, 119771. https://doi.org/10.1016/j.eswa.2023.119771

Nguyen, T. P., Nam, H., & Kim, D. (2023). Transformer-Based Attention Network for In-Vehicle Intrusion Detection. *IEEE Access*, *11*, 55389–55403. https://doi.org/10.1109/ACCESS.2023.3282110

Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, *22*(17), 6679. https://doi.org/10.3390/s22176679

Schell, O., & Kneib, M. (2023). *SPARTA: Signal Propagation-based Attack Recognition and Threat Avoidance for Automotive Networks*. https://doi.org/10.1145/3579856.3595788

Vita Santa Barletta, Caivano, D., Mirko De Vincentiis, Ragone, A., Scalera, M., & Serrano, M. A. (2023). V-SOC4AS: A Vehicle-SOC for Improving Automotive Security. *Algorithms*, *16*(2), 112–112. https://doi.org/10.3390/a16020112

Yang, L., & Shami, A. (n.d.). *A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles*. Retrieved August 16, 2023, from https://arxiv.org/pdf/2201.11812.pdf

Yang, L., Shami, A., Stevens, G., & De Rusett, S. (2022). LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in The Internet of Vehicles. *ArXiv:2208.03399 [Cs]*. https://arxiv.org/abs/2208.03399

Zenden, I., Wang, H., Iacovazzi, A., Vahidi, A., Blom, R., & Raza, S. (2023, April 1). *On the Resilience of Machine Learning-Based IDS for Automotive Networks*. IEEE Xplore. https://doi.org/10.1109/VNC57357.2023.10136285

Zhang, L., & Ma, D. (2022). A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks. *IEEE Access*, *10*, 10852–10866. https://doi.org/10.1109/access.2022.3145007