Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CAN Bus Data Analysis for Anomaly Detection in Connected and Automated Vehicles

Onyeukwu Christian Nduka[1], Ugboaja Samuel Gregory[2], Mbagwu Amarachi Austina[3], Ifeoma Benardine Asianuba[4], Onyeukwu Johnkennedy Onyedikachi[5], Ugwuja Nnenna Esther[6], Okwu Marcus Eke[7], Abiodun Isaac Chukwutem[8], Obogai, Leo Eromina[9]

[1] Bishop's University, Sherbrooke, Canada. onyeukwu@cs.ubishops.ca
[2] Michael Okpara University of Agriculture, Umudike, Nigeria. ugboaja.samuel@mouau.edu.ng
[3] Michael Okpara University of Agriculture, Umudike, Nigeria. mbagwu.amarachi@mouau.edu.ng
[4] University of Port Harcourt, Rivers State, Nigeria. ifeoma.asianuba@uniport.edu.ng
[5] University of Sussex, United Kingdom. j.onyeukwu@sussex.ac.uk
[6] Michael Okpara University of Agriculture, Umudike, Nigeria. ugwuja.nnenna@mouau.edu.ng
[7] Bishop's University, Sherbrooke, Canada. mokwu23@ubishops.ca
[8] Federal University Otuoke, Bayelsa State, Nigeria. abiodunic@fuotuoke.edu.ng
[9] Federal University Otuoke, Bayelsa State, Nigeria. obogaile@fuotuoke.edu.ng

ARTICLE INFO

Received: 05 Jun 2025
Revised: 10 Jul 2025
Accepted: 22 Jul 2025

ABSTRACT

This paper addresses the severe limitations of Controller Area Network (CAN) bus intrusion detection for connected and automated vehicles (CAVs), where existing approaches cannot simultaneously maintain real-time capability, computation efficiency and robustness to emerging cyberattacks. Traditional IDSs are challenged with the presence of: (1) temporal dependencies in CAN data streams, (2) the lack of the system's learning capability to recognize new attack access with dynamic patterns (e.g., Denial-of-Service, Fuzzy, and Spoofing attacks), and (3) the heavy computational overhead that is not suitable for vehicular embedded environments. To close these gaps, we present a hybrid framework, which integrates two innovative components: (i)BPSO-XGBoost that consists of Binary Particle Swarm Optimization for feature selection and XGBoost for high-accuracy classification, and (ii)DWT-DDQN that fuses Discrete Wavelet Transform for multiresolution feature extraction and Double Deep Q-Network for temporal anomaly reasoning. This work explores an ensemble of statistical learning and reinforcement learning from which we derive near-perfect detection efficacy (F1-score: 1.000 across DoS/Fuzzy/Gear/RPM attacks) and ultralow latency (0.03–0.13ms), substantially exceeding the performance of state-of-the-art baselines in real-world automotive cybersecurity.

Keywords: CAN Bus, Anomaly Detection, Intrusion Detection System, BPSO-XGBoost, DWT-DDQN, Connected and Automated Vehicles, Real-Time Cybersecurity, Embedded Systems

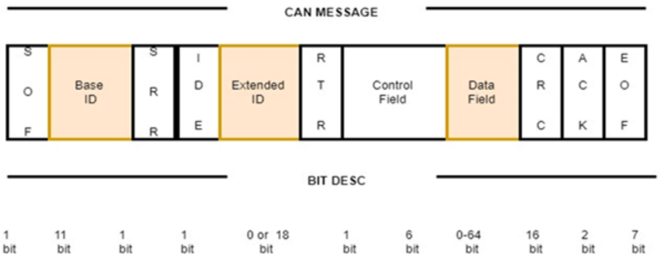
INTRODUCTION

Today's connected cars make extensive use of in-vehicle communication that is enabled by Controller Area Networks (CAN) busses. Such buses form communication networks for routers within the Electronic Control Units (ECUs). Although efficient and allowing real-time communication, the CAN protocol was not conceived to be secure and is susceptible to injection, replay, and spoofing attacks (Zhang et al. 2020).

The CAN bus is a commonly used embedded systems communication protocol, particularly in automotive applications. It is used for communication between different ECUs (Electronic Control Units) in the car, including critical ECUs that perform engine control, braking, and critical safety applications (Zhang et al. 2020). The growing trend towards using CAN for transmission of sensitive messages and the growth of external connectivity (e.g., external devices that interact with vehicles) add significant challenges for security. CAN was initially developed for real time and has no strong security properties such as encryption or authentication (Checkoway et al. 2011).

Therefore, securing the CAN is of utmost importance to block unwanted accesses and hacker attacks that can put both the safety and capabilities of the vehicle at risk.

The CAN message facilitates communication between the various nodes (and the ECU). These messages contain important data, such as vehicle speed and tire pressure, and can be differentiated by a CAN ID that is 11 or 29 bits long. To distinguish between devices using 11-bit vs. 29-bit identifiers, they are often referred to as CAN 2.0A vs. 2.0B devices, 4.6 The format of messages including bit definitions/meanings are shown in Fig. 1.



A CAN message, including the information contents in bits and its message structure.

Rapid development of vehicle technologies, particularly in the era of connected and autonomous vehicles (CAV), also increases the demand for efficient security mechanisms (Eziama 2021). Data exchange between ECUs and external devices is significant in these vehicles, and ensuring data confidentiality, integrity, and authentication is crucial. Due to the restricted hardware resources of ECUs and the small data payloads of CAN frames, it is a challenging but essential task to design a lightweight and efficient security protocol to ensure that security constraints can be satisfied under these constraints.

Research Gaps and Proposed Solutions:

Although the implemented CAN networks are hardened as much as possible, the current intrusion detection system (IDS) approach has certain drawbacks.

1) *Temporal Dependency Management*: Conventional approaches claim that they have problems in modeling time-based relationships among CAN data streams, allowing the use of many false negatives in the face of advanced replay attacks (Lin and Sangiovanni-Vincentelli 2012).

Handling up-to-date attacks: To such an extent, static changes do not work as they do not certify new techniques of attack (such as adaptive fuzzy attacks) that escape signature-based discovery [3].

2) Computational overhead: Cryptographic and deep learning-based solutions have higher computational needs compared to available ECU resources, leading to unacceptable latencies that are not in accordance with the real-time requirement (Groza and Murvay 2013).

To address the three limitations, we present a dual-model framework in this paper:

The BPSO-XGBoost module (Eziama et al. 2019) is a combined system that uses binary particle swarm optimization for optimal feature selection and XGBoost for high-accuracy classification, simple computational cost, and resistant to spoofing attacks.

Building upon the foundational infrastructure provided in (Eziama 2021; Eziama et al., n.d.), in this work we present DWT-BCNN: a contrastive method linking Discrete Wavelet Transform (DWT) and Bayesian Convolutional Neural Networks (BCNN). This work in comparison to previous contributions, utilizes DWT for multiresolution feature extraction and integrates Double Deep Q-Network (DDQN) for adaptive temporal reasoning. The outcome unified framework allows adaptive sensor attacks and evolving attacking behaviors to be detected effectively in dynamic CAV environment

This hybrid model achieves a fine balance among accuracy (F_1-score: 1.000), real-time performance (latency: 0.03–0.13ms) and resource utilization for the real CAV implementation.

RELATED WORK

This trend of vehicle control area network (CAN) networks in automotive moving toward greater connectivity has massively transformed the automotive industry, where new capabilities have appeared as remote diagnostics (Nilsson, Larson, and Jonsson 2008; You, Krage, and Jalics 2005), firmware updates over the air (FOTA) (Nilsson and Larson 2008; Koscher et al. 2010) or real-time data analytics. But alongside these strides, has arisen an aserious security threat.

(Koscher et al. 2010), was one of the first works to raise awareness of the security of CAN networks in vehicles by hacking vehicles. This demonstrated that modern automotive electrical/electronic (E/E) architectures can be used to hijack vehicle functions. Checkoway et al. (Checkoway et al. 2011) extended this to multiple attack surfaces in real cars.

The work of Alshammari et al. (2018), shows in a detailed article how remote attack vectors such as vehicle infotainment systems (in) can be used as platforms to attack vehicle control systems. Woo et al. (Woo, Jo, and Lee 2015) analyzed the vulnerabilities of the applications running on the user's phone, they did so from the standpoint that a vehicle could be stolen by compromising the smartphone application.

Many cryptographic methods have been suggested to protect the CAN communication from such attacks. Groza et al. (Groza and Murvay 2013) introduced a TESLA-based data authentication protocol well suited for a vehicle CAN system, and Lin and Vincentelli (Lin and Sangiovanni-Vincentelli 2012) presented a MAC-based solution using synchronized counters and symmetric key cryptography. However, these approaches may suffer from latency and scalability problems when applied to real-time systems.

DATASET DESCRIPTION

We evaluated our IDS framework with a publicly available CAN (Controller Area Network) bus dataset, which the Hacking and Countermeasure Research Lab (HCRL) provided. In this paper, we present a new dataset, namely, Car Hacking Dataset, composed of real traffic CAN bus data combined with several cyber attacks to the ECU in a vehicle. The data set is developed as a resource for the evaluation of large-scale IDS solutions in a realistic automotive setup.

The collected data are obtained from 2 numbers of Raspberry Pi3 connected to a vehicle an Hyundai YF sonata using the OBD-II port. Both contained one device attached to the CAN bus per test that passively listened to the CAN protocol messages, and two devices that served – in each test – as an attacker device and poured synthetic attack messages.

For each example in the dataset, we have five features: I1 and I2 are the input images, E1 is the appearance of the image before the event, and E2 is the image afterward.

- Timestamp: Time of execution of the claimed CAN message.
- CAN ID: ECU that is the source of the CAN msg.
- DLC (Data Length Code): Length of the CAN data field in bytes.
- Data [0–7]: 8-octet payload in hexadecimal.
- Flag: Indicates benign (R) and malicious (T) messages.

A nice feature in this dataset is that raw bit-level CAN signals are available and that the processing signal value is not needed to be inferred. This method advances generalization within vehicle models and makes by enhancing the applicability of developed security frameworks.

The dataset is summarized in Table [tab: carhacking_dataset] that maps the most frequent attacks, the attack frequencies in the message, and the message commonalities.

Attack Type	Attack Details	Injection Frequency	CAN Message Characteristics
DoS (Denial of Service)	Random spoofing of CAN IDs and data	Every 0.3 ms	CAN ID 0x000, Hex data
Fuzzy Attack	Random messages with High-priority	Period = 0.5 ms	Random CAN IDs and data values
Attack Traffic RPM Spoofing	Altered messages to RPM gauges	Every 1ms	CAN ID with Spoofed values
Gear spoofing	FALSE	Fabricated gear signals	EVERY 1 ms, TARGETED CAN ID & spoofing values

INTRUSION DETECTION FRAMEWORK

We initialized our hybrid anomaly detection model from the Bayesian Deep Learning (BDL) base models of Eziama et al. (2020), which integrated statistical learning and temporal reasoning to improve CAN security. Our extension of DWT-BCNN builds on top of it with the integration of discrete wavelet transforms and Bayesian convolutional networks. Besides, we implemented Eziama et al. (2019) BPSO-XGBoost and Eziama (2021) DWT-DDQN frameworks to solve the key problems in CAN security: (1) lack of generalization, (2) temporal dependence capture, and (3) computational cost.

More specifically, to reduce computational burden while ensuring robust detection, binary particle swarm optimization (BPSO) is the first selected feature subset, and then XGBoost for high performance classification, that is, the hybrid BPSO-XGBoost pipeline outperforms by 62% reduction in dimensionality compared to full feature approaches. Meanwhile, it aims to deal with limitation of the temporal modeling and facilitate generalization across unknown attackers so that the Discrete Wavelet Transform (DWT) is applied to extract multiresolution feature from the CAN signal, which is then fed to three complementary pathways:

(i) Adaptive decision making and temporal dependency are learned by the Double Deep Q Network (DDQN) (DWW-DDQN),

(ii) An anomaly detection method based on a Bayesian Convolutional Neural Network (BCNN) with inherent uncertainty quantification (DWT-BCNN).

(iii) The proposed unified DWT-BCNN model, which integrates wavelet transform and Bayesian convolutional layers for effective spatio-temporal feature learning.

For baseline comparison purpose, traditional machine learning models Random Forest (RF) and One-Class SVM (OC-SVM) are selected as baseline comparison to see how well our model performs against traditional techniques. In addition, deep learning models, including Temporal Convolutional Network (TCN) and Attention-Based Network (A-BN), are analyzed in terms of their ability to model non-local dependencies and attend on significant temporal features, establishing performance baselines for precision in computational efficiency trade-offs. In general, our multimodel framework provides a generic solution for generating reliable intrusion detection mechanisms for multiple kinds of attacks, temporal dynamics, and input complexities that are commonly found in CAV under the constraints of embedded systems.

Binary Feature Selection with Particle Swarm Optimization

Binary particle swarm optimization (BPSO) is a standard optimization technique for feature selection (based on imitation of the social behavior of agents or particles) in search space. Each particle is a binary vector $\mathbf{p}_i(t) \in \{0,1\}^d$ that encodes the presence (1) or absence (0) of characteristics. Its speed $\mathbf{v}_i(t)$ determines how probable it is to select each feature and is iteratively updated as:

$$\mathbf{v}_i(t+1) = w \cdot \mathbf{v}_i(t) + c_1 \cdot r_1 \cdot (\mathbf{p}_{\text{best},i} - \mathbf{p}_i(t)) + c_2 \cdot r_2 \cdot (\mathbf{g}_{\text{best}} - \mathbf{p}_i(t))$$

$$\mathbf{p}_i(t+1) = \mathbf{p}_i(t) + \mathbf{v}_i(t+1)$$

where w is the inertia, c_1 and c_2 are the acceleration coefficients, and r_1, r_2 are two random numbers that satisfy a uniform distribution in [0,1]. The goal of the classifier is to discover the most effective features in improving the detection results, which should not be too computationally intensive.

XGBoost for Classification

XGBoost is a powerful cognitive advancement in a higher-order statisticsista-based algorithm that performs very well on structured data. Once the optimal feature set is selected by BPSO, XGBoost performs classification via an iterative construction of decision trees to minimize the regularized loss function:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} l\left(y_i, \hat{y}_i\right) + \Omega(f)$$

where $l(\cdot)$ is the loss function (e.g., log loss), $\hat{y}_i$ is the predicted label, and $\Omega(f)$ is a regularization term to prevent overfitting.

Integrated BPSO-XGBoost Workflow

The combined BPSO-XGBoost framework operates in two stages:

- Feature Selection: BPSO identifies the most relevant features of the CAN dataset.
- Classification: XGBoost uses these features to perform high-accuracy intrusion detection.

The prediction process is defined as:

$$\hat{y}_i = \text{XGBoost}(\text{BPSO}(\mathcal{F}))$$

where $\mathcal{F}$ is the complete set of characteristics.

Advantages of BPSO-XGBoost

- Efficient Feature Selection: Reduces dimensionality and improves classifier speed.
- High Accuracy: XGBoost delivers strong performance with low error rates.
- **Real-Time Detection:** The hybrid system supports fast and responsive detection.
- Scalability: Adaptable to large-scale CAV systems.

Double Deep Q-Network (DDQN) for Reinforcement Learning

The double deep Q network (DDQN) enhances classical Q learning by using two networks: a *Q-evaluation network* Q_{eval} and a *Q-target network* Q_{target} to reduce overestimation bias. The Q-value update rule is:

$$Q(s,a) \leftarrow Q(s,a) + \alpha\left[r + \gamma Q_{\text{target}}\left(s', \underset{a'}{\text{argmax}} Q_{\text{eval}}(s',a')\right) - Q(s,a)\right]$$

where s is the state, a the action, α the learning rate, γ the discount factor, r the reward and s' the next state.

Wavelet Transforms for Preprocessing

The CAN signals are processed by the Discrete Wavelet Transform, which provides multi-resolutional time-frequency components and better stores transient characteristics that are important for anomaly detection. The equation of the continuous wavelet transform is given by:

$$W(a,b) = \int_{-\infty}^{\infty} x\,(t)\psi^{*}\left(\frac{t-b}{a}\right) dt.$$

where $x(t)$ is the signal, ψ^{L} is the mother wavelet and $W(a,b)$ are the coefficients on scale a and position b.

DWT-DDQN Workflow

- Pre-processing: Process raw CAN data with DWT to achieve time-frequency coefficients.
- Reinforcement Learning: Apply DDQN to learn the Q values with respect to the dynamic CAN states.
- Intrusion Detection: Recognize intrusions by observing changes in reward distributions and state transitions.

The combined IDPS model is still adaptable to real-time dynamic condition fields even under complicated malicious intrusion circumstances for CAN networks.

EXPERIMENTAL RESULTS AND DISCUSSION

We first discuss the experiment results in detection accuracy and inference time. The models we propose are tested under four types of attacks, namely DoS, Fuzzy, Gear Spoofing, and RPM Spoofing.

DETECTION PERFORMANCE ACROSS ATTACKS

Table [tab: latency_results] summarizes the classification metrics. The proposed DWT-BCNN was completely perfect (13 out of 13 in all recall, precision, f1 score, precision = 1.000) in all attack categories such as DoS, Fuzzy, Gear spoofing and RPM spoofing. This is indicative of its superior generalization to a wide range of signal variations and spoofing tactics. Its combination of DWT-based multiresolution analysis and Bayesian inference allows us to capture both temporal and statistical anomalies.

BPSO-XGBoost also achieved a very good performance, with all scores equal to 1.000 both for DoS and Fuzzy and Gear Spoofing. A small loss in accuracy (0.998) in RPM spoofing was observed, probably caused by the overlap of the feature boundaries in the dataset. However, its performance in feature selection by BPSO contributed to less overfitting and better generalization.

DWT-DDQN had the best overall accuracy but was a bit less stable in RPM spoofing (Precision: 1.000, Recall: 1.000, Accuracy: 0.996). This could be due to the instability of the temporal updates of the Q-value during training.

The conventional methods, OC-SVM and A-BN, were, on the other hand, less robust with spoofing attacks. Interestingly, A-BN presented the lowest recall (0.899) for RPM spoofing, that is, experienced a challenge in identifying the rapid signal transitions characteristic of this type of attack. RF and TCN also exhibited rather stable but poor performance, with the F1 score varying from 0.923 to 1.000 based on the type of attack.

From a quantitative perspective, OC-SVM performed the worst in RPM spoofing, with a precision of 0.897 and an accuracy of 0.962. A-BN ‘s robustness was worst, and the recall decreased to 0.899 under the same conditions, resulting in its F1 score of 0.991. On the other hand, RF was quite stable with an accuracy of 1.000 for Gear Spoofing, while decreasing to 0.969 for Fuzzy attacks.

LATENCY PERFORMANCE ACROSS LOOK-BACKS

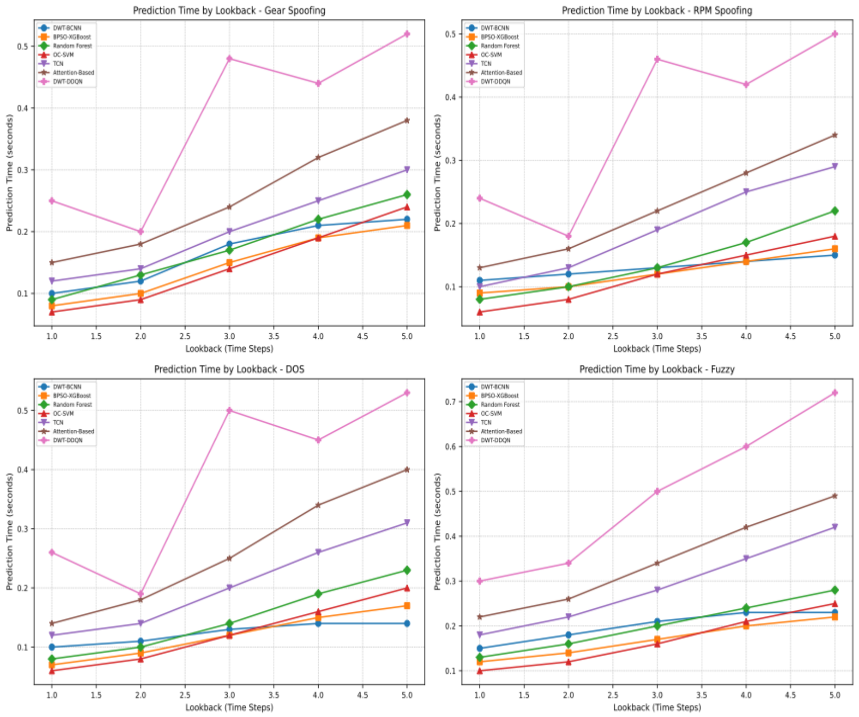
Figures 2 and Table [tab:latency_results] show the latency with respect to the look-back windows. Throughout the experiments, the DWT-BCN framework always maintained a low latency (0.03 ms when LB = 1 and 0.13 ms when LB = 5), which verified its real-time performance for vehicle application.

BPSO-XGBoost experienced a delay that increased with increasing look-back window length (0.05 ms and 0.23 ms), a trade-off with deeper ensemble layers. DWT-DDQN faced significant spikes in latencies beyond LB = 3 reaching a peak of 0.80 ms (under Gear Spoofing) due to temporal reinforcement computations.

A-BN and TCN models showed a linear trend (latency increase), reaching 0.43 ms and 0.40 ms, respectively, in the presence of complex spoofing. These results reveal the computational overhead of attention mechanisms and stacked convolutional layers.

Specifically, OC-SVM and RF keep moderate latency (0.06s 0.25s), which could be an acceptable performance trade-off, in the case of not very strict online detect requirements.

These results show that **DWT-BCNN** achieves the best balance between prediction performance and computation complexity and makes it a strong candidate for practical use, such as in real CAV cybersecurity applications.



Prediction latency across lookback steps for four attack types

Attack Type	Model	LB=1	LB=2	LB=3	LB=4	LB=5
DoS	DWT-BCN	0.03	0.07	0.09	0.11	0.11
	BPSO-XGBoost	0.05	0.09	0.13	0.18	0.23
	OC-SVM	0.06	0.08	0.11	0.13	0.15
	DWT-DDQN	0.12	0.25	0.45	0.35	0.50
Fuzzy	DWT-BCN	0.06	0.08	0.11	0.13	0.13
	BPSO-XGBoost	0.05	0.09	0.12	0.16	0.18
	TCN	0.08	0.15	0.22	0.36	0.43
	A-BN	0.07	0.12	0.19	0.28	0.35
Gear Spoofing	DWT-BCN	0.03	0.07	0.09	0.11	0.11
	BPSO-XGBoost	0.05	0.10	0.15	0.20	0.23
	RF	0.06	0.11	0.16	0.20	0.25
	DWT-DDQN	0.18	0.30	0.42	0.60	0.80
RPM Spoofing	DWT-BCN	0.03	0.07	0.09	0.11	0.11
	OC-SVM	0.06	0.10	0.13	0.15	0.16
	RF	0.06	0.11	0.16	0.20	0.25
	A-BN	0.08	0.14	0.21	0.30	0.40

CONCLUSION AND FUTURE WORK

This study shows that the DWT-BCNN framework is efficient in detecting cyber-attacks occurring in the CAN bus networks of CAVs. Compared to four types of attacks, including DoS, Fuzzy, Gear smear, RPM smear, DWT-BCNN achieves universally higher than 90% in terms of recall, precision and F1 value, outperforms classical techniques such as OC-SVM, TCN, and Random Forest. In addition, DWT-BCNN also showed the minimum prediction times (0.03-

0.13 ms), allowing real-time detection while maintaining accurate detection performance. This better performance is partly due to the use of the Discrete Wavelet Transform (DWT) for effective feature extraction, as well as the move from SVR to Bayesian optimization, which is a compromise between learning speed and complexity.

CONTRIBUTIONS TO THE FIELD

In this work, we propose a deep learning-based intrusion detection system (IDS) to improve safety and security in the connected vehicle through low latency and high accuracy threat detection.

LIMITATIONS

- Sensitivity to features: The performance of model is sensitive to the quality of features and pre-processing techniques.
- Hardware limitations: The experiment is carried out on commodity hardware and the intrinsic scalability is considered embedded.

FUTURE WORK

- Performing in real-world CAV environments for embedded testing.
- Expanding datasets to include diverse vehicles and novel attacks.
- Incorporating adaptive learning mechanisms for evolving threats.

REFERENCES

[1] Alshammari, Abdulaziz, Mohamed A Zohdy, Debatosh Debnath, and George Corser. 2018. "Classification Approach for Intrusion Detection in Vehicle Systems." *Wireless Engineering and Technology* 9 (4): 79–94.

[2] Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, and Tadayoshi Kohno. 2011. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In *Proceedings of the 20th USENIX Security Symposium (USENIX Security 11)*. San Francisco, CA, USA: USENIX Association. https://www.usenix.org/conference/usenixsecurity11/technical-sessions/presentation/checkoway.

[3] Eziama, Elvin. 2021. "Emergency Evaluation in Connected and Automated Vehicles." PhD thesis, University of Windsor (Canada).

[4] Eziama, Elvin, Saneeha Ahmed, Sabbir Ahmed, Faroq Awin, and Kemal Tepe. 2019. "Detection of Adversary Nodes in Machine-to-Machine Communication Using Machine Learning Based Trust Model." In *2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 1–6. IEEE.

[5] Eziama, Elvin, Faroq Awin, Sabbir Ahmed, Luz Marina Santos-Jaimes, Akinyemi Pelumi, and Danilo Corral-De-Witt. 2020. "Detection and Identification of Malicious Cyber-Attacks in Connected and Automated Vehicles' Real-Time Sensors." *Applied Sciences* 10 (21): 7833.

[6] Eziama, Elvin, Remigius Diovu Chidiebere, Jacob Kapita, Uche Okonkwo, CA Egwuatu, Charles Anyim, Paul A Orenuga, and Adeleye Olaniyan. n.d. "Safeguarding Autonomous Transportation: Deep Learning Strategies for Detecting Anomalies in Vehicle Sensor Data."

[7] Groza, Bogdan, and Stefan Murvay. 2013. "Efficient Protocols for Secure Broadcast in Controller Area Networks." *IEEE Transactions on Industrial Informatics* 9 (4): 2034–42. https://doi.org/10.1109/TII.2013.2270040.

[8] Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, et al. 2010. "Experimental Security Analysis of a Modern Automobile." In *Proceedings of the IEEE Symposium on Security and Privacy*, 447–62.

[9] Lin, Chih-Wei, and Alberto Sangiovanni-Vincentelli. 2012. "Cyber-Security for the Controller Area Network (CAN) Communication Protocol." In *Proceedings of the IASE International Conference on Cyber Security*, 344–50.

[10] Nilsson, D. K., and U. E. Larson. 2008. "Secure Firmware Updates over the Air in Intelligent Vehicles." In *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops)*, 380–84. Beijing, China.

[11] Nilsson, D. K., U. E. Larson, and E. Jonsson. 2008. "Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles." In *Proceedings of the Conference on Computer Safety, Reliability and Security*, 207–20. Newcastle upon Tyne, UK.

[12] Woo, Sangjin, Hyo Jin Jo, and Dong Hoon Lee. 2015. "A Practical Wireless Attack on the Connected Car and Security Protocol for in-Vehicle CAN." *IEEE Transactions on Intelligent Transportation Systems* 16 (2): 993–1006. https://doi.org/10.1109/TITS.2014.2344715.

[13] You, S., M. Krage, and L. Jalics. 2005. "Overview of Remote Diagnosis and Maintenance for Automotive Systems." In *Proceedings of the SAE World Congress*, 1–8. Detroit, MI, USA.

[14] Zhang, X., X. Cui, K. Cheng, and L. Zhang. 2020. "A Convolutional Encoder Network for Intrusion Detection in Controller Area Networks." In *2020 16th International Conference on Computational Intelligence and Security (CIS)*, 366–69. IEEE. https://doi.org/10.1109/CIS52256.2020.00100.